Geheimnisschutz zwischen Arbeitsrecht, Datenschutz und Gesellschaftsrecht

Inauguraldissertation
zur Erlangung des Grades eines Doktors
des Rechts
durch die
Rechts- und Staatswissenschaftliche Fakultät
der Rheinischen Friedrich-Wilhelms-Universität
Bonn

vorgelegt von

Tabea Benz
aus Berlin
2025

Dekan:	Herr Prof. Dr. Martin Böse
Erstreferent:	Herr Prof. Dr. Gregor Thüsing
Zweitreferent:	Herr Prof. Dr. Stefan Greiner

Tag der mündlichen Prüfung: 12. November 2024

Inhaltsverzeichnis

Abkürzungsverzeichnis

A) Worum es geht: Geschäftsgeheimnisschutz im Spannungsfeld zwischen Wettbewerb, Innovation und Rechtskonformität 1
I. Rechtspolitische Entwicklungen 11
II. Kernfragen und Gang der Darstellung 17
1. Kapitel B): Rechtliche Grundlagen des Geschäftsgeheimnisschutzes 18
2. Kapitel C): Reichweite und Grenzen des Geschäftsgeheimnisschutzes im Beschäftigungskontext 19
3. Kapitel D): Die Gewinnung neuen exklusiven Wissens: Eine Balance zwischen Innovation und Rechtskonformität 21
4. Kapitel E): Eine Zusammenfassung in 25 Thesen 22
5. Weiterer Forschungsbedarf 22

B) Rechtliche Grundlagen des Geschäftsgeheimnisschutzes 24
I. Rechtsrahmen und Funktion 24
1. Die Verankerung in der GR-CH 26
2. Die konventionsrechtliche Verankerung 27
3. Die grundgesetzliche Verankerung 28
a) Berufsfreiheit, Art. 12 Abs. 1 GG 28
b) Eigentumsfreiheit, Art. 14 Abs. 1 GG 29
c) Recht am eingerichteten und ausgeübten Gewerbebetrieb; Unternehmenspersönlichkeitsrecht 30
4. Zusammenfassender Überblick 31
II. Die gesetzgeberische Ausgestaltung des Geschäftsgeheimnisschutzes 32
1. Eine kurze Genese: Von §§ 17 bis 19 UWG a. F. zur Neukonzeption des GeschGehG 34
2. Die Grundstrukturen des GeschGehG: Ein Überblick 36
3. Ausgangspunkt: Das Vorliegen eines Geschäftsgeheimnisses 41

a) Geheime Information von wirtschaftlichem Wert 42
aa) Unternehmensbezug 43
bb) Geheimnischarakter 45
cc) Wirtschaftlicher Wert infolge der Geheimhaltung 49
(1) Problemaufriss: Der wirtschaftliche Wert als Ausschlusskriterium für rechtswidrige Informationen? 51
(2) Eine Betrachtung des Wortlauts in unionsrechtskonformer Auslegung 52
(3) Eine Betrachtung der Systematik 55
(4) Eine Betrachtung der Historie 56
(5) Eine Betrachtung des Telos 59
(6) Gesamtbetrachtung: Weshalb rechtswidrige Informationen von wirtschaftlichem Wert sind 60
dd) Zusammenfassender Überblick 61
b) Berechtigtes Geheimhaltungsinteresse 64
aa) Problemaufriss: Das berechtigte Geheimhaltungsinteresse als unionsrechtswidriges Ausschlusskriterium für rechtswidrige Informationen? 68
bb) Eine Betrachtung des Wortlauts anhand der Genese des GeschGehG 68
cc) Eine Betrachtung der Historie 70
dd) Eine Betrachtung der Systematik 72
ee) Eine Betrachtung des Telos 73
ff) Gesamtbetrachtung: Weshalb das berechtigte Geheimhaltungsinteresse kein unionsrechtswidriges Ausschlusskriterium für den Schutz rechtswidriger Informationen ist 74
c) Angemessene Geheimhaltungsmaßnahmen 76
aa) Auslegungsmöglichkeiten 77
(1) Eine Betrachtung des Wortlauts 78

(2) Eine Betrachtung der Historie 82
(3) Eine Betrachtung der Systematik 83
(4) Eine Betrachtung des Telos 84
(5) Was sagt die Rechtsprechung? 85
(6) Gesamtbetrachtung: Leitlinien für die Auslegung angemessener Geheimhaltungsmaßnahmen 90
bb) Auswirkungen rechtswidriger Geheimhaltungsmaßnahmen 93
(1) Auswirkungen auf Definitionsebene 94
(2) Auswirkungen auf den Nachweis eines Geheimnisverrats 97
(3) Zwischenfazit 99
cc) Zusammenfassender Überblick 102
4. Geheimhaltungsmaßnahmen im Beschäftigungskontext 104
a) Arbeitsvertragliche Sicherungsmechanismen 107
b) Überwachungs- und Kontrollmaßnahmen 117
aa) Präventive Überwachungsmaßnahmen 123
bb) Maßnahmen zu repressiven Zwecken 133
cc) Beteiligung des Betriebsrats 143
dd) Zwischenfazit 145
c) Bewerberprüfungen 147
d) Zusammenfassender Überblick 153
III. Weiterungen für das unternehmerische Compliance-System 159
IV. Eine erste Sammlung der Erkenntnisse 166

C) Der Geschäftsgeheimnisschutz: Reichweite und Grenzen im Beschäftigungskontext 173
I. Geschäftsgeheimnisschutz und Whistleblowing 174
1. Grundlagen des Whistleblowings 175
a) Rechtsrahmen und Funktion 176
b) Die gesetzgeberische Ausgestaltung des Whistleblowings 178

c) Das Verhältnis von GeschGehG und HinSchG im Lichte der GeschGeh-RL und der Whistleblowing-RL 181
aa) Sachlicher Anwendungsbereich 182
bb) Relevanz der subjektiven Motivlage 190
cc) Auslegungsmaßstab 194
dd) Haftungsausschluss 196
ee) Harmonisierende Auslegung zur Überwindung bestehender Friktionen 198
d) Zusammenfassender Überblick 201
2. Hinweisgeberschutz bei der Weitergabe von Geschäftsgeheimnissen durch Whistleblower 205
a) Die zulässige Weitergabe von Geschäftsgeheimnissen nach § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG 206
b) Problemaufriss: Ist ein interner Meldeweg bei der Weitergabe eines Geschäftsgeheimnisses vorrangig zu nutzen? 211
aa) Eine Betrachtung des Wortlauts 215
bb) Eine Betrachtung der Systematik 216
cc) Eine Betrachtung der Historie 217
dd) Eine Betrachtung des Telos 219
ee) Gesamtbetrachtung: Weshalb eine (Prüf-) Obliegenheit zur vorrangigen Nutzung eines internen Meldewegs besteht 220
c) Die zulässige Weitergabe von Geschäftsgeheimnissen nach § 5 Nr. 2 GeschGehG 224
3. Weiterungen für das unternehmerische Compliance-System 224
a) Verpflichtung zur vorrangigen Nutzung eines internen Meldewegs 227
b) Verpflichtung zur Abgabe einer internen Meldung 228

c) Zusätzlicher Identitätsschutz als Anreiz für eine interne Meldung 233
aa) Identitätsschutz nach den Vorgaben des HinSchG 235
bb) Identitätsschutz im Rahmen der DS-GVO 240
(1) Ausnahmen von der Informationspflicht 242
(a) Art. 14 Abs. 5 lit. b) DS-GVO 243
(b) Art. 14 Abs. 5 lit. c) DS-GVO 244
(c) § 29 Abs. 1 S. 1 BDSG 248
(d) §§ 8, 9 HinSchG 253
(2) Beschränkung der Datenauskunft 255
(3) Zwischenfazit 267
cc) Möglichkeiten zur Erhöhung des Identitätsschutzes 271
(1) Verzicht auf die Betroffenenrechte 272
(2) Einschaltung einer externen Ombudsperson 274
(3) Betriebsvereinbarung zur Erhöhung des Identitätsschutzes 275
dd) Zwischenergebnis 280
d) Zusammenfassender Überblick 282
II. Geschäftsgeheimnisschutz und das Recht auf Datenauskunft 290
1. Grundlagen des datenschutzrechtlichen Auskunftsrechts 291
a) Die Konzeption des Art. 15 DS-GVO 293
b) Inhaltliche Reichweite der Datenauskunft 296
2. Beschränkung der Datenauskunft nach Maßgabe des Geschäftsgeheimnisschutzes 299
3. Verhältnis der Datenauskunft zur Akteneinsicht 304
a) Regelungsinhalt des Einsichtsrechts 305
b) Verdrängungswirkung des § 83 Abs. 1 S. 1 BetrVG? 307

c) Berücksichtigungsfähigkeit der Geheimhaltungsinteressen 315
4. Zusammenfassender Überblick 316
III. Geschäftsgeheimnisschutz im Rahmen der Betriebsratsarbeit 322
1. Verschwiegenheitspflicht, § 79 Abs. 1 S. 1 BetrVG 323
2. Geheimnisschutz bei der Erlangung eines Geschäftsgeheimnisses 325
3. Whistleblower: Betriebsratsmitglied 328
4. Zusammenfassender Überblick 331
IV. Eine zweite Sammlung der Erkenntnisse 334

D) Die Gewinnung neuen exklusiven Wissens: Eine Balance zwischen Innovation und Rechtskonformität 347

E) Resümee: Eine Zusammenfassung 25 Thesen 357

Literaturverzeichnis 371
Materialienverzeichnis 398

Lebenslauf

Abkürzungsverzeichnis

a. A.	andere(r/n) Ansicht; Auffassung
a. F.	alte(n) Fassung
ABl.	Amtsblatt
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AfP	Archiv für Presserecht (Z)
AG	Aktiengesellschaft
AGG	Allgemeines Gleichbehandlungsgesetz
AktG	Aktiengesetz
Alt.	Alternative
Anm.	Anmerkung
AO	Abgabenordnung
ArbG	Arbeitsgericht
ArbGG	Arbeitsgerichtsgesetz
ArbnErfG	Gesetz über Arbeitnehmererfindungen
ArbR	Arbeitsrecht
ArbRAktuell	Arbeitsrecht Aktuell (Z)
ArbRB	Arbeits-Rechtsberater (Z)
ArbSchG	Arbeitsschutzgesetz
Art.	Artikel
ASiG	Arbeitssicherheitsgesetz
AuR	Arbeit und Recht (Z)
Az.	Aktenzeichen
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BAG	Bundesarbeitsgericht
BAGE	Entscheidungen des Bundesarbeitsgerichts (Amtliche Sammlung)
BAT	Bundes-Angestelltentarifvertrag
BB	Betriebs-Berater (Z)
BBG	Bundesbeamtengesetz
BBiG	Berufsbildungsgesetz
BC	Zeitschrift für Bilanzierung, Rechnungswesen und Controlling (Z)
Bd.	Band
BDA	Bundesvereinigung der Deutschen Arbeitgeberverbände
BDSG	Bundesdatenschutzgesetz

BeckOK	Beck-Online-Kommentar (K)
BeckRS	Beck-Online-Rechtsprechung
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofs in Strafsachen (Amtliche Sammlung)
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen (Amtliche Sammlung)
BImSchG	Bundes-Immissionsschutzgesetz
BPersVG	Bundespersonalvertretungsgesetz
BRAK	Bundesrechtsanwaltskammer
BRAO	Bundesrechtsanwaltsordnung
BT-Drs.	Bundestagsdrucksache
Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungs-gerichts (Amtliche Sammlung)
BVerwG	Bundesverwaltungsgericht
BW	Baden-Württemberg
bzgl.	bezüglich
BZRG	Gesetz über das Zentral- und das Erziehungsregister
bzw.	beziehungsweise
CB	Compliance-Berater (Z)
CCOO	Federación de Servicios de Comisiones Obreras (spanische Gewerkschaft)
CCZ	Corporate Compliance Zeitschrift (Z)
CDU	Christlich Demokratische Union Deutschlands
COM	Dokument der EU-Kommission
CR	Computer und Recht (Z)
CSDDD/CS3D-RL	Richtlinie der Europäischen Union zu unternehmerischen Sorgfaltspflichten im Bereich der Nachhaltigkeit
CSRD-RL	Richtlinie der Europäischen Union zur Nachhaltigkeitsberichterstattung
d. h.	das heißt
DatenschutzR	Datenschutzrecht

DAV	Deutscher Anwaltverein e. V.
DB	Der Betrieb (Z)
DesignG	Designgesetz
DGB	Deutscher Gewerkschaftsbund
DrittelbG	Drittelbeteiligungsgesetz
DSB	Datenschutz-Berater (Z)
DS-GVO/DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
DStR	Deutsches Steuerrecht (Z)
DuD	Datenschutz und Datensicherheit (Z)
DWWS	Kompakt Kommentar zur DS-GVO und BDSG von *Däubler/Wedde/Weichert/ Sommer* (K)
E	Entwurf
e. V.	eingetragener Verein
EBRG	Gesetz über Europäische Betriebsräte
EDSA	Europäischer Datenschutzausschuss
EG	Europäische Gemeinschaft; Erwägungsgrund
EGMR	Europäischer Gerichtshof für Menschenrechte
ehem.	ehemalige
Einl.	Einleitung
EMRK	Europäische Menschenrechtskonvention
EMRK-ZP 1	Erstes Zusatzprotokoll zur EMRK
EntgTranspG	Entgelttransparenzgeetz
ErfK	Erfurter Kommentar (K)
EU	Europäische Union
EuArbRK	Kommentar zum europäischen Arbeitsrecht von *Franzen/Gallner/Oetker* (K)
EuGH	Gerichtshof der Europäischen Union
EuR	Europarecht (Z)
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht (Z)
EWiR	Entscheidungen zum Wirtschaftsrecht und Kurzkommentare (Z)
etc.	et cetera
f./ff.	folgende/die folgenden
FD	Fachdienst Arbeitsrecht (Z)
FDP	Freie Demokratische Partei
Fn.	Fußnote

Frankfurt a. M.	Frankfurt am Main
FS	Festschrift
GA	Generalanwalt
gem.	gemäß
gen.	genannt
GenG	Genossenschaftsgesetz
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
GeschGeh-RL	Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen
GEW	Geistiges Eigentum und Wettbewerb
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GK	Großkommentar (K)
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GPS	Global Positioning System
GR-CH	Charta der Grundrechte der Europäischen Union
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Z)
GRUR-Prax	GRUR: Praxis im Immaterial-Güter und Wettbewerbsrecht (Z)
GRUR-RS	GRUR: Rechtsprechungssammlung
GVG	Gerichtsverfassungsgesetz
GWB	Gesetz gegen Wettbewerbs-beschränkungen
GWR	Gesellschafts- und Wirtschaftsrecht (Z)
h. M.	herrschende Meinung
HBG	Hessisches Beamtengesetz
Hdb.	Handbuch
HDSIG	Hessisches Datenschutz- und Informations-freiheitsgesetz
HGB	Handelsgesetzbuch
HinSchG	Hinweisgeberschutzgesetz
HinSchG-E	Hinweisgeberschutzgesetz-Entwurf
Hrsg./hrsg.	Herausgeber(in)/herausgegeben
Hs.	Halbsatz

HWK	Arbeitsrecht Kommentar von *Henssler/Willemsen/Kalb* (K)
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
ID	Identifikation
IP	Intellectual Property
IPRB	IP-Rechtsberater (Z)
IT	Informationstechnologie
JuS	Juristische Schulung (Z)
JZ	Juristenzeitung (Z)
K	Kommentar
K&R	Kommunikation und Recht (Z)
KI	Künstliche Intelligenz
KriPoZ	Kriminalpolitische Zeitschrift (Z)
KunstUrhG	Kunsturhebergesetz
LAG	Landesarbeitsgericht
LG	Landgericht
lit.	littera/Buchstabe
LkSG	Lieferkettensorgfaltspflichtengesetz
m.	mit
m. w. N.	mit weiteren Nachweisen
MitbestG	Gesetz über die Mitbestimmung der Arbeitnehmer
MMR	Multimedia und Recht, Zeitschrift für IT-Recht und Recht der Digitalisierung (Z)
MüKo	Münchener Kommentar (K)
n. F.	neue(n) Fassung
NDAs	Non-Disclosure-Agreements, Vertraulichkeitsvereinbarungen
NJW	Neue Juristische Wochenschrift (Z)
NK	Nomos Kommentar (K)
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht (Z)
NVwZ-RR	NVwZ: Rechtsprechungs-Report (Z)
NZA	Neue Zeitschrift für Arbeitsrecht (Z)
NZA-RR	NZA-Rechtsprechungs-Report (Z)
NZG	Neue Zeitschrift für Gesellschaftsrecht (Z)
NZWiSt	Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (Z)

öAT	Zeitschrift für das öffentliche Arbeits- und Tarifrecht (Z)
OLG	Oberlandesgericht
OWiG	Gesetz über Ordnungswidrigkeiten
P&DP	Privacy and Data Protection Journal (Z)
PatG	Patentgesetz
RAW	Recht Automobil Wirtschaft (Z)
RdA	Recht der Arbeit (Z)
RDi	Recht Digital (Z)
RDV	Recht der Datenverarbeitung (Z)
RefE	Referentenentwurf
RegE	Regierungsentwurf
RGZ	Entscheidungen des Reichsgerichts in Zivilsachen (Amtliche Sammlung)
RL	Richtlinie
Rn.	Randnummer(n)
Rs.	Rechtssache
Rspr.	Rechtsprechung
S.	Satz/Seite(n)
SEBG	Gesetz über die Beteiligung der Arbeitnehmer in einer Europäischen Gesellschaft
SGB	Sozialgesetzbuch
SJTK	Heidelberger Kommentar zur DS-GVO/ BDSG von *Schwartmann/Jaspers/Thüsing/ Kugelmann* (K)
sog.	sogenannte/sogenannter/sogenanntes
SPD	Sozialdemokratische Partei Deutschlands
SprAuG	Gesetz über Sprecherausschüsse der leitenden Angestellten
SR	Soziales Recht (Z)
st.	ständige
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
str.	streitig, strittig
TKG	Telekommunikationsgesetz
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
TTDSG	Telekommunikations-Telemedien-Datenschutzgesetz
TVöD	Tarifvertrag für den Öffentlichen Dienstag

TzBfG	Teilzeit- und Befristungsgesetz
u. a.	unter anderen(m)/und andere(r)
UAbs.	Unterabsatz
UK	United Kingdom/Vereinigtes Königreich Großbritannien
UN	United Nations (Vereinte Nationen)
UrhG	Urheberrechtsgesetz
US	United States (of America)
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	vom/von
Var.	Variante
VG	Verwaltungsgericht
vgl.	vergleiche
Vorb.	Vorbemerkung
VorstandsR-Hdb.	Handbuch Vorstandsrecht (K)
VwVfG	Verwaltungsverfahrensgesetz
Washington D. C.	Washington District of Columbia
WiJ	Journal der Wirtschaftsstrafrechtlichen Vereinigung e. V. (Z)
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht (Z)
WM	Wertpapier-Mitteilungen (Z)
WRP	Wettbewerb in Recht und Praxis (Z)
Z	Zeitschrift
z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz (Z)
ZfA	Zeitschrift für Arbeitsrecht (Z)
ZIP	Zeitschrift für Wirtschaftsrecht (Z)
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik (Z)
zit.	zitiert
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik (Z)
ZUM	Zeitschrift für Urheber- und Medienrecht (Z)
zust.	zustimmend
ZWeR	Zeitschrift für Wettbewerbsrecht (Z)
ZWE	Zeitschrift für Wohnungseigentumsrecht (Z)
ZWH	Zeitschrift für Wirtschaftsstrafrecht und Haftung im Unternehmen (Z)

A. Worum es geht: Geschäftsgeheimnisschutz im Spannungsfeld zwischen Wettbewerb, Innovation und Rechtskonformität

„*Wissen ist Macht.*“

lautet der berühmte Ausspruch des französischen Philosophen *Michel Foucault*, der auf den englischen Philosophen *Sir Francis Bacon* im 16./17. Jahrhundert zurückzuführen ist.[1] Er unterstreicht die grundlegende Wahrheit, dass das Zusammenspiel von Wissen und Macht den Schlüssel für Erfolg, institutionelle Stärke und Fortschritt bildet.[2] In der freien Wirtschaft dient Wissen in verschiedenen Kontexten als strategische Ressource, die insbesondere Unternehmen die Möglichkeit verleiht, ihre Umgebung aktiv mitzugestalten. Verfügen Unternehmen über exklusives Wissen zu neuen Technologien, Produktionsmethoden oder Produkten, können sie sich als Marktführer ihrer Branche behaupten. Darüber hinaus kann exklusives Wissen auch dazu beitragen, Geschäftsprozesse zu optimieren, ein besseres Verständnis für den Markt zu entwickeln und mögliche Engpässe frühzeitig zu identifizieren. Die Möglichkeiten sind vielfältig.

Unternehmen haben ein ureigenes Interesse daran, ihr exklusives Wissen vor dem Zugriff Dritter, wie beispielsweise nachahmenden Wettbewerbern, zu schützen. Diese Schutzbestrebungen sind Teil des betrieblichen Geheimnisschutzes und dienen der Wahrung der unternehmerischen Wettbewerbs- und Innovationsfähigkeit. Dessen ungeachtet sind Unternehmen, die die Rechtsform einer AG oder GmbH tragen, gesellschaftsrechtlich verpflichtet, im Rahmen ihrer Risiko-

---

1 Der Ausdruck "*Scientia potentia est*" (Wissen ist Macht) ist wiederkehrendes Element in den Werken von *Sir Francis Bacon*, vgl. „*Novum Organum Scientiarum*“ aus dem Jahre 1620. *Foucault* machte den Ausspruch zu einem zentralen Element seiner Thesen, vgl. *Brockhaus*, Geheimnisschutz und Transparenz, S. 1 m. w. N. „*Wissen ist Macht und Macht ist Wissen*“ formulierte auch *Karl Liebknecht* in seinen Reden im Jahr 1872.

2 Grundlegend: *Wegener,* Der geheime Staat.

vorsorge einen angemessenen Geheimnisschutz sicherzustellen.[3] Damit das Unternehmen hinreichend vor möglichen Schäden durch unerlaubte Erlangung, Nutzung oder Offenlegung geheimhaltungsbedürftiger Informationen geschützt ist, bedarf es insbesondere der Implementierung angemessener Geheimhaltungsmaßnahmen.[4] Die Sicherung exklusiven Wissens ist dementsprechend präventives Obligatorium und strategische Notwendigkeit zugleich. Der Ausspruch „*Wissen ist Macht*" greift folgerichtig zu kurz. Für die Unternehmenswelt muss er lauten: Wissen ist potenzielle Macht, die es strategisch zu nutzen und zu schützen gilt, um als Unternehmen wirtschaftlich zu bestehen.

Der betriebliche Geheimnisschutz wirft allerdings auch kritische gesellschaftspolitische Fragestellungen auf, wie beispielsweise die Frage nach der Gefahr eines möglichen Machtmissbrauchs. Einhalt gebieten unter anderem Vorgaben zur Transparenz, die einen fairen und rechtskonformen Wettbewerb sicherstellen sollen. Den Zusammenhang zwischen Transparenz und Macht arbeitet *Brockhaus* zutreffend heraus: „*Was rechtlichen Geheimnisschutz und was Transparenz verdient, sind Machtfragen*."[5] Dieser Leitgedanke mündet notwendigerweise in komplexe Abwägungsprozesse. Dabei gilt es, eine Balance zwischen dem Schutz betrieblicher Informationen und anderen schützenswerten Interessen zu finden, zu denen neben einem fairen Wettbewerb insbesondere auch das öffentliche Interesse an der Aufdeckung etwaiger Missstände und die Wahrung des Persönlichkeitsrechts der von einer Datenverarbeitung betroffenen Person zählen.

Wie weit der betriebliche Geheimnisschutz im Einzelnen reicht und unter welchen Voraussetzungen er zum Schutz gegenläufiger Interessen weichen muss, wird die folgende Darstellung untersuchen. Von besonderer Relevanz wird unter anderem die zulässige Weitergabe

---

3 § 93 Abs. 1 S. 1 AktG, § 43 Abs. 1 GmbHG.
4 §§ 2 Nr. 1 lit. b), 9 Nr. 2 GeschGehG.
5 *Brockhaus*, Geheimnisschutz und Transparenz, S. 1.

bzw. Offenlegung geheimer Informationen durch Whistleblower sein. Gleichzeitig drängen sich datenschutzrechtliche Fragestellungen im Zusammenhang mit der Datenauskunft auf, etwa inwieweit Geschäftsgeheimnisse zu beauskunften sind.

Teil des betrieblichen Geheimnisschutzes ist auch das Generieren neuen exklusiven Wissens. Dies beruht auf der Annahme eines symbiotischen Zusammenwirkens zwischen dem Generieren exklusiven Wissens und dessen Schutz. Während das exklusive Wissen in gewisser Weise die Frucht der Bemühungen eines Unternehmens um Innovation, Entwicklung und Forschung ist, dient der Schutz dieses Wissens dazu, dessen Exklusivität langfristig sicherzustellen. Wie *Michelle Obama* sinngemäß sagte: Wissen sei nicht nur ein Instrument der Macht, sondern auch ein Mittel zur Ermächtigung.[6] Im unternehmerischen Kontext gilt dieser Gedanke, soweit verfügbare Informationen das Unternehmen befähigen, die eigene Innovationskraft und Wettbewerbsposition zu stärken. Die effektive und strategische Nutzung neuer Technologien vermag es beispielsweise, große Datenmengen zu bewältigen und unternehmerisches Wachstum zu versprechen.

Doch auch die Integration von Technologien am Arbeitsplatz insbesondere im Kontext von Big Data und digitalen Überwachungssystemen wirft gesellschaftspolitische Fragen auf. Die Sammlung und Analyse von Kunden- oder Mitarbeiterdaten können in deren Privatsphäre eingreifen. Grenzen setzen insbesondere die datenschutzrechtlichen Vorgaben. Das datenschutzrechtliche Auskunftsrecht schafft die nötige Transparenz und versetzt die von einer Datenverarbeitung betroffene Person in die Lage, die Verarbeitung ihrer personenbezogenen Daten nachzuvollziehen, um ggf. deren Rechtmäßigkeit durchzusetzen. *Comenius* formuliert in diesem Zusammen-

---

6 *Michelle Obama*, ehem. First Lady der Vereinigten Staaten von Amerika, in ihrer Rede „*The power of education*“ in Washington D.C., 2013.

hang zutreffend: „*Unwissende sind ohnmächtig.“*[7] Laut *Comenius* sei Wissen als eine Form der Befähigung zu verstehen. In die gleiche Richtung zielen die Formulierungen von *Michelle Obama*, die in ihrer Rede die doppelte Rolle des Wissens als Werkzeug zur Machtausübung und als Mittel zur Befähigung von Individuen betonte.[8]

Übertragen auf die Datenauskunft bedeutet dies, dass die Kenntnis über die Datenverarbeitung die von ihr betroffene Person erst dazu ermächtigt, ihre Rechte gegenüber dem datenschutzrechtlich Verantwortlichen hinreichend wahrzunehmen.[9]

Die vorliegende Darstellung wird daher die nötige Balance zwischen betrieblichem Geheimnisschutz und informationellem Selbstbestimmungsrecht der von einer Datenverarbeitung Betroffenen herausarbeiten.

I. Rechtspolitische Entwicklungen

Der betriebliche Geheimnisschutz hat in den vergangenen Jahren eine bedeutsame gesetzgeberische Stärkung erfahren. Mit der GeschGeh-RL[10] hat der europäische Gesetzgeber den Geschäftsgeheimnisschutz im Jahr 2016 einem einheitlichen europäischen Schutzniveau zugeführt. Daraufhin hat der nationale Gesetzgeber mit dem GeschGehG ein neues Stammgesetz zum Schutz von Geschäfts-

---

7 Der Satz "*Unwissende sind ohnmächtig*" stammt von *Johann Amos Comenius*, einem tschechischen Theologen, Pädagogen und Schriftsteller, der im 17. Jahrhundert lebte. Er formulierte diesen Gedanken in seinem Werk „*Didactica Magna*“.

8 *Michelle Obama*, ehem. First Lady der Vereinigten Staaten von Amerika, während ihrer Rede „*The power of education*“ in Washington D.C., 2013.

9 Wer die datenschutzrechtlich verantwortliche Stelle ist, richtet sich nach Art. 4 Nr. 7 DS-GVO.

10 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. L 157 v. 15.06.2016, S. 1.

geheimnissen geschaffen, das 2019 in Kraft getreten ist.[11] Das GeschGehG definiert erstmalig den Begriff des Geschäftsgeheimnisses und kodifiziert ein ausdifferenziertes System von Ansprüchen des Geheimnisinhabers. Damit verbunden sind viele Einzelfragen, die unter anderem auf eine Vielzahl unbestimmter Rechtsbegriffe zurückzuführen sind und dem Rechtsanwender Spielraum für Interpretationen lassen.[12] Der Staffelstab liegt bei der Judikative, den vielen Auslegungsfragen entsprechende Konturen zu verleihen.[13] Zugleich stehen Unternehmen insbesondere vor der Herausforderung, angemessene Geheimhaltungsmaßnahmen zu implementieren, deren tatsächliches Vorliegen konstitutiv ist, um Schutz durch das GeschGehG zu erfahren. Erst die Konnexion gesetzlicher und (arbeits-) vertraglicher Verschwiegenheitspflichten, flankiert von technischen und organisatorischen Sicherungsmechanismen, vermag es, einen adäquaten Geschäftsgeheimnisschutz zu gewährleisten.

Auch nach Inkrafttreten des GeschGehG hatte sich der Gesetzgeber mit Fragen des Geschäftsgeheimnisschutzes auseinanderzusetzen. Insbesondere die Umsetzung der Whistleblowing-RL[14] durch das

---

11 Gesetz zum Schutz von Geschäftsgeheimnissen, BGBl. I v. 18.04.2019, S. 466; *Alexander*, AfP 2019, 1, 2; *Burghardt-Richter/Bode*, BB 2019, 2697; *Erlebach/Veljovic*, wistra 2020, 190; *Gramlich/Lütke*, wistra 2022, 97; *Hauck*, GRUR-Prax 2019, 223; *Hoppe/Oldekop*, Geschäftsgeheimnisse, Rn.11.

12 Aus Unternehmenssicht stellt sich beispielsweise die Frage, wie Geheimnisschutzkonzepte konkret auszugestalten sind, damit eine betriebliche Information dem Schutzregime des GeschGehG unterfällt. Dazu auch: *Alexander*, WRP 2019, 673, 679; *Brockhaus*, ZIS 2020, 102, 119; *Klinkert*, WRP 2019, Heft 06, Umschlagteil, I, (Editorial).

13 Beispiele sind u. a.: „wirtschaftlicher Wert" in § 2 Nr. 1 lit. a) GeschGehG, „angemessene Geheimhaltungsmaßnahmen" in § 2 Nr. 1 lit. b) GeschGehG, „berechtigtes Interesse" in § 2 Nr. 1 lit. c) GeschGehG und „Schutz eines berechtigten Interesses" in § 5 GeschGehG. Eine erste Rechtsprechungsübersicht zum GeschGehG findet sich bei *Apel/Nickl*, K&R 2022, 385.

14 Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, ABl. L 305 v. 26.11.2019, S. 17.

HinSchG[15] erforderte Vorgaben zum Verhältnis des Hinweisgeberschutzregimes zu dem des Geschäftsgeheimnisschutzes. Bedauerlicherweise hat der nationale Gesetzgeber die Gelegenheit verpasst, den aus Gründen der Rechtssicherheit gebotenen Gleichlauf zwischen GeschGehG und HinSchG herzustellen. Stattdessen wurde mit § 6 Abs. 1 HinSchG eine Erlaubnisnorm geschaffen,[16] die neben den Erlaubnistatbestand des § 5 Nr. 2 GeschGehG tritt.[17] Die erhoffte Rechtssicherheit an der Schnittstelle von Geschäftsgeheimnisschutz und Hinweisgeberschutz blieb damit aus. Insbesondere das neu gestaltete Eskalationsmodell ist Beleg dafür, dass es im Rahmen der Umsetzung der Whistleblowing-RL vordergründig um die Stärkung des Hinweisgeberschutzes ging, zu deren Gunsten schützenswerte, dem Hinweisgeberschutz gegenläufige unternehmerische (Geheimhaltungs-) Interessen in den Hintergrund gerückt wurden.[18] Denn obwohl es dem nationalen Gesetzgeber im Rahmen der Umsetzung der Whistleblowing-RL möglich war, den vom EGMR etablierten grundsätzlichen Vorrang einer internen Meldung in Gesetzestext zu überführen,[19] entschied sich der nationale Gesetzgeber für ein grundsätzlich zweistufiges Eskalationsmodell. Das HinSchG normiert nunmehr die allgemeine Möglichkeit einer externen Meldung, ohne dass hiervon einschränkend abgewichen werden kann.[20] Damit hat der nationale

---

15 Gesetz für einen besseren Schutz hinweisgebender Personen, BGBl. I v. 31.05.2023, Nr. 140.

16 Gemeint ist eine Erlaubnisnorm im Sinne des § 3 Abs. 2 GeschGehG.

17 BT-Drs. 20/3442, S. 71 in Umsetzung des Erwägungsgrunds 98 Whistleblowing-RL.

18 Der nationale Gesetzgeber entschied sich für eine Richtlinien überschießende Umsetzung. Während sich die Whistleblowing-RL in ihrem Anwendungsbereich auf die Meldung von Verstößen gegen bestimmtes Unionsrecht beschränkt, hat der nationale Gesetzgeber sämtliche strafbewehrte Verstöße sowie Verstöße, die bußgeldbewehrt sind, in den Schutzbereich des HinSchG aufgenommen, soweit die verletzte Vorschrift dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient, vgl. *Dzida/Seibt*, NZA 2023, 657.

19 EGMR, Urteil v. 21.07.2011 - 28274/08 - *Heinisch/Deutschland.*

20 §§ 7 Abs. 1 S. 1, 39 HinSchG.

Gesetzgeber den Beschäftigungsgebern das bestehende Vertrauen in eine grundsätzlich vorrangig interne Meldung genommen; obwohl sie es sind, die etwaige Missstände effektiv zu beheben vermögen. Die Formulierung in § 7 Abs. 1 S. 2 HinSchG, wonach Whistleblower eine interne Meldestelle bevorzugen sollen, wenn intern wirksam gegen den Verstoß vorgegangen werden kann und sie keine Repressalien zu befürchten haben, hilft den Unternehmen über dieses Dilemma nicht hinweg. Sie stehen vor der Herausforderung, Anreize für eine interne Meldung zu schaffen, um darauf hinzuwirken, dass sensible Information nicht nach außen gelangen. Neben der Schaffung anonymer Meldekanäle und Maßnahmen zur Erhöhung des Identitätsschutzes kommen insbesondere berufliche und finanzielle Anreize in Betracht. Darüber hinaus sind auch interne Meldepflichten zu erwägen.

Sowohl die Implementierung eines effektiven Hinweisgeberschutzsystems als auch die Schaffung von Anreizen zu dessen Nutzung sind spätestens mit Inkrafttreten des HinSchG als Teil des unternehmerischen Geheimnisschutzkonzepts zu verstehen und fließen in die Beurteilung angemessener Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG mit ein. Vor diesem Hintergrund nimmt sich die vorliegende Untersuchung dem dringend gebotenen Diskurs über Grund und Grenzen des betrieblichen Geheimnisschutzes im Widerstreit zum Hinweisgeberschutz an. Gab es vor Inkrafttreten des HinSchG nur vereinzelte Regelungen, die Whistleblower vor rechtlichen Sanktionen schützten,[21] sind die Anforderungen seit Inkrafttreten

[21] Gemeint sind Regelungen insbesondere im Finanzdienstleistungsbereich: § 4d Abs. 6 FinDAG, § 3b Abs. 5 BörsG; § 53 Abs. 5 GwG.

des HinSchG denkbar niedrig.[22] Dem Denunziantentum scheint Tür und Tor geöffnet, ist das Whistleblowing doch mittlerweile ein gesellschaftlich und rechtlich anerkanntes Phänomen.[23]

Zeitgleich etabliert sich ein stetig wachsendes Bedürfnis nach Transparenz in Bezug auf die Unternehmensführung. Unternehmen sehen sich infolgedessen mit immer mehr Berichtspflichten konfrontiert, die ihre nichtfinanziellen Bereiche betreffen.[24] Diese resultieren insbesondere aus einer zunehmenden Sensibilität für soziale Verantwortung, ethische Standards und der damit verbundenen allgemeinen Erwartung an Unternehmen, eine verantwortungsbewusste Unternehmensführung zu praktizieren. Die Wirksamkeit solcher Berichtspflichten ist jedoch kritisch zu hinterfragen. Insbesondere die beiden Evaluierungen der Bundesregierung zum EntgTranspG haben gezeigt, dass den Berichtspflichten für Unternehmen zum geschlechtsspezifischen Lohngefälle allenfalls geringe Wirksamkeit attestiert werden kann.[25]

---

[22] Hinweisgeberschutz besteht schon dann, wenn die hinweisgebende Person zum Zeitpunkt der Meldung oder Offenlegung hinreichenden Grund zu der Annahme hatte, dass die von ihr gemeldeten oder offengelegten Informationen der Wahrheit entsprechen. Die Anforderungen an die Verifizierung des Wahrheitsgehalts einer Information durch den Hinweisgeber sind denkbar niedrig gehalten: Einem Whistleblower soll es nach dem Willen des Gesetzgebers schon unzumutbar sein, sich um Verifizierung zu bemühen, sofern er fürchtet, dadurch entdeckt zu werden, vgl. BT-Drs. 20/5992, S. 78, 92. Einschränkend zu Recht: *Siemes,* CCZ 2022, 293, 302, wonach die Befürchtung nicht rein subjektiv sein darf; ebenso: *Thüsing/Musiol,* BB 2022, 2420, 2421.

[23] Siehe etwa: *Müller*, NZA 2002, 424, 425: Früher galten Whistleblower als Denunzianten. Diesem Verständnis entstammt auch der bekannte Ausspruch von *Hoffmann von Fallersleben* aus dem 19. Jahrhundert: „*Der größte Lump im ganzen Land, das ist und bleibt der Denunziant*."

[24] Etwa in Bezug auf die Unionsgesetzgebung: CSRD, CSDDD u. die Lohntransparenz-RL. Für die nationale Gesetzgebung: EntgTranspG, LkSG.

[25] BT-Drs. 19/11470, Erster Bericht der Bundesregierung zur Wirksamkeit des EntgTranspG; Zweiter Bericht der Bundesregierung zur Wirksamkeit des EntgTranspG, S. 8, 194 ff.

Ähnliche Ergebnisse dürften in Bezug auf die Umsetzungsgesetze zur CSRD-RL[26] und CSDDD-RL[27] zu erwarten sein.

Eine weitere rechtspolitische Entwicklung betrifft das zunehmende Bedürfnis nach einer Regulierung neuer Technologien.[28] So hat der europäische Gesetzgeber erst kürzlich mit der KI-Verordnung einen gesetzlichen Rahmen für den Einsatz von Künstlicher Intelligenz in Europa geschaffen.[29] Die Verordnung verfolgt einen risikobasierten Ansatz und zielt darauf ab, das Vertrauen in den Einsatz von KI-Systemen zu stärken. Für die Zukunft deuten sich außerdem Neuerungen im Datenschutzrecht an.[30] Mit der EuGH-Entscheidung zur Auslegung von Art. 88 Abs. 1 und Abs. 2 DS-GVO hat diese Überlegung an Fahrt gewonnen.[31] Richtig ist, dass Unternehmen mit dem verstärkten Einsatz digitaler Technologien und der zunehmenden Vernetzung von Geschäftssystemen höheren Risiken ausgesetzt sind, weil sie z. B.

---

26 Richtlinie (EU) 2022/2464 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 zur Änderung der Verordnung (EU) Nr. 537/2014 und der Richtlinien 2004/109/EG, 2006/43/EG und 2013/34/EU hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen, ABl. v. 16.12.2022, L 322, S. 15.

27 Directive of the European parliament and of the council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937.

28 Etwa Antidiskriminierungsstelle des Bundes, Diskriminierungsrisiken durch Algorithmen, S. 97 ff.; Algorithm Watch, Stellungnahme zum Zwischenbericht des UN-Beirats für Künstliche Intelligenz.

29 Verordnung (EU) COM (2021) 206 final des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union. Die überwiegenden Regelungen werden Anfang 2026 in Kraft treten.

30 Vgl. Koalitionsvertrag von SPD, Bündnis 90/Die Grünen und FDP, 20. Legislatur, S. 14: Der Koalitionsvertrag kündigt die Schaffung neuer Regelungen zum Beschäftigtendatenschutz an.

31 EuGH, Urteil v. 30.03.2023 - C-34/21, NZA 2023, 487; *Thüsing/Peisker,* NZA 2023, 213; *Böhm/Brams*, NZA-RR 2023, 625. Die Entscheidung führt nach hiesiger Auffassung zur Unionsrechtswidrigkeit des § 26 Abs. 1 S. 1 BDSG, siehe: Kapitel B) II. 4. b) aa).

anfälliger für Datendiebstahl werden.[32] Regulatorische Vorgaben können in diesem Kontext helfen, Risiken entgegenzuwirken. Darüber hinaus sind Nachbesserungen im Bereich des Datenschutzrechts geeignet, Rechtsklarheit zu schaffen. Neue Regelungen dürfen jedoch nicht zur Bremse für technologische Entwicklungen und Innovation werden. Wichtig bleibt eine ausgewogene Herangehensweise. Insbesondere ist an der technologieoffenen Ausgestaltung des Datenschutzrechts festzuhalten. Andernfalls droht eine Gefährdung der Wettbewerbsfähigkeit der Unternehmen und des Industriestandorts Deutschland.

II. Kernfragen und Gang der Darstellung

Die vorliegende Dissertation „*Geheimnisschutz zwischen Arbeitsrecht, Datenschutz und Gesellschaftsrecht*“ befasst sich mit der Reichweite und den Grenzen des betrieblichen Geheimnisschutzes, respektive des Geschäftsgeheimnisschutzes im Beschäftigungskontext und stellt anhand relevanter Schwerpunktthemen die notwendigen Bezüge zum gesellschaftsrechtlichen Pflichtenprogramm her.

Die Darstellung untersucht, unter welchen Voraussetzungen eine betriebliche Information dem Schutzregime des GeschGehG unterfällt (Kapitel B) und inwieweit gegenläufige Interessen mögliche Einschränkungen des Geschäftsgeheimnisschutzes im Beschäftigungskontext bedingen (Kapitel C). Schwerpunkte der Analyse bilden dabei insbesondere das Verhältnis des Geschäftsgeheimnisschutzes zum Hinweisgeberschutz und zu den datenschutzrechtlichen Betroffenen-

[32] Unternehmen müssen ihre Geschäftsgeheimnis-Strategien kontinuierlich anpassen, um mit den sich verändernden Anforderungen und Bedrohungen Schritt zu halten. Insbesondere moderne Arbeitsweisen wie mobiles Arbeiten stellen eine zusätzliche Herausforderung dar, da die Sicherheit sensibler Informationen in dezentralen Arbeitsumgebungen zu gewährleisten ist. Unternehmen müssen sicherstellen, dass ihre Sicherheitsmaßnahmen nicht nur auf die physischen Büroumgebungen zugeschnitten sind, sondern auch den spezifischen Anforderungen und Risiken des mobilen Arbeitens Rechnung tragen.

rechten. In einem weiteren Teil untersucht die vorliegende Arbeit Datenverarbeitungen im Beschäftigungskontext mittels derer exklusives Wissen zur Steigerung der eigenen Innovations- und Wettbewerbsfähigkeit generiert werden soll (Kapitel D).

Die Arbeit setzt sich mit den bestehenden Rechtsunsicherheiten auseinander und geht rechtsdogmatisch anhand der bekannten Auslegungskriterien vor. Ziel der Arbeit ist es, zentrale arbeitsrechtliche und datenschutzrechtliche Fragen im Bereich des Geschäftsgeheimnisschutzes zu klären, aus denen dann Weiterungen für das gesellschaftsrechtliche Pflichtenprogramm folgen.[33] Die Darstellung soll Leitlinien für die Auslegung der einschlägigen Rechtsnormen herausbilden und Rechtsanwendern eine stichhaltige Orientierungshilfe bieten.[34]

1. Kapitel B): Rechtliche Grundlagen des Geschäftsgeheimnisschutzes

Das Kapitel untersucht, unter welchen Voraussetzungen eine Information dem Schutzregime des GeschGehG unterfällt (Abschnitt II). Im Fokus steht die materiell-rechtliche Bewertung. Schwerpunktthemen bilden die Fragen, ob sog. „*rechtswidrige Informationen*“[35] ein rechtlich schutzfähiges Unternehmensgeheimnis sind und welche Anforderungen an den unbestimmten Rechtsbegriff der „*angemessenen Geheimhaltungsmaßnahmen*“ zu stellen sind.[36] Damit eine betriebliche Information dem Schutzregime des GeschGehG unterfällt, hat

---

[33] Nach § 93 Abs. 1 S. 1 AktG, § 43 Abs. 1 GmbHG, § 34 Abs. 1 S. 2 GenG ist die Geschäftsleitung zur sorgfältigen Unternehmensführung verpflichtet., vgl. *Thüsing*, in: Compliance, § 2 Rn.17, 20.

[34] Es besteht nach wie vor Unsicherheiten in Bezug auf die Reichweite des Geschäftsgeheimnisschutzes, insbesondere welche Informationen als Geschäftsgeheimnisse geschützt und wie die Ausnahmetatbestände auszulegen sind, siehe: Study on the Legal Protection of Trade Secrets, S. 23, 75.

[35] Gemeint sind Informationen illegalen Ursprungs oder Inhalts.

[36] § 2 Nr. 1 lit. b) GeschGehG.

der Arbeitgeber[37] unter anderem angemessene Geheimhaltungsmaßnahmen zu implementieren. Welche Maßnahmen dies im Einzelnen umfasst und welche Auswirkungen unwirksame Geheimhaltungsmaßnahmen auf das Vorliegen eines Geschäftsgeheimnisses im Sinne des § 2 Abs. 1 GeschGehG bzw. den Nachweis eines Geheimnisverrats haben, bedarf einer eingehenden Untersuchung. Grundsätzlich ist der Arbeitgeber in seiner Entscheidung frei, ob er Geheimhaltungsmaßnahmen in seinem Betrieb implementiert.[38] Etwas anderes gilt, soweit die gesellschaftsrechtlichen Regelungen Vorstand und Geschäftsführung zur Implementierung angemessener Geheimhaltungsmaßnahmen verpflichten (Abschnitt III). Es kann sich außerdem anbieten, Synergieeffekte des Geheimnisschutzkonzepts mit dem Datenschutzkonzept zu heben.

Leitfragen dieses Kapitels sind:
- Wann unterfällt eine Information dem GeschGehG-Schutzregime?
- Welche Besonderheiten gelten im Beschäftigungskontext?
- Was bedeutet das für das unternehmerische Compliance-System?

2. Kapitel C): Reichweite und Grenzen des Geschäftsgeheimnisschutzes im Beschäftigungskontext

Kapitel C) lotet die Reichweite des Geschäftsgeheimnisschutzes aus. Der Schutz vor unerlaubter Erlangung, Nutzung und Offenlegung von Geschäftsgeheimnissen gilt nicht uneingeschränkt.[39] Inwieweit ein Unternehmen zur Offenlegung bzw. Beauskunftung seiner Geschäftsgeheimnisse verpflichtet ist bzw. eine Weitergabe seiner geschützten Informationen durch Arbeitnehmer zu dulden hat, bedarf einer dezidierten Untersuchung. Zunächst wird das Verhältnis des Geschäftsgeheimnisschutzes zum Hinweisgeberschutz beleuchtet (Abschnitt I). Dabei gilt es, die bestehenden Friktionen zwischen GeschGehG und

---

[37] Aus Gründen der besseren Lesbarkeit bezieht sich die gewählte männliche Form immer auch auf weibliche, männliche und diverse Personen.
[38] Vgl. BT-Drs. 19/4724, S. 24.
[39] *Reinfeld,* Das neue GeschGehG, § 1 Rn.62.

HinSchG herauszuarbeiten und einer Lösung zuzuführen. Im Zuge der Nachforschungen wird untersucht, unter welchen Voraussetzungen Whistleblower bei der Weitergabe bzw. Offenlegung von Geschäftsgeheimnissen geschützt sind, respektive dem Geheimnisinhaber Schutz- und Abwehransprüche nach dem GeschGehG versagt bleiben. Juristisch betrachtet, bildet das Spannungsverhältnis zwischen Geschäftsgeheimnissen und Whistleblowing einen Konflikt widerstreitender Rechtspositionen, die jeweils grundrechtliche, unionsrechtliche und völkerrechtliche Verankerung erfahren haben und notwendigerweise in einen angemessenen Ausgleich zu bringen sind.[40] Dazu untersucht die vorliegende Arbeit auch, unter welchen Voraussetzungen ein interner Meldekanal vorrangig zu nutzen sein kann. Weitere Schwerpunkte bilden die Fragen, ob und inwieweit Arbeitnehmer zur Abgabe einer (vorrangig) internen Meldung verpflichtet werden können und inwiefern Unternehmen den Identitätsschutz bei der Nutzung eines internen Meldekanals erhöhen können. Ein besonderer Schwerpunkt liegt dabei in der Betrachtung des Identitätsschutzes des Whistleblowers im Verhältnis zu den datenschutzrechtlichen Betroffenenrechten der von der Meldung betroffenen Person.

Darüber hinaus wird der Geschäftsgeheimnisschutz im Verhältnis zu den datenschutzrechtlichen Betroffenenrechten analysiert (Abschnitt II). Neben allgemeinen Fragen zur Konzeption der Datenauskunft (Art. 15 DS-GVO), stellen sich konkrete Fragen nach der Berücksichtigung unternehmerischer Geheimhaltungsinteressen, auch bzgl. des personalaktenrechtlichen Einsichtsrechts (§ 83 Abs. 1 S. 1 BetrVG). Abschließend widmet sich das Kapitel dem Geschäftsgeheimnisschutz im Rahmen der Betriebsratsarbeit (Abschnitt III). Ist ein Betriebsratsmitglied zugleich ein Whistleblower, agiert es nicht

[40] Dies folgt für Grundrechte aus ihrer mittelbaren Drittwirkung. Die Rechte der GR-CH gehören zum Unionsprimärrecht. Sowohl die unionsrechtlichen Vorschriften als auch die jeweiligen Umsetzungs-Vorschriften sind bei Rechtsstreitigkeiten zwischen Privaten in Einklang mit der GR-CH auszulegen, vgl. statt vieler: BVerfG, Beschluss v. 11.04.2018 - 1 BvR 3080/09, BVerfGE 148, 267, NJW 2018, 1667, Rn.32.

mehr nur im Spannungsfeld zwischen Meinungsfreiheit und unternehmerischen Geheimhaltungsinteressen, sondern unterliegt zusätzlich dem Gebot der vertrauensvollen Zusammenarbeit (§§ 2 Abs. 1, 79 Abs. 1 S. 1 BetrVG), das nach hiesiger Auffassung eine vom HinSchG unabhängige Betrachtungsweise erfordert.[41]

Leitfragen dieses Kapitels sind:

- Wie können die Friktionen zwischen GeschGehG und HinSchG überwunden werden?
- Wem darf ein Whistleblower Geschäftsgeheimnisse melden?
- Was folgt daraus für die unternehmerischen Compliance-Systeme?
- Wann muss der datenschutzrechtlich Verantwortliche Geschäftsgeheimnisse beauskunften?
- Wie wird der Geschäftsgeheimnisschutz im Rahmen der Betriebsratsarbeit gewährleistet?

3. Kapitel D): Die Gewinnung neuen exklusiven Wissens im Beschäftigungskontext: Eine Balance zwischen Forschung, Innovation und Rechtskonformität

Die Erforschung neuen Wissens ist notwendige Voraussetzung, exklusive Informationen zu erlangen, die dann in einem nachgelagerten Schritt durch die Implementierung angemessener Geheimhaltungsmaßnahmen Schutz durch das GeschGehG erfahren können. Im Beschäftigungskontext stellt sich insbesondere die Frage, inwieweit der Einsatz algorithmusbasierter KI-Systeme zu Zwecken der Prozessoptimierung möglich ist. Die Herausforderung besteht darin, ein Gleichgewicht zwischen Persönlichkeitsschutz und berechtigtem Informationsbedürfnis zu schaffen.

---

41 Siehe: Kapitel C) III. 3.

Leitfrage dieses Kapitels ist:

- Was ist bei der Implementierung betrieblicher Maßnahmen zu Innovationszwecken im Beschäftigungskontext zu beachten?

4. Kapitel F): Eine Zusammenfassung in 25 Thesen

Abschließend werden die im Laufe dieser Arbeit gewonnenen Erkenntnisse thesenartig zusammengefasst. Auf die Art soll dem Leser ein schneller Überblick verschafft werden.

5. Weiterer Forschungsbedarf

Im Fokus dieser Arbeit stehen die Anforderungen im Bereich des Geschäftsgeheimnisschutzes, die der Gesetzgeber Unternehmen der Privatwirtschaft in Zusammenspiel mit dem gesellschaftsrechtlichen Pflichtenprogramm auferlegt. Angesichts der Vielzahl möglicher Fallgestaltungen beschränkt sich diese Arbeit auf eine Konturierung der Definition des Geschäftsgeheimnisses, deren Verständnis Voraussetzung für den Schutz durch das GeschGehG ist. In Anbetracht der nahezu unüberschaubaren Menge an Literatur zur Ausgestaltung betrieblicher Geheimnisschutzkonzepte lässt es die vorliegende Arbeit in Teilen bei allgemeinen Ausführungen und Grundsätzen bewenden. Dies betrifft insbesondere die Implementierung möglicher Geheimhaltungsmaßnahmen im Beschäftigungskontext und gilt auch in Bezug auf die Gewinnung neuen exklusiven Wissens, dessen vielgestaltige Möglichkeiten sich nicht abschließend ermitteln lassen. Die vorliegende Arbeit kann hier nur als Orientierungshilfe beispielhaft aufzeigen, was bei der Implementierung relevanter Maßnahmen zu beachten sein kann. Welche Sanktionen Geheimnisbrechern bei Verstößen gegen das GeschGehG auf Sekundärebene drohen, wird nicht näher beleuchtet.

Das Immaterialgüterrecht ist ebenfalls nicht Gegenstand der vorliegenden Untersuchung. Der Geschäftsgeheimnisschutz bildet eine eigenständige Rechtsposition, die nicht dem Immaterialgüterrecht

zugeordnet werden kann.[42] Im Vergleich zum Schutz des geistigen Eigentums gewährt das GeschGehG keinen absoluten Schutz, sondern weist lediglich eine mit dem Immaterialgüterrecht vergleichbare Struktur und Konzeption auf.[43] Privatgeheimnisse sind nur insoweit Gegenstand der vorliegenden Untersuchung, als sie Geschäftsgeheimnisse darstellen können. Ebenfalls spart die Untersuchung Vorschriften des öffentlichen Dienstes aus. Hält der Staat beispielsweise Mehrheitsbeteiligungen einer AG, können die hier gewonnenen Ergebnisse gleichwohl Geltung beanspruchen. Auch weitere Bereiche des Geheimnisschutzes, wie Amtsgeheimnisse und Steuergeheimnisse oder Informationszugangsrechte, bleiben außen vor. Hierfür wäre die Einbeziehung weiterer Rechtsgebiete nötig, die nicht dem Untersuchungsgegenstand zuordbar sind.

Die Grenzen des Geschäftsgeheimnisschutzes werden anhand ausgewählter Themenkomplexe das Arbeitsrecht betreffend ausgelotet. Grenzen, die der Geschäftsgeheimnisschutz im Bereich des investigativen Journalismus erfährt, sind demgemäß nicht Untersuchungsgegenstand. Richtschnur der Untersuchung ist die Einhaltung der gesetzlichen Vorgaben. Forschungsbedarf verbleibt in Bezug auf rechtlich mögliche und gebotene Gesetzesänderungen im Bereich des Geschäftsgeheimnisschutzes.

---

42 *Hauck*, GRUR-Prax 2019, 223; *Hauck*, NJW 2016, 2218, 2221; a. A.: *Kiefer*, WRP 2018, 910.

43 *Alexander*, AfP 2019, 1, 2; *Ohly*, in: Harte-Bavendamm/Ohly/Kalbfus GeschGehG, Einl. A. Rn.26; *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 110-114; *Thiel*, WRP 2019, 700, 702, 703. Zur Rechtsnatur von Geschäftsgeheimnissen umfassend: *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Drittes Kapitel, S. 216, 217.

B) Rechtliche Grundlagen des Geschäftsgeheimnisschutzes

Der Schutz betrieblicher Informationen dient der Schaffung von Wettbewerbsvorteilen und trägt dazu bei, dass sich Unternehmen am Markt behaupten und etablieren können. Trotz des zur Umsetzung der GeschGeh-RL am 26. April 2019 in Kraft getretenen GeschGehG existiert kein einheitliches Geschäftsgeheimnisschutzrecht in Deutschland. Zunächst gilt es, Rechtsrahmen und Funktion des Geschäftsgeheimnisschutzes herauszuarbeiten. Soweit die nachfolgenden Kapitel Interessenkollisionen mit dem Geschäftsgeheimnisschutz aufzeigen, kann auf dessen verfassungs-, unions- und völkerrechtliche Verankerung zurückgegriffen werden. Anschließend nimmt die Untersuchung die gesetzgeberische Ausgestaltung des Geschäftsgeheimnisschutzes in den Blick. Schwerpunktthema bildet die Definition des Geschäftsgeheimnisses gemäß § 2 GeschGehG. Ein umfassendes Begriffsverständnis ist grundlegende Voraussetzung stichhaltiger Aussagen über Weiterungen für das unternehmerische Geheimnisschutzkonzept.

I. Rechtsrahmen und Funktion

Der betriebliche Geheimnisschutz ist grund-, unions- und konventionsrechtlich verankert. Die Judikative hat die jeweiligen Schutzgehalte daher bei der Auslegung unbestimmter Rechtsbegriffe zu beachten. Für die Grundrechte folgt dies aus ihrer mittelbaren Drittwirkung.[44] Mitgliedstaatliche Regelungen zur Durchführung des Unionsrechts[45] sind ebenso wie die unionsrechtlichen Vorgaben im Lichte der

---

[44] Statt Vieler: BVerfG, Beschluss v. 11.04.2018 - 1 BvR 3080/09, BVerfGE 148, 267, NJW 2018, 1667 Rn.32.

[45] Vgl. *Jarass*, GR-CH, Art. 51 Rn.29-31. Das Umsetzungsgesetz der Whistleblowing-RL ist z. B. das HinSchG.

GR-CH[46] auszulegen.[47] Auch die EMRK und ihre durch den EGMR vollzogene Auslegung fließen in die Auslegung unbestimmter Rechtsbegriffe ein.[48] Mit ihrer Ratifizierung[49] im Jahr 1952 hat die EMRK den Rang einfachen Bundesgesetzes erhalten.[50] Über das Menschenrechtbekenntnis des Grundgesetzes hat die EMRK außerdem interpretationsleitenden Charakter für das Verständnis der verfassungsrechtlichen Grundprinzipien erlangt.[51] Zudem statuieren die Freiheiten der EMRK nach Art. 52 Abs. 2 GR-CH einen Mindeststandard für einen Großteil der dort verbürgten Grundrechte, die wie beschrieben über die unionsrechtskonforme Auslegung der nationalen Vorschriften mittelbare Wirkung entfalten.[52] Hinsichtlich des Schutzes von Geschäftsgeheimnissen kommen verschiedene grund-, unions- und völkerrechtliche Freiheitsrechte in Betracht,[53] deren Schutzgehalt in den folgenden Abschnitten untersucht wird.

---

46 Gemäß Art. 6 Abs. 1 EUV stehen die Rechte der GR-CH rechtlich gleichrangig neben AEUV und EUV.

47 Vgl. Art. 6 Abs. 1 Hs. 2 EUV; siehe auch: *Jarass*, GR-CH, Art. 51 Rn.38 bis 40 und Einl. Rn.68-70.

48 Für die Judikative folgt dies aus Art. 20 Abs. 3 GG. Vgl. auch *Stelkens*, in: Sachs/Schmitz/Stelkens, VwVfG, Europäisches Verwaltungsrecht, Rn.16-18a.

49 BGBl. II 1952, 685.

50 Mit Hinweis auf den Sonderstatus der EMRK aufgrund der Völkerrechtsfreundlichkeit des GG: *Stelkens*, in: Sachs/Schmitz/Stelkens, VwVfG, Europäisches Verwaltungsrecht Rn.16-18a; siehe auch: *Meyer-Ladewig/Nettesheim*, in: NK-GR-CH, Art. 1 EMRK Rn.5.

51 BVerfGE 74, 358, 370 - *Unschuldsvermutung II*; 111, 307, 315-330 - *Görgülü-Beschluss*; 128, 326, 366-372 -*Sicherungsverwahrung*; *Schmitt*, NZA-Beilage 2020, 50, 51.

52 *Jarass*, GR-CH, Art. 52 Rn.62, 63; *Preis/Seiwerth*, RdA 2019, 351, 356; *Schmitt*, RdA 2017, 365, 367, 368; *Schwerdtfeger*, in: NK-GR-CH, Art. 52 Rn.52-66.

53 Der verfassungsrechtliche Schutz von Geschäftsgeheimnissen ist anerkannt. Nicht abschließend geklärt ist die exakte grundrechtliche und chartarechtlich sowie konventionsrechtliche Verankerung, vgl. *Hofmann*, NVwZ, 2020, 718; *Kalbfus*, in: Harte-Bavendamm/Ohly/Kalbfus, GeschGehG, Einl. A Rn.165-170; *Libor*, AfP 2019, 25, 28; *Sixt*, Whistleblowing im Spannungsfeld, S. 80.

1. Die Verankerung in der GR-CH

Im Rahmen der GR-CH findet der betriebliche Geheimnisschutz Verankerung in dem Recht auf Achtung des Privat- und Familienlebens (Art. 7 GR-CH), dem Recht auf Schutz personenbezogener Daten (Art. 8 GR-CH), der Berufsfreiheit und dem Recht zu arbeiten (Art. 15 GR-CH), der unternehmerischen Freiheit (Art. 16 GR-CH) sowie dem Eigentumsrecht (Art. 17 GR-CH).[54] Das Recht der unternehmerischen Freiheit schützt die Betätigung aller Selbständigen und soll insoweit gegenüber der Berufsfreiheit vorrangig sein.[55] Geschützt sind Geschäftsgeheimnisse als wesentlicher Faktor zum Erhalt der Wettbewerbsfähigkeit.[56] Geheimnisschutz ist auch in dem Recht auf Achtung des Privatlebens (Art. 7 GR-CH) verankert, zu dem insbesondere das „*geschäftliche Privatleben*" zählt.[57] Vor diesem Hintergrund ist davon auszugehen, dass der Schutz personenbezogener Daten (Art. 8 GR-CH) ebenso juristischen Personen zu Gute kommen soll.[58] Dafür spricht unter anderem, dass der Datenschutz für die berufliche und wirtschaftliche Sphäre von Relevanz ist und Erwägungsgrund 34

---

54 Vgl. Erwägungsgrund 34 GeschGeh-RL; *Kalbfus*, in: Harte-Bavendamm/Ohly/Kalbfus, GeschGehG, Einl. A Rn.165.

55 Die genaue Grenzziehung zwischen Berufsfreiheit (Art. 15 GR-CH) und unternehmerischer Freiheit (Art. 16 GR-CH) ist noch offen, vgl. *Jarass*, GR-CH. Art. 15 Rn.4, 9 sowie Art. 16 Rn.4, 5; siehe auch: *Beyerbach*, Unternehmensinformation, S. 304-305; *Siebert*, Geheimnisschutz, S. 261. Für die unternehmerische Betätigung zieht das BVerfG Art. 16 GR-CH heran, vgl. BVerfGE 152, 216, 256, 257 - *Recht auf Vergessen II*.

56 *Beyerbach*, Unternehmensinformation, S. 305; *Hauck*, AfP 2021, 193, 200; *Siebert*, Geheimnisschutz, S. 260.

57 Gemeint sind die vertraulichen Informationen von Unternehmen, vgl. EuGH, Urteil v. 14.2.2008 - C-450/06 Rn.48, 49, 51 - *Varc*; dazu auch *Jarass*, GR-CH, Art. 7 Rn.13, 17; *Dobler,* Geschäftsgeheimnisschutz und investigativer Journalismus, Drittes Kapitel, S. 232 m. w. N.

58 Dies ist nicht vollends geklärt. Eine überzeugende Darstellung für den Schutz juristischer Personen findet sich bei *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Drittes Kapitel, S. 232 f.

GeschGeh-RL explizit Bezug auf Art. 8 GR-CH nimmt.[59] Wie Art. 14 Abs. 1 GG weist auch die Eigentumsfreiheit in Art. 17 GR-CH einen normgeprägten Schutzbereich auf, der im Wege mitgliedstaatlicher Regelungen einer Konkretisierung erfordert.[60] Der Begriff folgt demnach dem nationalen Verständnis und schützt jedes vermögenswerte sacheigentumsgleiche Recht, zu denen auch Geschäftsgeheimnisse zählen.[61]

2. Die konventionsrechtliche Verankerung

Auch die EMRK statuiert Rechte, die betriebliche Geheimhaltungsinteressen schützen. Zwar schützt die EMRK - im Gegensatz zu Art. 16 GR-CH - die unternehmerische Freiheit nicht ausdrücklich. Gleichwohl berücksichtigt der EGMR wirtschaftliche Interessen.[62] Anknüpfungspunkte bilden einerseits die Eigentumsfreiheit (Art. 1 EMRK-ZP 1) sowie das Recht auf Achtung des Privat- und Familienlebens (Art. 8 EMRK).[63] Letzteres beziehe sich laut EGMR auch auf den beruflichen und geschäftlichen Bereich.[64] Das Eigentumsrecht in Art. 1 EMRK-ZP 1 ist konventionsautonom auszulegen.[65] Der Begriff ist weit auszulegen und umfasst sowohl einzelne Vermögenswerte als

---

59 Eher restriktiv: EuGH, Urteil v. 09.11.2010 - C-92/09, C-93/09 Rn.53 - *Schecke u. Eifert*; Urteil v. 17.12.2015 - C-419/14 Rn.79 - *WebMindLicenses*, wonach, ein personaler Bezug vorhanden sein müsse. Weiter dagegen die Literaturmeinung, insbesondere *Beyerbach* geht von einem informationellen Selbstbestimmungsrecht für Unternehmen aus, vgl. *Beyerbach*, Unternehmensinformation, S. 307-310.

60 *Jarass*, GR-CH, Art. 17 Rn.6; *Beyerbach*, Unternehmensinformation, S. 297-300.

61 *Dobler,* Geschäftsgeheimnisschutz und investigativer Journalismus, Drittes Kapitel, S. 235; *Jarass*, NVwZ 2006, 1089, 1090.

62 EGMR, Urteil v. 21.07.2011 - 28274/08 - *Heinisch*/*Deutschland*.

63 *Schmitt*, RdA 2017, 365, 367, dort Fn.33.

64 EGMR, Urteil v. 16.12.1992 - 13710/88 - *Niemietz/Deutschland*; *Siebert*, Geheimnisschutz, S. 37, 177; *Wolf*, Schutz des Betriebs- und Geschäftsgeheimnisses, S. 151, 152; vgl. auch EuGH, Urteil v. 14.02.2008 - C-450/06 Rn.48 - *Varec*.

65 *Beyerbach*, Unternehmensinformation, S. 301.

auch die Gesamtheit der unternehmerischen Vermögenswerte.[66] Damit erstreckt sich der Schutz auch auf Geschäftsgeheimnisse.

3. Die grundgesetzliche Verankerung

Grundgesetzlich erfahren Geschäftsgeheimnisse Schutz durch die Berufsfreiheit (Art. 12 Abs. 1 GG), die Eigentumsfreiheit (Art. 14 Abs. 1 GG) und das Recht am eingerichteten und ausgeübten Gewerbebetrieb (Art. 14 Abs. 1 GG bzw. Art. 12 Abs. 1 GG). Darüber hinaus ist ein Schutz über das Unternehmenspersönlichkeitsrecht aus Art. 2 Abs. 1 GG zu erwägen.

a) Berufsfreiheit, Art. 12 Abs. 1 GG

Die Berufsfreiheit (Art. 12 Abs. 1 GG) schützt Unternehmen vor Ausforschung und Veröffentlichung ihrer Geschäftsgeheimnisse.[67] Unternehmen können sich im Rahmen ihrer grundrechtlichen Berufsfreiheit auf das Recht zur ungestörten Teilnahme am Wettbewerb, das Recht zur freien wirtschaftlichen Verwertung geschaffener Werte und das Recht auf Außendarstellung zum Schutz vor Ehrverletzung und Rufschädigung berufen.[68] Geschützt ist die wirtschaftliche Verwertung beruflich erlangter Erkenntnisse und Vermögenspositionen, deren Geheimhaltung der Gewinnung eines Wettbewerbsvorsprungs gegenüber anderen Marktteilnehmern dient und besonderer Ausdruck

---

66 Beispielhaft: EGMR, Urteil v. 11.03.2012 - 23780/08 - *Malik/Vereingites Königreich*.

67 Die Berufsfreiheit ist für juristische Personen anwendbar, vgl. Art. 19 Abs. 3 GG, vgl. BVerfG, NJW 2005, 883, 884; BVerfGE 115, 205, 230, 231 - *Geschäfts- und Betriebsgeheimnis*; BVerfG, NJW 2014, 1581, 1582. Siehe dazu grundlegend auch: *Beyerbach*, Unternehmensinformation, S. 122-126 m. w. N.

68 BVerfGE 106, 275, 298 - Arzneimittelfestbetrag; 110, 274, 288 - Ökosteuer; BVerfGE 148, 40, 50 - *staatliches Informationshandeln*; BVerfG, NJW 2005, 883, 884; BGH GRUR 2016, 710, 715.

unternehmerischer Freiheit ist.[69] Die Berufsfreiheit garantiert demnach über ihre jeweiligen Teilausprägungen die exklusive Nutzung eines Geschäftsgeheimnisses durch das berechtigte Unternehmen.[70] Dieser Bereich betrieblicher Geheimhaltung wird auch über das Recht am eingerichteten und ausgeübten Gewerbebetrieb sowie das Unternehmenspersönlichkeitsrecht geschützt.[71]

b) Eigentumsfreiheit, Art. 14 Abs. 1 GG

Die Eigentumsfreiheit weist einen normgeprägten Schutzbereich auf, der über das einfache Recht Konkretisierung erfährt.[72] Erfasst sind alle vermögenswerten Positionen, die dem Einzelnen im Sinne eines Ausschließlichkeitsrechts zur eigenen Nutzung zugeordnet sind.[73] Spätestens seit Inkrafttreten des GeschGehG bestehen keine Zweifel mehr darüber, dass Geschäftsgeheimnisse unter die Eigentumsfreiheit (Art. 14 Abs. 1 GG) fallen. Der Geheimnisinhaber besitzt die alleinige Nutzungs- und Dispositionsbefugnis im Sinne einer grundsätzlichen Verfügungsmöglichkeit, die er zum eigenen Vorteil ausüben kann.[74] Darüber hinaus kann der Geheimnisinhaber andere Personen durch Unterlassungsansprüche von der Nutzung des Geschäftsgeheimnisses ausschließen und Ausgleich für unbefugte Nutzungen

---

69 *Beyerbach*, Unternehmensinformation, S. 176; *Rossi*, NVwZ 2019, 1847; *Cha,* Betriebs- und Geschäftsgeheimnisse, S. 147.

70 BVerfGE 115, 205, 230, 231 - *Geschäfts- und Betriebsgeheimnis.*

71 Die Gerichte prüfen das Recht am eingerichteten und ausgeübten Gewerbebetrieb in diesem Zusammenhang stets mit, vgl. BGHZ 16, 172 - *Dücko*; 17, 117 - *Forschungskosten*; BGH NJW 2018, 2877.
Siehe: Kapitel B) I. c).

72 Für juristische Personen folgt dies aus Art. 19 Abs. 3 GG, vgl. *Axer*, in: BeckOK-GG, Art. 14 Rn.37; *Remmert*, in: Dürig/Herzog/Scholz GG, Art. 19 Rn.37-41. Der Eigentumsbegriff ist gegenüber dem Eigentumsbegriff des BGB eigenständig, vgl. *Axer*, in: BeckOK-GG, Art. 14 Rn.1.

73 Ständige Rechtsprechung: Beispielhaft BVerfG 78, 58, 71; BVerfG NJW 1992, 36, 37; 89, 1, 6; BVerfGE 112, 93, 107; *Schmidt*, in: ErfK-ArbR, Art. 14 Rn.4.

74 BVerfG 53, 257, 290, 291; 83, 201, 209.

geltend machen.[75] Dies genügt, um Geschäftsgeheimnissen den Schutz aus Art. 14 Abs. 1 GG zuzusprechen.

c) Recht am eingerichteten und ausgeübten Gewerbebetrieb; Unternehmenspersönlichkeitsrecht

Das Recht am eingerichteten und ausgeübten Gewerbebetrieb (Art. 12 Abs. 1 GG i. V. m. Art. 14 Abs. 1 GG) schützt den Gewerbebetrieb als Zusammenfassung aller zum Vermögen des Unternehmens gehörenden Sachen und Rechte.[76] Gemeint ist zum einen die Substanz des Betriebs und darüber hinaus alles, was den Betrieb in seiner Gesamtheit zur Betätigung in der freien Wirtschaft befähigt.[77] Die Substanz des Betriebs beschreibt den Unternehmenswert zu dem folgerichtig auch Geschäftsgeheimnisse zählen.[78] Wie die Berufsfreiheit (Art. 12 Abs. 1 GG) schützt auch das Recht am eingerichteten und ausgeübten Gewerbebetrieb eine sogenannte betriebliche Geheimsphäre, die Grundlage der betrieblichen Betätigung ist und ein Mindestmaß an Vertraulichkeit sicherstellen soll. Nicht abschließend geklärt ist die exakte grundrechtliche Verankerung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb.[79] Da sowohl die wirtschaftliche Betätigung des Unternehmens als auch Vermögenspositionen des Betriebs geschützt sind, überzeugt im Ergebnis eine Zusammenschau von Art. 12 Abs. 1 GG und Art. 14 Abs. 1 GG.

---

75 §§ 6, 10, 11 GeschGehG.

76 BGHZ 78, 41, 44; 349, 356; BVerfGE 68, 193, 222, 223; auch das Reichsgericht hat ein Recht am Gewerbebetrieb anerkannt, vgl. RGZ 58, 24; 51, 369; 56, 271.

77 BGHZ 29, 65, 70; BGHZ 23, 157, 163; 45, 150, 157; 138, 311, 316, 317.

78 Vgl. BGH GRUR 2006, 1044, 1046; ArbG Düsseldorf, Urteil v. 23.01.2020 - 12 Ga 5/20 Rn.37; vgl. BGHZ 107, 117, 122; *Förster*, in: BeckOK-BGB, §823 Rn.181; *Sprau*, in: Grüneberg BGB, § 823 Rn.138, 139.

79 Offenlassend: BVerfGE 51, 193, 221, 22; BVerfGE 58, 300, 353; ausführlicher *Cha*, Betriebs- und Geschäfts-geheimnisse, S. 67-68; *Depenheuer*, in: FS-*Schenke*, S. 103, 104; *Koreng*, GRUR 2010, 1065, 1066, 1067.

Das Unternehmenspersönlichkeitsrecht kommt zum Tragen, soweit es um den Schutz der Unternehmensreputation geht.[80] Dabei ist zu beachten, dass Unternehmen nur insoweit Persönlichkeitsrechte zustehen können, wie diese an Art. 2 Abs. 1 GG anknüpfen und Lücken der besonderen Freiheitsgarantien schließen.[81] Vor diesem Hintergrund tritt das Unternehmenspersönlichkeitsrecht in aller Regel hinter die speziellen Grundrechtsgewährleistungen zurück.[82] Insbesondere die Berufsfreiheit erfasst das Recht auf Außendarstellung.[83]

4. Zusammenfassender Überblick

Jede nationale Rechtsvorschrift ist im Einklang mit dem GG, der GR-CH und der EMRK auszulegen. Dabei ist der rechtliche Schutz von Geschäftsgeheimnissen in mehrfacher Hinsicht verfassungs-, charta- und konventionsrechtlich abgesichert. Die verschiedenen Rechte schützen jeweils unterschiedliche Teilbereiche. Während die Berufsfreiheit und das Recht am eingerichteten und ausgeübten Gewerbebetrieb ebenso wie das Unternehmenspersönlichkeitsrecht eine betriebliche Geheimsphäre zum Schutzobjekt nehmen, knüpft die Eigentumsfreiheit an die Rechtsposition des Geheimnisinhabers im Sinne einer vermögenswerten und sacheigentumsgleichen Zuordnung an.[84] Unterfällt eine Information dem Schutz des GeschGehG, steht diese unter dem Schutz der Eigentumsfreiheit nach Art. 14 Abs. 1 GG und Art. 17 GR-CH. Verfassungsrechtlich betrachtet, stehen Eigentumsfreiheit und Berufsfreiheit gleichrangig in sog. Idealkonkurrenz

---

80 *Dobler,* Geschäftsgeheimnisschutz und investigativer Journalismus, Drittes Kapitel, S. 223 m. w. N.

81 Eine Berufung auf Art. 1 Abs. 1 GG ist Unternehmen nicht möglich, Art. 19 Abs. 3 GG, vgl. BVerfGE 106, 28, 42-44; *Claßen*/*Hassel*, IPRB 2020, 65, 66 m. w. N.

82 Ausführlich: *Dobler,* Geschäftsgeheimnisschutz und investigativer Journalismus, Drittes Kapitel, S. 226 ff.

83 BVerfG 105, 252, 279; BVerfG, NJW-RR 2004, 1710, 1712.

84 *Gajeck*, Wirtschaftsgeheimnis, S. 213.

nebeneinander.[85] Das Unternehmenspersönlichkeitsrecht greift demgegenüber subsidiär. Parallel zum grundrechtlichen Eigentumsschutz unterfallen Geschäftsgeheimnisse, die einen sacheigentumsgleichen Vermögenswert verkörpern, der Eigentumsfreiheit aus Art. 17 GR-CH und Art. 1 EMRK-ZP 1. Den Schutz einer beruflichen Geheimsphäre stellt die unternehmerische Freiheit aus Art. 16 GR-CH sicher, die außerdem von Art. 8 EMRK sowie von Art. 7 GR-CH geschützt wird. Geschäftsgeheimnisse werden auch durch Art. 8 GR-CH geschützt.

II. Die gesetzgeberische Ausgestaltung des Geschäftsgeheimnisschutzes

Mit dem Inkrafttreten des GeschGehG im Jahr 2019 hat der nationale Gesetzgeber dem Schutz von Geschäftsgeheimnissen in Umsetzung der GeschGeh-RL ein eigenes Stammgesetz gewidmet.[86] Damit steht Unternehmen ein mit dem Recht des geistigen Eigentums vergleichbarer Sonderrechtsschutz zur Verfügung,[87] der neben umfassenden Schutz- und Abwehrrechten des Geheimnisinhabers eine eigene Strafnorm enthält.[88]

Flankierend zu den Vorschriften des GeschGehG finden sich zahlreiche spezialgesetzliche Geheimhaltungspflichten für besondere

---

85 *Cha*, Betriebs- und Geschäftsgeheimnisse, S. 143-145, 156, 157; *Gajeck*, Wirtschaftsgeheimnis, S. 209-213.

86 *Alexander*, AfP 2019, 1, 2; *Burghardt-Richter*/*Bode*, BB 2019, 2697; *Erlebach*/*Veljovic*, wistra 2020, 190; *Gramlich*/*Lütke*, wistra 2022, 97; *Hauck*, GRUR-Prax 2019, 223; *Hoppe*/*Oldekop*, Geschäftsgeheimnisse, Rn.11.

87 Vgl. *Alexander*, AfP 2019, 1, 2; *Burghardt-Richter*/*Bode*, BB 2019, 2697; *Hauck*, GRUR-Prax 2019, 223; *Thiel*, WRP 20192, 700, 702-703.

88 Strafnormen aus dem Bereich des Geheimnisschutzes finden sich auch in §§ 202a, 202b, 202d, 203, 242, 353b, 355 StGB, § 85 GmbHG, § 404 AktG, § 151 Abs. 2 GenG.

Geheimnisträger.[89] Arbeitsvertraglich ist der Arbeitnehmer bereits aus seiner Treuepflicht heraus zur Verschwiegenheit über vertrauliche Informationen verpflichtet, soweit ein erkennbares Geheimhaltungsinteresse des Arbeitgebers besteht, vgl. § 241 Abs. 2 BGB.[90] Verschwiegenheitspflichten werden zudem arbeitsvertraglich vereinbart oder sie wirken über kollektivrechtliche Regelungen auf das Arbeitsverhältnis. Verstößt ein Arbeitnehmer gegen seine Verschwiegenheitspflicht wird der Arbeitgeber neben den Ansprüchen aus dem GeschGehG arbeitsrechtliche Maßnahmen in Erwägung ziehen. Sollte eine vertrauliche Information nicht dem Anwendungsbereich des GeschGehG unterfallen, greifen die allgemeinen zivilrechtlichen Haftungsansprüche,[91] deren Voraussetzungen für den Arbeitgeber jedoch deutlich schwerer nachzuweisen sind.[92] Vorstand und Geschäftsführung sind deshalb aufgrund ihrer Pflicht zur sorgfältigen Unternehmensführung verpflichtet, dafür Sorge zu tragen, dass geheime Informationen in den Anwendungsbereich des GeschGehG fallen.[93] Dies erfordert ein umfassendes Begriffsverständnis des Geschäftsgeheim-

---

89 Hierzu zählen insbesondere die §§ 93 Abs. 1 S. 3, 116 S. 2 AktG für die Organe von Kapitalgesellschaften und §§ 34 Abs. 1 S. 3, 41 GenG für den Vorstand und den Aufsichtsrat der Genossenschaft, deren Vorschriften für Geschäftsführer und Aufsichtsräte der GmbH entsprechend anwendbar sind, vgl. *Ziemons*, in: GmbHG-Kommentar, § 43 Rn.291. Weitere Geheimhaltungspflichten sind in §§ 29, 35 SprAuG, § 116 AktG i. V. m. § 25 MitbestG, § 1 Abs. 1 Nr. 3 DrittelbG, § 3 Abs. 2 MontanMitBestG, § 24 ArbnErfG, § 179 Abs. 7 SGB IX, § 10 BPersVG, § 41 SEBG, § 35 EBRG, § 90 HGB, § 52 S. 2 ArbGG, § 3 Abs. 1 TVöD normiert. Auszubildende sind nach § 13 S. 2 Nr. 6 BBiG verpflichtet, über Betriebs- und Geschäftsgeheimnisse Stillschweigen zu bewahren. § 79 Abs. 1 BetrVG verpflichtet unter anderem die Mitglieder des Betriebsrats zur Verschwiegenheit.

90 *Reinfeld*, in: Hdb-ArbR, § 30 Rn.16.

91 Mögliche Anspruchsgrundlagen können sich hier vor allem aus den §§ 280 Abs. 1, 241 Abs. 2, 242 BGB und §§ 823, 824, 826, 1004 BGB (analog) ergeben, deren Voraussetzungen für den Arbeitgeber im Einzelfall jedoch deutlich schwerer nachzuweisen sind.

92 Vgl. *Fuhlrott/Hiéramente,* in: BeckOK-GeschGehG, § 2 Rn.21a; *Fuhlrott/Hiéramente*, DB 2019, 967, 968; *Dann/Markgraf,* NJW 2019, 1774, 1775.

93 Vgl. § 93 Abs. 1 S. 1 AktG, § 43 Abs. 1 GmbHG, § 34 Abs. 1 S. 2 GenG.

nisses, dessen Untersuchung sich die nachfolgenden Abschnitte unter Zuhilfenahme der bekannten Auslegungsmethoden annehmen wird. Dazu soll zunächst die Entstehungsgeschichte des GeschGehG aufgezeigt werden, die für die historische Auslegung unbestimmter Rechtsbegriffe relevant ist. Sodann geht es um ein systematisches Verständnis des GeschGehG, ehe der Definition des Geschäftsgeheimnisses in seinen Einzelheiten nachgegangen wird. Schwerpunkte bilden u. a. die Schutzfähigkeit rechtswidriger Informationen sowie die Auslegungsmöglichkeiten der „*angemessenen Geheimhaltungsmaßnahmen*“ i. S. d. § 2 Abs. 1 Nr. b) GeschGehG. Die Definition des Geschäftsgeheimnisses entscheidet über die Schutzfähigkeit von Informationen und ist damit Ausgangspunkt aller nachfolgenden Ableitungen.

1. Eine kurze Genese: Von §§ 17 bis 19 UWG a. F. zur Neukonzeption des GeschGehG

Bis zum Inkrafttreten des GeschGehG am 26. April 2019 war der Geschäftsgeheimnisschutz nur fragmentarisch in §§ 17 bis 19 UWG a. F. geregelt und wurde deshalb unter anderem für unübersichtlich,[94] rudimentär,[95] unzureichend[96] und reformbedürftig[97] betitelt. In Ermangelung einer Legaldefinition blieb es der Rechtsprechung überlassen, eine Definition des Geschäftsgeheimnisbegriffs zu entwickeln.[98] Betriebs- und Geschäftsgeheimnisse waren demnach

---

94 *Ohly*, GRUR 2019, 441.

95 *Alexander*, AfP 2019, 1; *Becker*/*Kussnik*, RAW 2018, 119, 129; *Brammsen*, BB 2018, 2446; *Schuth*, Neure- gelung zum Schutz der Geschäftsgeheimnisse, S. 43.

96 *Apel*/*Walling*, DB 2019, 891, 892; *Druschel*/*Jauch*, BB 2018, 1218.

97 *Ohly*, GRUR 2014, 1, 2, 11; *Harte-Bavendamm*, in: FS-*Köhler*, S. 235, *Harte-Bavendamm,* in: Harte-Bavendamm/Ohly/Kalbfus GeschGehG, Einl. A. 2 Rn.53.

98 Beispielhaft LG Stuttgart, WM 2019, 166, 174; *Kalbfus*, Know-how-Schutz, S. 68; *Reinfeld*, GeschGehG, § 1 Rn.36; *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 65, 66; siehe auch: *Thüsing*/*Rombey*, ZD 2020, 221, 222.

Informationen mit Unternehmensbezug, die nicht offenkundig waren und nach dem bekundeten oder erkennbaren Geheimhaltungswillen des Inhabers geheim gehalten werden sollten und bezüglich derer ein berechtigtes wirtschaftliches Geheimhaltungsinteresse des Informationsinhabers gegeben sein musste.[99] Dabei war die Unterscheidung zwischen Betriebs- und Geschäftsgeheimnissen dem Grunde nach bedeutungslos.[100]

Im Jahr 2013 legte die Europäische Kommission einen Richtlinien-Vorschlag für die GeschGeh-RL vor, der am 8. Juni 2016 beschlossen und bis 9. Juni 2018 in nationales Recht umzusetzen war. Die GeschGeh-RL bezweckt einen europaweiten Mindest-Geschäftsgeheimnisschutz und definiert den Begriff des Geschäftsgeheimnisses.[101] Die Definition orientiert sich an dem bis dahin lediglich auf völkerrechtlicher Ebene bindenden Art. 39 Abs. 2 TRIPS, der sein Vorbild wiederum im Recht der Vereinigten Staaten von Amerika findet.[102] Mit Inkrafttreten der GeschGeh-RL sollte diese Definition Eingang in das Unionsrecht finden. Der deutsche Gesetzgeber hat die GeschGeh-RL - ein wenig verspätet - durch das GeschGehG in Form eines neuen Spezialgesetzes zum Schutz von Geschäftsgeheimnissen umgesetzt. Zu Recht wurde in diesem Zusammenhang die Unterscheidung zwischen Betriebs- und Geschäftsgeheimnissen aufgegeben.[103]

Mit Inkrafttreten des GeschGehG sahen sich viele Unternehmen gezwungen, ihre Geheimnisschutzkonzepte auf den Prüfstand zu stellen. Hintergrund war, dass das tatsächliche Vorliegen angemessener Geheimhaltungsmaßnahmen nunmehr neue Voraussetzung für die

---

99 Grundlegend: RGZ 149, 329, 334; BGH, GRUR 1955, 424, 425; GRUR 1961, 40, 43; BGHSt, 41, 140, 142; BGH, GRUR 2003, 356, 358 m. w. N.; *Kalbfus*, Know-how-Schutz, S. 68.

100 *Kalbfus*, Know-how-Schutz, S. 69, 70; *Rody*, Geschäfts- und Betriebsgeheimnisse, S. 38, 39.

101 Vgl. Art. 19 Abs. 1 S. 1 GeschGeh-RL.

102 BT-Drs. 19/4724, S. 24; *Ohly*, GRUR 2019, 441, 442.

103 Vgl. BT-Drs. 19/4724, S. 24, 40; BVerwG, NVwZ 2020, 715, 716.

Schutzfähigkeit einer Information geworden war, vgl. § 2 Nr. 1 lit. b) GeschGehG.

2. Die Grundstrukturen des GeschGehG: Ein Überblick

Das GeschGehG gibt Unternehmen verschiedene Schutz- und Abwehrrechte an die Hand, um den Schutz ihrer Geschäftsgeheimnisse durchzusetzen. Diese finden sich in §§ 6 ff. GeschGehG und setzen den Verstoß gegen ein in § 4 GeschGehG normiertes Handlungsverbot voraus.[104] Der Begriff des Geschäftsgeheimnisses wird in § 2 Abs. 1 Nr. 1 GeschGehG legaldefiniert. Dazu sogleich ausführlich im nächsten Abschnitt. Die Ansprüche richten sich gegen den Rechtsverletzer (§ 2 Nr. 3 GeschGehG).[105] Anspruchsberechtigt ist der

---

[104] § 6 GeschGehG gibt dem Geheimnisinhaber Unterlassungs- und Beseitigungsansprüche an die Hand. § 7 GeschGehG normiert Ansprüche auf Vernichtung, Herausgabe, Rückruf, Entfernung aus den Vertriebswegen und Rücknahme vom Markt und erlangt insbesondere in Fällen rechtsverletzender Produkte Bedeutung. § 10 GeschGehG regelt den Schadensersatzanspruch des Geheimnisinhabers gegenüber dem Rechtsverletzer, der auf den Ersatz eines Vermögensschadens oder - soweit dies der Billigkeit im Sinne des § 242 BGB entspricht (beispielsweise in Fällen einer Rufschädigung) - auf eine Entschädigung in Geld gerichtet sein kann. Die in §§ 6 ff. GeschGehG normierten Schutz- und Abwehransprüche des Geheimnisinhabers gegenüber dem Rechtsverletzer können nach Maßgabe der §§ 9, 14 GeschGehG bei Unverhältnismäßigkeit oder aus Gründen des Missbrauchs vollständig ausgeschlossen sein. § 9 Nr. 2 GeschGehG berücksichtigt in diesem Zusammenhang auch die getroffenen Geheimhaltungsmaßnahmen. Sofern der Missbrauchseinwand greift, kann dem Rechtsverletzer ein Aufwendungsersatzanspruch nach § 14 S. 2 GeschGehG zustehen.

[105] Rechtsverletzer ist jede natürliche oder juristische Person, die entgegen § 4 GeschGehG ein Geschäftsgeheimnis rechtswidrig erlangt, nutzt oder offenlegt, ohne dass eine Tatbestandsausnahme im Sinne des § 5 GeschGehG greift oder die Handlung nach § 3 GeschGehG gestattet ist. Soweit die Voraussetzungen einer Wissens- oder Handlungszurechnung eines Organs nach § 31 BGB (analog) vorliegen, können auch juristische Personen Rechtsverletzer im Sinne des § 2 Nr. 3 GeschGehG sein, vgl. *Ellenberger*, in: Grüneberg § 31 BGB, Rn.3.

Inhaber des Geschäftsgeheimnisses (§ 2 Nr. 2 GeschGehG).[106] Strafrechtlichen Schutz erfahren Geschäftsgeheimnisse über § 23 GeschGehG.[107]

Wer erlaubt im Sinne des § 3 GeschGehG handelt, kann schon dem Wortlaut nach nicht gegen ein Handlungsverbot (§ 4 GeschGehG) verstoßen. Soweit § 3 Abs. 1 GeschGehG eingangs nur die Erlangung nennt, kann darunter auch die Nutzung oder Offenlegung zu fassen sein. § 3 Abs. 1 GeschGehG trifft insofern eine grundsätzliche Entscheidung über die Zulässigkeit der dort genannten Fälle.[108] Wird ein Geschäftsgeheimnis im Sinne des § 3 Abs. 1 GeschGehG rechtmäßig erlangt, so ist gleichermaßen auch dessen Nutzung und Offenlegung erlaubt.[109] § 3 Abs. 2 GeschGehG erlaubt Handlungen, die durch Gesetz, aufgrund eines Gesetzes oder durch Rechtsgeschäft gestattet

---

[106] Nach §§ 1 Abs. 3 Nr. 4 Var. 1 GeschGehG bleiben die Vorschriften des Arbeitnehmererfindungsgesetzes unberührt. Ein Arbeitgeber kann daher auch dann Inhaber eines Geschäftsgeheimnisses sein, wenn der Arbeitnehmer als Erfinder in Betracht kommt.

[107] Daraus geht hervor, dass nicht jeder Verstoß gegen das Handlungsverbot des § 4 GeschGehG mit einer Strafe belegt ist. Nach § 23 Abs. 1 GeschGehG wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen, ein Geschäftsgeheimnis entgegen § 4 Abs. 1 Nr. 1 GeschGehG erlangt, oder entgegen § 4 Abs. 2 Nr. 1 lit. a) GeschGehG nutzt oder offenlegt oder entgegen § 4 Abs. 2 Nr. 3 GeschGehG als eine bei einem Unternehmen beschäftigte Person, der das Geschäftsgeheimnis im Rahmen des Beschäftigungsverhältnisses anvertraut oder zugänglich wurde, dieses während des Beschäftigungsverhältnisses offenlegt.

[108] *Spieker*, in: BeckOK-GeschGehG, § 3 Rn.4.

[109] *Spieker*, in: BeckOK-GeschGehG, § 3 Rn.4. Der Gesetzgeber betont in diesem Zusammenhang, dass es sich bei Geschäftsgeheimnissen um keine Ausschließlichkeitsrechte handelt. Bestehende Immaterialgüterrechte seien daher weiterhin zu beachten, vgl. BT-Drs. 19/4724, S. 26.

[109] BT-Drs. 19/4724, S. 20; BeckOK-Geschäftsgeheimnis/*Spieker,* § 3 Rn.8.

sind.[110] Wer sich auf eine Tatbestandsausnahme des § 5 GeschGehG berufen kann, ist ebenfalls kein Rechtsverletzer.[111] Geschützt sind insbesondere die Meinungs- und Pressefreiheit, Fallkonstellationen des Whistleblowings sowie die Offenlegung von Geschäftsgeheimnissen durch Arbeitnehmer gegenüber der Arbeitnehmervertretung, wenn dies zu deren Aufgabenerfüllung erforderlich ist. Aus dem Wortlaut „*insbesondere*" ergibt sich, dass es über die genannten Fälle hinaus weitere unbenannte Fälle geben kann. Das Kriterium des „*berechtigten Interesses*" dient dabei der Sicherstellung des obligatorisch zu berücksichtigenden Verhältnismäßigkeitsgrundsatzes, unabhängig davon ob es sich um einen benannten oder unbenannten Fall des § 5 GeschGehG handelt.[112] Ob das berechtigte Interesse des Handelnden das Geheimhaltungsinteresse des Geheimnisinhabers im Einzelfall überwiegt, ist im Rahmen einer Interessenabwägung zu entscheiden.

§ 4 GeschGehG normiert die Handlungsverbote zum Schutz von Geschäftsgeheimnissen. Nach § 4 Abs. 1 Nr. 1 GeschGehG darf ein Geschäftsgeheimnis nicht durch unbefugten Zugang, unbefugte Aneignung oder unbefugtes Kopieren von Dokumenten,

---

[110] *Preis/Seiwerth,* RdA 2019, 351, 357, 358. Eine Gestattung im Sinne des § 3 Abs. 2 GeschGehG liegt auch dann vor, wenn eine Verpflichtung zur Erlangung, Nutzung oder Offenlegung besteht, siehe auch: *Hiéramente*, in: BeckOK-GeschGehG, § 3 GeschGehG, Rn.28 ff. Im Strafverfahren ist hier insbesondere an die Pflicht zur Zeugenaussage auf Anordnung des Richters bzw. der Staatsanwaltschaft zu denken, §§ 48 Abs. 1, 161a Abs. 1 S. 1 StPO. Im Arbeitsrecht dürfte vor allem die Offenlegung von Geschäftsgeheimnissen gegenüber Personen gemeint sein, wie z. B. der Datenschutzbeauftragte (§ 38 BDSG), der Betriebsarzt (§ 2 ASiG) oder der Störfallbeauftragte (§ 58a BImSchG), soweit die Offenlegung für die Wahrnehmung des jeweiligen Aufgabenbereichs erforderlich ist.

[111] Vgl. BT-Drs. 19/4724, S. 28; *Thüsing/Rombey,* ZD 2020, 221, 222.

[112] Die Verhältnismäßigkeitserwägungen sind im Rahmen des § 5 Nr. 2 GeschGehG anhand des öffentlichen Interesses zwingend mit einfließen zu lassen. Eine gesonderte Interessenabwägung bedarf es dann nicht, siehe: Kapitel C) I. 1. cc). § 5 Nr. 2 GeschGehG präzisiert das berechtigte Interesse als „*öffentliches Interesse*", vgl. *Hauck*, AfP 2021, 193, 203; *Alexander*, AfP 2019, 1, 3, 6. Vgl. auch Erwägungsgrund 21 GeschGeh-RL; BT-Drs. 19/4724, S. 28.

Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten oder aus denen sich das Geschäftsgeheimnis ableiten lässt, erlangt werden. Es genügt, dass die genannten Objekte einen Bezug zum Geschäftsgeheimnis aufweisen. Dies hat zur Folge, dass auch äußere Merkmale von Dateien geschützt sein können, sofern diese Rückschlüsse auf das jeweilige Geschäftsgeheimnis zulassen.[113] Unbefugt handelt, wer ohne tatbestandsausschließendes Einverständnis des Geheimnisinhabers handelt oder die Grenzen einer bestehenden Befugnis überschreitet. Eine Befugnis kann sich beispielsweise aus einer (arbeits-) vertraglichen Vereinbarung oder in Form einer gesetzlichen Gestattung ergeben. Dies folgt auch aus § 3 Abs. 2 GeschGehG. Andere Befugnisgründe, wie beispielsweise ein grundrechtskonformes Handeln, kommen im Rahmen der Tatbestandsausnahme des § 5 GeschGehG zum Tragen.[114]

§ 4 Abs. 1 Nr. 2 GeschGehG hat gegenüber der Nr. 1 die Funktion eines Auffangtatbestandes und ermöglicht eine interessengerechte Abwägung im Einzelfall zur Unterbindung treuwidrigen Verhaltens.[115] Darüber hinaus verbietet § 4 Abs. 2 GeschGehG die Nutzung und Offenlegung von Geschäftsgeheimnissen, die nach § 4 Abs. 1 Nr. 1 oder Nr. 2 GeschGehG durch eine eigene Handlung erlangt wurden. Ein Handlungsverbot besteht ferner für denjenigen,

---

[113] BVerwG, NVwZ 2020, 715, 717.

[114] BT-Drs. 19/4724, S. 27; *Brockhaus*, ZIS 2020, 111; a. A.: *Alexander*, in: Köhler/Bornkamm/Feddersen UWG, § 4 GeschGehG, Rn.21-35; *Hiéramente*, in: BeckOK-GeschGehG, § 4 Rn.21-25; *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Siebtes Kapitel, S. 506, 507.

[115] BT-Drs. 19/4724, S. 27. Da die unbestimmten Rechtsbegriffe einer Auslegung zugänglich sind und Verstöße gegen § 4 Abs.1 Nr. 2 GeschGehG keine strafrechtliche Relevanz nach § 23 GeschGehG haben, verstößt die Regelung nicht gegen das rechtsstaatliche Bestimmtheitsgebot, vgl. Art. 20 Abs. 1 und 2 GG.

der gegen ein Nutzungs- oder Offenlegungsverbot verstößt.[116] Wurde das Geschäftsgeheimnis über eine andere Person erlangt, kann das Handlungsverbot nach § 4 Abs. 3 S. 1 GeschGehG einschlägig sein.

In den §§ 15 ff. GeschGehG finden sich prozessuale Sonderregelungen für Geheimnisstreitsachen, die den allgemeinen Vorschriften der ZPO und des GVG vorgehen.[117] Nach der Legaldefinition des § 16 Abs. 1 GeschGehG liegt eine Geheimnisstreitsache bei Klagen vor, durch die Ansprüche nach dem GeschGehG geltend gemacht werden.[118] Hilft das Gericht dem Antrag ab, wird während des Gerichtsverfahrens lediglich einer begrenzten Anzahl an Personen Zugang zum Gerichtsaal gestattet und den Prozessbeteiligten untersagt, das Geschäftsgeheimnis außerhalb des Verfahrens zu nutzen oder

---

[116] BT-Drs. 19/4724, S. 27. Eine Offenlegung meint in diesem Kontext jede Eröffnung des Geschäftsgeheimnisses gegenüber einem Dritten, der zum Zeitpunkt der Offenlegung nicht bereits mit dem Willen des Geheimnisinhabers Kenntnis über die geheime Information hat bzw. haben durfte. Eine Nutzung beschreibt jede über das bloße Innehalten hinausgehende Verwendung eines Geschäftsgeheimnisses, soweit es sich dabei nicht um eine Offenlegung handelt.

[117] BT-Drs. 19/4724, S. 34; *Schulte*, ArbRB 2019, 143, 147. Das Gericht der Hauptsache kann auf Antrag einer Partei die streitgegenständlichen Informationen ganz oder teilweise als geheimhaltungsbedürftig einstufen, wenn diese ein Geschäftsgeheimnis sein können, § 16 Abs. 1 GeschGehG. Für den Antrag reicht es aus, dass glaubhaft gemacht wird, dass ein Geschäftsgeheimnis vorliegen könnte. Die Einstufungsentscheidung ergeht per Gerichtsbeschluss, vgl. BeckOK-GeschGehG/*Gregor,* § 16 Rn.1 ff. Insbesondere der zivilprozessuale Beibringungsgrundsatz birgt regelmäßig die Gefahr, ohne eine Offenlegung des jeweiligen Geheimnisses den Rechtsstreit zu verlieren. Der europäische Gesetzgeber hat den Gerichten in diesem Zusammenhang in Art. 9 GeschGeh-RL klare Handlungsmöglichkeiten mit an die Hand gegeben, die der nationale Gesetzgeber in §§ 16 ff. GeschGehG umgesetzt hat, vgl. *Ohly,* GRUR 2019, 441, 449, 450.

[118] *Reinfeld*, Das neue GeschGehG, § 6 Rn.13.

offenzulegen.[119] Daraus resultiert eine Geheimhaltungspflicht der beteiligten Personen während und nach Abschluss des Verfahrens, es sei denn, den beteiligten Personen ist das Geschäftsgeheimnis außerhalb des Verfahrens zur Kenntnis gelangt. Soweit die ordentliche Gerichtsbarkeit gegeben ist (§ 13 GVG), sind die Landgerichte ausschließlich zuständig, vgl. § 15 Abs. 1 GeschGehG.[120]

3. Ausgangspunkt: Das Vorliegen eines Geschäftsgeschäftsgeheimnisses

Die Definition des Geschäftsgeheimnisses beruht im Wesentlichen auf Art. 2 Nr. 1 der GeschGeh-RL, die sich an Art. 39 Abs. 2 TRIPS[121] orientiert und damit ihr Vorbild im Recht der Vereinigten Staaten von Amerika findet.[122] Die Definition des Unionsgesetzgebers ist viergeteilt: Es bedarf (1.) einer Information, die (2.) geheim und (3.) aufgrund ihres Geheimnischarakters von kommerziellem Wert ist und die (4.) Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist. Der deutsche Gesetzgeber hat diese Definition nicht eins zu eins übernommen.[123]

---

[119] Vgl. §§ 16 Abs. 2, 18 GeschGehG. In diesem Zusammenhang normiert § 17 GeschGehG eine eigenständige Sanktionsmöglichkeit für Verstöße gegen das Nutzungs- und Offenbarungsverbot. Sollte das Nutzungs- und Offenbarungsverbot der §§ 16 Abs. 2, 18 GeschGehG im Einzelfall nicht bestehen, sind weiterhin die Handlungsverbote des § 4 GeschGehG zu beachten.

[120] Die Arbeitsgerichtsbarkeit bleibt davon unberührt. Im Arbeitsgerichtsprozess greifen die Vorschriften der §§ 16 ff. GeschGehG, BT-Drs. 19/4724, S. 34; *Reinfeld*, Das neue GeschGehG, § 6 Rn.5.

[121] Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums; vgl. *Alexander*, WRP 2019, 673, 676; *Brost*/*Wolsing*, ZUM 2019, 898, 899; *Ohly*, GRUR 2019, 441, 442; *Schutz*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 157.

[122] BT-Drs. 19/4724, S. 24; *Ohly*, GRUR 2019, 441, 442; siehe auch: *Kalbfus*, GRUR-Prax, 2017, 391; *McGuire*, IPRB 2018, 202, 203.

[123] Anders als viele andere EU-Mitgliedstaaten, vgl. *Brost*/*Wolsing*, ZUM 2019, 898, 899; *Ohly*, GRUR 2019, 441, 442; *Schlack*, ZWeR 2019, 192, 199; *Apel*/*Walling*, DB 2019, 891, 893, 894; *Brammsen*, in: Brammsen/Apel GeschGehG, § 2 Rn.14, 16.

Nach der Definition des § 2 Nr. 1 GeschGehG bedarf es (1.) einer Information, die (2.) geheim und (3.) aufgrund ihres Geheimnischarakters von wirtschaftlichem Wert sowie (4.) Gegenstand angemessener Geheimhaltungsmaßnahmen ist und (5.) an der ein berechtigtes Interesse an der Geheimhaltung besteht.

Bemerkenswert ist, dass der Unionsgesetzgeber vom kommerziellen Wert der Information spricht, während der nationale Gesetzgeber einen wirtschaftlichen Wert verlangt. Außerdem wurden die beiden Voraussetzungen in Art. 2 Nr. 1 lit. a) und lit. b) GeschGeh-RL, die denen in Art. 39 Abs. 2 lit. a) und lit. b) TRIPS entsprechen, formal zu einer Voraussetzung zusammengezogen.[124] Der nationale Gesetzgeber hat die Definition des Geschäftsgeheimnisses außerdem um ein fünftes Element ergänzt, namentlich das des „*berechtigten Interesses an der Geheimhaltung*". Dies geschah auf Empfehlung des Rechtsausschusses des Deutschen Bundestags und führt zu Fragestellungen, denen sich die folgenden Abschnitte widmen.[125]

a) Geheime Information von wirtschaftlichem Wert

Gegenstand des Geheimnisses ist eine Information, über die eine Person oder ein Personenkreis exklusives Wissen hat.[126] Schutzobjekt sind einerseits Tatsachen, also Geschehnisse, Zustände oder Verhältnisse der Vergangenheit oder Gegenwart, die einem objektiven Beweis zugänglich sind.[127] Auch subjektive Ansichten, Meinungen und Wertungen können schutzfähige Informationen darstellen, wenn und

---

[124] *Harte-Bavendamm*, in: Harte-Bavendamm/Ohly/Kalbfus GeschGehG, § 2 Rn.3, 36; *Ohly*, GRUR 2019, 441.

[125] Dies steht dem Anliegen einer einheitlichen unionsweiten Begriffsdefinition entgegen, vgl. BT-Drs. 19/8300, S. 4, 13, 14; BT-Drs. 19/4724, S. 24; *Apel*/*Walling*, DB 2019, 891, 894.

[126] „*Geheim*" ist daher stets in einem relativen Sinne zu verstehen, vgl. *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Zweites Kapitel, S. 118 m. w. N.

[127] *Hiéramente,* in: BeckOK-GeschGehG*,* § 2 Rn.2; *Brammsen*, Lauterkeitsstrafrecht, § 17 UWG Rn.11.

soweit sie nach außen hin wahrnehmbar sind, beispielsweise durch Verschriftlichung oder mündliche Überlieferung.[128] Neben kaufmännischen und technischen Informationen kommen daher auch innere Tatsachen, wie z. B. ein bevorstehender Personalabbau, Verkaufsabsichten oder Investitionspläne oder Negativinformationen[129] (z. B. Produktionsprobleme) in Betracht.[130] Der Begriff der Informationen ist denkbar weit zu verstehen und unterliegt keinen qualitativen Maßgaben.[131]

aa) Unternehmensbezug

Darüber hinaus ist zu klären, ob es eines konkreten Bezugs der Information zum Geschäftsbetrieb bedarf. Ein solcher war unter der vormaligen Regelung in §§ 17 bis 19 UWG a. F. durch die Rechtsprechung herausgebildet worden. Der Wortlaut des § 2 Nr. 1 GeschGehG hilft insofern nicht weiter. Aus ihm geht nicht hervor, ob die Information für deren Schutzfähigkeit Unternehmensbezug aufweisen muss. Für ein solches Erfordernis spricht jedoch Erwägungsgrund 11 GeschGeh-RL, der „*geschäftsbezogene Informationen*“ erwähnt. Ähnlich stellt Erwägungsgrund 14 GeschGeh-RL auf „*Know-how, Geschäftsinformationen und technischen Informationen*“ ab. Auch nach dem Willen des Gesetzgebers soll das Kriterium des Unternehmensbezugs fortbestehen. In der Gesetzesbegründung zum GeschGehG heißt es, dass die nationale Definition im Wesentlichen der

---

[128] *Alexander*, in: Köher/Bornkamm/Feddersen, UWG, § 2 GeschGehG Rn.26; *Hiéramente,* in: BeckOK-GeschGehG*,* § 2 Rn.2; *Brammsen*, Lauterkeitsstrafrecht, § 17 UWG Rn.11.

[129] *Kalbfus*, GRUR 2016, 1009, 1011.

[130] BT-Drs. 19/4724, S. 24, 26; LAG Schleswig-Holstein, Beschluss v. 20.05.2015 - 3 TaBV 35/14, NZA-RR 2016, 77.

[131] Qualitative Anforderungen finden sich beispielsweise im Immaterialgüterrecht bzgl. der Eigenart (§ 2 Abs. 1, Abs. 3 DesignG) oder der Schöpfungshöhe (§ 2 Abs. 2 UrhG), der Neuheit (§§ 1, 3 Abs. 1 PatG, § 2 Abs. 1, Abs. 2 DesignG) oder erfinderischen Tätigkeit (§ 1 Abs. 1, Abs. 4 PatG), vgl. *Alexander*, WRP 2017, 1034, 1037; *Wunner*, WRP 2019, 710, 711.

bisherigen Definition, also der unter §§ 17 bis 19 UWG a. F. zu Betriebs- und Geschäftsgeheimnissen herausgebildeten Definition, entsprechen soll.[132] Zweck sei die Abgrenzung zu rein privaten Geheimnissen, die im geschäftlichen Verkehr nicht verwertbar seien. Nach dem Willen des Gesetzgebers soll sich das Erfordernis des Unternehmensbezugs aus einer Zusammenschau von Art. 2 Nr. 1 lit. c), Nr. 2 GeschGeh-RL und § 2 Nr. 1 lit. b) Nr. 2 GeschGehG ergeben.

Diese Sichtweise überzeugt. Aus der Inhaberschaft eines Geschäftsgeheimnisses, das die rechtmäßige Kontrolle über die Information voraussetzt, ergibt sich eine Zuordnung zu einem bestimmten Unternehmen. Im Ergebnis besteht das Erfordernis eines Unternehmensbezugs der Information daher weiter.[133] Welche Anforderungen damit an eine Information gestellt werden, ergibt sich aus der vormaligen Rechtsprechung zu §§ 17 bis 19 UWG a. F.: Notwendig ist, dass die Information der Sphäre eines bestimmten Unternehmens unmittelbar zuordbar ist, respektive in einem eindeutigen Zusammenhang zu diesem steht, weil sie für den Geheimnisinhaber marktrelevant ist.[134] Keinen Unternehmensbezug haben z. B. geheime Informationen öffentlicher Einrichtungen und Stellen sowie nicht unternehmerisch tätige Interessenverbände oder gemeinnützige Stiftungen.[135]

Zu beachten ist, dass auch Privatgeheimnisse Unternehmensbezug aufweisen können.[136] Zwar nennt Erwägungsgrund 14 der GeschGeh-RL lediglich Know-how, Geschäftsinformationen und technische Informationen. Diese Aufzählung ist jedoch als Mindestmaß der zu schützenden Informationen zu verstehen und nicht abschließend.[137]

---

132 BT-Drs. 19/4724, S. 24. Siehe auch: Kapitel B) II.1.

133 A. A.: *Hoeren*, in: Hoeren/Münker GeschGehG, § 2 Rn.7, 8.

134 *Kalbfus*, Know-how-Schutz, S. 73-74; vgl. OLG Hamm, WRP 1993, 118, 119.

135 *Alexander*, in: Köhler/Bornkamm/Feddersen UWG, § 2 GeschGehG Rn.85; *Alexander*, WRP 2017, 1034, 1038.

136 *Reinfeld*, in: Hdb-ArbR, § 30 Rn.5, 16 ff.

137 BT-Drs. 19/4724, S. 24; explizit: Know-how, Geschäftsinformationen und technologische Informationen, vgl. *Alexander*, AfP 2019, 1, 5.

Der Wortlaut des § 2 Nr. 1 GeschGehG steht einer weiten Interpretation nicht im Wege. Zudem deutet der Verweis des § 1 Abs. 3 Nr. 1 GeschGehG auf § 203 StGB darauf hin, dass Privatgeheimnisse dem GeschGehG unterfallen. Auch Informationen aus dem privaten Bereich können folgerichtig Geschäftsgeheimnisse sein und dem Schutzregime des GeschGehG unterfallen. Voraussetzung bleibt, dass ein Unternehmensbezug besteht, um eine Abgrenzung zu rein privaten Informationen zu erzielen. Weist eine Information neben dem Unternehmensbezug einen Bezug zu privaten Lebenssphären, steht dies ihrer Schutzfähigkeit demgemäß nicht entgegen.[138] Maßgeblich sind die Umstände des jeweiligen Einzelfalls, wobei die wachsende Vermarktung des Privat- und Geschäftslebens eine trennscharfe Abgrenzung zunehmend erschwert.[139] Ein Unternehmensbezug einer privaten Information kann z. B. bei schwerer Krankheit einer Führungsgröße bestehen.[140] Informationen über den kritischen Gesundheitszustand der obersten Hierarchieebene wirken sich auf die Wettbewerbsposition börsennotierter Unternehmen aus.[141]

bb) Geheimnischarakter

Nach § 2 Nr. 1 lit. a) GeschGehG darf die Information weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile bekannt sein. Der nationale Gesetzgeber hat die Vorgaben der GeschGeh-RL nahezu wortgleich übernommen. Allerdings formulieren GeschGehG-RL und GeschGehG enger als die übrigen Sprachfassungen anderer Mitgliedstaaten. Während Art. 2 Nr. 1 lit. a) GeschGeh-RL von einem Kumulativverhältnis der Voraussetzungen ausgeht („*weder […] noch*“), verlangen die Sprachfassungen anderer

---

[138] *Alexander*, in: Köhler/Bornkamm/Feddersen UWG, § 2 GeschGehG Rn.84; *Ohly*, GRUR 2019, 441, 442.

[139] *Hoppe*/*Oldenkop*, Geschäftsgeheimnisse, Rn.64; *Ohly*, GRUR 2019, 441, 442.

[140] *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Zweites Kapitel, S. 127.

[141] *Alexander*, AfP 2019, 1, 5.

Mitgliedstaaten lediglich deren alternatives Vorliegen („*entweder […] oder*“).[142] Bedeutung erlangt dieser Umstand insbesondere mit Blick auf Datensammlungen, deren Inhalte jeweils einzeln öffentlich zugänglich sind, z. B. im Fall von Kundenlisten.[143] Diese wären - ginge es nach der deutschen Sprachfassung - konsequenterweise nicht schutzfähig. Die deutsche Sprachfassung ist damit restriktiver als die der anderen europäischen Länder. Fraglich ist, wie damit umzugehen ist. Zu beachten ist, dass grundsätzlich alle Sprachfassungen einer Richtlinie gleichrangig nebeneinanderstehen und damit in der gleichen Weise Verbindlichkeit erlangen.[144] Dennoch verbietet es sich laut EuGH, eine Vorschrift des Unionsrechts isoliert, also ausschließlich in einer ihrer Sprachfassungen zu betrachten.[145] Weichen die verschiedenen Sprachfassungen voneinander ab, sei die Vorschrift nach dem wirklichen Willen ihres Urhebers und dem von diesem verfolgten Zweck der Regelung auszulegen.[146] Der Unionsgesetzgeber hat mit Inkrafttreten der GeschGeh-RL die unionsweite Harmonisierung des Geschäftsgeheimnisbegriffs nach dem Vorbild der Regelung in Art. 39 Abs. 2 TRIPS bezweckt, die wie die übrigen Sprachfassungen der Richtlinie von einem Alternativverhältnis ausgeht. Das Kumulativerfordernis der deutschen Sprachfassung steht diesem Harmonisierungsgedanken als einzige entgegen. Es ist daher überzeugend die nationale Formulierung im Lichte des Art. 39 Abs. 2 TRIPS als Alternativverhältnis zu begreifen.[147] Dies entspricht dem Willen des Unionsgesetzgebers und seinen Bestrebungen eines einheitlichen europaweiten Begriffsverständnisses. Folgerichtig ist § 2 Nr. 1 lit. a) GeschGehG im Sinne eines „*weder […] noch*“-Verhältnisses zu verstehen. Besteht eine Information also aus mehreren Bestandteilen, ist

---

142 Ausführlich: *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Zweites Kapitel, S. 130.

143 Stellungnahme Max-Planck-Institut, RefE-GeschGehG v. 17.04.2018.

144 *Alexander*, WRP 2017, 1034, 1037 m. w. N.

145 EuGH, Urteil v. 03.06.2010 - C-569/08, Rn.35; EuGH, Urteil v. 03.04.2014 - C-515/12 Rn.19.

146 EuGH, Urteil v. 19.12.2013 - C-281/12, Rn.26.

147 Dieses Verständnis bezieht sich auf Art. 2 Nr. 1 lit. a) GeschGeh-RL und Art. 2 Nr. 1 lit. a) GeschGehG.

sie auch dann geheim, wenn ihre Einzelteile öffentlich zugänglich sind. In diesen Fällen kommt es dann auf den Geheimnischarakter der konkreten Anordnung bzw. Zusammensetzung der Daten an.[148] Im Ergebnis ist also auch die Kundenliste schutzfähiges Objekt im Sinne des GeschGehG. Gleichwohl bleibt der nationale Gesetzgeber aufgefordert, die missverständliche Regelung einer klarstellenden Korrektur zuzuführen.

Eine Information ist geheim, wenn sie ausschließlich dem Geheimnisinhaber bzw. zur Vertraulichkeit verpflichteten Dritten bekannt ist, wobei die Größe dieses Personenkreises unbeachtlich ist.[149] Ist die Information nur gegenüber einem Fachpublikum allgemein bekannt bzw. nicht ohne Weiteres zugänglich, ist sie ebenfalls geheim.[150] Allerdings wird mit jeder Erweiterung der Personengruppe anhand aller maßgebenden Einzelumstände zu prüfen sein, ob die Information weiterhin als geheim einzustufen ist.[151] Maßgeblich ist, ob der Geheimnisinhaber den „*Kreis der Mitwisser*" noch überblicken bzw. nachvollziehen kann.[152] Bereits unter § 17 UWG a. F. war anerkannt, dass eine Information jedenfalls dann nicht mehr geheim ist, wenn sie entweder allgemein bekannt oder derart zugänglich ist, dass unter Zuhilfenahme lauterer Mittel und ohne nennenswerten Aufwand eine

---

148 *Hiéramente,* in: BeckOK-GeschGehG, § 2 Rn.8.

149 BGH, Urteil v. 22.03.2018 - I ZR 118/16, GRUR 2018, 1161.

150 *Hiéramente,* in: BeckOK-GeschGehG, § 2 Rn.7 ff. 576.

151 In diesem Zusammenhang ist auch an die öffentliche Transparenz von Unternehmensdaten zu denken. Das Reichsgericht zählte im Jahr 1897 die Bilanz eines Kaufmanns zu dessen „Betriebs- und Geschäftsgeheimnissen". Mittlerweile wurde das Bilanz- und Kapitalmarktrecht allerdings europarechtlich harmonisiert und sieht die Offenlegung finanzieller Daten von Kapital- und Personengesellschaften vor. Der Geheimnischarakter dieser Informationen dürfte damit verloren gegangen sein.

152 Stellvertretend für viele: *Apel*/*Nickl*, K&R 2022, 385, 387; *Harte-Bavendamm*, in: Harte-Bavendamm/Ohly/Kalbfus GeschGehG, § 2 Rn.26; *Schutz*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 162. Weitere Nachweise bei *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Zweites Kapitel, S. 133, Fn.569.

tatsächliche Möglichkeit zur Kenntniserlangung besteht.[153] Dieser Grundgedanke ist auf das GeschGehG zu übertragen.[154]

Eine Information verliert ihren Geheimnischarakter nicht dadurch, dass sie in Erfüllung einer Anzeigepflicht offengelegt wird.[155] Dies gilt insbesondere dann, wenn die Offenlegung gegenüber einer Person erfolgt, die ihrerseits zur Vertraulichkeit verpflichtet ist.[156] Dies ergibt sich einerseits aus § 4 Abs. 2 Nr. 2, Nr. 3 GeschGehG, der davon ausgeht, dass auch andere Personen Kenntnis sowie Nutzungsrechte an der Information haben können.[157] Auch § 3 Abs. 2 GeschGehG spricht für diese Lesart, wonach die erlaubte Nutzung oder Offenlegung eines Geschäftsgeheimnisses den Verbotstatbestand entfallen lässt, nicht jedoch den Geheimnischarakter der Information. Offenbart der Arbeitgeber beispielsweise gegenüber dem Betriebsrat in Erfüllung seiner Unterrichtungspflicht Geschäftsgeheimnisse (§ 80 Abs. 2 BetrVG), bleibt der Geheimnischarakter der Information bestehen, da die Betriebsratsmitglieder ihrerseits zur Geheimhaltung verpflichtet sind (§ 79 Abs. 1 BetrVG).[158] Auch aus dem Arbeitsvertrag kann sich eine Anzeigepflicht des Arbeitgebers aus seiner Fürsorgeverantwortung gegenüber dem Arbeitnehmer ergeben. So kann der Arbeitgeber unter Umständen im Einzelfall dazu verpflichtet sein, auf eine problematische wirtschaftliche Situation des Unternehmens

---

153 BGH, GRUR 1958, 297, 299.

154 So auch *Brammsen*, in: Brammsen/Apel, GeschGehG § 2 Rn.26; *Hoppe*/*Oldenkop*, Geschäftsgeheimnisse, Rn.82, 88; OLG Stuttgart, WRP 2021, 242, 256.

155 Weitere Meldepflichten des Arbeitgebers bestehen beispielsweise nach § 28 a SGB IV i. V. m. DEÜV, §§ 312, 313 SGB II, § 320 Abs. 1 und Abs. 3 SGB III, §§ 198 ff. SGB V.

156 OLG Karlsruhe, Beschluss v. 13.10.2022 - 6 W 39/22, Rn.30, GRUR-Prax 2022, 665.

157 Ebenso: *Hiéramente*, in: BeckOK-GeschGehG, § 2 Rn.10.

158 Zum Geschäftsgeheimnisschutz im Rahmen der Betriebsratsarbeit, siehe: Kapitel C) III.

hinzuweisen.[159] Dies betrifft auch die Anbahnungsphase, wenn ein Arbeitnehmer in zulässiger Weise von einem Konkurrenzunternehmen abgeworben werden soll und die tatsächliche Beschäftigung aufgrund eines geplanten Stellenabbaus nicht sicher scheint.[160] In diesen Fällen ist die Geheimhaltung des Bewerbers über vertragliche Vertraulichkeitsvereinbarungen abzusichern. Sobald die Medien allerdings Kenntnis von der Information haben und diese verbreiten, ist davon auszugehen, dass diese ihres Geheimnischarakters verlustig gegangen ist.

cc) Wirtschaftlicher Wert infolge der Geheimhaltung

§ 2 Nr. 1 lit. a) GeschGehG setzt voraus, dass die Information geheim ist und aus diesem Umstand ein wirtschaftlicher Wert resultiert. Im Vergleich zur GeschGeh-RL fällt auf, dass der deutsche Gesetzgeber die beiden Voraussetzungen in Art. 2 Nr. 1 lit. a) und lit. b) GeschGeh-RL formal zu einer Voraussetzung zusammengezogen hat.[161] Darüber hinaus weicht der nationale Gesetzgeber sprachlich von der Definition der GeschGeh-RL ab. Während die GeschGeh-RL einen „*kommerziellen Wert*“ der Information verlangt, fordert das GeschGehG einen „*wirtschaftlichen Wert*“. Dies führt zu der Frage, ob damit eine inhaltliche Abweichung von der GeschGeh-RL einhergeht.[162] Anhaltspunkte für ein von der GeschGeh-RL abweichendes Begriffsverständnis des wirtschaftlichen Werts liegen nicht vor. Stattdessen deutet die Gesetzesbegründung mit ihrem Verweis auf Erwägungsgrund 14 GeschGeh-RL in die entgegengesetzte Richtung.[163] Es ist davon auszugehen, dass „*kommerzieller Wert*“ und „*wirt-*

---

159 *Reinfeld*, in: Hdb-ArbR, § 34 Rn.117. Ebenso dürfte eine Hinweispflicht auf akute Zahlungsschwierigkeiten zu Beginn des Arbeitsverhältnisses in Betracht kommen, vgl. BAG, Urteil v. 14.07.2005 - 8 AZR 300/04, NZA 2005, 1298.

160 Vgl. *Reinfeld*, in: Hdb-ArbR, § 34 Rn.117.

161 Ebenso: *Harte-Bavendamm*, in: Harte-Bavendamm/Ohly/Kalbfus GeschGehG, § 2 Rn.3, 36; *Ohly*, GRUR 2019, 441, 442.

162 *Thüsing/Rombey*, ZD 2020, 221, 222.

163 BT-Drs. 19/4724, S. 24.

schaftlicher Wert“ gleichbedeutend sind.[164] Hintergrund der abweichenden Formulierung könnte sein, dass die Formulierung „*wirtschaftlicher Wert*“ im deutschen Sprachgebrauch geläufiger ist und der Gesetzgeber sich deshalb für diese Abweichung entscheiden hat, ohne dass damit eine inhaltliche Abweichung vom Begriffsverständnis der GeschGeh-RL einhergehen sollte.[165]

Sowohl § 2 Nr. 1 lit. a) GeschGehG als auch Art. 2 Nr. 1 lit. b) GeschGeh-RL verlangen, dass der wirtschaftliche bzw. kommerzielle Wert der Information aus ihrer Unbekanntheit resultieren muss. Hinsichtlich der Kausalverbindung ist zu fragen, ob damit nur solche Informationen gemeint sind, die erst durch ihre Geheimhaltung einen Wert erlangen.[166] Dies hätte zur Folge, dass Informationen, denen unabhängig von ihrer Geheimhaltung ein wirtschaftlicher bzw. kommerzieller Wert anhaftet, nicht schutzfähig wären. Ein Blick auf die Rechtsprechungshistorie streitet gegen diese einschränkende Lesart. Bereits unter §§ 17 bis 19 UWG a. F. waren Informationen wie Kundenlisten, Rezepturen, Planungsunterlagen oder technisches Know-how als Geschäftsgeheimnisse anerkannt.[167] Diesen Informationen wohnt bereits in aller Regel ein wirtschaftlicher Wert inne, ohne dass es für deren Werthaltigkeit auf eine zusätzliche Geheimhaltung ankommt. Es liegen keine Anhaltspunkte dafür vor, dass der (Unions-) Gesetzgeber diesen Informationen mit Inkrafttreten der GeschGeh-RL bzw. des GeschGehG ihre Schutzfähigkeit als Geschäftsgeheimnis entziehen wollte.

---

[164] Ebenso: *Alexander*, AfP 2019, 1, 4; a. A.: DGB-Stellungnahme zum Regierungs-E GeschGehG v. 18.05.2018, S. 6; *Hauck*, AfP 2021, 193, 197; vgl. auch: *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 170-172.

[165] So auch: *Trebeck/Schulte-Wissermann,* NZA 2018, 1175, 1176, 1177.

[166] Bejahend: *Dann*/*Markgraf*, NJW 2019, 1774, 1775; *Hauck*, WRP 2018, 1032, 1033.

[167] Dazu auch: *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Zweites Kapitel, S. 137.

Mithin würde ein derart enges Verständnis Sinn und Zweck der Regelungen zuwiderlaufen, die auf eine Stärkung des Schutzes von Unternehmensgeheimnissen abzielen. Einer solchen Stärkung widerspräche es, würden einzelne Informationen, die unter der vormaligen Rechtslage schutzfähig waren, nun unter der neuen Rechtslage ihre Schutzfähigkeit verlieren. Die Kausalverbindung zwischen Geheimhaltung und Wertigkeit einer Information ist daher weit auszulegen. Ausreichend ist folgerichtig, dass eine Information durch die Geheimhaltung einen (potenziellen) Wertzuwachs erfährt, die Geheimhaltung für den wirtschaftlichen bzw. kommerziellen Wert also zumindest auch von Bedeutung ist.[168] Ein bloß ideelles Schutzinteresse an der Information genügt dagegen nicht.[169]

Darüber hinaus stellt sich die Frage, ob ein wirtschaftlicher bzw. kommerzieller Wert an sogenannten „*rechtswidrigen Informationen*" bestehen kann.[170] Gemeint sind Informationen illegalen Ursprungs oder Inhalts.[171] Ihrer Schutzfähigkeit wird in den folgenden Abschnitten anhand der bekannten Auslegungsmethoden nachgegangen.

(1) Problemaufriss: Der wirtschaftliche Wert als Ausschlusskriterium für rechtswidrige Informationen?

Die Schutzfähigkeit rechtswidriger Informationen war schon unter der vorherigen Rechtslage unter §§ 17 bis 19 UWG a. F. ein vieldiskutiertes Thema, das im Rahmen der GeschGeh-RL und dem GeschGehG nun insbesondere unter dem Aspekt eines möglicherweise fehlenden

---

168 So auch: *Alexander*, WRP 2017, 1034, 1039; *Hiéramente,* in: BeckOK-GeschGehG*,* § 2 Rn.1 m. w. N.

169 *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Zweites Kapitel, S. 136.

170 *Schreiber*, NZWiSt 2019, 332, 333; *Schröder*, ZRP 2020, 212, 214; *Aldoney Ramírez*, Schutz von Geschäfts- und Betriebsgeheimnissen, S. 344-345.

171 Z. B.: Kartellabsprachen, Kartellverstöße, Steuerstraftaten.

wirtschaftlichen bzw. kommerziellen Werts fortbesteht.[172] Stimmen in der Literatur führen das Erfordernis eines wirtschaftlichen Werts als Ausschlusskriterium für rechtswidrige Tatsachen an, weil ihnen kein eigenständiger „*positiver Vermögenswert*" zukäme.[173] Gestützt werden diese restriktiven Ansätze durch Erwägungsgrund 14 GeschGeh-RL, der Informationen einen realen oder potenziellen Handlungswert abverlangt.[174] Vor diesem Hintergrund differenzieren Teile des Schrifttums auch danach, ob der Wettbewerbsvorteil ausschließlich auf die Geheimhaltung eines Rechtsverstoßes zurückzuführen sei oder die Information zugleich ein werthaltiges „*Know-How*" enthalte.[175] Nur letztere seien nach dieser Auffassung schutzwürdig, da Unternehmen aus illegalen Tatsachen keine Wettbewerbsvorteile erwachsen dürften.

(2) Eine Betrachtung des Wortlauts in unionsrechtskonformer Auslegung

Der Wortlaut bezieht keine Stellung zu der Frage, ob rechtswidrige Informationen Geschäftsgeheimnisse im Sinne des § 2 Nr. 1

---

[172] Die Diskussion wird auch am Erfordernis des berechtigten Geheimhaltungsinteresses festgemacht. Siehe: Kapitel B), II, 3. b).

[173] *Alexander*, WRP 2017, 1034, 1039; *Hauck*, WRP 2018, 1032, 1033, 1036; *Kalbfus*, GRUR 2016, 1009, 1011; *Schmitt*, RdA 2017, 365, 369; offenlassend: *Brockhaus*, ZIS 2020, 102, 109, 110; *Hauck*, AfP 2021, 193, 197, 199; *Granetzny*/*Krause*, CCZ 2020, 29, 33; *Harte-Bavendamm*, in: Harte-Bavendamm/Ohly/Kalbfus Gesch-GehG, § 2 Rn.39; *Hoppe*/*Oldekop*, Geschäftsgeheimnisse, Rn.101; *Schuth,* Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 192-195, der die Schutzfähigkeit am berechtigten Interesse scheitern lässt. Vereinzelt wird differenziert, ob rechtswidrige Informationen produktives Know-how darstellen (wie z. B. im Dieselskandal die fehlerhafte Software), vgl. *Schreiber*, NZWiSt 2019, 332, 335; *Goldhammer*, NVwZ 2017, 1809, 1812.

[174] *Goldhammer*, NVwZ 2017, 1809, 1812; *Hauck*, WRP 2018, 1032, 1034; *Kalbfus*, GRUR 2016, 1009, 1011; *Schreiber*, NZWiSt 2019, 332, 335; grundsätzlich enges Begriffsverständnis: *Schuth,* Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 166-169.

[175] *Schreiber*, NZWiSt 2019, 332, 335; *Goldhammer*, NVwZ 2017, 1809, 1812.

GeschGehG sein können. Auch die Definition des Unionsgesetzgebers in Art. 2 Nr. 1 GeschGeh-RL äußert sich nicht. Wie im Abschnitt zuvor aufgezeigt, verlangt die Definition des wirtschaftlichen bzw. kommerziellen Werts eine Information, die durch die Geheimhaltung einen (potenziellen) Wertzuwachs erfährt, wobei es dem Wortlaut nach ohne Bedeutung ist, ob diese Information rechtswidrigen Inhalts oder Ursprungs ist. Maßgeblich ist, ob rechtswidrige Informationen infolge der Geheimhaltung einen (potenziellen) Wertzuwachs erfahren können.

Als Argument gegen die Schutzfähigkeit rechtswidriger Informationen wird Erwägungsgrund 14 GeschGeh-RL ins Feld geführt.[176] Dabei wird jedoch verkannt, dass die GeschGeh-RL die Werthaltigkeit einer Information weit versteht. So soll der kommerzielle Wert explizit auch daran festgemacht werden können, ob eine Offenlegung der Information den Interessen des Inhabers Schaden zufügen kann, weil dessen „*geschäftlichen oder finanziellen Interessen, die strategische Position oder die Wettbewerbsfähigkeit (…) untergraben werden.*“[177] Auch der Zweck der GeschGeh-RL spricht gegen einen Ausschluss rechtswidriger Informationen. Zweck der GeschGeh-RL ist zuvörderst, Unternehmen in ihrer Tätigkeit und vermögenswerten Positionen zu schützen, um einen funktionierenden Wettbewerb zu gewährleisten und Innovation zu steigern.[178] Daneben enthält die Richtlinie auch Vorgaben zum Schutz des investigativen Journalismus und für

---

[176] Erwägungsgründe bringen allerdings nur eine allgemeine Zielrichtung zum Ausdruck, vgl. *Steinmann*, WRP 2019, 703, 709 m. w. N.
Dennoch darauf beziehend: *Goldhammer*, NVwZ 2017, 1809, 1812; *Hauck*, WRP 2018, 1032, 1034; *Kalbfus*, GRUR 2016, 1009, 1011; *Schreiber*, NZWiSt 2019, 332, 335; grdstzl. enges Begriffsverständnis: *Schuth,* Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 166-169.

[177] LAG Baden-Württemberg, Urteil v. 18.08.2021 - 4 SaGa 1/21 Rn.30; *Hiéramente*, Stellungnahme zum Regierungs-E GeschGehG als Sachverständiger, abgedruckt im Wortprotokoll Nr. 19/30, S. 73-101; *Ohly*, GRUR 2019, 441, 443; vgl. auch *Rody*, Geschäfts- und Betriebsgeheimnisse, S. 128, 129.

[178] Erwägungsgrund 3 GeschGeh-RL.

Hinweisgeber in Art. 5 GeschGeh-RL. Diese Vorgabe ist als Ausnahmevorschrift konzipiert und sieht grundsätzlich eine obligatorische Interessenabwägung vor, um Einzelfallgerechtigkeit zu erreichen.[179] Um dem primären Zweck der GeschGeh-RL zu entsprechen, sind rechtswidrige Informationen daher erst im Rahmen des Art. 5 GeschGeh-RL zu berücksichtigen, der eine Korrektur im Einzelfall ermöglicht und überzeugender Garant für sachgerechte Ergebnisse ist.[180] Dies ergibt sich dementsprechend auch aus systematischen Überlegungen. Art. 5 GeschGeh-RL wäre nahezu ohne eigenen Anwendungsbereich, würde es rechtswidrigen Informationen bereits auf Definitionsebene an der Schutzfähigkeit fehlen.

Für den Schutz rechtswidriger Informationen durch die GeschGeh-RL spricht außerdem das Ineinandergreifen von GeschGeh-RL und Whistleblowing-RL. Nach Art 3 Abs. 2 GeschGeh-RL gilt „*der Erwerb, die Nutzung oder die Offenlegung eines Geschäftsgeheimnisses (…) insofern als rechtmäßig, als der Erwerb, die Nutzung oder die Offenlegung durch Unionsrecht oder nationales vorgeschrieben oder erlaubt ist.*“ Ergänzend heißt es in Erwägungsgrund 98 Whistleblowing-RL: „*Personen, die Geschäftsgeheimnisse in einem beruflichen Kontext erlangt haben, sollten nur dann den durch diese Richtlinie gewährten Schutz - auch vor zivilrechtlicher Haftung - genießen, wenn sie die in dieser Richtlinie festgelegten Bedingungen erfüllen, wozu auch gehört, dass die Offenlegung notwendig war, um einen Verstoß, der in den sachlichen Anwendungsbereich dieser Richtlinie fällt, aufzudecken. Sind diese Bedingungen erfüllt, so ist die Offenlegung von Geschäftsgeheimnissen als nach dem Unionsrecht erlaubt*

---

[179] Sofern ein benannter Fall vorliegt, führt die obligatorische Interessenabwägung zur obligatorischen Berücksichtigung des Verhältnismäßigkeitsgrundsatzes anhand des jeweiligen unbestimmten Rechtsbegriffs, etwa im Rahmen des § 5 Nr. 2 GeschGehG anhand des „*öffentlichen Interesses*“. Eine gesonderte Interessenabwägung anhand des Begriffs des „*berechtigten Interesses*“ erfolgt dann nicht. Siehe: Kapitel C) I. 1. cc).

[180] Erwägungsgrund 21 GeschGeh-RL, Art. 11 Abs. 2 GeschGeh-RL und § 9 GeschGehG.

im Sinne von Artikel 3 Absatz 2 der Richtlinie (EU) 2016/943 zu betrachten."

Die Offenlegung von Geschäftsgeheimnissen ist demnach erlaubt, sofern die Voraussetzungen der Whistleblowing-RL erfüllt sind. Hinweisgeber legen in aller Regel Informationen rechtswidrigen Inhalts offen. Wären diese nicht schutzfähig im Sinne des Art. 2 Nr. 1 GeschGehG würde Art. 3 Abs. 2 GeschGeh-RL gar nicht erst zur Anwendung kommen, was wiederum dem Verhältnis von GeschGeh-RL und Whistleblowing-RL widerspräche.

Die Einordnung des Whistleblowings als erlaubte Handlung ist daher als Bekenntnis zur Schutzfähigkeit rechtswidriger Informationen zu verstehen.[181] Im Rahmen der GeschGeh-RL hat sich folgerichtig der Wille des Unionsgesetzgebers niedergeschlagen, dass rechtswidrige Geheimnisse vom Schutzbereich erfasst sind. Die GeschGeh-RL schützt alle Informationen, die für den Inhaber von wirtschaftlichem oder strategischem Interesse sind. Dies entspricht dem soeben herausgebildeten Verständnis des kommerziellen Werts und bedarf keiner einschränkenden Korrektur. Die unionsrechtskonforme Auslegung des wirtschaftlichen Werts im Sinne des § 2 Nr. 1 GeschGehG führt zu der Annahme einer Wertigkeit rechtswidriger Informationen, da Unternehmen im Falle ihres Bekanntwerdens immense Wertverluste durch Reputationsschäden und Schadensersatzforderungen drohen.[182]

(3) Eine Betrachtung der Systematik

Das systematische Zusammenspiel der Definition mit den Ausnahmetatbeständen in § 5 GeschGehG bzw. Art. 5 GeschGeh-RL legt die Schutzfähigkeit rechtswidriger Informationen nahe, da andernfalls die

---

[181] *Schröder*, ZRP 2020, 212, 214.

[182] So auch: *Hauck*, der aber letztlich doch zum Ausschluss rechtswidriger Informationen gelangt, vgl. *Hauck*, GRUR-Prax 2019, 223, 224.

Ausnahmetatbestände regelmäßig leerliefen.[183] Dies streitet für die Annahme, dass rechtswidrige Informationen einen wirtschaftlichen bzw. kommerziellen Wert aufweisen und rechtswidrige Informationen im Rahmen der Tatbestandsausnahme in § 5 GeschGehG Berücksichtigung finden.[184]

(4) Eine Betrachtung der Historie

Genau wie das GeschGehG heute, enthielt auch § 17 UWG a. F. keine ausdrückliche Regelung, die sich zu dieser Problematik verhält. Das Schrifttum verortete die Diskussion um die Schutzfähigkeit rechtswidriger Informationen bei dem Erfordernis des „*berechtigten Interesses*".[185] Dieses Kriterium hatte sich durch die Rechtsprechung herausgebildet und war nach objektivem Maßstab anhand der Wertigkeit der Information zu beurteilen.[186] Auf die Art sollte sichergestellt sein, dass nicht völlig belanglose Informationen von § 17 UWG a. F. geschützt sind.[187] Das Erfordernis des berechtigten Interesses integrierte insofern eine Art Bagatellgrenze, um eine objektive Überprüfung des Geheimhaltungswillens zu erreichen.[188] Weitere Einzelheiten zur Reichweite des Geheimhaltungswillens waren jedoch umstritten, so auch die Schutzfähigkeit rechtswidriger Informationen.

Einige Autoren lehnten die Schutzfähigkeit rechtswidriger Informationen kategorisch ab, sog. „*Tatbestandslösung*" zu §§ 17 bis 19 UWG

---

183 *Hoppe*/*Oldenkop*, Geschäftsgeheimnisse, Rn.101; vorsichtiger: *Hiéramente*, in: BeckOK-GeschGehG, § 2 Rn.78.4; a. A.: *Hauck*, GRUR-Prax 2019, 223, 225.

184 Ausführlich dazu auch *Dobler,* Geschäftsgeheimnisschutz und investigativer Journalismus, Zweites Kapitel, S. 168 ff.

185 BGH, GRUR 1955, 424, 425, 426; GRUR 1961, 40, 43; GRUR 2003, 356, 358; GRUR 2006, 1044, 1046; BAGE 41, 21, 29, 30; *Brammsen*, Lauterkeitsstrafrecht, § 17 UWG Rn.19.

186 *Wolters*, in: GK-UWG, § 17 Rn.27; *Schuth,* Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 182-186.

187 *Harte-Bavendamm*, in: Harte-Bavendamm/Henning-Bodewig UWG, § 17 Rn.6.

188 *Hiéramente*, in: BeckOK-GeschGehG, § 2 Rn.71.

a. F.[189] Berechtigte Interessen seien nur solche, die von der Rechtsordnung positiv anerkannt würden und dürften dieser nicht zuwiderlaufen.[190] Ein Rechts- oder Sittenverstoß sei deshalb ohne Geheimhaltungswert.[191] Andere Stimmen sprachen sich wiederum für die Schutzfähigkeit rechtswidriger Informationen aus, wobei nachgelagert eine Interessenabwägung stattzufinden habe, sog. *Rechtfertigungslösung*" zu §§ 17 bis 19 UWG a. F.[192] Darüber hinaus existierten auch differenziertere Lösungswege.[193]

---

189 Dazu zählen: *Aldoney Ramírez*, Schutz von Geschäfts- und Betriebsgeheimnissen, S. 346-351, 367, 368, um Hürden für Whistleblower abzuschaffen; *Alexander*, AfP 2019, 1, 4, 5; *Alexander*, in: Köhler/Bornkamm/Feddersen UWG, § 2 GeschGehG Rn.78-82; *Brockhaus*, ZIS 2020, 102, 108; Stellungnahme des DGB zum Regierungs-E GeschGehG v. 18.05.2018, S. 6-8, 16, 21, abgedruckt im Wortprotokoll Nr. 19/30, S. 47-65; *Hauck*, WRP 2018, 1032, 1034, 1035; *Kreis*, Whistleblowing, S. 59-63; *Schmitt*, RdA 2017, 365, 369; *Rützel*, GRUR 1995, 557, 561; *Schnabel*, CR 2016, 342, 344-348; *Schmitt*, NZA-Beilage 2020, 50, 52, 53; *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 88-91; zurückhaltend: *Apel*/*Walling*, DB 2019, 891, 894; eher ablehnend, sich aber nicht festlegend: *Preis*, in: ErfK-ArbR, § 611a BGB Rn.814, 815.

190 *Brockhaus*, ZIS 2020, 102, 104; *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 89, 90.

191 Vgl. *Engländer*/*Zimmermann*, NZWiSt 2012, 328, 332, 333; *Rützel*, GRUR 1995, 557, 558-560.

192 *Apel*/*Walling*, DB 2019, 891, 894 befürworten zwar eine Lösung über die Interessenabwägung, vermuten aber dennoch den Ausschluss unter § 2 Nr. 1 lit. c) GeschGehG; vgl. auch *Azar*, JuS 2017, 930, 933; *Brammsen*, Lauterkeitsstrafrecht, § 17 UWG Rn.24; *Garden*/*Hiéramente*, BB 2019, 963, 967; *Gärtner*/*Oppermann*, BB 2019, Heft 35, Umschlagteil, I (Die Erste Seite); *Kalbfus*, Know-how-Schutz, S. 79-81; *Ohly*, in: Ohly/Sosnitza UWG, § 17 Rn.12; *Rengier*, in: Fezer/Büscher/Obergfell UWG, § 17 Rn.21; *Rody*, Geschäfts- und Betriebsgeheimnisse, S. 116-119; differenzierter: *Sixt*, Whistleblowing im Spannungsfeld, S. 85-90; *Westermann*, Hdb. Know-How-Schutz, S. 22; offenlassend: *Redder*, Schutz von Whistleblowern, S. 127; nicht eindeutig: LG Stuttgart, WM 2019, 166, 174, 175.

193 Vgl. exemplarisch *Beyerbach*, Unternehmensinformation, S. 100, 101. Nach *Beyerbach* sei der Schutz nicht pauschal ausgeschlossen. Informationen über Sachverhalte, die gegen die öffentliche Ordnung verstoßen oder die guten Sitten bzw. eine Straftat von erheblicher Tragweite darstellen, seien jedenfalls nicht schutzwürdig.

Der nationale Gesetzgeber geht davon aus, dass das Erfordernis des wirtschaftlichen bzw. kommerziellen Werts mit der damaligen Definition unter §§ 17 bis 19 UWG a. F. übereinstimmt.[194] Dies ergibt sich aus der Gesetzesbegründung zu § 2 Nr. 1 lit. a) GeschGehG.[195] In Anbetracht dessen weisen Stimmen im Schrifttum darauf hin, dass das heutige Erfordernis des wirtschaftlichen Werts enger als das des damaligen „*berechtigten Interesses*“ sei. Dies habe den Ausschluss rechtswidriger Informationen zur Folge.[196] Dieser Gedankengang überzeugt jedoch nicht. Zu beachten ist zunächst, dass der Verweis des Gesetzgebers auf die alte Rechtslage mit Blick auf die Frage der Schutzfähigkeit rechtswidriger Informationen ohne Aussagekraft ist. Die Frage der Schutzfähigkeit rechtswidriger Informationen war schon damals ungeklärt. Der Verweis auf eine ungeklärte Situation ist insofern ungeeignet, um Klärung herbeizuführen. Stattdessen ist der Verweis auf die alte Rechtslage so zu interpretieren, dass das Kriterium des wirtschaftlichen bzw. kommerziellen Werts lediglich dazu dient, belanglose Informationen aus dem Schutzbereich auszunehmen, so wie es bereits damals der Fall war.[197]

Der Blick auf die Historie vermag folglich nicht überzeugen, um zur Annahme einer fehlenden Schutzfähigkeit rechtswidriger Informationen zu gelangen. Vielmehr gilt es, den Verweis auf Erwägungsgrund 14 GeschGeh-RL zu berücksichtigen. Erwägungsgrund 14 GeschGeh-RL unterliegt einem weiten Verständnis in Bezug auf den kommerziellen Wert einer Information, weshalb von der grundsätzlichen Wertigkeit rechtswidriger Informationen auszugehen ist.[198]

---

194 BT-Drs. 19/4724, S. 24.
195 BT-Drs. 19/4724, S. 24.
196 *Kalbfus*, GRUR 2016, 1009, 1011; *Steinmann*, WRP 2019, 703, 709.
197 BT-Drs. 19/4724, S. 24.
198 Siehe: Kapitel B) II. 3. a) cc).

(5) Eine Betrachtung des Telos

Zweck des GeschGehG ist die Stärkung des Geschäftsgeheimnisschutzes in Umsetzung der GeschGeh-RL durch ein eigenes Stammgesetz.[199] Ziel ist es, ein einheitliches Schutzniveau zum Schutz der unternehmerischen Geheimhaltungsinteressen in der Europäischen Union zu verwirklichen, um einen funktionierenden Wettbewerb zu ermöglichen und Innovation zu steigern. Ein Ausschluss der Schutzfähigkeit rechtswidriger Informationen würde dem Schutzzweck des GeschGehG und der GeschGeh-RL insoweit widersprechen, als einzelne Informationen dem Schutzbereich entfallen würden und Unternehmen großen Risiken ausgesetzt wären. Ein zu leichtfertiger Umgang mit Geschäftsgeheimnissen zieht schnell irreversible Schäden nach sich. Dies betrifft nicht nur den Bereich des Whistleblowings. Auch Wettbewerber hätten ohne Weiteres Zugriff auf rechtswidrige Informationen Dritter. Es widerspricht daher dem Zweck des GeschGehG in Umsetzung der GeschGeh-RL, rechtswidrigen Informationen pauschal den Schutz zu versagen.

Hinzu kommt, dass die Beurteilung der Rechtswidrigkeit einer Information in der Europäischen Union aufgrund der unterschiedlichen nationalen Rechtsordnungen stark divergieren kann. Dies steht dem Bestreben der GeschGeh-RL entgegen, ein einheitliches Begriffsverständnis innerhalb der Europäischen Union zu etablieren.[200] Darüber hinaus hat der nationale Gesetzgeber mittels § 5 GeschGehG einen geeigneten Weg gefunden, Einzelfallgerechtigkeit zu erzielen. Die obligatorische Interessenabwägung stellt sachgerechte Ergebnisse sicher, auch in Bezug auf rechtswidrige Informationen.[201] Es entspricht

---

199 Siehe: Kapitel B) II. 1. und 2.

200 *Hoppe*/*Oldekop*, Geschäftsgeheimnisse, Rn.101.

201 Sofern ein benannter Fall vorliegt, wird aus der obligatorischen Interessenabwägung eine obligatorische Berücksichtigung des Verhältnismäßigkeitsgrundsatzes anhand des jeweiligen unbestimmten Rechtsbegriffs. Eine eigenständige Interessenabwägung anhand des Begriffs des „*berechtigten Interesses*“ erfolgt nicht. Siehe auch: Kapitel C) I. 1. c) cc).

daher dem Telos des GeschGehG, rechtswidrige Informationen erst im Rahmen des § 5 GeschGehG zu berücksichtigen.[202] Dies ergibt sich dementsprechend auch aus systematischen Überlegungen. § 5 GeschGehG wäre nahezu ohne eigenen Anwendungsbereich, würde es rechtswidrigen Informationen bereits auf Definitionsebene an der Schutzfähigkeit fehlen.

(6) Gesamtbetrachtung: Weshalb rechtswidrige Informationen von wirtschaftlichem Wert sind

Insbesondere die Auslegung des Wortlautes in Verbindung mit den Gesetzesmaterialien und der allgemeinen Schutzrichtung des GeschGehG sprechen für die Werthaltigkeit rechtswidriger Informationen. Das Kriterium des wirtschaftlichen bzw. kommerziellen Werts dient dem Ausschluss belangloser Informationen, die auch unter der bisherigen Definition nicht schutzfähig waren. Die Werthaltigkeit einer Information ist unionsrechtskonform weit auszulegen. Der Begrifflichkeit kann daher sowohl ein positives als auch ein negatives Wertverständnis zugrunde gelegt werden. Der Verweis des nationalen Gesetzgebers auf Erwägungsgrund 14 GeschGeh-RL belegt, dass Informationen bereits dann von wirtschaftlichem bzw. kommerziellen Wert sein sollen, soweit sie für den Geheimnisinhaber von wirtschaftlicher Bedeutung sind, weil sie entweder unmittelbar über einen (potenziellen) Wert verfügen oder sie das Unternehmen aufgrund ihrer Geheimhaltung vor wirtschaftlichen Nachteilen bewahren und deshalb vermögenswert sind.[203] Damit sind auch solche Informationen werthaltig, deren Bekanntwerden Reputationsverluste oder (Vermögens-) Schäden bzw. Geldbußen zur Konsequenz haben würden. Die Geheimhaltung rechtswidriger Information verhindert Reputationsverluste oder gegen das Unternehmen gerichtete Schadensersatzansprüche bzw. Geldbußen. Das Vermeiden bzw. Umgehen von

---

[202] Vgl. Erwägungsgrund 21 GeschGeh-RL, Art. 11 Abs. 2 GeschGeh-RL und § 9 GeschGehG.

[203] *Hoppe*/*Oldenkop*, Geschäftsgeheimnisse, Rn.101; a. A.: OLG Frankfurt, Urteil v. 17.05.2022 - 11 U 115/21 Rn.44.

Schadensersatzansprüchen stellt insofern mittelbar einen Vermögenswert dar. Dieses Verständnis überzeugt auch in systematischer Hinsicht. So bleibt genug Raum, um über § 5 GeschGehG interessengerechte Lösungen zu finden. Auch der Schutzzweck der GeschGeh-RL und des GeschGehG streiten für die grundsätzliche Wertigkeit einer rechtswidrigen Information. Eine restriktive Auslegung birgt die Gefahr eines divergierenden Begriffsverständnisses innerhalb der Europäischen Union. Ein solches will die GeschGeh-RL jedoch verhindern. Im Ergebnis weisen rechtswidrige Informationen daher in aller Regel einen wirtschaftlichen Wert auf.[204]

dd) Zusammenfassender Überblick

Das Vorliegen eines Geschäftsgeheimnisses erfordert eine geheime Information von wirtschaftlichem Wert, § 2 Nr. 1 lit. a) GeschGehG. Der Begriff der Informationen ist weit zu verstehen und unterliegt keinen qualitativen Vorgaben. Aus der vormaligen Rechtsprechung zu §§ 17 bis 19 UWG a. F. folgt, dass die Information der Sphäre eines bestimmten Unternehmens unmittelbar zuordbar sein muss, respektive in einem eindeutigen Zusammenhang zu diesem stehen muss, weil sie für den Geheimnisinhaber marktrelevant ist (sog. „*Unternehmensbezug*“).[205] Auch Informationen aus dem privaten Bereich können Geschäftsgeheimnisse sein und dem Schutzregime des GeschGehG unterfallen. Insbesondere der Verweis in § 1 Abs. 3 Nr. 1 GeschGehG auf § 203 StGB deutet darauf hin, dass Privatgeheimnisse dem GeschGehG unterfallen. Maßgeblich sind die Umstände des jeweiligen Einzelfalls, wobei die wachsende Vermarktung des Privat- und Geschäftslebens eine trennscharfe Abgrenzung erschwert.

---

[204] Ebenso: *Apel*/*Walling*, DB 2019, 891, 894; *Hiéramente*, in: BeckOK-GeschGehG, § 2 Rn.75; *Schröder*, ZRP 2020, 212, 214. Auf die untergeordnete Bedeutung in der Praxis hinweisend: *Dobler,* Geschäftsgeheimnisschutz und investigativer Journalismus, Zweites Kapitel, S. 146.

[205] Siehe: Kapitel B) II. 3. a) aa).

Die „*weder […] noch*“ - Formulierung in § 2 Nr. 1 lit. a) GeschGehG ist im Sinne eines alternativen Verständnisses („*entweder […] oder*“) zu begreifen. Dies entspricht dem Willen des Unionsgesetzgebers und seinen Bestrebungen eines einheitlichen europaweiten Begriffsverständnisses in Anlehnung an Art. 39 Abs. 2 TRIPS. Besteht eine Information aus mehreren Bestandteilen, ist sie demnach auch dann geheim, wenn ihre Einzelteile öffentlich zugänglich sind. In diesen Fällen kommt es dann auf den Geheimnischarakter der konkreten Anordnung bzw. Zusammensetzung der Daten an. Damit ist auch die Kundenliste schutzfähiges Objekt im Sinne des GeschGehG. Gleichwohl bleibt der nationale Gesetzgeber aufgefordert, die missverständliche Regelung einer klarstellenden Korrektur zuzuführen.

Eine Information ist geheim, wenn sie ausschließlich dem Geheimnisinhaber bzw. zur Vertraulichkeit verpflichteten Dritten bekannt ist, wobei die Größe dieses Personenkreises unbeachtlich ist. Maßgeblich ist, ob der Geheimnisinhaber den „*Kreis der Mitwisser*“ noch überblicken bzw. nachvollziehen kann. Eine Information verliert ihren Geheimnischarakter nicht dadurch, dass sie in Erfüllung einer Anzeigepflicht offengelegt wird. Dies gilt insbesondere dann, wenn die Offenlegung gegenüber einer Person erfolgt, die ihrerseits zur Vertraulichkeit verpflichtet ist und ergibt sich insbesondere aus § 4 Abs. 2 Nr. 2, Nr. 3 GeschGehG, der davon ausgeht, dass andere Personen als der Geheimnisinhaber Kenntnis sowie Nutzungsrechte an der Information haben können. Auch § 3 Abs. 2 GeschGehG spricht für diese Lesart, wonach die erlaubte Nutzung oder Offenlegung eines Geschäftsgeheimnisses den Verbotstatbestand entfallen lässt, nicht jedoch den Geheimnischarakter der Information.

§ 2 Nr. 1 lit. a) GeschGehG setzt weiter voraus, dass die Information geheim ist und aus diesem Umstand ein wirtschaftlicher Wert resultiert. Auffällig ist, dass der Unionsgesetzgeber vom „*kommerziellen Wert*“ der Information spricht, während der nationale Gesetzgeber einen „*wirtschaftlichen Wert*“ verlangt. Es ist davon auszugehen, dass die Formulierungen inhaltlich gleichbedeutend sind. Hintergrund

dürfte sein, dass die Formulierung „*wirtschaftlicher Wert*“ im deutschen Sprachgebrauch geläufiger ist und der Gesetzgeber sich deshalb für diese Abweichung entschieden hat, ohne dass damit eine inhaltliche Abweichung vom Begriffsverständnis der GeschGeh-RL einhergeht. Mithin ist die Kausalverbindung zwischen Geheimhaltung und Wertigkeit einer Information weit auszulegen. Ausreichend ist, dass eine Information durch die Geheimhaltung einen (potenziellen) Wertzuwachs erfährt, die Geheimhaltung für den wirtschaftlichen bzw. kommerziellen Wert zumindest auch von Bedeutung ist.

Darüber hinaus stellt sich die Frage, ob ein wirtschaftlicher bzw. kommerzieller Wert an so-genannten „*rechtswidrigen Informationen*“ bestehen kann. Gemeint sind Informationen illegalen Ursprungs oder Inhalts. Die Schutzfähigkeit rechtswidriger Informationen war schon unter der vorherigen Rechtslage unter §§ 17 bis 19 UWG a. F. ein vieldiskutiertes Thema, das im Rahmen der GeschGeh-RL und dem GeschGehG fortbesteht. Insbesondere die Auslegung des Wortlauts in Verbindung mit den Gesetzesmaterialien und der allgemeinen Schutzrichtung sprechen für die Werthaltigkeit rechtswidriger Informationen. Das Kriterium des wirtschaftlichen bzw. kommerziellen Werts dient lediglich dem Ausschluss belangloser Informationen, die auch unter der bisherigen Definition nicht schutzfähig waren. Die Werthaltigkeit einer Information ist weit auszulegen. Der Verweis des nationalen Gesetzgebers auf Erwägungsgrund 14 GeschGeh-RL belegt, dass Informationen bereits dann von wirtschaftlichem bzw. kommerziellen Wert sind, soweit sie für den Geheimnisinhaber von wirtschaftlicher Bedeutung sind, weil sie entweder unmittelbar über einen (potenziellen) Wert verfügen oder sie das Unternehmen aufgrund ihrer Geheimhaltung vor wirtschaftlichen Nachteilen bewahren und deshalb vermögenswert sind. Letzteres trifft insbesondere auf rechtswidrige Informationen zu, da ihr Bekanntwerden regelmäßig zu Reputationsverlusten oder anderen (Vermögens-) Schäden bzw. Geldbußen führt. Dieses Verständnis überzeugt auch in systematischer Hinsicht. So bleibt genug Raum, um über § 5 GeschGehG interessengerechte Lösungen zu finden. Eine restriktive Auslegung birgt zudem die

Gefahr eines divergierenden Begriffsverständnisses innerhalb der Europäischen Union. Im Ergebnis weisen rechtswidrige Informationen daher in aller Regel einen wirtschaftlichen Wert auf.

b) Berechtigtes Geheimhaltungsinteresse

§ 2 Nr. 1 lit. c) GeschGehG verlangt ein „*berechtigtes Interesse an der Geheimhaltung*“.[206] Im Vergleich zur GeschGeh-RL hat der nationale Gesetzgeber mit diesem Kriterium die Definition des Geschäftsgeheimnisses um ein weiteres Element ergänzt. Dies geschah auf Empfehlung des Rechtsausschusses des Deutschen Bundestags, der in diesem Kontext insbesondere auf Erwägungsgrund 14 GeschGeh-RL sowie die Sorge einer Beschränkung von Arbeitnehmerinteressen bzw. des investigativen Journalismus verweist.[207] Bemerkenswert ist, dass der Wortlaut in § 2 Nr. 1 lit. c) GeschGehG von dem in Erwägungsgrund 14 GeschGeh-RL abweicht. Während die Richtlinie auf ein „*legitimes Interesse*“ an der Geheimhaltung hinweist, fordert der nationale Gesetzgeber ein „*berechtigtes Interesse*“. Der Gesetzgeber hat das Wort „*legitim*“ durch „*berechtigt*“ ersetzt. Wie auch schon im Rahmen der Formulierung des wirtschaftlichen Werts dürfte der Gesetzgeber auch in diesem Fall die sprachliche Abweichung aus Verständlichkeitsüberlegungen gewählt haben.[208] Dafür spricht, dass das berechtigte Geheimhaltungsinteresse ein im Zeitpunkt der Einführung

---

[206] Ein Geheimnisbrecher im Sinne des § 4 GeschGehG kann mangels rechtmäßiger Kontrolle über das Geschäftsgeheimnis kein berechtigtes Geheimhaltungsinteresse vorweisen und infolgedessen nicht zugleich Geheimnisinhaber gemäß § 2 Nr. 2 GeschGehG sein, vgl. *Hiéramente*, in: BeckOK-GeschGehG, § 2 Rn.83 m. w. N.

[207] BT-Drs. 19/8300, S. 4, 13, 14; BT-Drs. 19/4724, S. 24; *Apel*/*Walling*, DB 2019, 891, 894.

[208] Zur sprachlichen Abweichung des GeschGehG von der GeschGeh-RL hinsichtlich des wirtschaftlichen bzw. kommerziellen Werts. Siehe: Kapitel B) II. 3. a) cc).

des GeschGehG bekannter Terminus war, der sich durch die Rechtsprechung zu §§ 17 bis. 19 UWG a. F. herausgebildet hat.[209]

Problematisch ist jedoch, dass die GeschGeh-RL das „*legitime Interesse*“ an der Geheimhaltung lediglich im Rahmen ihres Erwägungsgrundes 14 GeschGeh-RL nennt. Anders als der „*kommerzielle Wert*“, der eine tatbestandliche Verankerung in Art. 2 Nr. 1 lit. c) GeschGeh-RL erfahren hat und im Lichte des Erwägungsgrundes 14 GeschGeh-RL auszulegen ist, fehlt diese tatbestandliche Verknüpfung hinsichtlich des legitimen Interesses an der Geheimhaltung in Art. 2 Nr. 1 GeschGeh-RL. Der nationale Gesetzgeber hat demnach ein zusätzliches Kriterium zum Tatbestand des Geschäftsgeheimnisbegriffs erklärt. Dies führt zu der Frage, ob das Erfordernis des berechtigten Geheimhaltungsinteresses einer unionsrechtskonformen Auslegung zugänglich ist. Aus der Rechtsprechung des EuGH folgt in diesem Zusammenhang, dass „*die Begründungserwägungen eines Gemeinschaftsrechtsakts rechtlich nicht verbindlich sind und weder herangezogen werden können, um von den Bestimmungen des betreffenden Rechtsakts abzuweichen, noch, um diese Bestimmungen in einem Sinne auszulegen, der ihrem Wortlaut offensichtlich widerspricht.*“[210] Zu klären ist also, ob es sich bei dem Erfordernis des berechtigten Interesses in § 2 Nr. 1 lit. c) GeschGehG um eine unzulässige Abweichung von der Definition des Geschäftsgeheimnisses im Sinne des Art. 2 Nr. 1 GeschGeh-RL handelt bzw. ob die Abweichung in einem offensichtlichen Widerspruch zum Wortlaut der GeschGeh-RL steht.

Die GeschGeh-RL setzt mit Blick auf den Geschäftsgeheimnisbegriff einen unionsweiten Mindestschutzstandard für geheime Informatio-

---

[209] BT-Drs. 19/8300, S. 13, 14; *Ohly,* GRUR 2019, 441, 444; *Dann/Markgraf*, NJW 2019, 1774, 1776; *Preis/Seiwerth*, RdA 2019, 351, 353.

[210] EuGH, Urteil v. 24.11.2005 - C-136/04 Rn.32; EuGH, Urteil v. 19.06.2014 - C-345/13.

nen fest.[211] Der nationale Gesetzgeber bleibt befugt, anhand einer abweichenden Begriffsdefinition eine Stärkung des Geschäftsgeheimnisschutzes herbeizuführen.[212] Gemeint ist der Fall, dass eine Information nach dem nationalen Regelwerk Schutz erfährt, obwohl diese nach der Definition der GeschGeh-RL nicht geschützt sein soll. Demgegenüber darf der nationale Gesetzgeber keine abweichende Begriffsdefinition schaffen, die eine Absenkung des Geschäftsgeheimnisschutzes zur Folge hätte. Eine Absenkung liegt vor, wenn die nationale Definition des GeschGehG Informationen nicht schützt, für die nach der GeschGeh-RL Schutz vorgesehen ist. Eine solche Regelung wäre unionsrechtswidrig. Fraglich ist demnach, ob das zusätzliche Kriterium des berechtigten Geheimhaltungsinteresses eine unionsrechtswidrige Absenkung des Geschäftsgeheimnisschutzes nach sich zieht. Für eine unzulässige Abweichung „*nach unten*“ spricht laut einigen Stimmen im Schrifttum, dass das Kriterium des berechtigten Geheimhaltungsinteresses - formal betrachtet - eine zusätzliche

---

[211] Vgl. Erwägungsgrund 14 GeschGeh-RL. Auch hinsichtlich der Ausnahmetatbestände in § 5 GeschGehG wäre eine Beschränkung nicht möglich, vgl. Art. 1 Abs. 2 lit. d) i. V. m. Erwägungsgrund 12 GeschGeh-RL. In Betracht kommt lediglich eine Ausweitung bzw. Konkretisierung, vgl. *Naber/Peukert/Seeger*, NZA 2019, 583, 588; für die Tarifvertragsparteien anhand des § 1 Abs. 3 Nr. 3 GeschGehG: *Trebeck/Schulte-Wissermann*, NZA 2018, 1175, 1180. Zu den Grenzen der vertraglichen Abdingbarkeit des GeschGehG: *Alexander*, WRP 2020, 1385, 1390, 1391; *Apel*/*Boom*, GRUR-Prax 2020, 225.

[212] *Dobler,* Geschäftsgeheimnisschutz und investigativer Journalismus, Zweites Kapitel, S. 125, 159 weist zutreffend darauf hin, dass die GeschGeh-RL einen kombinierten Regelungsansatz aus Voll- und Mindestharmonisierung verfolgt. Siehe auch: *Gärtner*/*Oppermann,* BB 2019, Heft 35, Umschlagteil I (Die Erste Seite); *Ohly*, GRUR 2019, 441, 444; *Schlack,* ZWeR 2019, 192, 199.

Anforderung für den Schutz einer Information darstellt.[213] Aus diesem Umstand erhöhter Voraussetzungen folge ein im Vergleich zur GeschGeh-RL engeres und damit unionsrechtswidriges Begriffsverständnis. Dieses Ergebnis ist jedoch zu kurz gedacht. Nicht jede abweichende bzw. zusätzliche Formulierung führt auch inhaltlich zu einer Absenkung des europäischen Schutzniveaus. Vielmehr bedarf es einer dezidierten Prüfung, wie das Kriterium des berechtigten Geheimhaltungsinteresses auszulegen ist.

Dafür gilt es zu klären, inwieweit das berechtigte Geheimhaltungsinteresse in den übrigen Voraussetzungen aufgeht. Damit geht erneut die Frage der Schutzfähigkeit sog. „*rechtswidriger Informationen*" einher, die nach hiesiger Auffassung durch die GeschGeh-RL geschützt sind. Vor diesem Hintergrund ist die Schutzfähigkeit rechtswidriger Informationen zwingende unionsrechtliche Vorgabe für das GeschGehG.[214] Sollte das Erfordernis des berechtigten Geheimhaltungsinteresses zu einem Ausschluss sog. rechtswidriger Informationen nach dem GeschGehG führen, wäre dies unionsrechtswidrig. Sollte das berechtigte Interesse dagegen vollständig von den übrigen Voraussetzungen in § 2 Abs. 1 Nr. 1 lit. a) und b) GeschGehG erfasst sein, wären die Voraussetzungen in Art. 2 Nr. 1 GeschGeh-RL durch § 2 Abs. 1 Nr. 1 lit. c) GeschGehG lediglich formal erhöht und das Kriterium des berechtigten Geheimhaltungsinteresses wäre unionsrechtskonform.

---

[213] Für die Unionsrechtswidrigkeit: *Harte-Bavendamm*, in: Harte-Bavendamm/Ohly/Kalbfus GeschGehG, § 2 Rn.68, 69; *Schlack*, ZWeR 2019, 192, 199; tendenziell auch *Glincke*, in: Keller/Schönknecht/Glinke GeschGehG, § 2 Rn.91; *Ohly*, GRUR 2019, 441, 444; a. A.: *Brockhaus*, ZIS 2020, 102, 110, 111; *Hauck*, AfP 2021, 193, 198, 199; *Preis*, in: ErfK-ArbR, § 611a BGB Rn.814; *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 193.195, 198; *Naber*/*Peukert*/*Seeger*, NZA 2019, 583, 584.

[214] *Gärtner*/*Oppermann*, BB 2019, Heft 35, Umschlagteil I (Die Erste Seite).

aa) Problemaufriss:
Das berechtigte Geheimhaltungsinteresse als unionsrechtswidriges Ausschlusskriterium für rechtswidrige Informationen?

Einige Stimmen im Schrifttum sehen in dem Kriterium eine normative Einschränkung des Geschäftsgeheimnisbegriffs, um sog. rechtswidrigen Informationen die Schutzfähigkeit abzusprechen.[215] Ein berechtigtes Interesse sei im Sinne des Erwägungsgrunds 14 GeschGeh-RL ein legitimes Interesse, also ein solches, das von der Rechtsordnung gebilligt werde. Rechtswidrige Informationen würden dagegen von der Rechtsordnung missbilligt, weshalb an ihnen kein berechtigtes Geheimhaltungsinteresse bestehen könne. Andere Stimmen führen in diesem Zusammenhang § 5 Nr. 2 GeschGehG an, der den Schutz rechtswidriger Informationen voraussetze, um zur Annahme einer tatbestandlichen Ausnahme zu gelangen.[216]

bb) Eine Betrachtung des Wortlauts anhand der Genese des GeschGehG

Der Wortlaut des § 2 Nr. 1 lit. c) GeschGehG bezieht keine Stellung zu der Frage, ob rechtswidrige Informationen Geschäftsgeheimnisse sein können. Bereits vor Inkrafttreten des GeschGehG war das Erfordernis eines berechtigten Interesses durch die Rechtsprechung zu §§ 17 bis 19 UWG a. F. aufgestellt worden.[217] Dieser Umstand wird jedoch erst im Rahmen der historischen Betrachtungsweise relevant.[218] Für die Wortlautbetrachtung erlangt die vormalige Definition

---

[215] *Hauck*, WRP 2018, 1032, 1034; in die gleiche Richtung: DGB-Stellungnahme zum Regierungs-E GeschGehG v. 04.12.2018, S. 6; *Böning*/*Heidfeld*, AuR 2018, 555, 556.

[216] *Brockhaus*, ZIS 2020, 102, 110, 111; *Hauck*, AfP 2021 2021, 193, 198, 199; *Preis*, in: ErfK-ArbR, § 611a BGB Rn.814; *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 193.195, 198; *Naber*/*Peukert*/*Seeger*, NZA 2019, 583, 584.

[217] *Wolters*, in: GK-UWG, § 17 Rn.27; *Schuth,* Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 182-186.

[218] Dazu sogleich im nächsten Abschnitt.

nur insoweit Bedeutung, dass sie es vermag, die formale Abweichung zwischen dem Erwägungsgrund 14 GeschGeh-RL („*legitimes Interesse*“) und § 2 Nr. 1 lit. c) GeschGehG („*berechtigtes Interesse*“) plausibel zu erklären.[219] Es ist davon auszugehen, dass sich der nationale Gesetzgeber für eine von Erwägungsgrund 14 GeschGeh-RL abweichende Formulierung entschieden hat, weil das berechtigte Interesse ein im Zeitpunkt der Einführung des GeschGehG bekannter Terminus war, der sich durch die Rechtsprechung zu § 17 UWG a. F. herausgebildet hatte.[220]

Im Übrigen liefert das Gesetzgebungsverfahren zum GeschGehG keine ergiebigen Anhaltspunkte, ob und inwieweit das „*berechtigte Interesse*“ Ausschlusskriterium für die Schutzfähigkeit rechtswidriger Informationen sein soll. Zwar forderten einige Stimmen während des Gesetzgebungsverfahrens den Ausschluss rechtswidriger Informationen, um die Wirkungen des GeschGehG im Bereich des Hinweisgeberschutzes und des investigativen Journalismus´ abzuschwächen.[221] Der Gesetz-geber hat daraufhin allerdings nicht nur das Erfordernis des berechtigten Geheimhaltungsinteresses in die Begriffsdefinition des Geschäftsgeheimnisses aufgenommen, sondern darüber hinaus den bis dahin noch als Rechtfertigungsregelung ausgestalteten § 5 GeschGehG in eine Tatbestandsausnahme verwandelt. Da dies synchron erfolgte, lässt sich aus der Ergänzung des „*berechtigten Interesses*“ in

---

[219] Vgl. *Alexander*, WRP 2019, 673, 674; *Hoppe*/*Oldenkop*, Geschäftsgeheimnisse, Rn.258; *Naber*/*Peukert*/*Seeger*, NZA 2019, 583; *Nöbel*/*Veljovic*, CB 2020, 34, 36.

[220] Vgl. BT-Drs. 19/8300, S. 13, 14; *Ohly,* GRUR 2019, 441, 444; *Dann/Markgraf*, NJW 2019, 1774, 1776; *Preis/Seiwerth*, RdA 2019, 351, 353. Siehe dazu auch: Kapitel B) II. 1.

[221] *Brost*/*Wolsing*, ZUM 2019, 898, 901; *Hoppe*/*Oldekop*, Geschäftsgeheimnisse, Rn.12; vgl. auch *Apel*/*Walling*, DB 2019, 891, 892; *Ohly*, in: Harte-Bavendamm/Ohly/Kalbfus GeschGehG, § 5 Rn.2; *Müllmann*, ZRP 2019, 25, 26; *Böning*, in: Wortprotokoll Nr. 19/30, S. 13; *Hiéramente*, in: Wortprotokoll Nr. 19/30, S. 25, 26; *Semsrott*, in: Wortprotokoll Nr. 19/30, S. 22. Sämtliche Wortprotokolle beziehen sich auf die öffentliche Anhörung im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestags am 12.12.2018, zum RefE-GeschGehG zu BT-Drs. 19/4724.

§ 2 Nr. 1 lit. c) GeschGehG nicht viel schlussfolgern. Fest steht jedenfalls, dass der Gesetzgeber die Frage des Ausschlusses rechtswidriger Informationen nicht zeitgleich sowohl im Rahmen der Begriffsdefinition als auch im Rahmen des § 5 GeschGehG geregelt haben kann.[222] Ein Ausschluss rechtswidriger Informationen auf Definitionsebene steht einer Berücksichtigung im Rahmen des § 5 GeschGehG entgegen, weil § 5 GeschGehG das Vorliegen einer geschützten Information voraussetzt. Wo der nationale Gesetzgeber die Frage der Schutzfähigkeit rechtswidriger Informationen verankert hat, lässt sich daher nicht anhand der Genese des GeschGehG abschließend ausermitteln. Dieser Frage muss mittels anderer Auslegungsmethoden weiter nachgegangen werden.

cc) Eine Betrachtung der Historie

Vor Inkrafttreten des GeschGehG wurde das Erfordernis eines berechtigten Interesses durch die Rechtsprechung zu §§ 17 bis 19 UWG a. F herausgebildet.[223] Es liegt nahe, dass der nationale Gesetzgeber mit dem zusätzlichen Kriterium in § 2 Nr. 1 lit. c) GeschGehG betonen wollte, dass die ursprüngliche Voraussetzung in das GeschGehG überführt worden ist.[224] Schon unter §§ 17 bis 19 UWG a. F. war umstritten, ob rechtswidrige Informationen über das berechtigte Interesse

[222] Die Formulierung, der Schutz für die Veröffentlichung rechtswidriger Informationen sei „*doppelt genäht*“, überzeugt daher nicht, vgl. *Ohly*, GRUR 2019, 441, 443, 44.

[223] *Wolters*, in: GK-UWG § 17 Rn.27; *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 182-186.

[224] Vgl. *Reinfeld*, GeschGehG, § 1 Rn.160.

ausgeschlossen sein sollen.[225] Das berechtigte Interesse war nach objektivem Maßstab anhand der Wertigkeit der Information zu beurteilen.[226] Auf die Art sollte eine objektive Überprüfung des Geheimhaltungswillens erreicht werden und sichergestellt sein, dass nicht völlig belanglose Informationen von § 17 UWG a. F. geschützt sind.[227] In diesem Zusammenhang wurde auch die Schutzfähigkeit rechtswidriger Informationen diskutiert; allerdings bezog sich diese Diskussion zuvörderst auf die Wettbewerbsrelevanz, also auf die Wertigkeit der jeweiligen Information.[228] Der nationale Gesetzgeber hat das Erfordernis der Werthaltigkeit jedoch bereits hinreichend über das neue Kriterium des wirtschaftlichen Werts an einer Information in

---

[225] Für einen Ausschluss über den Tatbestand (sog. „*Tatbestandslösung*"), um Hürden für Whistleblower abzuschaffen: *Aldoney*/*Ramírez*, Schutz von Geschäfts- und Betriebsgeheimnissen, S. 346-351, 367, 368, *Alexander*, AfP 2019, 1, 4, 5; *Alexander*, in: Köhler/Bornkamm/Feddersen UWG, § 2 GeschGehG Rn.78-82; *Brockhaus*, ZIS 2020, 102, 108; Stellungnahme des DGB zum Regierungs-E GeschGehG v. 18.05.2018, S. 6-8, 16, 21, abgedruckt im Wortprotokoll Nr. 19/30, S. 47-65; *Hauck*, WRP 2018, 1032, 1034, 1035; *Kreis*, Whistleblowing, S. 59-63; *Schmitt*, RdA 2017, 365, 369; *Rützel*, GRUR 1995, 557, 561; *Schnabel*, CR 2016, 342, 344-348; *Schmitt*, NZA-Beilage 2020, 50, 52, 53; *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 88-91; eher zurückhaltend: *Apel*/*Walling*, DB 2019, 891, 894; eher ablehnend, sich aber nicht festlegend: *Preis*, in: ErfK-ArbR, § 611a BGB Rn.814, 815. Andere sprechen sich für eine „*Rechtfertigungslösung"* unter §§ 17-19 UWG a. F. aus: *Brammsen*, Lauterkeitsstrafrecht, § 17 UWG Rn.24; *Garden*/*Hiéramente*, BB 2019, 963, 967; *Gärtner*/*Oppermann*, BB 2019, Heft 35, Umschlagteil, I (Die Erste Seite); *Kalbfus*, Know-how-Schutz, S. 79-81; *Ohly*, in: Ohly/Sosnitza UWG, § 17 Rn.12; *Rengier*, in: Fezer/Büscher/Obergfell UWG, § 17 Rn.21; *Rody*, Geschäfts- und Betriebsgeheimnisse, S. 116-119; differenzierter: *Sixt*, Whistleblowing im Spannungsfeld, S. 85-90; *Westermann*, Hdb. Know-How-Schutz, S. 22; offenlassend: *Redder*, Schutz von Whistleblowern, S. 127; nicht eindeutig: LG Stuttgart WM 2019, 166, 174, 175.

[226] *Wolters*, in: GK-UWG, § 17 Rn.27; *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 182-186.

[227] *Harte-Bavendamm*, in: Harte-Bavendamm/Henning-Bodewig, UWG, § 17 Rn.6.

[228] Vgl. zum Verwaltungsrecht: BVerwG, Beschluss v. 05.04.2013 - 20 F 4/12 Rn.12 m. w. N.; VG Berlin, Urteil v. 13.08.2020 - 2 K 52.18 Rn.28.

§ 2 Nr. 1 lit. a) GeschGehG geregelt, welches nach hiesiger Auffassung den Schutz rechtwidriger Informationen umfasst. Dass der Gesetzgeber mit dem Erfordernis des „*berechtigten Interesses an der Geheimhaltung*“ beabsichtigt, von der hergebrachten Auffassung abzuweichen, hätte zumindest eines Hinweises bedurft und kann nicht ohne entsprechende Anhaltspunkte unterstellt werden.[229] Stattdessen führt die historische Betrachtungsweise zu der Erkenntnis, dass das berechtigte Interesse den Fortbestand des unter §§ 17 - 19 UWG a. F. herausgebildeten Kriteriums verdeutlichen will, im Übrigen aber vollständig in dem Erfordernis des wirtschaftlichen Werts aufgeht. Rechtsanwender, die die neue Definition lesen, sollten wohl nicht davon überrascht werden, dass die althergebrachte Formulierung keine Erwähnung findet.

dd) Eine Betrachtung der Systematik

Das systematische Zusammenspiel der Definition mit den Ausnahmetatbeständen in § 5 GeschGehG bzw. Art. 5 GeschGeh-RL legt die Schutzfähigkeit rechtswidriger Informationen nahe, da andernfalls die Ausnahmetatbestände regelmäßig leerliefen.[230] Dies streitet für die Annahme, dass ein berechtigtes Interesse an rechtswidrigen Informationen bestehen kann und rechtswidrige Informationen im Rahmen der Tatbestandsausnahme in § 5 GeschGehG Berücksichtigung finden.[231]

---

[229] So auch: *Dobler,* Geschäftsgeheimnisschutz und investigativer Journalismus, Zweites Kapitel, S. 168, 170 mit Hinweis auf u. a.: BVerwG, Beschluss v. 05.03.2020 - 20 F 3/19 Rn.11.

[230] *Dann*/*Markgraf*, NJW 2019, 1774, 1776; *Hoppe*/*Oldekop*, Geschäftsgeheimnisse, Rn.101, 260, unter Hinweis auf die Systematik des GeschGehG, die zwischen der Definition des Geschäftsgeheimnisses und den Ausnahmetatbeständen unterscheidet; a. A.: *Hauck*, GRUR-Prax 2019, 223, 225.

[231] *Dann*/*Markgraf*, NJW 2019, 1774, 1776; *Nöbel*/*Veljovic*, CB 2020, 34, 37. Mit der Gegenposition sich ausführlich befassend: *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, S. 173.

ee) Eine Betrachtung des Telos

Zweck des GeschGehG in Umsetzung der GeschGeh-RL ist die Stärkung des Geschäftsgeheimnisschutzes mit dem Ziel, ein unionsweit einheitliches Schutzniveau zu verwirklichen, das einen funktionierenden Wettbewerb ermöglicht und Anreize für mehr Innovation schafft. Ein Ausschluss der Schutzfähigkeit rechtswidriger Informationen würde dem Schutzzweck von GeschGehG und GeschGeh-RL insoweit widersprechen, als einzelne Informationen dem Schutzbereich entfallen würden und Unternehmen infolgedessen großen Risiken ausgesetzt wären.[232] Es widerspricht daher dem Zweck des GeschGehG in Umsetzung der GeschGeh-RL, rechtswidrigen Informationen pauschal den Schutz zu versagen.[233] Hinzu kommt, dass die Beurteilung der Rechtswidrigkeit einer Information in der Europäischen Union aufgrund der unterschiedlichen nationalen Rechtsordnungen stark divergieren kann. Dies steht dem Bestreben der GeschGeh-RL, ein einheitliches Begriffsverständnis innerhalb der Europäischen Union zu etablieren, entgegen.[234] Darüber hinaus hat der nationale Gesetzgeber mittels § 5 GeschGehG einen geeigneten Weg gefunden, Einzelfallgerechtigkeit zu erzielen. Die grundsätzlich obligatorische Interessenabwägung stellt sachgerechte Ergebnisse sicher, auch in Bezug auf rechtswidrige Informationen. Es entspricht daher dem Zweck des GeschGehG rechtswidrige Informationen erst im Rahmen des § 5 GeschGehG zu berücksichtigen.[235]

---

232 Siehe: Kapitel B) II. 1. und 2.

233 Ebenso: *Hiéramente,* Stellungnahme zum Regierungs-E GeschGehG als Sachverständiger, abgedruckt im Wortprotokoll Nr. 19/30, S. 73-101.

234 *Hoppe*/*Oldekop*, Geschäftsgeheimnisse, Rn.101.

235 Vgl. auch die systematische Betrachtungsweise: § 5 GeschGehG wäre nahezu ohne eigenen Anwendungsbereich, würde es rechtswidrigen Informationen bereits auf Definitionsebene an der Schutzfähigkeit fehlen; vgl. Erwägungsgrund 21 GeschGeh-RL, Art. 11 Abs. 2 GeschGeh-RL und § 9 GeschGehG.

ff) Gesamtbetrachtung: Weshalb das berechtigte Geheimhaltungsinteresse kein unionsrechtswidriges Ausschlusskriterium für den Schutz rechtswidriger Informationen ist

Wortlaut und Historie legen nahe, dass der nationale Gesetzgeber das Kriterium des berechtigten Interesses nur deshalb in § 2 Nr. 1 lit. c) GeschGehG ergänzt hat, damit sofort erkennbar ist: Das bekannte Kriterium des berechtigten Geheimhaltungsinteresses besteht auch unter der neuen Definition im GeschGehG fort, ohne dass damit eine inhaltliche Änderung einhergeht. Zu berücksichtigen ist dabei, dass das berechtigte Interesse unter der vormaligen Regelung in §§ 17 bis 19 UWG a. F. dem Ausschluss belangloser Informationen diente und deshalb eine Werthaltigkeit im Sinne einer Wettbewerbsrelevanz forderte. Legt man dieses Verständnis dem berechtigten Interesse in § 2 Nr. 1 lit. c) GeschGehG zugrunde, geht das Kriterium vollständig in dem des wirtschaftlichen Werts nach § 2 Nr. 1 lit. a) GeschGehG auf und führt zu keiner Absenkung des Schutzniveaus. Das berechtigte Geheimhaltungsinteresse stellt demnach keine zusätzliche Voraussetzung an die Schutzfähigkeit einer Information im Hinblick auf die GeschGeh-RL und berücksichtigt das Mindestschutzgebot der GeschGeh-RL hinreichend.

§ 2 Nr. 1 lit. c) GeschGehG ist nicht unionsrechtswidrig. Stattdessen stellt § 5 GeschGehG den Hinweisgeberschutz sowie den Schutz der Medien hinreichend sicher und ermöglicht dank der obligatorischen Verhältnismäßigkeitserwägungen eine hohe Einzelfallgerechtigkeit.[236] Dies stimmt mit der Systematik und dem Telos des GeschGehG überein. Beide Betrachtungsweisen gelangen übereinstimmend zu der Annahme, dass rechtswidrige Informationen über die Ausnahmeregelung in § 5 GeschGehG Berücksichtigung finden. Das Gesetz hält mit § 5 GeschGehG einen geeigneten Anknüpfungspunkt für die Frage der Schutzfähigkeit rechtswidriger Informationen bereit,

[236] Auch Whistleblower können unredlich agieren, dieser Umstand muss berücksichtigungsfähig bleiben.

der das Bedürfnis nach einem einschränkenden Begriffsverständnis entfallen lässt. Das Erfordernis des „*berechtigten Geheimhaltungsinteresses*“ in § 2 Nr. 1 lit. c) GeschGehG führt demgemäß nicht zum Ausschluss sog. rechtswidriger Informationen und ist unionsrechtskonform.

Der Geschäftsgeheimnisbegriff schützt folgerichtig sämtliche Informationen, unabhängig von der Frage ihrer Rechtmäßigkeit bzw. Rechtswidrigkeit. Gestützt wird diese Auffassung ebenfalls durch eine Entscheidung des BGH aus dem Jahr 2020.[237] Darin heißt es, dass das Merkmal des berechtigten Interesses „*in keinem Fall in einer Weise interpretiert werden dürfe, welche die Voraussetzungen des Geheimnisschutzes mit der Frage vermenge, ob das Geheimhaltungsinteresse gegenüber einem öffentlichen Interesse an der Offenlegung von Informationen zurücktreten müsse.*“ Weiter wird zutreffend herausgearbeitet, dass andernfalls der grundrechtlich gebotene und einfachrechtlich nunmehr von §§ 1, 2 GeschGehG angestrebte Schutz solcher Informationen entwertet würde. Der BGH schlussfolgert sodann überzeugend, dass GeschGeh-RL und GeschGehG so zu interpretieren seien, dass auf tatbestandlicher Ebene keine besonders strengen Anforderungen gestellt werden dürften, sondern der Ausgleich nachgelagert im Rahmen eines Abwägungsprozesses widerstreitender Interessen realisiert werden müsse.[238] Dies bestätigt das hier gefundene Ergebnis, die Frage der Schutzbedürftigkeit rechtswidriger Informationen erst im Rahmen des § 5 GeschGehG abschließend zu beurteilen. Auf Definitionsebene besteht dagegen die unwiderlegliche Vermutung (sog. „*Fiktion*“), dass an einer Information, die wirtschaftlichen Wert aufweist, auch ein berechtigtes Interesse an ihrer Geheimhaltung im

[237] BGH, NVwZ-RR 2020, 1117, 1119, obgleich die Entscheidung nicht vor dem Hintergrund einer Geheimnisstreitsache ergangen ist, so auch: *Hoppe*/*Oldekop*, Geschäftsgeheimnisse, Rn.260.

[238] BGH, NVwZ-RR 2020, 1117, 1119.

Sinne des § 2 Nr. 1 lit. a) und lit. c) GeschGehG besteht und diese schutzfähig ist.[239]

c) Angemessene Geheimhaltungsmaßnahmen

Der Schutz des GeschGehG setzt nach §§ 2 Nr. 1 lit. b), 9 Nr. 2 GeschGehG das Vorliegen angemessener Geheimhaltungsmaßnahmen durch den rechtmäßigen Inhaber der geheimen Information voraus.[240] Die deutsche Vorschrift entspricht nahezu wörtlich dem Richtlinientext in Art. 2 Nr. 1 lit. c) GeschGeh-RL und ist die wohl meistdiskutierte Komponente des Geheimnisbegriffs. Der Begriff der angemessenen Geheimhaltungsmaßnahmen hat in seiner Eigenschaft als unbestimmter Rechtsbegriff bereits eine gewisse Konturierung durch die Rechtsprechung erfahren. Gleichwohl wird das Definitionselement die unternehmerische Praxis auch weiterhin angesichts seiner mannigfaltigen Ausgestaltungsmöglichkeiten vor große Herausforderungen stellen.[241] Unternehmen sind aufgefordert, ihre Geheimnisschutzkonzepte fortwährend auf den Prüfstand zu stellen. Dies einerseits, um die Risiken, die mit dem voranschreitenden technologischen Fortschritt einhergehen, hinreichend zu adressieren. Darüber hinaus kann die Rechtsprechung Anlass dazu geben, das eigene Geheimnisschutzkonzept mit den durch die Judikative gesetzten Maßstäben abzugleichen und entsprechend auf- oder umzurüsten.[242] Zeichnen sich beispielsweise im Rahmen neuer Entscheidungen bestimmte

---

[239] *Ohly,* GRUR 2019, 441, 444, 445; vgl. auch: *Hiéramente,* in: BeckOK-GeschGehG, § 2 Rn.72 ff.

[240] Eine Pflicht zur Implementierung angemessener Geheimhaltungsmaßnahmen besteht grundsätzlich nicht. Etwas anderes gilt für die Geschäftsleitung eines Unternehmens, soweit die Implementierung angemessener Geheimhaltungsmaßnahmen in Erfüllung der Pflicht zur sorgfältigen Unternehmensführung zu erfolgen hat, vgl. § 93 Abs. 1 S. 1 AktG, § 43 Abs. 1 GmbHG, § 34 Abs. 1 S. 2 GenG. Siehe: Kapitel B) III.

[241] Zweifel an der Bestimmtheit der Norm bestehen insofern nicht. Es handelt sich um einen unbestimmten Rechtsbegriff, der durch die Rechtsprechung fortlaufend ausgeformt wird.

[242] Es bleibt der Judikative vorbehalten, dem Angemessenheitsbegriff in § 2 Nr. 1 lit. b) GeschGehG weitere Bestimmtheit zu verleihen.

Richtungen oder Strömungen ab, haben Unternehmen ihre eigenen Geheimnisschutzkonzepte daran zu messen.

Damit ein Unternehmen hinreichend vor möglichen Schäden durch unerlaubte Erlangung, Nutzung oder Offenlegung geheimhaltungsbedürftiger Informationen geschützt ist, bedarf es der Implementierung angemessener Geheimhaltungsmaßnahmen.[243] Dem Geheimnisinhaber obliegt der Nachweis, dass die geschützte Information Gegenstand angemessener Geheimhaltungsmaßnahmen im Sinne der §§ 2 Nr. 1 lit. b), 9 Nr. 2 GeschGehG ist.[244] Welche Geheimhaltungsmaßnahmen im Einzelnen zu implementieren sind, ist unternehmensbezogen zu entscheiden.[245] In Betracht kommen z. B. (arbeits-) vertragliche Verschwiegenheitsvereinbarungen sowie Maßnahmen im betrieblichen Ablauf, wie beispielsweise wechselnde, komplexe Passwörter, regelmäßige Software-Updates, Taschenkontrollen, der verschlüsselte Versand von E-Mails, Virenschutzprogramme, Alarmanlagen, Videoüberwachungen und Zugangssperren technischer und räumlicher Art, um nur einige der zahlreichen Möglichkeiten zu nennen.[246]

aa) Auslegungsmöglichkeiten

Aufgrund ihrer besonderen Bedeutung für die unternehmerische Praxis, werden die Anforderungen, die mit dem Kriterium der angemessenen Geheimhaltungsmaßnahmen verbunden sind, in den folgenden Abschnitten einer umfassenden Untersuchung zugeführt. Dafür gilt es zunächst ein Verständnis für den Begriff der angemessenen Geheimhaltungsmaßnahmen anhand der bekannten Auslegungs-

---

[243] §§ 2 Nr. 1 lit. b), 9 Nr. 2 GeschGehG; vgl. auch *Dann*/*Markgraf*, NJW 2019, 1774, 1775; *Fuhlrott*, in: BeckOKGeschGehG, § 2 Rn.21a.

[244] *Apel/Walling,* DB 2019, 891, 894; *Fuhlrott/Hiéramente*, DB 2019, 967, 968; vgl. LAG Köln BeckRS 2019, 44850; ArbG Aachen, NZA-RR 2022, 178 Rn.71.

[245] Vgl. BT-Drs. 19/4724, S. 24.

[246] Zum Geschäftsgeheimnisschutz im Beschäftigungskontext ausführlich siehe: Kapitel B. II. 4.

methoden zu entwickeln. Für die unternehmerische Praxis sollen sodann unter Berücksichtigung der bisherigen Rechtsprechung Leitlinien für die Auslegung angemessener Geheimhaltungsmaßnahmen aufgestellt werden.

(1) Eine Betrachtung des Wortlauts

§ 2 Nr. 1 lit. b) GeschGehG setzt in Umsetzung des Art. 2 Nr. 1 lit. c) GeschGeh-RL eine Information voraus, die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist. Aus dem Wortlaut „*angemessen*“ folgt, dass bei der Beurteilung der getroffenen Geheimhaltungsmaßnahmen Verhältnismäßigkeitserwägungen zu treffen sind, die anhand der objektiven Umstände des jeweiligen Einzelfalls vorzunehmen sind.[247] Zunächst gilt es, das mit der Geheimhaltungsmaßnahme verfolgte legitime Ziel zu benennen. Auf den ersten Blick scheint dies einfach: Dem Geheimnisinhaber geht es um den Schutz seiner geheimen Information durch das GeschGehG. Allerdings bedarf es insoweit einer Konkretisierung. Aus § 9 GeschGehG folgt, dass Verhältnismäßigkeitserwägungen dazu führen können, dass das Schutz- und Abwehrsystem des GeschGehG im Einzelfall nicht greift. Als Beispiel für einen solchen Ausschluss nennt § 9 Nr. 2 GeschGehG sodann die getroffenen Geheimhaltungsmaßnahmen.[248] Unverhältnismäßig im Sinne des § 9 Nr. GeschGehG dürfte es z. B. sein, wenn eine Person Schutzansprüchen nach dem GeschGehG ausgesetzt ist, obwohl diese vernünftigerweise nicht erkennen konnte, dass die genutzte Information geheim ist und aufgrund ihrer Geheimhaltung vor Erlangung, Nutzung und Offenlegung geschützt ist.[249] Dem Geheimnisinhaber

---

[247] Art. 11 Abs. 2 der Richtlinie 2016/943/EU. Siehe dazu auch: OLG Hamm, Urteil v. 15.09.2020 - 4 U 177/19, MMR 2021, 506. Die Entscheidung ist beim BGH unter dem Az. I ZR 186/20 anhängig.

[248] § 2 Nr. 1 lit. b) GeschGehG und § 9 Nr. 2 GeschGehG sind dementsprechend zusammen zu lesen.

[249] Erwägungsgrund 14 GeschGeh-RL formuliert in diesem Kontext eine „*legitime Erwartung*“ des Geheimnisinhabers, dass die Vertraulichkeit der Information gewahrt wird.

geht es also auch darum, mittels den Umständen nach angemessenen Geheimhaltungsmaßnahmen sicherzustellen, dass die Schutzansprüche des GeschGehG nicht aus Verhältnismäßigkeitsgründen ausgeschlossen sind. Angemessene Geheimhaltungsmaßnahmen sind daher insbesondere solche, die sicherstellen, dass Personen, die mit der Information üblicherweise in Berührung kommen, vernünftigerweise erkennen können, dass die Information geheim und infolge ihrer Geheimhaltung vor Erlangung, Nutzung und Offenlegung geschützt ist, wobei die Erkennbarkeit der Geheimhaltung objektiv anhand aller maßgebenden Umstände des Einzelfalls zu beurteilen ist. Maßgeblicher Zeitpunkt für die Beurteilung der getroffenen Geheimnismaßnahmen ist dementsprechend der des jeweiligen Geheimnisverrats (sog. ex-ante Betrachtungsweise).[250]

Der Verhältnismäßigkeitsgrundsatz stellt auf Definitionsebene sicher, dass dem Geheimnisinhaber nichts Unmögliches oder Unzumutbares abverlangt wird. Geheimnisschutzkonzepte sind folgerichtig unternehmensspezifisch zu betrachten. Außerdem bedarf es keines perfekten, lückenlosen, bestmöglichen, optimalen oder absolut wirksamen Geheimnisschutzes, um zur Annahme angemessener Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG zu gelangen.[251] Maßgeblich für das Bestehen der Schutzansprüche nach dem GeschGehG ist eine Einzelfallabwägung, bei der das Interesse des Unternehmens an der Geheimhaltung der zu schützenden Information mit dem für das Unternehmen möglichen und zumutbaren Aufwand, den das Unternehmen getroffen hat, um die Erkennbarkeit der Geheimhaltung dieser Information zu erreichen, ins Verhältnis zu setzen ist. Die Gesetzesbegründung nennt in diesem Zusammenhang

---

250 *Alexander*, WRP 2017, 1034, 1039.

251 OLG Hamm, WRP 2021, 223, 236; LAG Düsseldorf, MMR 2021, 181, 184; LAG Baden-Württemberg, Urteil v. 18.08.2021 - 4 SaGa 1/21 Rn.33; OLG Hamm, WRP 2021, 223, 236; OLG Düsseldorf, WRP 2021, 1080, 1083. Bestätigend: *Fuhlrott*, in BeckOK-GeschGehG § 2 Rn.20 mit dem Hinweis, dass eine solche Lesart eine zu große Beschränkung des Begriffsverständnisses zur Konsequenz hätte.

insbesondere den „*Wert, die Bedeutung und die Natur des Geheimnisses, die Größe des Unternehmens, die Art der Kennzeichnung, die üblichen Geheimhaltungsmaßnahmen im Unternehmen und die Kosten*“ als berücksichtigungsfähige Umstände.[252]

Ebenso unternehmensspezifisch ist zu beurteilen, inwieweit die jeweiligen Aspekte heranzuziehen und zu gewichten sind. Dies bezieht sich einerseits auf die Frage, ob alle der genannten Aspekte zwingend in die Einzelfallabwägung einfließen müssen und ob die jeweiligen Aspekte unterschiedlich gewichtet werden können. Für eine differenzierte Einzelfallabwägung, die sowohl die jeweiligen Aspekte als auch deren Gewichtung unternehmensspezifisch festlegt, spricht der Verhältnismäßigkeitsgrundsatz. Je umfassender und flexibler die jeweilige Abwägung stattfindet, desto prägnanter und sachgerechter die Abwägungsergebnisse. Sollte sich die Erkennbarkeit der Geheimhaltung einer Information im Einzelfall bereits aus der Natur des Geheimnisses ergeben, sind Geheimhaltungsmaßnahmen dennoch nicht entbehrlich.

Dafür streitet die Formulierung in § 2 Nr. 1 lit. b) GeschGehG, die voraussetzt, dass aufgrund der objektiven Umstände auch tatsächlich Geheimhaltungsmaßnahmen getroffen wurden. Dies überzeugt, da die bloße Erkennbarkeit der Geheimhaltung gegenüber denjenigen belanglos ist, die geheime Informationen aus eigennützigen Gründen oder in Schädigungsabsicht für sich oder andere nutzbar machen wollen. Geheimhaltungsmaßnahmen dienen daher nicht nur zur Sicherstellung der Erkennbarkeit ihrer Geheimhaltung, sondern müssen auch den Schutz vor unberechtigtem Zugriff hinreichend adressieren. Ein Untätigbleiben im Vertrauen darauf, die Information werde nicht entdeckt, reicht demgemäß nicht aus, um zu der Annahme eines angemessenen Schutzniveaus zu gelangen.

---

[252] BT-Drs. 19/4724, S. 24; *Apel/Walling*, DB 2019, 891, 895; *Fuhlrott/Hiéramente*, DB 2019, 967, 970; *Reinfeld*, Das neue GeschGehG, § 1 Rn.182, 183.

Offen bleibt, ob auch eine einzelne Maßnahme für den Schutz des GeschGehG genügen kann oder ob die Information von wenigstens zwei Geheimhaltungsmaßnahmen geschützt sein muss. Für letztere Lesart spricht zunächst die im Plural gewählte Formulierung „*Geheimhaltungsmaßnahmen*“ in § 2 Nr. 1 lit. b) GeschGehG. Nach hiesiger Auffassung kann in diese Formulierung allerdings kein quantitatives Erfordernis in Bezug auf die getroffenen Geheimhaltungsmaßnahmen hineingelesen werden. Eine rein zahlenmäßige Beurteilung der getroffenen Geheimhaltungsmaßnahmen liefe dem Verhältnismäßigkeitsgrundsatz zuwider. Ist eine einzelne Maßnahme für sich genommen bereits angemessen, so widerspricht es dem Verhältnismäßigkeitsgrundsatz, den Schutz der Information durch das GeschGehG an das Vorliegen weiterer Geheimhaltungsmaßnahmen zu knüpfen (sog. Übermaßverbot). Für diese Lesart spricht auch die Zweckrichtung des GeschGehG in Umsetzung der GeschGeh-RL, die auf eine Stärkung des Geschäftsgeheimnisschutzes und ein einheitliches Begriffsverständnis innerhalb der Europäischen Union zielt. Um diesen beiden Schutzbestrebungen gerecht zu werden, ist der Begriff der angemessenen Geheimhaltungsmaßnahmen niedrigschwellig auszulegen. Ein angemessenes Schutzniveau kann also auch dann gegeben sein, wenn die zu schützende Information lediglich durch eine einzelne Maßnahme geschützt ist. Maßgeblich ist, ob diese einzelne Maßnahme einen den Umständen des jeweiligen Einzelfalls angemessenen Schutz gewährt, wenngleich dieser Fall in der betrieblichen Praxis von geringer Bedeutung sein dürfte. Unternehmen werden angesichts der drohenden Risiken tendenziell eher mehr als das in § 2 Nr. 1 lit. b) GeschGehG geforderte Maß an Sicherheitsvorkehrungen implementieren.

Ereignet sich ein Geheimnisverrat, führt dieser Umstand nicht automatisch zu der Annahme eines fehlenden Schutzniveaus. Maßgeblich ist, ob das Unternehmen im Zeitpunkt des Geheimnisverrats berechtigterweise davon ausgehen durfte, die geheime Information sei hinreichend geschützt. Im Übrigen entscheiden die jeweiligen Umstände des Einzelfalls darüber, in welchem Zeitraum Anpassungen am

Schutzkonzept vorzunehmen sind und wann eine zu zögerliche Verfolgung eines Geheimnisverrats ein fehlendes Schutzniveau bedingt. Dabei kommt es auch darauf an, welche personellen und finanziellen Ressourcen dem Unternehmen zur Verfügung stehen. Ob Sicherungsvorkehrungen mehrmals umgangen worden sein müssen, um zur Annahme eines fehlenden Schutzniveaus zu gelangen, ist nicht eindeutig. Nach hiesiger Auffassung kann eine einmalige Umgehung der Sicherheitsvorkehrungen genügen, soweit diese erhebliche Sicherheitslücken im System aufzeigen, die daraufhin nicht geschlossen wurden, wobei es auch hier wiederum auf die verfügbaren finanziellen und personellen Ressourcen des Unternehmens ankommt. Maßgeblich bleiben die Umstände des jeweiligen Einzelfalls.

Zusammengefasst ergibt die Wortlautauslegung folgende Richtschnur: Maßgeblich für das Vorliegen angemessener Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG ist eine Einzelfallabwägung, bei der das Interesse des Unternehmens an der Geheimhaltung der Information mit dem für das Unternehmen möglichen und zumutbaren Aufwand, den das Unternehmen tatsächlich unternommen hat, um die Erkennbarkeit der Geheimhaltung zu erreichen und die Information vor unberechtigtem Zugriff zu schützen, ins Verhältnis zu setzen ist.

(2) Eine Betrachtung der Historie

Die vormaligen Voraussetzungen, die sich durch die Rechtsprechung unter §§ 17 bis 19 UWG a. F. herausgebildet hatten, kannten das Erfordernis der angemessenen Geheimhaltungsmaßnahmen nicht. Stattdessen bedurfte es eines bekundeten, subjektiven Geheimhaltungswillens des Informationsinhabers.[253] Dieses Erfordernis diente dazu, schlicht unbekannte Tatsachen aus dem Schutzbereich auszunehmen, weshalb die Anforderungen denkbar niedrig gehalten

[253] Zur ehemaligen Definition unter §§ 17 bis 19 UWG a. F. Siehe: Kapitel B) II. 1.

waren.[254] Dementsprechend war auch von einer Vermutung des Geheimhaltungswillens die Rede, weil das berechtigte Geheimhaltungsinteresse die Wettbewerbsrelevanz der geheimen Information implizierte.[255] Der nationale Gesetzgeber ist von der damaligen Definition insoweit abgerückt, dass es nunmehr eines objektiv erkennbaren Geheimhaltungswillens bedarf. Der subjektive Maßstab des §§ 17 bis 19 UWG a. F. wurde durch einen objektiven ersetzt.[256] Dennoch solle die Auslegung der angemessenen Geheimhaltungsmaßnahmen laut Gesetzesbegründung auf Grundlage der bisherigen Definition zu §§ 17 bis 19 UWG a. F. erfolgen.[257] Daraus folgt, dass der Gesetzgeber nach wie vor keine hohen Anforderungen an das Vorliegen eines objektiv erkennbaren Geheimhaltungswillens stellen will. Maßgeb-lich ist, ob sich der erkennbare Geheimhaltungswille objektiv manifestiert hat, wobei es nicht zwingend einer expliziten oder konkludenten Äußerung des Geheimnisinhabers bedarf.[258] Entscheidend ist also, ob eine Person, die mit der Information in Berührung kommt, vernünftigerweise davon auszugehen hat, dass die Information geheim und infolge ihrer Geheimhaltung vor Erlangung, Nutzung und Offenlegung geschützt ist, wobei sich die Geheimhaltung auch aus der Natur der geheim zu haltenden Tatsache ergeben kann.

(3) Eine Betrachtung der Systematik

Auch systematische Erwägungen legen nahe, dass keine zu hohen Anforderungen an das Vorliegen angemessener Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG zu stellen sind. Sollte die Geltendmachung von Schutzansprüchen angesichts der

---

[254] BGH, GRUR 1977, 539, 540; BGHSt 41, 140, 142, 143; BGH, GRUR 2006, 1044, 1046; LAG Düsseldorf, MMR 2021, 181, 183.

[255] *Berger*/*Tunze*, ZIP 2020, 52, 56.

[256] BT-Drs. 19/4724, S. 24; *Dann*/*Markgraf*, NJW 2019, 1774, 1775; *Dumont*, BB 2018, 2441, 2443.

[257] BT-Drs. 19/4724, S. 24; *Weigert*, NZA 2020, 209, 212. Das gilt nach hiesiger Auffassung jedoch nur, soweit dies in unionsrechtskonformer Auslegung der GeschGeh-RL möglich ist.

[258] In diese Richtung auch: *Weigert*, NZA 2020, 209, 212.

getroffenen Geheimhaltungsmaßnahmen im Einzelfall unverhältnismäßig erscheinen, findet dies sein Korrektiv in § 9 Nr. 2 GeschGehG. Danach sind Schutzansprüche ausgeschlossen, wenn dies unter Berücksichtigung der getroffenen Geheimhaltungsmaßnahmen im Einzelfall unverhältnismäßig ist. Ein Blick in andere Regelwerke wie z. B. das LkSG und die DS-GVO zeigt, dass auch dort auf den Angemessenheitsbegriff im Zusammenhang mit der Implementierung bestimmter Schutzkonzepte zurückgegriffen wird. Nach § 4 Abs. 1 S. 1 LkSG müssen Unternehmen beispielsweise ein angemessenes und wirksames Risikomanagement zur Einhaltung ihrer Sorgfaltspflichten aus dem LkSG einrichten, wobei der Angemessenheitsbegriff lediglich im Sinne einer „*Bemühenspflicht*“ zu verstehen ist.[259] Auch das Datenschutzkonzept erfordert ein angemessenes Schutzniveau in Bezug auf die Datensicherheit.[260] Telos des Angemessenheitsbegriffs ist es, Verhältnismäßigkeitserwägungen mit einfließen zu lassen, um den Unternehmen nicht Unmögliches oder Unzumutbares abzuverlangen.

(4) Eine Betrachtung des Telos

Sowohl das GeschGehG als auch die GeschGeh-RL bezwecken eine Stärkung des Geschäftsgeheimnisschutzes. Damit steht das GeschGehG unter der Maßgabe, dass von seinen Erfordernissen auf

---

[259] Vgl. BAFA-Handreichung zur Angemessenheit im Sinne des LkSG, S. 3.

[260] Nach Art. 24 Abs. 1 S. 1 i. V. m. Art. 32 DS-GVO sind Unternehmen verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Allerdings ist zu beachten, dass die Anforderungen an die Datensicherheit nach Art. 32 DS-GVO den Anforderungen an die angemessenen Geheimhaltungsmaßnahmen lediglich ähneln, vgl. auch *Thüsing/Rombey*, ZD 2020, 221, 222; *Weigert*, NZA 2020, 209, 210, 213. DS-GVO und GeschGehG gehen von einem unterschiedlichen Verständnis des Angemessenheitsbegriffs aus. Dennoch kann es sich lohnen, bestehende Synergien im Rahmen der Schutzkonzepte zu realisieren. Zum unterschiedlichen Verständnis des Angemessenheitsbegriffs im Sinne von GeschGehG und DS-GVO, siehe: Kapitel B) III.

Definitionsebene keine abschreckende Wirkung ausgehen darf.[261] Verliert das Unternehmen beispielsweise aufgrund der Implementierung angemessener Geheimhaltungsmaßnahmen an Wettbewerbsfähigkeit, widerspricht dies einer Stärkung des Geschäftsgeheimnisschutzes. An das Kriterium der angemessenen Geheimhaltungsmaßnahmen dürfen daher keine zu hohen Anforderungen gestellt werden. Als Korrektiv dient sodann § 9 Nr. 2 GeschGehG. Danach sind Schutzansprüche ausgeschlossen, wenn dies unter Berücksichtigung der getroffenen Geheimhaltungsmaßnahmen im Einzelfall unverhältnismäßig ist.

(5) Was sagt die Rechtsprechung?

Durch die Rechtsprechung zu § 2 Nr. 1 lit. b) GeschGehG hat der unbestimmte Rechtsbegriff der angemessenen Geheimhaltungsmaßnahmen bereits eine erste Konturierung erfahren. Diese gilt es im Folgenden zu beleuchten und mit den im vorherigen Abschnitt gefundenen Ergebnissen abzugleichen. Abschließend wird die Rechtsprechung einer kurzen Bewertung zugeführt.

Im Hinblick auf das allgemeine Verständnis des angemessenen Schutzniveaus führt das LAG Düsseldorf richtig aus, dass die Angemessenheit nach den konkreten Umständen des Einzelfalls im Sinne einer Verhältnismäßigkeitsprüfung zu würdigen sei.[262] Auch das OLG Hamm betont zutreffend, dass es sich bei dem Begriff um ein flexibles und offenes Tatbestandsmerkmal handele, „*das dem Gedanken der Verhältnismäßigkeit folgt*“.[263] Ein angemessenes Schutzniveau bestehe nicht erst dann, wenn von einem „*bestmöglichen*“ oder

[261] In diese Richtung auch: *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Zweites Kapitel, S. 150-152.
[262] LAG Düsseldorf, Urteil v. 03.06.2020 - 12 SaGa 4/20 Rn.81.
[263] OLG Hamm, Urteil v. 15.09.2020 - 4 U 177/19, MMR 2021, 506.

„*optimalen*“ Schutz auszugehen ist.[264] Im Rahmen einer anderen Entscheidung betonte das OLG Hamm, dass angemessene und vernünftige, nicht jedoch „*absolut wirksame*“ oder „*unumgehbare Schutzmaßnahmen*“ erforderlich seien.[265] Diese grundsätzlichen Ausführungen zum Verständnis der angemessenen Geheimhaltungsmaßnahmen stimmen mit den oben gefundenen Ergebnissen überein. Soweit das OLG Hamm auf „*branchen-übliche Sicherheitsstandards*“ als „*wichtigen Anhaltspunkt für die Angemessenheit von Geheimhaltungsmaßnahmen*“ verweist, ist dem unter der Maßgabe zuzustimmen, dass Branchenstandards entwicklungsoffen gestaltet sind. Bei Vorliegen gegenteiliger Anhaltspunkte kann daher im Einzelfall auch ein abweichendes Vorgehen gerechtfertigt sein.

Nicht ausreichend für ein angemessenes Schutzniveau sei nach Auffassung des LAG Hamm das bloße Vertrauen darauf, dass die Information nicht entdeckt werde.[266] Dies deckt sich ebenfalls mit den zuvor gefundenen Ergebnissen.[267] Ebenso unzureichend sei das Schutzniveau nach richtiger Auffassung des OLG Stuttgart, wenn es Arbeitnehmern erlaubt sei, aus dem sog. Home Office uneingeschränkt auf Informationen zuzugreifen und diese auf eigenen Geräten oder Datenspeichern zu sichern.[268] Hier fehlt es nach hiesiger Auffassung an der erkennbaren Geheimhaltung der geschützten Information.

---

[264] Vgl. OLG Hamm, Urteil v. 15.09.2020 - 4 U 177/19, MMR 2021, 506; LAG Düsseldorf, Urteil v. 03.06.2020 - 12 SaGa 4720, GRUR-RS 2020, 23408 Rn.80; OLG Düsseldorf, Urteil v. 19.11.2020 - 2 U 575/19, GRUR-RS 2020, 35613 Rn.34; *Fuhlrott*, in: BeckOK-GeschGehG, § 2 Rn.20; *Naber/Peukert/Seeger*, NZA 2019, 583.

[265] OLG Hamm WRP 2021, 223, 237; OLG Stuttgart GRUR-RS 2020, 35613 Rn.167; LAG Baden-Württemberg MMR 2022, 79, 80; OLG Schleswig, GRUR-RS 2022, 9007 Rn.57.

[266] LAG Hamm, Urteil v. 23.06.2021 - 10 SaGa 9/21, Rn.24, BeckRS 2021, 41734.

[267] Dafür spricht die Formulierung in § 2 Nr. 1 lit. b) GeschGehG, die voraussetzt, dass anhand der objektiven Umstände auch tatsächlich Geheimhaltungsmaßnahmen getroffen wurden.

[268] OLG Stuttgart, Urteil v. 19.11.2020 - 2 U 575/19, GRUR-RS 2020, 35613.

Nicht genügen solle laut OLG Hamm ein kostensparendes Ergreifen nur eines Minimums an Schutzvorkehrungen, damit eine Information dem Schutz des GeschGehG unterfällt.[269] Konkret heißt es: „*Umgekehrt kann es zur Wahrung der Angemessenheit nicht genügen, wenn der Unternehmer - vielleicht um hohe Kosten und einen gesteigerten Organisationsaufwand zu vermeiden - lediglich ein Minimum an Schutzvorkehrungen ergreift*.“[270] Diese Formulierung steht in Widerspruch zu den zuvor gefundenen Ergebnissen. Nach hiesiger Auffassung kann auch ein Minimum an Schutzvorkehrungen ausreichen, um zur Angemessenheit der getroffenen Geheimhaltungsmaßnahmen zu gelangen. Voraussetzung ist, dass das Minimum an getroffenen Schutzvorkehrungen das notwendige Maß i. S. d. § 2 Nr. 1 lit. b) GeschGehG erfüllt. Maßgeblich ist eine umfassende Einzelfallabwägung unter Beachtung des Verhältnismäßigkeitsgrundsatzes, in deren Rahmen das Interesse des Unternehmens an der Geheimhaltung der Information mit dem für das Unternehmen möglichen und zumutbaren Aufwand, den das Unternehmen tatsächlich unternommen hat, um die Erkennbarkeit der Geheimhaltung zu erreichen und die Information vor unberechtigtem Zugriff zu schützen, ins Verhältnis zu setzen ist. Stehen einem Unternehmen mehrere geeignete Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus zur Verfügung, darf es sich folgerichtig für die kostengünstigste Variante entscheiden, ohne dass der Schutz nach dem GeschGehG verloren geht. In diesem Sinne darf sich ein Unternehmen durchaus auf ein entsprechendes Minimum beschränken.

Darüber hinaus führt das OLG Hamm aus: „*Bei einem weltweit agierenden Unternehmen mit marktbeherrschender Stellung ist ein hohes Maß an Sicherheitsvorkehrungen angemessen*.“[271] Diese Formulierung ist nach hiesiger Auffassung zu pauschal gewählt. Richtig ist, dass die marktbeherrschende Stellung eines Unternehmens einen

[269] OLG Hamm, Urteil v. 15.09.2020 - 4 U 177/19, GRUR-RS 2020, 34822.
[270] OLG Hamm, Urteil v. 15.09.2020 - 4 U 177/19, GRUR-RS 2020, 34822.
[271] OLG Hamm, Urteil v. 15.09.2020 - 4 U 177/19, GRUR-RS 2020, 34822.

berücksichtigungsfähigen Umstand im Rahmen der Beurteilung der angemessenen Geheimhaltungsmaßnahmen darstellen kann. Daraus allein können jedoch keine pauschalen Ableitungen in Bezug auf das Maß an Sicherheitsvorkehrungen gezogen werden. Der Umstand der Marktbeherrschung führt lediglich zu der Annahme, dass Sicherheitsvorkehrungen im Hinblick auf eine Vielzahl an Informationen nötig sind, um die marktbeherrschende Stellung abzusichern. Die notwendige Identifikation dieser Informationen dient in einem ersten Schritt dazu herauszufinden, welchen Risiken prioritär entgegengewirkt werden muss. Nachdem alle schützenswerten Informationen identifiziert sind, kommt es dann in einem nächsten Schritt auf das erkennbare Geheimhaltungsinteresse sowie die verschiedenen Zugriffsmöglichkeit an.[272] Im Rahmen der daran anschließenden Festlegung konkreter Maßnahmen kann sodann der Umstand der Marktbeherrschung relevant werden, sollte aus der Marktbeherrschung beispielsweise folgen, dass entsprechende finanzielle und personelle Ressourcen verfügbar sind. Dabei ist zu beachten, dass auch ein finanziell gut aufgestelltes Unternehmen berechtigt ist, aus mehreren gleich wirksamen Maßnahmen diejenige auszuwählen, die am kostengünstigsten ist. Dies entspricht dem Verhältnismäßigkeitsgrundsatz. Vor diesem Hintergrund verbieten sich pauschale Aussagen, die allgemein schlussfolgern, einem marktbeherrschenden Unternehmen seien per se komplexe und wartungsintensive Geheimhaltungsmaßnahmen möglich und zumutbar. Die Grenze des Möglichen und Zumutbaren ist stets unternehmensbezogen zu bestimmen. Zwar dürfte im Grundsatz davon auszugehen sein, dass ein marktbeherrschendes Unternehmen mehr Ressourcen verfügbar hält als ein kleines Unternehmen. Doch auch ein marktbeherrschendes Unternehmen kann z. B. in finanzielle Schieflage geraten. Wichtig ist daher, dass aus dem Umstand der Marktbeherrschung keine vorschnellen Schlüsse gezogen werden, die die Beachtung der jeweiligen Einzelfallumstände

---

[272] *Scholtyssek*/*Judis*/*Krause*, CCZ 2020, 23, 27; *Dann*/*Markgraf*, NJW 2019, 1774, 1776; *Dumont*, BB 2018, 2441, 2443; *Fuhlrott*, in: BeckOK-GeschGehG, § 2 Rn.23; *Hoppe*/*Oldekop*, Geschäftsgeheimnisse, Rn.129; *Maaßen*, GRUR 2019, 352, 356.

unberücksichtigt lassen. Gleiches gilt mit Blick auf ein eher kleines Unternehmen: Auch hier können die finanziellen Mittel je nach Einzelfall eher klein oder besonders groß sein.

Darüber hinaus ist den weiteren Ausführungen des OLG Hamm zuzustimmen, wenn es formuliert: „*Sicherungsvorkehrungen genügen den Anforderungen nicht, wenn sie mehrfach umgangen worden sind, ohne dass das Unternehmen angemessen reagiert hätte. Es ist zwingend erforderlich, in Anbetracht der Bedeutung des Geschäftsgeheimnisses jedem Hinweis auf eine Umgehung sorgfältig nachzugehen und das Sicherheitskonzept zeitnah anzupassen oder Sanktionen zu ergreifen.*“[273] Zutreffend ist, dass ein Geheimnisverrat nicht gleichbedeutend mit einem fehlenden angemessenen Schutzniveau ist. Ereignet sich ein Geheimnisverrat gibt dieser Anlass, die bis dahin getroffenen Maßnahmen auf den Prüfstand zu stellen und gegebenenfalls entsprechende Anpassungen vorzunehmen. Dabei entscheiden die jeweiligen Umstände des Einzelfalls, in welchem Zeitraum etwaige Anpassungen vorzunehmen sind und ob eine zu zögerliche Verfolgung eines Geheimnisverrats ein fehlendes Schutzniveau bedingen kann. Ob Sicherungsvorkehrungen mehrmals umgangen worden sein müssen, um zur Annahme eines fehlenden Schutzniveaus zu gelangen, ist nach der Entscheidung des OLG Hamm nicht eindeutig. Nach hiesiger Auffassung kann eine einmalige Umgehung der Sicherheitsvorkehrungen genügen, wenn diese beispielsweise erhebliche Sicherheitslücken aufzeigt, die nicht zeitnah geschlossen worden sind, wobei es auch hier auf die Umstände des jeweiligen Einzelfalls ankommen muss, insbesondere unter Berücksichtigung der verfügbaren finanziellen und personellen Ressourcen.

Insgesamt tendiert die zum Angemessenheitsbegriff im Sinne des § 2 Nr. 1 lit. b) GeschGehG ergangene Rechtsprechung in Teilen zu pauschalisierenden Formulierungen. Diese kollidieren mit den zuvor aufgestellten Erkenntnissen insoweit, dass die maßgebenden Um-

[273] OLG Hamm, Urteil v. 15.09.2020 - 4 U 177/19, GRUR-RS 2020, 34822.

stände des jeweiligen Einzelfalls dadurch drohen, zu kurz zu geraten. Es bleibt daher abzuwarten, inwieweit der hier gewonnene Eindruck im Rahmen künftiger Entscheidungen der Judikative an Bestätigung gewinnen wird.

(6) Gesamtbetrachtung: Leitlinien für die Auslegung angemessener Geheimhaltungsmaßnahmen

Aus dem Wortlaut „*angemessen*“ folgt, dass bei der Beurteilung angemessener Geheimhaltungsmaßnahmen Verhältnismäßigkeitserwägungen anzustellen sind.[274] Verhältnismäßig bedeutet, dass Geheimnisschutzkonzepte unternehmensspezifisch zu betrachten sind und es keines perfekten, lückenlosen oder absolut wirksamen Geheimnisschutzes bedarf, um zur Annahme angemessener Geheimhaltungsmaßnahmen zu gelangen.[275] Ebenso unternehmensspezifisch ist zu beurteilen, inwieweit die jeweiligen Aspekte heranzuziehen und zu gewichten sind. Je umfassender und flexibler die jeweilige Abwägung stattfindet, desto prägnanter und sachgerechter die Abwägungsergebnisse. Entscheidend für das Vorliegen angemessener Geheimhaltungsmaßnahmen ist eine Einzelfallabwägung, bei der das Interesse des Unternehmens an der Geheimhaltung der Information mit dem für das Unternehmen möglichen und zumutbaren Aufwand, den das Unternehmen tatsächlich unternommen hat, um die Erkennbarkeit der Geheimhaltung zu erreichen und die Information vor unberechtigtem Zugriff zu schützen, ins Verhältnis zu setzen ist.

---

[274] OLG Hamm, Urteil v. 15.09.2020 - 4 U 177/19, MMR 2021, 506; LAG Düsseldorf, MMR 2021, 181, 184; LAG Baden-Württemberg, Urteil v. 18.08.2021 - 4 SaGa 1/21 Rn.33.

[275] OLG Hamm, WRP 2021, 223, 236; LAG Düsseldorf, MMR 2021, 181, 184; LAG Baden-Württemberg, Urteil v. 18.08.2021 - 4 SaGa 1/21 Rn.33; OLG Hamm, WRP 2021, 223, 236; OLG Düsseldorf, WRP 2021, 1080, 1083; vgl. auch *Fuhlrott*, in: BeckOK-GeschGehG, § 2 Rn.20 mit dem Hinweis, dass eine solche Lesart eine zu große Beschränkung des Begriffsverständnisses zur Konsequenz hätte.

Die Gesetzesbegründung nennt in diesem Zusammenhang zutreffend den „*Wert, die Bedeutung und die Natur des Geheimnisses, die Größe des Unternehmens*,[276] *die Art der Kennzeichnung, die üblichen Geheimhaltungsmaßnahmen im Unternehmen und die Kosten*“ als berücksichtigungsfähige Umstände.[277] Dabei ist die häufig anzutreffende Schlussfolgerung - je schutzbedürftiger die Information, desto höher das zu implementierende Schutzniveau - nicht zwingend.[278] Denn je wertvoller eine Information ist, desto offensichtlicher kann die Erkennbarkeit ihrer Geheimhaltung sein.[279] Insofern kann auch die Wertigkeit einer Information eine tragende Rolle im Rahmen der Implementierung angemessener Geheimhaltungsmaßnahmen einnehmen. Die Judikative neigt in diesem Kontext zu pauschalisierenden Formulierungen. Der Verhältnismäßigkeitsgrundsatz erfordert jedoch die notwendige Berücksichtigung aller maßgebenden Umstände des jeweiligen Einzelfalls. Hier bleiben die weiteren Entwicklungen abzuwarten.

Die historische Auslegung führt zu der Annahme, dass an die Erkennbarkeit der Geheimhaltung einer Information keine zu hohen Anforderungen gestellt werden dürfen. Laut Gesetzesbegründung soll die Auslegung auf Grundlage der bisherigen Definition zu § 17 UWG a. F. erfolgen, deren Voraussetzungen denkbar niedrig waren. In die gleiche Richtung zielen systematische Überlegungen. Sollte die Geltendmachung von Schutzansprüchen angesichts der getroffenen Geheimhaltungsmaßnahmen im Einzelfall unverhältnismäßig scheinen, findet dies sein Korrektiv in § 9 Nr. 2 GeschGehG.

---

276 OLG Hamm, Urteil v. 15.09.2020 - 4 U 177/19, MMR 2021, 506.

277 BT-Drs. 19/4724, S. 24 f.; *Apel/Walling*, DB 2019, 891, 895; *Fuhlrott*/*Hiéramente*, DB 2019, 967, 970; *Reinfeld*, Das neue GeschGehG, § 1 Rn.182 f.

278 Exemplarisch: *Fuhlrott*/*Hiéramente*, DB 2019, 967, 970; *Dumont*, BB 2018, 2441, 2443.

279 Sollte sich die Geheimhaltung auf eine Information beziehen, die auf den ersten Blick eher unwichtig scheint, bedarf es eines erhöhten Aufwandes, um ihre Geheimhaltung erkennbar zu machen.

§ 2 Nr. 1 lit. b) GeschGehG ist daher in Zusammenhang mit § 9 Nr. 2 GeschGehG zu lesen. Das Telos des GeschGehG in Umsetzung der GeschGeh-RL streitet ebenfalls dafür, keine zu hohen Anforderungen an die Voraussetzung der angemessenen Geheimhaltungsmaßnahmen zu stellen. Insbesondere darf von dem Erfordernis der angemessenen Geheimhaltungsmaßnahmen keine abschreckende Wirkung für den Geschäftsgeheimnisschutz ausgehen. Eine solche widerspräche dem Anliegen des (Unions-) Gesetzgebers, den Geschäftsgeheimnisschutz mit den Regelungen des GeschGehG in Umsetzung der GeschGeh-RL zu stärken.

Folgerichtig dürfen die Anforderungen an die angemessenen Geheimhaltungsmaßnahmen i. S. d. § 2 Nr. 1 lit. b) GeschGehG nicht überspannt werden. Dies gilt im Besonderen mit Blick auf die erkennbare Geheimhaltung einer Information. Hintergrund ist, dass jede Äußerung des Geheimhaltungswillens immer auch die Gefahr birgt, bislang Unwissende dazu herauszufordern, in unberechtigterweise an die geheime Information zu gelangen. Während sich die Geheimhaltungsmaßnahmen in Bezug auf die Erkennbarkeit der Geheimhaltung regelmäßig an diejenigen richtet, die berechtigterweise mit der geheimen Information in Berührung kommen, stellen Zugriffsbeschränkungen sicher, dass unberechtigte Personen keinen Zugriff erhalten. Ein Untätigbleiben im Vertrauen darauf, die Information werde nicht entdeckt, reicht daher nicht aus, um zu der Annahme eines angemessenen Schutzniveaus zu gelangen. Demgegenüber kann ein angemessenes Schutzniveau auch dann gegeben sein, wenn die Information lediglich durch eine einzelne Maßnahme geschützt ist. Maßgeblich ist, ob die einzelne Maßnahme einen den Umständen des jeweiligen Einzelfalls angemessenen Schutz gewährt, wenngleich dieser Fall in der betrieblichen Praxis von geringer Bedeutung sein dürfte.

Unternehmen werden angesichts der drohenden Risiken tendenziell eher mehr als das in § 2 Nr. 1 lit. b) GeschGehG geforderte Maß an Sicherheitsvorkehrungen implementieren. Ereignet sich ein Geheimnisverrat, kommt es darauf an, ob das Unternehmen berechtigterweise

davon ausgehen durfte, dass die geheime Information zum Zeitpunkt des Geheimnisverrats hinreichend geschützt gewesen ist. Die jeweiligen Umstände des Einzelfalls entscheiden darüber, in welchem Zeitraum Anpassungen am Schutzkonzept vorzunehmen sind und wann eine zu zögerliche Verfolgung eines Geheimnisverrats ein fehlendes Schutzniveau bedingt. Nach hiesiger Auffassung kann auch eine einmalige Umgehung der Sicherheitsvorkehrungen genügen, wenn diese erhebliche Sicherheitslücken im System aufzeigt und diese daraufhin nicht geschlossen wurden.

Angesichts der fortschreitenden Technologien können insbesondere Zugriffsbeschränkungen komplex und teuer sein. Der Wandel der Zeit zwingt Unternehmen dazu, ihre Geheimnisschutzkonzepte fortlaufend weiterzuentwickeln. Inwieweit das gelingt, darüber entscheiden auch die verfügbaren finanziellen und personellen Ressourcen eines Geheimnisinhabers.

bb) Auswirkungen rechtswidriger Geheimhaltungsmaßnahmen

Die vorstehenden Erkenntnisse lassen die Frage unbeantwortet, wie sich die Implementierung rechtswidriger Geheimhaltungsmaßnahmen auf die Beurteilung des Angemessenheitsbegriffs auswirkt. „*Rechtswidrige Maßnahmen*“ meint in diesem Kontext sowohl unwirksame als auch unzulässige Maßnahmen. Während vertragliche Verschwiegenheitsvereinbarungen bei Vorliegen eines Unwirksamkeitsgrundes „*unwirksam*“ sind,[280] können organisatorische und technische Geheimhaltungsmaßnahmen insbesondere aufgrund eines datenschutzrechtlichen Verstoßes „*unzulässig*“ sein.[281] Im Folgenden soll zunächst untersucht werden, wie sich die Unwirksamkeit bzw. Unzulässigkeit einer Geheimhaltungsmaßnahme auf Definitionsebene im Rahmen der Beurteilung des angemessenen Schutzniveaus auswirkt.

---

[280] §§ 134, 138, 307 Abs. 1 und 2 BGB.

[281] Auch an die Beteiligungsrechte des Betriebsrats ist in diesem Kontext zu denken, insbesondere: §§ 87 Abs. 1 Nr. 1, Nr. 6 und Nr. 7 BetrVG.

Der Vollständigkeit halber werden daran anschließend die Auswirkungen auf den Nachweis eines Geheimnisverrats beleuchtet, ehe die Ergebnisse einer zusammenfassenden Betrachtung zugeführt werden.

(1) Auswirkungen auf Definitionsebene

Dieser Abschnitt untersucht anhand der bekannten Auslegungsmethoden, inwieweit unwirksame bzw. unzulässige Geheimhaltungsmaßnahmen im Rahmen der Beurteilung eines angemessenen Schutzniveaus berücksichtigungsfähig sind, § 2 Nr. 1 lit. b) GeschGehG. Kein überzeugendes Argument ist in diesem Kontext die Illegalität der unwirksamen bzw. unzulässigen Geheimhaltungsmaßnahmen als solche. Die vorherigen Abschnitte haben gezeigt, dass auch sog. *„rechtswidrige Informationen*“, die illegalen Inhalts oder Ursprungs sind, schutzfähig im Sinne des GeschGehG sind.[282]

Aus der Formulierung „*angemessen*“ folgt, dass bei der Beurteilung der getroffenen Geheimhaltungsmaßnahmen Verhältnismäßigkeitserwägungen anhand der objektiven Umstände des jeweiligen Einzelfalls anzustellen sind.[283] Der Verhältnismäßigkeitsgrundsatz streitet für die grundsätzliche Berücksichtigungsfähigkeit unwirksamer bzw. unzulässiger Geheimhaltungsmaßnahmen im Rahmen des § 2 Nr. 1 lit. b) GeschGehG. Je umfassender und flexibler die jeweilige Abwägung stattfindet, desto prägnanter und sachgerechter die Abwägungsergebnisse. Auch die Historie, die Systematik und das Telos des GeschGehG in Umsetzung der GeschGeh-RL legen ein weites Verständnis des Angemessenheitsbegriffs nahe. Insbesondere das Telos des GeschGehG in Umsetzung der GeschGeh-RL streitet dafür, keine zu hohen Anforderungen an die Voraussetzung der angemessenen

[282] Zur Schutzfähigkeit rechtswidriger Informationen: Kapitel B) II. 3. a) cc) und Kapitel B) II. 3. b).

[283] Art. 11 Abs. 2 GeschGeh-RL, sowie OLG Hamm, WRP 2021, 223, 236; LAG Düsseldorf, MMR 2021, 181, 184; LAG Baden-Württemberg, Urteil v. 18.08.2021 - 4 SaGa 1/21 Rn.33; OLG Hamm, WRP 2021, 223, 236; OLG Düsseldorf, WRP 2021, 1080, 1083.

Geheimhaltungsmaßnahmen zu stellen. Zu hohe Anforderungen stünden dem Anliegen des (Unions-) Gesetzgebers entgegen, den Geschäftsgeheimnisschutz zu stärken. Das OLG Schleswig führt in diesem Kontext zutreffend aus: „*Aus der Unwirksamkeit einer Verschwiegenheitsklausel folgt nicht zwingend, dass sie im Rahmen angemessener Geheimhaltungsmaßnahmen unbeachtlich (ist)*."[284] Dies überzeugt insbesondere vor dem Hintergrund, dass § 9 Nr. 2 GeschGehG als Korrektiv dient und unverhältnismäßige Ergebnisse verhindert. Grundsätzlich können daher auch rechtswidrige Geheimhaltungsmaßnahmen im Rahmen des § 2 Nr. 1 lit. b) GeschGehG Berücksichtigung finden.

Voraussetzung für das Bestehen des Schutz- und Abwehrsystems des GeschGehG ist, dass die Berücksichtigung der rechtswidrigen Maßnahme nicht unverhältnismäßig ist, vgl. § 9 Nr. 2 GeschGehG. Dafür bedarf es einer gesonderten Abwägung. Maßgeblich ist, ob der Geheimnisinhaber im Zeitpunkt des Geheimnisverrats berechtigterweise von der Rechtmäßigkeit der Geheimhaltungsmaßnahme ausgehen durfte. Entscheidungserhebliche Umstände können beispielsweise sein, wie viel Zeit seit Bekanntwerden einer der Wirksamkeit entgegenstehenden Rechtsprechung vergangen ist und ob diese Rechtsprechung öffentlichkeitswirksam durch die Medien gegangen ist. Auch der Umstand, dass es sich um ein (noch anfechtbares) erstinstanzliches Urteil oder ein Grundsatzurteil eines letztinstanzlichen Gerichts handelt, kann sich entscheidungserheblich auswirken. Hält ein Unternehmen beispielsweise an einer unwirksamen vertraglichen Vereinbarung fest, obwohl es deren Unwirksamkeit kannte oder infolge grober Fahrlässigkeit nicht kannte, sprechen gute Gründe gegen das Bestehen der Schutz- und Abwehransprüche nach § 9 Nr. 2

[284] OLG Schleswig, Urteil v. 28.04.2022 - 6 U 39/21, GRUR-RS 2022, 9007; *Leistner*, WRP 2021, 835 ff.; *Apel*/*Stolz,* GRUR-Prax 2021, 1-3; a. A.: *Hauck,* GRUR 2022, 530, 535.

GeschGehG, wobei es auch hier auf die weiteren Umstände des Einzelfalls ankommt.[285]

Berücksichtigungsfähig sind demnach alle Geheimhaltungsmaßnahmen, die wirksam bzw. zulässig sind oder bei denen der Geheimnisinhaber berechtigterweise davon ausgehen durfte, dass sie es sind. Berücksichtigungsfähig meint in diesem Kontext, dass die jeweiligen Maßnahmen Teil der getroffenen Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG sind, ohne dass aus deren Rechtswidrigkeit ein Anspruchsausschluss nach § 9 Nr. 2 GeschGehG droht. Durfte der Geheimnisinhaber z. B. in berechtigterweise von der Wirksamkeit einer arbeitsvertraglichen Verschwiegenheitsklausel ausgehen, kann diese für die Beurteilung der erkennbaren Geheimhaltung der geschützten Information herangezogen werden. Sollte der Geheimnisinhaber dagegen in unberechtigter Weise von der Wirksamkeit bzw. Zulässigkeit einer Geheimhaltungsmaßnahme ausgegangen sein, ist die unwirksame bzw. unzulässige Maßnahme nicht berücksichtigungsfähig.

Stellen allerdings ohnehin anderweitige Sicherungsmaßnahmen die Erkennbarkeit der Geheimhaltung sowie den Schutz der Information vor unberechtigtem Zugriff im Sinne des § 2 Nr. 1 lit. b) GeschGehG sicher, kommt es auf die Berücksichtigungsfähigkeit der rechtswidrigen Maßnahmen nicht an.[286] Vor diesem Hintergrund hat das OLG Schleswig zutreffend entschieden, dass die Wirksamkeit einer arbeitsvertraglichen Verschwiegenheitsklausel unbeachtlich sei, sofern die übrigen Maßnahmen zur Sicherstellung eines angemessenen Geheimnisschutzes ausreichen.[287] Gleiches gilt für Zweifelsfragen in Bezug auf die Wirksamkeit oder Zulässigkeit einer Geheimhaltungsmaßnahme. Stellen anderweitige Sicherungsmittel sicher, dass die

---

[285] In diesem Zusammenhang könnten z. B. die Maßstäbe des § 122 Abs. 2 BGB herangezogen werden.

[286] So auch: ArbG Aachen, Urteil v. 13.01.2022 - 8 Ca 1229/20, NZA-RR 2022, 178, Rn.77.

[287] OLG Schleswig, Urteil v. 28.04.2022 - 6 U 39/21.

Information erkennbar geheim und vor unberechtigtem Zugriff geschützt ist, können Geheimhaltungsmaßnahmen, deren Wirksamkeit bzw. Zulässigkeit im Einzelfall nicht sicher feststeht, außen vor bleiben. Im Ergebnis spielt die Berücksichtigungsfähigkeit einer getroffenen Geheimhaltungsmaßnahme folgerichtig nur dann eine Rolle, wenn keine anderweitigen Sicherungsvorkehrungen zur Annahme eines angemessenen Schutzniveaus gereichen.

(2) Auswirkungen auf den Nachweis eines Geheimnisverrats

Die Frage der Berücksichtigungsfähigkeit unwirksamer bzw. unzulässiger Maßnahmen im Rahmen des § 2 Nr. 1 lit. b) GeschGehG führt zu der Frage, inwieweit der Geheimnisinhaber berechtigt ist, einen etwaigen Geheimnisverrat mittels Informationen nachzuweisen, die einer unzulässigen Geheimhaltungsmaßnahme entstammen. Nach der Rosenberg´schen Formel ist der Geheimnisinhaber für den Geheimnisverrat darlegungs- und beweispflichtig.[288] Im Streitfall finden allerdings nur solche Tatsachen in das gerichtliche Prozessgeschehen Eingang, die keinem Sachvortrags- oder Beweisverwertungsverbot unterfallen. Ein solches kann aus der datenschutzrechtlichen Unzulässigkeit einer Geheimhaltungsmaßnahme resultieren.[289] Hintergrund ist, dass die datenschutzrechtlichen Vorgaben Ausfluss des informationellen Selbstbestimmungsrechts sind (Art. 2 Abs. 1 und Art. 1 Abs. 1 GG).

Das BAG führt hierzu zutreffend aus: „*Ein Sachvortrags- oder Beweisverwertungsverbot wegen einer Verletzung des gemäß*

---

288 Vgl. *Rosenberg*, Die Beweislast, S. 98.

289 Vgl. BAG, Urteil v. 20.10.2016 - 2 AZR 395/15, NZA 2017, 443; BAG, Urteil v. 13.12.2007 - 2 AZR 537/06, NZA 2008, 1008; BAG, Urteil v. 27.03.2003 - 2 AZR 51/02; NZA 2003, 1193. Demgegenüber führt eine Missachtung der zwingenden Beteiligungsrechte des Betriebsrats (§ 87 Abs. 1 BetrVG) für sich genommen nicht zur Annahme eines gerichtlichen Beweisverwertungsverbots in Bezug auf die durch die Maßnahme erlangten Informationen, § 46 Abs. 2 S. 1 ArbGG i. V. m. § 286 ZPO.

Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützten allgemeinen Persönlichkeitsrechts (...) kann sich im arbeitsgerichtlichen Verfahren aus der Notwendigkeit einer verfassungskonformen Auslegung des Prozessrechts - etwa von § 138 Abs. 3, § 286, § 331 Abs. 1 S. 1 ZPO - ergeben."[290] Weiter heißt es, dass das Gericht wegen der nach Art. 1 Abs. 3 GG bestehenden Grundrechtsbindung und der Verpflichtung zu einer rechtsstaatlichen Verfahrensgestaltung im Streitfall zu prüfen habe, ob die Verwertung der Daten und der Erkenntnisse, die sich aus diesen Daten ergeben, mit dem allgemeinen Persönlichkeitsrecht des von der Datenverarbeitung Betroffenen vereinbar sei.[291] Zu beachten sei jedoch, dass nicht jeder Verstoß gegen die datenschutzrechtlichen Vorgaben zwingend zur Annahme eines Beweisverwertungsverbotes führe.[292] Ein solches könne nach richtiger Auffassung des BAG nur angenommen werden, sofern mit der prozessualen Verwertung eine Grundrechtsverletzung einhergehe oder verfestigt werde.[293]

Den Ausführungen des BAG ist zuzustimmen. Aufgrund der Grundrechtsbindung hat das Gericht lediglich diejenigen Beweismittel unberücksichtigt zu lassen, deren Verwertung einen unzulässigen, mithin erheblichen Eingriff in die verfassungsrechtlich geschützten Persönlichkeitsrechte bedeutet, vgl. Art. 1 Abs. 3 GG.[294] Handelt es sich beispielsweise um einen Verstoß gegen eine formelle Verfahrensvorschrift, resultiert daraus in aller Regel noch kein Beweisverwer-

---

290 BAG 29.06.2017 - 2 AZR 597/16, NZA 2017, 1179 Rn.21.

291 BAG 29.06.2017 - 2 AZR 597/16, NZA 2017, 1179 Rn.21; BAG, Urteil v. 20.10.2016 - 2 AZR 395/15, NZA2017, 443 Rn.18, 22.

292 *Schmidt/Plote*, NZA 2022, 1297, 1304.

293 BAG, Urteil v. 21.11.2013 - 2 AZR 797/11, NJW 2014,810; BAG, Urteil v. 21.06.2012 - 2 AZR 153/11, NZA 2012, 1027; *Thüsing*/*Pötters,* in: Compliance, § 11 Rn.67.

294 BAG, Urteil v. 27.07.2017 - 2 AZR 681/16, NZA 2017, 1327; BAG, Urteil v. 29.06.2017 - 2 AZR 597/16, NZA 2017, 1179. Sollte sich im Rahmen einer Interessenabwägung herausstellen, dass der Eingriff in das Persönlichkeitsrecht gerechtfertigt war, steht dies der Annahme eines gerichtlichen Beweisverwertungsverbots entgegen, vgl. *Thüsing/Granetzny,* in: Compliance*,* § 20 Rn.45, 48 m. w. N.

tungsverbot.[295] Sollte es einer Geheimhaltungsmaßnahme demgegenüber an einer datenschutzrechtlichen Legitimation fehlen, verstößt dies gegen die Grundprinzipien der DS-GVO, die den Schutz des Rechts auf informationelle Selbstbestimmung der von der Datenverarbeitung betroffenen Person sicherstellen.[296] Verstöße gegen die datenschutzrechtlichen Grundprinzipien der DS-GVO führen daher aufgrund ihrer Grundrechtsrelevanz regelmäßig zur Annahme eines Beweisverwertungsverbots.[297] Informationen, die aus einer solch datenschutzrechtswidrigen Verarbeitung entstammen, können nicht in den Prozess zum Nachweis eines Geheimnisverrats eingebracht werden. Demzufolge kann die datenschutzrechtliche Unzulässigkeit einer Geheimhaltungsmaßnahme Auswirkungen auf den Nachweis eines Geheimnisverrates haben. Relevant wird dies beispielsweise, wenn der Geheimnisinhaber seine Schutzansprüche nach §§ 6 ff. GeschGehG gerichtlich durchzusetzen versucht oder die Wirksamkeit einer Kündigung, die Gegenstand eines Kündigungsschutzprozesses ist, vom Nachweis des Geheimnisverrats abhängt.[298]

(3) Zwischenfazit

Unwirksame bzw. unzulässige Geheimhaltungsmaßnahmen können im Rahmen des § 2 Nr. 1 lit. b) GeschGehG Berücksichtigung finden, sofern dies dem Grundsatz der Verhältnismäßigkeit entspricht. Berücksichtigungsfähig meint in diesem Kontext, dass die jeweiligen Maßnahmen Teil der getroffenen Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG sind, ohne dass aus deren Rechtswidrigkeit ein Anspruchsausschluss nach § 9 Nr. 2 GeschGehG

---

295 *Thüsing*/*Pötters*, in: Compliance, § 21 Rn.44, 45.

296 Gemeint sind insbesondere Art. 5 und Art. 6 DS-GVO.

297 Vgl. BAG, Urteil v. 28.03.2019 - 8 AZR 421/17, NZA 2019, 1212.

298 Bei Verstößen gegen die datenschutzrechtlichen Vorgaben drohen Arbeitgebern außerdem empfindliche Buß-geldzahlungen nach Art. 83 DS-GVO. Darüber hinaus können Beseitigungs- und Unterlassungsansprüche nach §§ 12, 862, 1004 BGB (analog) sowie Schadensersatzansprüche nach §§ 241 Abs. 1, 280 Abs. 1 BGB und §§ 23 Abs. 1, 824, 826 BGB bzw. Art. 82 DS-GVO in Betracht kommen.

droht. Dies ist anhand einer eigenständigen Abwägung zu beurteilen, bei der es darauf ankommt, ob der Geheimnisinhaber zum Zeitpunkt des Geheimnisverrats berechtigterweise von der Rechtmäßigkeit der Geheimhaltungsmaßnahme ausgehen durfte. Dies ist beispielsweise dann nicht der Fall, wenn ein Unternehmen an einer unwirksamen vertraglichen Vereinbarung festhält, obwohl es deren Unwirksamkeit kannte oder infolge grober Fahrlässigkeit nicht kannte, wobei die weiteren Umstände des Einzelfalls maßgeblich bleiben. Berücksichtigungsfähig sind demnach alle Geheimhaltungsmaßnahmen, die rechtmäßig sind oder bei denen der Geheimnisinhaber berechtigterweise davon ausgehen durfte, dass sie es sind.[299]

Stellen anderweitige Sicherungsmaßnahmen die Erkennbarkeit der Geheimhaltung sowie den Schutz der Information vor unberechtigtem Zugriff sicher, kommt es auf die Berücksichtigungsfähigkeit der rechtswidrigen Maßnahme nicht an.[300] Gleiches gilt für den Fall, sollten Zweifel daran bestehen, ob eine Geheimhaltungsmaßnahme unwirksam bzw. unzulässig ist. Die Frage der Berücksichtigungsfähigkeit einer getroffenen Geheimhaltungsmaßnahme stellt sich daher nur, sofern keine anderweitigen Sicherungsvorkehrungen für die Annahme eines angemessenen Schutzniveaus im Sinne des § 2 Nr. 1 lit. b) GeschGehG vorhanden sind.

Sollte eine unwirksame arbeitsvertragliche Verschwiegenheitsklausel im Einzelfall nicht berücksichtigungsfähig sein, kann stattdessen die arbeitsvertragliche Treuepflicht des Arbeitnehmers berücksichtigungsfähig sein. Voraussetzung ist, dass die unwirksame Verschwiegenheitsklausel bestimmt genug ist, die nötige Erkennbarkeit des

---

[299] Ist der Geheimnisinhaber dagegen in unberechtigterweise davon ausgegangen, dass die getroffenen Maßnahmen wirksam bzw. zulässig seien, sind diese nach hiesiger Auffassung nicht berücksichtigungsfähig.

[300] Vgl. ArbG Aachen, Urteil v. 13.01.2022 - 8 Ca 1229/20, NZA-RR 2022, 178 Rn.77.

arbeitgeberseitigen Geheimhaltungsinteresses sicherzustellen.[301] Die Unwirksamkeit der arbeitsvertraglichen Verschwiegenheitsklausel steht der Annahme eines berechtigten Geheimhaltungsinteresses nicht entgegen. Vielmehr ist die arbeitsvertragliche Klausel in ihrer Eigenschaft als (unwirksame) Geheimhaltungsmaßnahme in der Regel hinreichender Beleg dafür, dass ein berechtigtes unternehmerisches Interesse an dem Schutz der Information besteht. Andernfalls wäre diese nicht implementiert worden. Dies ist jedoch einzelfallbezogen zu entscheiden. Besteht die arbeitsvertragliche Treuepflicht, bleiben arbeitsrechtliche Maßnahmen im Falle eines Geheimnisverrats möglich.[302] Dagegen ist die Geltendmachung einer vereinbarten Vertragsstrafe aufgrund der Unwirksamkeit der Klausel nicht möglich, vgl. § 139 BGB.

Die Frage der Berücksichtigungsfähigkeit unwirksamer bzw. unzulässiger Maßnahmen im Rahmen des § 2 Nr. 1 lit. b) GeschGehG führt zu der Folgefrage, inwieweit der Geheimnisinhaber in der Lage ist, einen Geheimnisverrat mittels Informationen nachzuweisen, die einer unzulässigen Geheimhaltungsmaßnahme entstammen. Ein Beweisverwertungsverbot besteht, sofern mit der prozessualen Verwertung eine Grundrechtsverletzung einhergeht oder eine solche verfestigt wird.[303] Insbesondere Verstöße gegen die datenschutzrechtlichen Grundprinzipien der DS-GVO führen aufgrund ihrer Grundrechtsrelevanz regelmäßig zu der Annahme eines Beweisverwertungsverbots.[304] Informationen, die aus einer solch datenschutzrechtswidrigen Verarbeitung entstammen, können nicht in den Prozess eingebracht werden. Relevant wird dies beispielsweise, wenn der

---

[301] Die arbeitsvertragliche Treuepflicht verlangt ein für den Arbeitnehmer erkennbares und berechtigtes Geheimhaltungsinteresse des Arbeitgebers. Ist die Klausel aufgrund von Unbestimmtheit unwirksam, ist die erkennbare Geheimhaltung nicht sichergestellt.

[302] Vgl. *Reinfeld*, Das neue GeschGehG, § 1 Rn.198 f.

[303] BAG, Urteil v. 21.11.2013 - 2 AZR 797/11, NJW 2014,810; BAG, Urteil v. 21.06.2012 - 2 AZR 153/11, NZA 2012, 1027; *Thüsing*/*Pötters,* in: Compliance*,* § 11 Rn.67.

[304] BAG, Urteil v. 28.03.2019 - 8 AZR 421/17, NZA 2019, 1212.

Geheimnisinhaber seine Schutzansprüche nach §§ 6 ff. GeschGehG gerichtlich durchzusetzen versucht oder die Wirksamkeit einer Kündigung, die Gegenstand eines Kündigungsschutzprozesses ist, vom Nachweis des Geheimnisverrats abhängt.[305]

cc) Zusammenfassender Überblick

Das Merkmal der angemessenen Geheimhaltungsmaßnahmen stellt die Unternehmenspraxis vor Herausforderungen. Während sich Geheimhaltungsmaßnahmen in Bezug auf die Erkennbarkeit der Geheimhaltung vorrangig an diejenigen richten, die berechtigterweise mit der geheimen Information in Berührung kommen, stellen Zugriffsbeschränkungen sicher, dass unberechtigte Personen erst gar keinen Zugriff erhalten. Letztere können angesichts der fortschreitenden Technologien komplex und teuer sein. Insbesondere der Wandel der Zeit zwingt Unternehmen dazu, ihre Geheimnisschutzkonzepte fortlaufend zu hinterfragen und weiterzuentwickeln. Nach hiesiger Auffassung dürfen die Anforderungen an die Angemessenheit der getroffenen Geheimhaltungsmaßnahmen nicht überspannt werden. Dafür streiten insbesondere Historie, Systematik und das Telos des GeschGehG in Umsetzung der GeschGeh-RL. Das Telos stellt sicher, dass die Anforderungen an die angemessenen Geheimhaltungsmaßnahmen keine abschreckende Wirkung für den Geschäftsgeheimnisschutz entfalten. Aus dem Verhältnismäßigkeitsgrundsatz folgt wiederum, dass Unternehmen nichts Unzumutbares oder Unmögliches abverlangt werden darf. Soweit die Geltendmachung von Schutzansprüchen angesichts der getroffenen Geheimhaltungsmaßnahmen im Einzelfall unverhältnismäßig erscheint, findet dies sein Korrektiv in

[305] Bei Verstößen gegen die datenschutzrechtlichen Vorgaben drohen Arbeitgebern außerdem empfindliche Buß-geldzahlungen, Art. 83 DS-GVO. Darüber hinaus können Beseitigungs- und Unterlassungsansprüche nach §§ 12, 862, 1004 BGB (analog) sowie Schadensersatzansprüche nach §§ 241 Abs. 1, 280 Abs. 1 BGB und §§ 823 Abs. 1, 824, 826 BGB bzw. Art. 82 DS-GVO in Betracht kommen.

§ 9 Nr. 2 GeschGehG. § 2 Nr. 1 lit. b) GeschGehG und § 9 Nr. 2 GeschGehG sind daher zusammen zu verstehen.

Welche Anforderungen konkret an die angemessenen Geheimhaltungsmaßnahmen zu stellen sind, ist unternehmensbezogen anhand aller maßgebenden Umstände zu entscheiden.[306] Maßgeblich für das Vorliegen angemessener Geheimhaltungsmaßnahmen ist eine Einzelfallabwägung, bei der das Interesse des Unternehmens an der Geheimhaltung der zu schützenden Information mit dem für das Unternehmen möglichen und zumutbaren Aufwand, den das Unternehmen tatsächlich unternommen hat, um die Erkennbarkeit der Geheimhaltung zu erreichen und die Information vor unberechtigtem Zugriff zu schützen, ins Verhältnis zu setzen ist. Ein Untätigbleiben im Vertrauen darauf, die Information werde nicht entdeckt, reicht nicht aus. Ereignet sich ein Geheimnisverrat, folgt daraus nicht automatisch die Unangemessenheit des Schutzniveaus. Stattdessen entscheiden die Umstände des Einzelfalls darüber, ob das Unternehmen im Zeitpunkt des Geheimnisverrats berechtigterweise davon ausgehen durfte, die geheime Information sei hinreichend geschützt gewesen.

Rechtswidrige Geheimhaltungsmaßnahmen sind berücksichtigungsfähig, sofern dies dem Grundsatz der Verhältnismäßigkeit entspricht, vgl. § 9 Nr. 2 GeschGehG.[307] Hierzu ist anhand einer gesonderten Abwägung zu beurteilen, ob der Geheimnisinhaber im Zeitpunkt des Geheimnisverrats berechtigterweise von der Rechtmäßigkeit der

---

[306] Die Gesetzesbegründung nennt in diesem Zusammenhang zutreffend den „*Wert, die Bedeutung und die Natur des Geheimnisses, die Größe des Unternehmens*, *die Art der Kennzeichnung, die üblichen Geheimhaltungsmaßnahmen im Unternehmen und die Kosten*“ als berücksichtigungsfähige Umstände, vgl. BT-Drs. 19/4724, S. 24 f. sowie *Beyerbach*, Unternehmensinformation, S. 307-310.

[307] Berücksichtigungsfähig meint in diesem Kontext, dass die jeweiligen Maßnahmen Teil der getroffenen Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG sind, ohne dass aus deren Rechtswidrigkeit ein Anspruchsausschluss nach § 9 Nr. 2 GeschGehG droht. Ausführlicher siehe: Kapitel B) II. 3. c) bb).

Geheimhaltungsmaßnahme ausgehen durfte. Stellen anderweitige Sicherungsmaßnahmen ein angemessenes Schutzniveau sicher, kommt es auf die Berücksichtigungsfähigkeit der rechtswidrigen Maßnahme nicht an.[308] Sollte eine unwirksame arbeitsvertragliche Verschwiegenheitsklausel im Einzelfall nicht berücksichtigungsfähig sein, kann stattdessen die arbeitsvertragliche Treuepflicht des Arbeitnehmers berücksichtigungsfähig sein. Voraussetzung ist, dass die unwirksame Klausel bestimmt genug ist, die nötige Erkennbarkeit des arbeitgeberseitigen Geheimhaltungsinteresses sicherzustellen. Die datenschutzrechtliche Unzulässigkeit einer Maßnahme kann dem Nachweis eines Geheimnisverrats entgegenstehen, sofern ein Beweisverwertungsverbot in Bezug auf Informationen, die der unzulässigen Datenverarbeitung entstammen, besteht.

Der Angemessenheitsbegriff hat durch die Judikative bereits eine erste Konturierung erfahren. Bemerkenswert ist, dass die Gerichte in Teilen zu pauschalisierenden Formulierungen neigen.[309] Dies mag vor dem Hintergrund einer besseren Handhabbarkeit des Angemessenheitsbegriffs in der unternehmerischen Praxis nachvollziehbar sein. Dabei darf jedoch nicht übersehen werden, dass der Verhältnismäßigkeitsgrundsatz die Berücksichtigung aller maßgebenden Umstände des jeweiligen Einzelfalls erfordert. Es bleibt daher abzuwarten, inwieweit es der Judikative künftig gelingen wird, exakte Schlussfolgerungen auf der Grundlage von Einzelfallentscheidungen zu treffen. Eine Orientierung bieten die gefundenen Ergebnisse dieser Arbeit.

4. Geheimhaltungsmaßnahmen im Beschäftigungskontext

Die Geheimhaltungsmaßnahmen im Beschäftigungskontext sind vielgestaltig. In der Regel wird es auf eine Kombination organisatorischer, rechtlicher und technischer Maßnahmen hinauslaufen, deren Zusam-

---

[308] Vgl. ArbG Aachen, Urteil v. 13.01.2022 - 8 Ca 1229/20, NZA-RR 2022, 178 Rn.77.

[309] Siehe: Kapitel B) II. 3. c) aa) (5).

menwirken den betrieblichen Geheimnisschutz sicherstellen. Ziel ist es, im Wege der Implementierung von den Umständen nach angemessenen Geheimhaltungsmaßnahmen dafür Sorge zu tragen, dass die geheime Information dem Schutz des GeschGehG unterfällt, § 2 Nr. 1 lit. b) GeschGehG, ohne dass dieser aus Verhältnismäßigkeitsgründen droht, versagt zu bleiben, vgl. § 9 Nr. 2 GeschGehG.[310]

Welche konkreten Maßnahmen dies erfordert, ist unternehmensspezifisch anhand aller maßgebenden Umstände zu beurteilen. Maßgebliche Richtschnur ist eine Einzelfallabwägung, bei der das Interesse des Unternehmens an der Geheimhaltung der Information mit dem für das Unternehmen möglichen und zumutbaren Aufwand, den das Unternehmen tatsächlich unternommen hat, um die Erkennbarkeit der Geheimhaltung zu erreichen und die Information vor unberechtigtem Zugriff zu schützen, ins Verhältnis zu setzen ist.[311] Daraus ergeben sich insbesondere zwei relevante Zielvorgaben, anhand derer die jeweiligen Geheimhaltungsmaßnahmen auszurichten sind. Einerseits geht es darum, die Geheimhaltung der Information für diejenigen erkennbar zu machen, die mit ihr berechtigterweise in Berührung kommen. Andererseits geht es darum, die Information vor unberechtigtem Zugriff zu schützen.

Zu beachten ist, dass die arbeitsvertragliche Treuepflicht für sich genommen ungeeignet ist, die Geheimhaltung einer Information erkennbar zu machen. Dafür spricht, dass die arbeitsvertragliche Treuepflicht ihrerseits das Vorliegen eines erkennbaren berechtigten betrieblichen Interesses an der Geheimhaltung voraussetzt.[312] Darüber hinaus haben die vorherigen Erkenntnisse gezeigt, dass ein Untätigbleiben des Geheimnisinhabers im Vertrauen darauf, die Information werde nicht entdeckt, nicht ausreicht, um zu der Annahme eines

---

[310] Zur Frage der Berücksichtigungsfähigkeit rechtswidriger Maßnahmen, siehe: Kapitel B) II. 3. c) bb).

[311] Siehe: Kapitel B) II. 3. c) aa) (6).

[312] Vgl. *Holthausen*, NZA 2019, 1377, 1379; *Reinfeld*, in: Hdb-ArbR, § 30 Rn.16, 18 m. w. N.

angemessenen Schutzniveaus zu gelangen.[313] Dieses Verständnis gilt es in Bezug auf die Treuepflicht, die mit Bestehen des Arbeitsverhältnisses diesem immanent ist, zu berücksichtigen.[314] Damit eine Information unter den Schutz des GeschGehG fällt, muss der Arbeitgeber folgerichtig proaktiv Geheimhaltungsmaßnahmen implementieren, die die Erkennbarkeit der Geheimhaltung gegenüber denjenigen Arbeitnehmern sicherstellt, die üblicherweise mit der geheimen Information in Berührung kommen. Die arbeitsvertragliche Treuepflicht stellt sodann sicher, dass ein Arbeitnehmer, der mit einer erkennbar geheimen Information in Berührung kommt, zur Verschwiegenheit verpflichtet ist.

Neben arbeitsvertraglichen Sicherungsmechanismen kommen insbesondere technische und organisatorische Maßnahmen in Betracht. Diese können beispielsweise Verschwiegenheitsvereinbarungen, Wettbewerbsverbote, Rückgabepflichten, Überwachungs- und Kontrollmaßnahmen sowie Bewerberprüfungen umfassen.[315] Auch mögliche Meldepflichten der Arbeitnehmer in Bezug auf eine Liebesbeziehung zu Mitarbeitern eines Konkurrenzunternehmens können eine Sicherheitsvorkehrung sein. Befindet sich ein Arbeitnehmer mit sensibler Position in Folge der Liebesbeziehung in einem Interessenkonflikt zu seinem Arbeitgeber, hat der Arbeitgeber ein berechtigtes Interesse daran, von der Beziehung zu erfahren, §§ 241 Abs. 2, 242, 611a BGB, um dem Arbeitgeber z. B. ein anderes Aufgabengebiet zuzuweisen oder eine Versetzung in Erwägung zu ziehen. Maßgeblich sind die Umstände des jeweiligen Einzelfalls. Beispiele technischer und organisatorischer Maßnahmen sind insbesondere die Verwendung von wechselnden, komplexen Passwörtern, Zahlencodes, regelmäßige

---

313 Siehe: Kapitel B) II. 3. c).

314 Vgl. BAG, Urteil v. 03.07.2003, NZA 2004, 427, 429; BAG, Urteil v. 23.10.2008, NZA 2009, 855 Rn.23; BAG, Urteil v. 08.05.2014, NZA 2014, 1258 Rn.26. Die Treuepflicht wird aus § 242 BGB hergeleitet und ist eine Nebenpflicht des Arbeitnehmers aus dem Arbeitsvertrag, vgl. *Joussen*, in: BeckOK-ArbR, § 611a Rn.463.

315 Dazu sogleich in den folgenden Abschnitten: Kapitel B) II. 4. b) und c).

Software-Updates, Taschenkontrollen, der verschlüsselte Versand von E-Mails, Virenschutzprogramme, Einschränkungen der Downloadmöglichkeiten, Protokollierungen, Alarmanlagen, Videoüberwachung und Zugangssperren technischer und räumlicher Art. Denkbar ist ferner die Aufbewahrung sensibler Informationen in geschlossenen Räumen bzw. die Speicherung auf einem nicht mit dem Internet verbundenen Computer. Regelmäßige Schulungen tragen zusätzlich dazu bei, die Belegschaft im Umgang mit geschützten Informationen zu sensibilisieren.

Angesichts der nahezu unüberschaubaren Möglichkeiten in Bezug auf die konkrete Ausgestaltung betrieblicher Geheimnisschutzkonzepte im Beschäftigungskontext können die nachfolgenden Abschnitte lediglich beispielhaft aufzeigen, was im Rahmen der Implementierung relevanter Geheimhaltungsmaßnahmen zu beachten ist. In Teilen wird es die Untersuchung daher bei allgemeinen Ausführungen und Grundsätzen belassen.

a) Arbeitsvertragliche Sicherungsmechanismen

Arbeitsrechtliche Verschwiegenheitspflichten dienen dazu, die Geheimhaltung einer geschützten Information erkennbar zu machen. Sie richten sich in aller Regel an diejenigen, die üblicher- und berechtigterweise mit der geschützten Information in Berührung kommen. Indem sie den Geheimnischarakter der jeweiligen Information in das Bewusstsein der mit ihnen in Berührung kommenden Person rufen, wird ihnen eine psychologische Wirkung zuteil. Diese Wirkung kann durch die Aufnahme einer Vertragsstrafenregelung noch einmal verstärkt werden.[316] Eine Verschwiegenheitspflicht kann auch im Wege

[316] *Fuhlrott/Hiéramente*, DB 2019, 967, 971.

des Direktionsrechts zugewiesen werden, § 106 GewO.[317] So ist z. B. die Kennzeichnung einer Tatsache als „*vertraulich*“ auf das arbeitgeberseitige Direktionsrecht rückführbar.[318] Arbeitnehmer sind darüber hinaus in ihrer Eigenschaft als Betriebsratsmitglied oder Mitglied des Wirtschaftsausschusses zur Verschwiegenheit verpflichtet.[319] Die arbeitsvertraglichen und betriebsverfassungsrechtlichen Verschwiegenheitspflichten bestehen in diesen Fällen nebeneinander.[320] Verstößt ein Arbeitnehmer während des bestehenden Arbeitsverhältnisses gegen eine Verschwiegenheitspflicht, wird der Arbeitgeber eine außerordentliche Kündigung und ggf. die Geltendmachung einer für diese Fälle zuvor vereinbarten Vertragsstrafe in Erwägung ziehen. Ist eine vertrauliche Information zugleich ein Geschäftsgeheimnis im Sinne des GeschGehG, stehen dem Arbeitgeber zusätzlich die Schutz- und Abwehrrechte der §§ 6 ff. GeschGehG zur Verfügung.[321] Fällt eine vertrauliche Information demgegenüber nicht in den Schutzbereich

---

[317] Gerade vor dem Hintergrund, dass konkrete Schäden im Einzelfall nur schwer nachweisbar sind, empfiehlt sich für Arbeitgeber die Vereinbarung einer Vertragsstrafe. Dabei ist darauf zu achten, dass die Höhe der Vertragsstrafe den Arbeitnehmer nicht unangemessen benachteiligt. Stellt die Vertragsstrafe hinsichtlich des abgesicherten Schadens eine unzulässige Übersicherung des Arbeitgebers dar, ist die Vereinbarung nach § 307 Abs. 1 BGB bzw. § 138 Abs. 1 BGB unwirksam, vgl. *Reinfeld*, in: Hdb-ArbR, § 30 Rn.18; vgl. auch *Grüneberg*, in: Grüneberg, § 309 BGB Rn.33; *Dendorfer-Ditges*, in: Hdb-ArbR, § 35 Rn.32.

[318] *Reinfeld*, in: Hdb-ArbR, § 30 Rn.16.

[319] Vgl. §§ 79 Abs. 1, 99 Abs. 1 S. 3, 102 Abs. 2 S. 5, 107 Abs. 3 S. 4 BetrVG; *Thüsing*, in: Richardi, § 79 BetrVG Rn.3.

[320] *Niklas*, ArbRB 2020, 122.

[321] *Ohly*, GRUR 2019, 441, 445.

des GeschGehG, greifen im Übrigen die allgemeinen zivilrechtlichen Haftungsansprüche.[322]

Arbeitsvertragliche Vertraulichkeitsvereinbarungen haben insbesondere den Anforderungen des Transparenzgebots zu entsprechen und dürfen keine unangemessene Benachteiligung für den Arbeitnehmer bedeuten, § 307 Abs. 1 BGB. Dazu müssen die Vertraulichkeitsvereinbarungen die geschützten Informationen hinreichend spezifizieren.[323] Maßgeblich ist außerdem das Bestehen eines berechtigten betrieblichen Interesses, das es im Rahmen einer Einzelfallabwägung zu ermitteln gilt.[324] Eine entgeltbezogene Verschwiegenheitsklausel stellt beispielsweise in der Regel keine unangemessene Benachteiligung dar, sofern eine Offenbarung der Entgelthöhe dazu geeignet ist,

---

[322] In Betracht kommen die allgemeinen Schadensersatzansprüche nach §§ 280 Abs. 1, 241 Abs. 2, 242 BGB aus dem Arbeitsvertrag und nach §§ 823 Abs. 1 und 2, 824, 826 BGB aus deliktischer Handlung, vgl. *Fuhlrott/Hiéramente,* in: BeckOK-GeschGehG, § 2 Rn.21a; *Fuhlrott/Hiéramente*, DB 2019, 967, 968; *Dann/Markgraf,* NJW 2019, 1774, 1775. Kann der Arbeitgeber einen betriebsbezogenen Eingriff in seinen eingerichteten und ausgeübten Gewerbebetrieb nachweisen, sind auch Unterlassungsansprüche nach §§ 1004, 823 Abs. 1 BGB analog denkbar, vgl. *Herrler*, in: Grüneberg, § 1004 BGB Rn.4; *Sprau*, in: Grüneberg, § 823 BGB Rn.133. Macht der Arbeitgeber einen Schadensersatzanspruch geltend, kann er entweder seinen entgangenen Gewinn oder den vom Geheimnisbrecher erwirtschafteten Wert beanspruchen, vgl. *Reinfeld,* Das neue GeschGehG, § 4 Rn.142, 139. Alternativ kann der Arbeitgeber seinen Schaden auch im Wege einer Lizenzanalogie berechnen, vgl. BAG, Urteil v. 24.06.1986 - 3 AZR 486/84, AP BGB § 611 Betriebsgeheimnis Nr. 4. Inwieweit eine Haftungsprivilegierung des Arbeitnehmers nach den Grundsätzen des innerbetrieblichen Schadensausgleichs möglich ist, hängt im Einzelfall von der Schwere des nachweisbaren Verschuldensvorwurfs ab (§ 254 BGB analog bzw. § 242 BGB), vgl. *Griese*, in: Küttner*,* Kapitel A.3.c) Rn.12 ff. m. w. N.

[323] Begrenzende Wirkung haben insbesondere die Regelungen der §§ 134, 138, 242, 307 ff. BGB.

[324] BAG, Beschluss v. 26.02.1987 - 6 ABR 46/84, NZA 1988, 63; LAG Hamm, Urteil v. 05.10.1988 - 15 Sa 1403/88, BeckRS 1988, 6934.

den Betriebsfrieden nachhaltig zu stören.[325] Dem steht zwar entgegen, dass sich nur im Wege einer Offenlegung eine etwaige geschlechtsbezogene Lohnungleichbehandlung aufdecken lässt. Zur Auflösung dieses Interessenkonflikts hat der Gesetzgeber allerdings das Auskunftsrecht zur Überprüfung der Einhaltung des Entgeltgleichheitsgebots geschaffen. Beruft sich ein Arbeitnehmer auf sein Auskunftsrecht nach § 10 Abs. 1 EntgTranspG, werden die betrieblichen Geheimhaltungsinteressen des Arbeitgebers dahingehend berücksichtigt, dass das Auskunftsrecht vom Vorliegen mindestens sechs Vergleichspersonen des jeweils anderen Geschlechts abhängt, um etwaige Individualisierungen zu verhindern, vgl. § 12 Abs. 3 S. 2 EntgTranspG.[326] Im Übrigen bleiben entgeltbezogene Verschwiegenheitsklauseln möglich, soweit ein berechtigtes betriebliches Interesse besteht. Dies wird

---

[325] Auch eine Verschwiegenheitsvereinbarung, die sich auf eine individuell ausgehandelte Abfindungshöhe im Rahmen von Aufhebungsverträgen erstreckt, ist in aller Regel zulässig.

[326] Gemäß § 12 Abs. 3 S. 2 EntgTranspG besteht der Auskunftsanspruch nicht, wenn die Vergleichstätigkeit von weniger als sechs Beschäftigten des jeweils anderen Geschlechts ausgeübt wird. Dies dient insofern auch dem Schutz des informationellen Selbstbestimmungsrechts derjenigen Arbeitnehmer, auf die sich der Auskunftsanspruch bezieht und der Wahrung des Betriebsfriedens. Im Übrigen müssen die betrieblichen Geheimhaltungsinteressen zurücktreten. Dies gilt auch, soweit der Arbeitnehmer die Offenlegung seines Gehalts für etwaige Gehaltsverhandlungen im Rahmen eines Bewerbungsverfahrens für eine anderweitige Stelle erforderlich hält, vgl. *Roloff*, RdA 2019, 28, 40; *Reinfeld*, in: Hdb-ArbR, § 30 Rn.20. Der Arbeitnehmer ist z. B. berechtigt, gegenüber einem potenziellen Arbeitgeber sein bisheriges Gehalt als Mindestvergütung zu fordern, vgl. BAG, Urteil v. 19.05.1983 - 2 AZR 171/81, AP BGB § 123 Nr. 25. Dazu ebenfalls *Thüsing*, in: Richardi, § 94 BetrVG Rn.28 m. w. N. Möglich erscheint nach hiesiger Auffassung auch eine berechtigte Offenlegung gegenüber einem potenziellen Arbeitgeber, wenn das bisherige Gehalt ausnahmsweise Rückschlüsse auf die Eignung des Arbeitnehmers in seiner Eigenschaft als Bewerber zulässt.

sich mit Blick auf die bevorstehende Umsetzung der Lohntransparenz-Richtlinie[327] in absehbarer Zeit ändern.[328]

Besondere Relevanz erlangt die Frage der unangemessenen Benachteiligung einer arbeitsvertraglichen Verschwiegenheitsklausel, soweit diese den Schutz geheimer Informationen über das Ende des Arbeitsverhältnisses hinaus gewährleisten soll, § 307 Abs. 1 BGB. Wirksamkeitsvoraussetzung ist auch hier das Bestehen eines berechtigten betrieblichen Interesses, das im Rahmen einer Interessenabwägung anhand der maßgebenden Einzelfallumstände zu ermitteln ist.[329] Dazu ist das Geheimhaltungsinteresse des Arbeitgebers mit dem von der Berufsfreiheit geschützten Interesse des Arbeitnehmers, sein erworbenes Wissen für sein berufliches Fortkommen nutzbar zu machen (Art. 12 Abs. 1 GG), in einen angemessenen Ausgleich zu bringen.[330]

---

[327] Richtlinie des Europäischen Parlaments und des Rates zur Stärkung der Anwendung des Grundsatzes des gleichen Entgelts für Männer und Frauen bei gleicher oder gleichwertiger Arbeit durch Lohntransparenz und Durchsetzungsmechanismen (EU) 2023/970 COM (2021) 93 final.

[328] Die Lohntransparenz-RL ist bis zum 7. Juni 2026 in nationales Recht umzusetzen. Die Unzulässigkeit entgeltbezogener Verschwiegenheitsklauseln nach Art. 7 Abs. 5 Lohntransparenz-RL erstreckt sich nach hiesiger Auffassung nicht auf das Bewerbungsverfahren, weil sich Art. 2 Abs. 3 Lohntransparenz-Richtlinie ausdrücklich nur auf Art. 5 Lohntransparenz-RL bezieht. Unternehmen können daher auch weiterhin mittels entgeltbezogener Verschwiegenheitsklauseln der Gefahr entgegenwirken, dass ein vermeintlicher Bewerber das Informationsrecht (Art. 8 und EG 32 S. 4, 5 Lohntransparenz-RL) missbraucht, um an sensible Gehaltsinformationen für ein Konkurrenzunternehmen zu gelangen.

[329] §§ 138, 241 Abs. 2, 242, 307 ff. BGB. Vgl. BAG, Beschluss v. 26.02.1987 - 6 ABR 46/84, NZA 1988, 63; LAG Hamm, Urteil v. 05.10.1988 – 15 Sa 1403/88, BeckRS 1988, 6934.

[330] Vgl. *Fuhlrott/Fischer,* NZA, 2022, 809, 810. Der Arbeitnehmer kann nur insoweit einer gesonderten Geheimhaltungspflicht unterworfen werden, als er dadurch nicht unangemessen benachteiligt bzw. in seiner Berufsfreiheit nicht unzumutbar beschränkt wird. BGH, Urteil v. 03.05.2001 - I ZR 153/99, GRUR 2002, 91 zu § 17 Abs. 2 UWG a. F.; BAG, Urteil v. 15.12.1987 - 3 AZR 474/86, NZA 1988, 502; BGH, Urteil v. 21.12.1962 - I ZR 47/61, GRUR 1963, 367; *Preis*, in: ErfK-ArbR, § 611a BGB Rn.717.

Enthält eine Verschwiegenheitsvereinbarung eine sog. „*Catch-All-Klausel*“, hindert diese den Arbeitnehmer in unzumutbarer Weise an seinem beruflichen Fortkommen und ist infolgedessen unzulässig.[331] Dafür spricht, dass „*Catch-All-Klauseln*“ pauschal und ohne nähere Konkretisierung zum Stillschweigen über sämtliche Geschäftsgeheimnisse und sonstige vertrauliche Informationen verpflichten.[332]

Das ArbG Aachen führt in diesem Zusammenhang zutreffend aus: „*Eine allgemein gehaltene arbeitsvertragliche Regelung, die sich uferlos auf alle während des Arbeitsverhältnisses erhaltenen betrieblichen Informationen erstreckt (sog. Catch-all-Klausel), ist keine angemessene Geheimhaltungsmaßnahme im Sinne von § 2 Nr. 1b GeschGehG. Es bedarf hierfür vielmehr einer konkreten und transparenten Regelung*.“[333] Diese Auffassung wurde zu Recht durch das LAG Köln bestätigt.[334]

Hervorzuheben ist, dass die Unwirksamkeit einer sog. Catch-all-Klausel auch aus ihrer Intransparenz folgt. Um dem Transparenzgebot des § 307 Abs. 1 S. 2 BGB zu entsprechen, muss aus einer Verschwiegenheitsvereinbarung hinreichend hervorgehen, was im Einzelfall erlaubt und was verboten ist.[335] Nach richtiger Entscheidung des LAG Düsseldorf ist eine Klausel unwirksam, wenn sie alle Geschäftsvorgänge

---

[331] Sog. „*Catch-All-Klauseln*“ verpflichten den Arbeitnehmer, sämtliche seiner beim bisherigen Arbeitgeber erworbenen Fähigkeiten und Kenntnisse geheim zu halten, vgl. *Fuhlrott/Fischer,* NZA, 2022, 809, 812.

[332] *Fuhlrott/Fischer*, NZA, 2022, 809, 812; unter Hinweis auf: ArbG Aachen, Urteil v. 13.01.2022 - 8 Ca 1229/20, NZA-RR 2022, 178; ArbG Hamburg, Urteil v. 27.01.2022 - 4 Ca 356/20, BeckRS 2022, 4994; LAG Köln, Urteil v. 02.12.2021 - 2 SaGa 20/19, BeckRS 2019, 44850; LAG Düsseldorf, Urteil v. 03.06.2020 - 12 SaGa 4/20, MMR 2021, 181; LAG Köln BeckRS 2019, 44850; LAG Düsseldorf WRP 2020, 1509. Eine Definition inkl. Beispielkatalog soll dagegen wirksam sein, vgl. *Apel*/*Stolz* GRUR-Prax 2021, 1, 2 und LAG Baden Württemberg MMR 2022, 79; hierzu auch: *Simon*/*Vogel*, CB 2022, 172, 180.

[333] ArbG Aachen, Urteil v. 13.01.2022 - 8 Ca 1229/20, NZA-RR 2022, 178.

[334] LAG Köln, Urteil v. 28.09.2022 - 11 Sa 128/22.

[335] *Fuhlrott/Fischer*, NZA, 2022, 809, 810, 812.

erfasst, die im Rahmen der Tätigkeit bekannt werden und nicht zwischen sensiblen Informationen und solchen, die es nicht sind, differenziert.[336] Zu beachten ist außerdem, dass derartige Klauseln regelmäßig als ein faktisches nachvertragliches Wettbewerbsverbot zu werten sind, deren Unwirksamkeit sich darüber hinaus in aller Regel aus einer fehlenden Karenzentschädigung ergibt.[337] Zulässig ist hingegen eine Verschwiegenheitsvereinbarung, die dem ausscheidenden Arbeitnehmer die Veräußerung vertraulicher Kundenlisten untersagt.[338] An dieser Stelle empfiehlt sich auch eine Herausgabe- oder Vernichtungspflicht des ausscheidenden Arbeitnehmers hinsichtlich aller betrieblicher Daten. Anders als sog. Catch-All-Klauseln, sind umfassende Rückgabevereinbarungen in Bezug auf die Rückgabe der Geschäftsunterlagen bei Beendigung des Arbeitsverhältnisses zulässig.[339] Der Arbeitnehmer bleibt dann berechtigt, sein erworbenes Wissen, das auf diesen Unterlagen fußt, für sein weiteres berufliches Fortkommen zu nutzen.

---

336 LAG Düsseldorf, Urteil v. 03.06.2020, MMR 2021, 181 Rn.116. Darüber hinaus sei eine Klausel mit Blick auf Art. 12 Abs. 1 GG unwirksam, wenn sie „*ohne inhaltliche Konkretisierung in allgemeiner Art und Weise*" Geschäftsgeheimnisse zu erfassen versucht, ohne dass eine zeitliche Begrenzung vorgesehen ist, vgl. LAG Köln, Urteil v. 02.12.2019 - 2 SaGa 20/19, Beck RS 2019, 44850. Hintergrund sei, dass eine „*lebenslange Bindung*" die Berufsfreiheit unzulässig einschränke, vgl. auch LAG Köln, Urteil v. 28.09.2022 - 11 Sa 128/22; *Preis*, in: ErfK-ArbR, § 611a BGB Rn.817.

337 § 110 GewO i. V. m. § 74 Abs. 2 HGB, vgl. *Fuhlrott/Fischer,* NZA 2022, 809, 812.

338 Will der Arbeitnehmer nach Beendigung seines Arbeitsverhältnisses eine Rezeptur zur Vermarktung eines verbesserten Produktes nutzen, genießt die Berufsfreiheit des Arbeitnehmers Vorrang gegenüber dem Geheimhaltungsinteresse des bisherigen Arbeitgebers, da der Arbeitnehmer andernfalls in unzumutbarer Weise in seinem beruflichen Fortkommen gehindert wäre, so das BAG, Urteil v. 16.03.1982 - 3 AZR 83/79, NJW 1983, 134 und BAG, Urteil v. 15.12.1987 - 3 AZR 474/86, NZA 1988, 502.

339 BAG, Urteil v. 14.12.2011 - 10 AZR 283/10, ZD 2012, 385 m. Anm. *Sörup*; LAG Düsseldorf, Urteil v. 03.06.2020, MMR 2021, 181.

Zu beachten ist, dass mit der Beendigung des Arbeitsverhältnisses auch die arbeitsvertraglichen Verschwiegenheitsklauseln, die den Schutz geheimer Informationen über das Ende des Arbeitsverhältnisses hinaus gewährleisten sollen, enden. Insofern bedarf es einer Klärung, inwieweit ein ausgeschiedener Arbeitnehmer nach Beendigung des Arbeitsverhältnisses zur Verschwiegenheit über vertrauliche Informationen verpflichtet sein kann und welche Rolle arbeitsvertraglichen Klauseln zuteilwird. Zu den gesetzlich normierten Verschwiegenheitspflichten, die über die Beendigung des Arbeitsverhältnisses hinaus fortbestehen, gehören § 79 Abs. 1 S. 1 BetrVG und §§ 24 Abs. 2, 26 ArbnErfG. Inwieweit die arbeitsvertragliche Treuepflicht in Form einer sog. „*nachwirkenden Verschwiegenheitspflicht*“ fortbesteht, bedarf einer Konkretisierung.[340] Richtig ist, dass ein Arbeitnehmer nur insoweit einer nachwirkenden Verschwiegenheitspflicht unterliegen kann, als er dadurch nicht in unzumutbarer Weise in seiner Berufsfreiheit beschränkt wird.[341] Verfassungsrechtlich ergibt sich dies aus der in Art. 12 Abs. 1 GG verankerten Berufsfreiheit, die das berufliche Fortkommen des Arbeitnehmers schützt.[342] Grundsätzlich ist der Arbeitnehmer demnach frei, auf sein bei einem früheren Arbeitgeber redlich erworbenes Wissen für das eigene berufliche Fortkommen zurückzugreifen.[343] Stützt sich das erworbene Wissen allerdings auf vertrauliche Informationen des bisherigen Arbeitgebers, ist im Rahmen einer Interessenabwägung aller maßgebenden Umstände des jeweiligen Einzelfalls darüber zu entscheiden, inwieweit eine Verwertung durch den ausgeschiedenen Arbeitnehmer im Rahmen seiner neuen Tätigkeit zulässig ist. Dazu ist das Geheimhaltungsinteresse des bisherigen Arbeitgebers mit dem in der Berufsfreiheit des Arbeitnehmers verankerten Interesse, sein Wissen für das eigene berufliche Fortkommen zu verwerten, in einen angemessenen Ausgleich zu bringen.

---

340 Vgl. *Spindler*/*Veil*, in: BeckOK-GK § 116 Akt Rn.116.

341 *Reinfeld*, in: Hdb-ArbR, § 30 Rn.34 ff.

342 *Reinfeld*, in: Hdb-ArbR, § 30 Rn.34 ff.

343 BGH, Urteil v. 03.05.2001 - I ZR 153/99, GRUR 2002, 91; BAG, Urteil v. 15.06.1993 - 9 AZR 558/91, NZA 1994, 502.

Der europ. Gesetzgeber weist in Art. 1 Abs. 3 lit. b) GeschGeh-RL darauf hin, dass die Mobilität des Arbeitnehmers nicht durch eine Beschränkung der Nutzung von Erfahrungen und Fähigkeiten beeinträchtigt werden darf, die dieser im normalen Verlauf seiner Tätigkeit ehrlich erworben hat.[344] Demnach darf ein ausgeschiedener Arbeitnehmer Geschäftsgeheimnisse immer dann in zulässiger Weise im Rahmen seiner neuen Tätigkeit einsetzen, sofern diese zu seinen redlich erworbenen Erfahrungen und Fähigkeiten zählen. Das arbeitgeberseitige Geheimhaltungsinteresse tritt in diesen Fällen zurück. Ob eine vertrauliche Information zu den redlich erworbenen Erfahrungen und Fähigkeiten eines ausgeschiedenen Arbeitnehmers gehört, führt im Einzelfall zu Abgrenzungsschwierigkeiten. Kennzeichnend für die Erfahrungen und Fähigkeiten eines Arbeitnehmers ist nach hiesiger Auffassung, dass diese in der Person des Arbeitnehmers verankert sind. Dies setzt beispielsweise voraus, dass ein Abruf der vertraulichen Information ohne Weiteres, also ohne die Zuhilfenahme angefertigter Unterlagen, möglich ist.[345] Soweit ein ausgeschiedener Arbeitnehmer nach Beendigung des Arbeitsverhältnisses vertrauliche Informationen in schriftlich fixierter Weise vorhält, dürften diese demzufolge in aller Regel nicht zu dessen Erfahrungen und Fähigkeiten gehören. Die Verwertung schriftlich fixierter Informationen beruht in aller Regel nicht auf dem Erfahrungswissen des Arbeitnehmers, sondern wird erst dadurch möglich, dass der ausgeschiedene Arbeitnehmer die vertrauliche Information nach Belieben nachschlagen und in Erinnerung rufen kann. Das Geheimhaltungsinteresse des Arbeitgebers überwiegt in diesen Fällen folgerichtig regelmäßig. Dieses Ergebnis steht mit einer Entscheidung des BGH aus dem Jahre 1999 in

---

344 *Harte-Bavendamm*, in: GeschGehG, § 1 Rn.19.

345 BGH, Urteil v. 14.01.1999 - I ZR2/97, GRUR 1999, 934, 935 zu § 17 Abs. 2 UWG a. F. Sollte der Arbeitnehmer die vertraulichen Informationen im Rahmen des bisherigen Arbeitsverhältnisses allerdings nur deshalb auswendig gelernt haben, um sie dann - nach Beendigung des Arbeitsverhältnisses - gegenüber einem Konkurrenzunternehmen als seinem neuen Arbeitgeber treuwidrig offenzulegen, scheidet eine Verwertung nach den Grundsätzen von Treu und Glauben aus, § 242 BGB, vgl. *Reinfeld*, in: Hdb-ArbR, § 30 Rn.37.

Einklang.[346] Aus Sicht des BGH hänge die Frage der Verwertbarkeit maßgeblich davon ab, in welcher Form der Arbeitnehmer sein Wissen bereithalte. Soweit der Arbeitnehmer sein Wissen aus seinem Gedächtnis abrufe, unterliege er keiner Verschwiegenheitspflicht. Nutze der Arbeitnehmer hingegen vertrauliche Informationen aus schriftlichen Dokumenten oder Dateien, die er während des bisherigen Arbeitsverhältnisses angefertigt bzw. auf einem privaten Endgerät abgespeichert habe, sei deren Nutzung unbefugt.[347] Diese Ausführungen stimmen mit den zuvor entwickelten Grundsätzen überein.

Wirkt die Treuepflicht nach alledem fort, stellt die beendete arbeitsvertragliche Verschwiegenheitsklausel die notwendige Erkennbarkeit des arbeitgeberseitigen Geheimhaltungsinteresses sicher.[348] Das Ende der arbeitsvertraglichen Verschwiegenheitsklausel steht der Annahme eines berechtigten Geheimhaltungsinteresses insofern nicht entgegen. Vielmehr ist die arbeitsvertragliche Klausel Beleg dafür, dass ein berechtigtes unternehmerisches Interesse an dem Schutz der Information besteht. Andernfalls wäre diese nicht zuvor vereinbart worden. Folgerichtig zählt auch eine arbeitsvertragliche Verschwiegenheitsklausel, die die Verschwiegenheit über das Ende des Arbeitsvertrages hinaus adressiert, zu den Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG. Etwas anderes gilt, sollte die arbeitsvertragliche Verschwiegenheitsklausel aus anderen Gründen unwirksam sein, weil sie z. B. nicht hinreichend transparent genug ist. Um bestehende Rechtsunsicherheiten zu vermeiden, bietet sich der Abschluss einer gesonderten Verschwiegenheitsvereinbarung mit dem ausscheidenden Arbeitnehmer an, wobei die Vereinbarung eines nachvertraglichen Wettbewerbsverbots das höchste Maß an Rechtssicherheit

---

[346] BGH, Urteil v. 14.01.1999 - I ZR2/97, GRUR 1999, 934, 935 zu § 17 Abs. 2 UWG a. F.

[347] BGH, Urteil v. 27.04.2006 - I ZR126/03, GRUR 2006, 1044 zu 17 Abs. 2 UWG a. F.; BGH, Urteil v. 19.12.2002 - I ZR 119/00, NJW-RR 2003, 833 zu § 17 Abs. 2 UWG a. F.

[348] Die arbeitsvertragliche Treuepflicht verlangt ein für den Arbeitnehmer erkennbares und berechtigtes Geheimhaltungsinteresse des Arbeitgebers. Stellvertretend für Viele: *Joussen*, in: BeckOK-ArbR § 611a Rn.466.

bietet, allerdings auch den höchsten Wirksamkeitsanforderungen unterliegt.[349]

b) Überwachungs- und Kontrollmaßnahmen

Überwachungs- und Kontrollmaßnahmen sind ebenfalls Teil der betrieblichen Geheimnisschutzkonzepte und zählen zu den Geheimhaltungsmaßnahmen im Beschäftigungskontext, vgl. § 2 Nr. 1 lit. b) GeschGehG. Zu den verschiedenen Überwachungs- und Kontrollmaßnahmen im Bereich des Geschäftsgeheimnisschutzes gehören Überwachungsmaßnahmen, die auf die Regeltreue der Beschäftigten hinwirken sowie Maßnahmen, die eine effektive Aufarbeitung im Falle eines Geheimnisverrats gewährleisten. Darüber hinaus können auch Zugriffsbeschränkungen eine kontrollierende bzw. überwachende Wirkung entfalten. Werden beispielsweise Zugriffsbeschränkungen eingeführt, geben diese ggf. Aufschluss darüber, wo sich ein Mitarbeiter zu welcher Zeit aufgehalten hat. Welche Überwachungsmaßnahmen im Einzelnen zu implementieren sind, ist unternehmensbezogen zu entscheiden. Zu unterscheiden ist zwischen präventiven und repressiven Überwachungsmaßnahmen. Präventive Überwachungsmaßnahmen stellen beispielsweise sicher, dass Unberechtigte keinen Zugriff auf die geschützte Information haben und dienen der Kontrolle der ordnungsgemäßen Erbringung der Arbeitsleistung, um

[349] Das nachvertragliche Wettbewerbsverbot unterliegt jedoch den besonderen Wirksamkeitsvoraussetzungen nach § 110 GewO i. V. m. §§ 74 ff. HGB. Will der Arbeitgeber das Umwerben seiner Kunden durch den ausscheidenden Arbeitnehmer für die Zukunft verhindern, bedarf es daher einer entschädigungspflichtigen Wettbewerbsabrede nach § 110 GewO i. V. m. §§ 74 ff. HGB, vgl. BAG, Urteil v. 15.12.1987 - 3 AZR 474/86, NZA 1988, 502. So muss ein wirksames Wettbewerbsverbot unter anderem eine Karenzentschädigung enthalten und bedarf der Schriftform. Außerdem muss der bisherige Arbeitgeber ein berechtigtes Geheimhaltungsinteresse verfolgen, § 110 GewO i. V. m. § 74a Abs. 1 S. 1 HGB. Dagegen kann ein mit einem Geschäftsleiter vereinbartes nachvertragliches Wettbewerbsverbot lediglich einer gerichtlichen Angemessenheitskontrolle unterzogen werden, vgl. auch dazu *Reinfeld*, in: Hdb-ArbR, § 30 Rn.34 ff.

die Beschäftigten zur Regeltreue anzuhalten. Werden Überwachungsmaßnahmen zur Aufklärung eines Geheimnisverrats eingesetzt (sog. Internal Investigations), hat dies repressiven Charakter.[350] Die Aufklärung eines Geheimnisverrats dient dazu, die bestehenden Sicherheitslücken zu identifizieren und zu schließen sowie den Regelverstoß zu sanktionieren. Die daran anknüpfenden arbeitsrechtlichen Maßnahmen wie z. B. Abmahnung oder Kündigung demonstrieren Effektivität und Schlagkraft des unternehmerischen Compliance-Systems. Nicht zu unterschätzen ist in diesem Zusammenhang die abschreckende Wirkung einer Kündigung gegenüber den anderen Beschäftigten. Eine Kündigung infolge eines Geheimnisverrats wirkt daher immer auch präventiv. Aus unternehmerischer Sicht dienen Aufklärungsmaßnahmen außerdem dazu, Reputationsschäden sowie Schadensersatzforderungen Dritter entgegenzuwirken. Ist es in der Vergangenheit zu einem Geheimnisverrat gekommen, kann dies ein Beleg dafür sein, dass die bisherigen Geheimhaltungsmaßnahmen nachgeschärft werden müssen.[351] Wird bekannt, dass ein Unternehmen nicht in der Lage ist, kriminelle Handlungen seiner Beschäftigten zu erkennen, abzustellen und sodann die nötigen arbeitsrechtlichen Konsequenzen einzuleiten, kann sich dies rufschädigend für das Unternehmen auswirken.

Begrenzende Wirkung in Bezug auf Überwachungs- und Kontrollmaßnahmen im Beschäftigungskontext haben insbesondere die datenschutzrechtlichen Vorgaben. Personenbezogene Daten dürfen nur insoweit verarbeitet werden, als dies auf eine datenschutzrechtliche Legitimationsgrundlage gestützt werden kann.[352] Die Legitimationsgrundlagen im Bereich des Beschäftigungskontext enthält Art. 88 Abs. 1 DS-GVO i. V. m. § 26 BDSG. Dazu zählen

---

350 *Petri*, in: Kramer, IT-ArbRecht, § 5 Rn.163.

351 Die Geschäftsleitung eines Unternehmens ist aufgrund ihrer Pflicht zur sorgfältigen Unternehmensführung ohnehin zur fortlaufenden Prüfung o. Anpassung des Geheimnisschutzkonzeptes verpflichtet, § 93 Abs. 1 S. 1 AktG, § 43 Abs. 1 GmbHG, § 34 Abs. 1 S. 2 GenG.

352 Art. 6 DS-GVO.

beispielsweise eine Betriebsvereinbarung, vgl. Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 4 BDSG oder eine Einwilligung, vgl. § 26 Abs. 2 BDSG.[353] Letztere spielt im Beschäftigungskontext allerdings eine eher untergeordnete Rolle. Das hierarchische Machtgefälle zwischen Arbeitgeber und Arbeitnehmer steht der obligatorischen Freiwilligkeit für eine wirksame Einwilligung regelmäßig entgegen.[354] Mit Blick auf die Legitimationsgrundlage des Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 1 S. 1 BDSG muss jedoch nach der Entscheidung des EuGH von der Unionsrechtswidrigkeit des § 26 Abs. 1 S. 1 BDSG ausgegangen werden.[355] Es ist davon auszugehen, dass § 26 Abs. 1 S. 1 BDSG keine „*spezifischere Vorschrift*" im Sinne des Art. 88 Abs. 1 DS-GVO ist. Aus dem Wortlaut des Art. 88 Abs. 1 DS-GVO ergibt sich nach Auffassung des EuGH, dass spezifischere Vorschriften einen eigenen Regelungsgehalt mit Bezug zum Beschäftigungskontext aufweisen müssten, der sich von den allgemeinen Regeln der DS-GVO unterscheide, wobei die Vorgaben des Art. 88 Abs. 2 DS-GVO zwingend einzuhalten seien.[356]

Der EuGH formuliert dazu: „*So dürfen sich diese [spezifischeren] Vorschriften (...) nicht auf eine Wiederholung der Bestimmungen der*

---

353 Eine Betriebsvereinbarung bietet sich insbesondere vor dem Hintergrund des zwingenden Mitbestimmungsrechts in § 87 Abs. 1 Nr. 6 BetrVG an.

354 Art. 4 Nr. 11, Art. 7 Abs. 4, Art. 9 Abs. 2 lit. a) DS-GVO i. V. m. § 26 Abs. 2 und 3 S. 2 BDSG. Nach § 26 Abs. 2 S. 2 BDSG ist eine Einwilligung nur dann freiwillig, wenn für den Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder wenn Arbeitgeber und Arbeitnehmer mit der Datenverarbeitung gleichgelagerte Interessen verfolgen. Außerdem bietet eine Einwilligung aufgrund ihrer Widerruflichkeit unter Umständen keine dauerhafte Legitimationsgrundlage, vgl. Art. 7 Abs. 3 DS-GVO, § 26 Abs. 2 S. 4 BDSG sowie Art. 22 Abs. 1 lit. c) DS-GVO.

355 Gegenstand des Verfahrens waren die hessischen Normen § 23 Abs. 1 S. 1 HDSIG und § 86 Abs. 4 HBG, die den Vorgaben in § 23 Abs. 1 S. 1 BDSG stark ähneln. Das VG Wiesbaden hatte Zweifel an deren Vereinbarkeit mit der DS-GVO und legte die Frage dem EuGH vor, Beschluss v. 21.12.2020 - 23 K 360/20.WI.PV.

356 EuGH, Urteil v. 30.03.2023 - C-34/21, Rn.65, 71.

DS-GVO beschränken, sondern müssen auf den Schutz der Rechte und Freiheiten der Beschäftigten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext abzielen und geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen." Diese Vorgabe betont der EuGH noch einmal an anderer Stelle: „*[Es] darf (...) sich bei den auf der Grundlage von Art. 88 I DS-GVO erlassenen „spezifischeren Vorschriften" nicht lediglich um eine Wiederholung der in Art. 6 DS-GVO genannten Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten und der in Art. 5 DS-GVO angeführten Grundsätze für diese Verarbeitung oder um einen Verweis auf diese Bedingungen und Grundsätze handeln*."[357] Darüber hinaus heißt es, dass jede Verarbeitung personenbezogener Daten zum einen mit den in Art. 5 DS-GVO aufgestellten Grundsätzen im Einklang stehen und zum anderen einem der in Art. 6 DS-GVO aufgeführten Grundsätze in Bezug auf die Rechtmäßigkeit der Verarbeitung entsprechen müsse.[358]

Zu prüfen ist daher, ob § 26 Abs. 1 S. 1 BDSG lediglich den Regelungsgehalt des Art. 6 Abs. 1 S. 1 lit. b) DS-GVO wiederholt. Der direkte Vergleich zwischen Art. 6 Abs. 1 S. 1 lit. b) DS-GVO und § 26 Abs. 1 S. 1 BDSG zeigt, dass nach beiden Vorschriften Datenverarbeitungen erlaubt sind, sofern sie erforderlich sind. Insofern wiederholt § 26 Abs. 1 S. 1 BDSG die Vorgaben des Art. 6 Abs. 1 S. 1 lit. b) DS-GVO und setzt sie in den Kontext des Beschäftigungsverhältnisses.[359] Dadurch wird jedoch keine eigenständige Regelung oder Konkretisierung in Bezug auf Datenverarbeitungen im Beschäftigungskontext getroffen, die über die Regelung in Art. 6 Abs. 1 S. 1 lit. b) DS-GVO hinausgeht. Es ist daher davon auszugehen, dass die

---

[357] EuGH, Urteil v. 30.03.2023 - C-34/21, Rn.71.

[358] EuGH, Urteil v. 30.03.2023 - C-34/21, Rn.69 mit Verweis auf: EuGH, Urteil v. 22.06.2021 - C-439/19, Rn.96.

[359] Die Vorgaben des EuGH sind insofern verbindlich. Ihm obliegt die Auslegungshoheit über die DS-GVO, vgl. EuGH, Urteil v. 02.06.2022 - C-587/20, Rn.25, 26 m. w. N. = NZA 2022, 1183.

Regelung in § 26 Abs. 1 S. 1 BDSG lediglich eine Wiederholung des Art. 6 Abs. 1 S. 1 lit. b) DS-GVO darstellt und keine „*spezifischere Vorschrift*“ im Sinne des Art. 88 Abs. 2 DS-GVO ist.[360]

Rechtsfolge ist, dass § 26 Abs. 1 S. 1 BDSG unangewendet bleiben muss.[361] Andernfalls könnte dies den unmittelbaren und zwingenden Vorrang der DS-GVO verschleiern.[362] Für die Praxis ändert sich dadurch allerdings nicht viel.[363] Datenverarbeitungen sind nunmehr im selben Umfang auf Art. 6 Abs. 1 S. 1 lit. f) DS-GVO zu stützen.[364] Die unter § 26 Abs. 1 S.1 BDSG entwickelten Maßstäbe beanspruchen insofern weiterhin Geltung, wenn auch unter anderer Vorschrift.[365] Um diesem Umstand hinreichend Rechnung zu tragen, wird die vorliegende Arbeit im Folgenden Datenverarbeitungen zu Zweck-

---

360 EuGH, Urteil v. 30.03.2023 - C-34/21 Rn.65, NZA 2023, 487 - m. Anm. *Meinecke*; vgl. dazu auch: *Thüsing*/*Peisker* NZA 2023, 213, 214, gestützt auf die Schlussanträge des GA *Sánchez-Bordona* v. 22.09.2022 - C - 34/21, ECLI:EU:C:2022:710 Rn.78 = BeckRS 2022, 24515.

361 Vgl. EuGH, Urteil v. 30.03.2023 - C-34/21 Rn.82 - m. Anm. *Meinecke*; so auch: *Thüsing*/*Peisker* NZA 2023, 213, 214, gestützt auf die Schlussanträge des GA *Sánchez-Bordona* v. 22.09.2022 - C-34/21, E-CLI:EU:C:2022:710 Rn.78 = BeckRS 2022, 24515.

362 Vgl. EuGH, Urteil v. 30.03.2023 - C-34/21 Rn.81-83.

363 Zu derselben Einschätzung gelangt das Land Hessen in Bezug auf § 23 HDSIG im Rahmen seiner Handreichung zur Verarbeitung personenbezogener Daten von Beschäftigten in Reaktion auf die Entscheidung des EuGH, Urteil v. 30.03.2023 - C-34/21.

364 Bestätigt wird diese Sichtweise auch dadurch, dass § 6 Abs. 1 S. 1 lit. f) DS-GVO im Beschäftigungskontext anwendbar ist und inhaltlich nicht von § 26 Abs. 1 S. 1 BDSG abweicht. Allg. zum Verhältnis der spezifischeren Vorschriften (Art. 88 Abs. 1 DS-GVO) zu Art. 6 Abs. 1 S. 1 lit. f) DS-GVO siehe auch: *Franzen*, in: ErfK-ArbR, § 26 BDSG Rn.4, der zu der Zeit noch wie viele andere von der Unionsrechtsmäßigkeit des § 26 Abs. 1 S. 1 BDSG ausging und der Frage einer eigenständigen Anwendbarkeit des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO neben § 26 Abs. 1 S. 1 BDSG im Unternehmenskontext nachging. Art. 6 Abs. 1 S. 1 lit. b) DS-GVO kommt ebenfalls als Legitimationsgrundlage in Betracht. Diese ist jedoch auf Datenverarbeitungen zu Zwecken der „*Erfüllung*“ des Arbeitsvertrags beschränkt.

365 Vgl. BAG, Urteil v. 07.05.2019 - 1 ABR 53/17, BAGE 166, 309 Rn.42, NZA 2019, 1218 zu § 32 BDSG a. F.

en des § 26 Abs. 1 S. 1 BDSG auf die Legitimationsgrundlage des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO stützen und diese in Zusammenhang mit § 26 Abs. 1 S. 1 BDSG zitieren. War das BAG bislang davon ausgegangen, dass § 26 Abs. 1 S. 1 BDSG „*offenkundig*" unionsrechtsgemäß ist, muss es hiervon künftig Abstand nehmen.[366] Der EuGH wird mit großer Wahrscheinlichkeit zur Unionsrechtswidrigkeit des § 26 Abs. 1 S. 1 BDSG gelangen, sollte er danach gefragt werden. Der EuGH trägt insofern die Auslegungshoheit über Art. 88 Abs. 1 und 2 DS-GVO.[367]

Nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 1 BDSG) dürfen demnach personenbezogene Daten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies unter anderem für dessen Durchführung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes erforderlich ist.[368] Die Frage der datenschutzrechtlichen Zulässigkeit betrieblicher überwachungsmaßnahmen zu Zwecken des Geheimnisschutzes läuft daher auch weiterhin auf eine umfassende Interessenabwägung zwischen dem Interesse des Arbeitgebers am betrieblichen Geheimnisschutz (Art. 12 Abs. 1 und Art. 14 Abs. 1 GG) und dem Recht des von der Datenverarbeitung betroffenen Arbeitnehmers auf informationelle Selbstbestimmung (Art. 2 Abs. 1, Art. 1 Abs. 1 GG) nach Maßgabe des Verhältnismäßigkeitsgrundsatzes hinaus. Bewirkt die Überwachung eine Drucksituation, die bei objektiver Betrachtung zu einem psychischen Anpassungsdruck führt, sind die Anforderungen an die datenschutzrechtliche Zulässigkeit hoch.[369]

---

366 BAG, Urteil v. 07.05.2019 - 1 ABR 53/17, BAGE 166, 309 Rn.47 f. = NZA 2019, 1218. So auch die überwiegende Meinung im Schrifttum, § 26 Abs. 1 S. 1 BDSG, vgl. stellvertretend für viele: *Franzen*, in: ErfK-ArbR § 23 BDSG § 26 Rn.5 m. w. N.

367 EuGH, Urteil v. 02.06.2022 - C-587/20, Rn.25, 26 m. w. N. = NZA 2022, 1183.

368 Vgl. BT-Drs. 18/11325, S. 97 zu § 26 BDSG.

369 Vgl. BAG, Beschluss v. 25.04.2017 - 1 ABR 46/15, NZA 2017, 1205, Rn.20, 28 ff.; BAG, Beschluss v. 26.08.2008 - 1 ABR 16/07, NZA 2008, 1187 Rn.15; BAG, Beschluss v. 29.06.2004 - 1 ABR 21/03, NZA 2004, 1278.

Beispiele betrieblicher Maßnahmen, die einen psychischen Anpassungsdruck bewirken können, sind insbesondere Videoüberwachungssysteme, GPS-Tracker sowie Maßnahmen zur Überwachung der elektronischen Kommunikation. Erweist sich eine Überwachungsmaßnahme als datenschutzrechtlich unzulässig, kann der Verstoß ein Beweisverwertungsverbot bedingen.[370] Informationen, die einer solchen Maßnahme entstammen, können unter Umständen nicht in den Prozess eingebracht werden. Der Nachweis eines Geheimnisverrats kann also von der datenschutzrechtlichen Zulässigkeit der jeweiligen Geheimhaltungsmaßnahme abhängen.[371]

In Anbetracht der Vielgestaltigkeit der verschiedenen Kontroll- und Überwachungsmaßnahmen belässt es die vorliegende Darstellung im Folgenden bei allgemeinen Ausführungen. Sie kann hier nur beispielhaft aufzeigen, was bei der Implementierung relevanter Kontroll- und Überwachungsmaßnahmen zu beachten sein kann. Zunächst wird die Zulässigkeit präventiver Überwachungsmaßnahmen im Bereich des Geschäftsgeheimnisschutzes anhand relevanter Praxisbeispiele näher beleuchtet. Anschließend widmet sich die Darstellung der Zulässigkeit repressiver Überwachungsmaßnahmen als Teil des Geheimnisschutzkonzepts. Der Vollständigkeit halber wird überblicksartig auf die möglichen Beteiligungsrechte des Betriebsrats eingegangen. Abschließend werden die gefundenen Erkenntnisse in einem Zwischenfazit zusammengefasst.

aa) Präventive Überwachungsmaßnahmen

Präventive Überwachungsmaßnahmen im Bereich des Geheimnisschutzes wirken auf die Regeltreue der Arbeitnehmer hin. Ihr Ziel ist es, sicherzustellen, dass Unberechtigte keinen Zugriff auf die

[370] BAG, Urteil v. 27.07.2017 - 2 AZR 681/16, NZA 2017, 1327.
[371] Zur Frage des Bestehens eines Beweisverwertungsverbots siehe auch: Kapitel B) II. 3. c) bb) (2).

geschützte Information haben.[372] Darüber hinaus verhindern präventive Geheimhaltungsmaßnahmen, dass die geschützte Information den Kreis derjenigen verlässt, die berechtigterweise Kenntnis von ihr haben. Soweit ein Arbeitnehmer berechtigten Zugriff auf die geschützte Information hat, wirken präventive Kontrollmaßnahmen demgemäß darauf hin, dass der Arbeitnehmer seiner Verschwiegenheitspflicht nachkommt.

Datenschutzrechtliche Legitimationsgrundlage präventiver Überwachungsmaßnahmen wird regelmäßig Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 1 BDSG) oder eine Betriebsvereinbarung sein.[373] Nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 1 BDSG) dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies unter anderem für die Durchführung des Beschäftigungsverhältnisses nach Maßgabe des Verhältnismäßigkeitsgrundsatzes erforderlich ist.[374] In der Gesetzesbegründung zu § 26 Abs. 1 S. 1 BDSG heißt es: *„Im Rahmen der Erforderlichkeitsprüfung sind die widerstreitenden Grundrechtspositionen zur Herstellung praktischer Konkordanz abzuwägen. Dabei sind die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem Ausgleich zu bringen, der beide Interessen möglichst weitgehend*

---

[372] Zugriffsbeschränkungen können eine kontrollierende bzw. überwachende Wirkung entfalten, soweit diese z. B. Aufschluss darüber geben, wo sich ein Mitarbeiter zu welcher Zeit aufgehalten hat.

[373] Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 4 DS-GVO.

[374] Der im Rahmen des § 32 BDSG a. F. angewandte Grundsatz der Verhältnismäßigkeit gilt auch im Rahmen des § 26 Abs. 1 S. 1 BDSG, vgl. BT-Drs. 18/11325, S. 97; *Thüsing*, in: Compliance, § 3 Rn.17; *Malorny*, JuS 2022, 289, 294. Infolge der Entscheidung des EuGH zu § 23 HDSIG ist allerdings davon auszugehen, dass Datenverarbeitungen im Beschäftigungskontext nicht mehr auf § 26 Abs. 1 S. 1 BDSG, sondern jedenfalls auf Art. 6 Abs. 1 S. 1 lit. f) DS-GVO gestützt werden müssen, EuGH, Urteil v. 30.03.2023 - C-34/21. Auch dort findet eine Interessenabwägung statt, sodass die unter § 32 BDSG a. F. entwickelten Grundsätze nunmehr im Rahmen des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO Beachtung finden.

berücksichtigt."[375] Folglich ist das informationelle Selbstbestimmungsrecht der Arbeitnehmer (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) mit dem Interesse des Arbeitgebers, mittels präventiver Überwachungsmaßnahmen Geheimnisverrat vorzubeugen (Art. 12 Abs. 1 und Art. 14 Abs. 1 GG), im Wege einer praktischen Konkordanz in einen schonenden Ausgleich zu bringen.[376]

Zentrales Abwägungskriterium ist die Eingriffsintensität der Überwachungsmaßnahme. Je schwerwiegender und umfangreicher der Eingriff ist, desto höher wiegt der Persönlichkeitsschutz.[377] Die Eingriffsintensität hängt z. B. davon ab, welche Nachteile den Beschäftigten aus der Überwachungsmaßnahme drohen und ob nach Dauer und Art der Maßnahme ein psychischer Anpassungsdruck erzeugt wird. Ist im Einzelfall davon auszugehen, dass eine Maßnahme einen psychischen Anpassungsdruck erzeugt, sind die Anforderungen an die datenschutzrechtliche Legitimation hoch.[378] Auch die Streubreite einer Überwachungsmaßnahme ist zu berücksichtigen.[379] Von Bedeutung ist z. B., ob eine Kontrollmaßnahme nur stichprobenartig oder dauerhaft bzw. verdeckt oder offen erfolgt. Stehen dem Arbeitgeber mehrere Überwachungsmaßnahmen gleicher Eignung zur Verfügung, ist diejenige auszuwählen, die die Persönlichkeitsrechte der Beschäftigten am wenigsten tangiert.[380] Grundsätzlich ist eine offen durchgeführte Überwachung gegenüber einer verdeckt durchgeführten Maßnahme das mildere Mittel, obgleich verdeckte Maßnahmen im

---

375 BT-Drs. 18/11325, S. 97.

376 Der Begriff der „*Erforderlichkeit*" dient den Grundrechten als Einfallstor (sog. „*mittelbare Drittwirkung*"), vgl. BVerfG, Beschluss v. 11.04.2018 - 1 BvR 3080/09, BVerfGE 148, 267, NJW 2018, 1667, Rn.32.

377 BAG, Urteil v. 27.07.2017 - 2 AZR 681/16, NZA 2017, 1327.

378 Vgl. BAG, Beschluss v. 25.04.2017 - 1 ABR 46/15, NZA 2017, 1205, Rn.20, 28 ff.; BAG, Beschluss v. 26.08.2008 - 1 ABR 16/07, NZA 2008, 1187 Rn.15; BAG, Beschluss v. 29.06.2004 - 1 ABR 21/03, NZA 2004, 1278.

379 BVerfG, Urteil v. 11.03.2008 - 1 BvR 2074/05, 1 BvR 1254/07, NJW 2008, 1505.

380 BAG, Urteil v. 29.06.2017 - 2 AZR 597/16, NZA 2017, 1179; BAG, Urteil v. 17.11.2016 - 2 AZR 730/15, NZA 2017, 394.

Rahmen präventiver Überwachungsmaßnahmen von Vornherein ausscheiden müssen.[381] Dafür spricht, dass nur eine offene Überwachungsmaßnahme dazu geeignet ist, eine Verhaltungssteuerung herbeizuführen, wobei Einzelheiten ggf. auch verdeckt bleiben dürfen.[382] Maßgeblich sind die jeweiligen Umstände des Einzelfalls.

Entscheidet sich der Arbeitgeber zu einer Überwachung der elektronischen Kommunikation, kommt z. B. ein Zugriff auf E-Mail-Konten oder E-Mail-Logfiles, das Mithören von Telefongesprächen oder die Implementierung von Keyloggern in Betracht. In diesem Zusammenhang stellt sich die Frage, ob der Arbeitgeber dem Fernmeldegeheimnis gemäß § 3 Abs. 1 und Abs. 3 TTDSG unterliegt. Wäre dies der Fall, bliebe dem Arbeitgeber der Zugriff auf die Inhalte eines E-Mail-Kontos weitestgehend verwehrt. Entscheidend ist, ob der Arbeitgeber als Dienstanbieter bzw. Mitwirkender eines Anbieters im Sinne des § 3 Abs. 2 TTDSG anzusehen ist. Ein „*Angebot*" im Sinne des § 3 Abs. 2 TTDSG setzt seinem Wortlaut nach die Möglichkeit des Arbeitnehmers voraus, dieses anzunehmen bzw. abzulehnen.[383] In Fällen eines Privatnutzungsverbots ist der Arbeitnehmer jedoch arbeitsvertraglich zur Nutzung der Kommunikationseinrichtung verpflichtet.[384] Der Arbeitnehmer hat folgerichtig keine Wahlmöglichkeit, die Nutzung der Kommunikationseinrichtung anzunehmen oder abzulehnen. Da in Fällen eines Privatnutzungsverbots schon kein „*Angebot*" im Sinne des § 3 Abs. 2 TTDSG vorliegt, ist das Fernmeldegeheimnis (§ 3 Abs. 1 und Abs. 3 TTDSG) für den Arbeitgeber insoweit unbeachtlich.

---

381 VG Wiesbaden, Urteil v. 17.01.2022 - 6 K 1164/21.WI.

382 *Thüsing/Pötters*, in: Compliance, § 11 Rn.41; *Thüsing/Traut*, in: Compliance, § 9 Rn.65.

383 *Thüsing*, in: Compliance, § 3 Rn.63 zur Vorgängerregelung im TKG, deren Zweckrichtung weiterhin Bedeutung hat, BT-Drs. 19/27441, S. 2.

384 Der Arbeitgeber kann die Nutzung der dienstlichen IT mitbestimmungsfrei verbieten und ist nicht verpflichtet, eine private Nutzung zu erlauben, vgl. *Stück*, CCZ 2020, 77.

Damit bleibt zu klären, wie dies in Fällen der erlaubten Privatnutzung zu beurteilen ist. Diese Frage war bereits vor Inkrafttreten des TTDSG am 1. Dezember 2021 unter der vormaligen Regelung in § 88 Abs. 2 TKG a. F. Streitthema.[385] Diese Regelung wurde nun in § 3 TTDSG überführt.[386] Der Streit, ob der Arbeitgeber als Dienstanbieter bzw. Mitwirkender eines Anbieters im Falle der erlaubten Privatnutzung zu qualifizieren ist, besteht damit unverändert fort. Zuletzt hatte sich unter § 88 Abs. 2 TKG a. F. ein Verständnis herausgebildet, dass der Arbeitgeber in Fällen der erlaubten Privatnutzung nicht als Dienstanbieter zu qualifizieren sei.[387] Zu Recht wurde darauf hingewiesen, dass ein geschäftsmäßiges Angebot voraussetze, dass dieses an Dritte, die außerhalb der Sphäre des Arbeitgebers stehen, gerichtet sein müsse. Übertragen auf den Beschäftigungskontext ist festzuhalten, dass der Arbeitnehmer der Sphäre des Arbeitgebers angehört, weshalb die erlaubte Privatnutzung auch unter der Neuregelung des § 3 Abs. 2 Nr. 2 TTDSG kein geschäftsmäßiges Angebot eines Telekommunikationsdienstes darstellen kann. Dafür spricht auch das Telos des TTDSG. Nach seinem Sinn und Zweck soll das TTDSG den Wettbewerb im Bereich der Telekommunikation gewährleisten und ein ausreichendes und angemessenes Angebot von Dienstleistungen sicherstellen.[388] Der Arbeitgeber tritt in Fällen der erlaubten Privatnutzung jedoch nicht als Wettbewerber am Markt auf. Es geht ihm lediglich darum, seinen Mitarbeitern zur Erhöhung der eigenen Arbeitgeberattraktivität, eine kostenfreie Zusatzleistung zu gewähren. Insofern liegt der Schluss nahe, dass das TTDSG für den Arbeitgeber in Fällen der erlaubten Privatnutzung keine Anwendung findet.

Darüber hinaus folgt aus § 257 Abs. 1 Nr. 2 und Nr. 3 HGB, dass der Arbeitgeber in seiner Eigenschaft als Kaufmann Zugriff auf die

---

385 Ausführlich zum damaligen Streitstand: *Thüsing*, in: Compliance, § 3 Rn.74.

386 BT-Drs. 19/27441, S. 2.

387 *Wünschelbaum*, NJW 2022, 1561; *Thüsing*, in: Compliance, § 3 Rn.74.

388 *Thüsing*, in: Compliance, § 3 Rn.63 zur Vorgängerregelung im TKG, deren Zweckrichtung weiterhin Bedeutung hat, BT-Drs. 19/27441, S. 2.

betriebliche Korrespondenz haben muss. Nur so kann der Arbeitgeber im Einzelfall beurteilen, ob es sich um aufbewahrungspflichtige Handelsbriefe handelt, zu denen auch elektronisch versandte E-Mails zählen.[389] Wäre der Arbeitgeber jedoch als Dienstanbieter bzw. Mitwirkender eines Anbieters im Sinne des § 3 Abs. 2 TTDSG zu qualifizieren, würde das Fernmeldegeheimnis einen solchen Zugriff weitestgehend unmöglich machen. Ähnliches folgt auch aus der Aufbewahrungspflicht aus § 147 AO. Im Ergebnis sprechen daher überzeugende Gründe dafür, den Arbeitgeber auch in Fällen der erlaubten Privatnutzung nicht als Dienstanbieter bzw. Mitwirkenden eines Anbieters im Sinne des § 3 Abs. 2 TTDSG zu qualifizieren. Folgerichtig ist das Fernmeldegeheimnis für den Arbeitgeber unbeachtlich. Dies gilt sowohl für Fälle eines Privatnutzungsverbotes als auch für Fälle einer erlaubten Privatnutzung.

Die datenschutzrechtliche Zulässigkeit der Überwachung der elektronischen Kommunikation ist daher ausschließlich anhand des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 1 BDSG) zu beurteilen. Danach ist der Zugriff auf einen ausschließlich dienstlich geführten E-Mail-Account in aller Regel zulässig.[390] Im Übrigen ist der Arbeitnehmer aus Verhältnismäßigkeitsgründen anzuweisen, private und dienstliche E-Mails getrennt voneinander zu organisieren bzw. die privaten E-Mails als privat zu kennzeichnen, ehe der Arbeitgeber tatsächlich darauf zugreift. Kommt der Arbeitnehmer dem nicht nach, kann der Arbeitgeber diese Unterscheidung selbst vornehmen,

---

389 Eine Verletzung des Briefgeheimnisses (§ 202 StGB) liegt nur vor, wenn an den Beschäftigten adressierte Post mit der Kennzeichnung „*persönlich*/*vertraulich*“ unerlaubt geöffnet wird, vgl. LAG Hamm, Urteil v. 19.02.2003 - 14 Sa 1972/02, NZA-RR 2003, 346; *Stück,* CCZ 2020, 77, 82.

390 BAG, Urteil v. 15.08.2002 - 2 AZR 214/01, NZA 2003, 432; LAG Hessen, Urteil v. 21.09.2018 - 10 Sa 601/18, NZA-RR 2019, 130 Rn.82; vgl. LAG Berlin-Brandenburg, Urteil v. 16.02.2011 - 4 Sa 2132/10, NZA-RR 2011, 342, 344; *Traut*, in: Compliance, § 9 Rn.834, 35 m. w. N.

beispielsweise anhand der Betreffzeile.[391] Einer Einwilligung des Arbeitnehmers bedarf es dafür nicht.[392] Andernfalls könnten Arbeitnehmer durch die Verweigerung ihrer Einwilligung über die Zugriffsmöglichkeiten des Arbeitgebers entscheiden. Dies kann u. a. vor dem Hintergrund der Aufbewahrungspflichten in § 257 Abs. 1 Nr. 2 und Nr. 3 HGB bzw. § 147 AO nicht überzeugen. Aus Verhältnismäßigkeitsgründen kann es sich anbieten, den Zugriff lediglich stichprobenartig oder im Wege einer Stichwortsuche in Bezug auf zufällig ausgewählte E-Mail-Konten durchzuführen.

Greift der Arbeitgeber auf Big Data Analyse-Techniken zurück, treffen diese nicht nur über den Inhalt einer E-Mail Aussagen, sondern sind darüber hinaus auch dazu in der Lage, weitere Zusammenhänge sichtbar zu machen.[393] Für Arbeitnehmer geht die Anwendung von Big Data Analyse-Techniken daher regelmäßig mit der Gefahr einer unzulässigen Totalüberwachung ihres Arbeitsverhaltens einher. Maßgeblich bleiben jedoch stets die Umstände des jeweiligen Einzelfalls. Der Einsatz eines Keylogger-Systems bietet sich z. B. an, um zu kontrollieren, ob geschützte Informationen über die dienstlichen IT-Einrichtungen an Dritte weitergegeben werden.

Entscheidet sich der Arbeitgeber für den Einsatz eines Keylogger-Systems, kann dies unter Umständen einen psychischen Anpassungsdruck auslösen.[394] Aus Gründen der Verhältnismäßigkeit sind Keylogger-Systeme zu präventiven Zwecken daher allenfalls stichprobenartig und nur in Bezug auf zufällig ausgewählte Beschäftigte möglich.[395]

---

391 Vgl. LAG Berlin-Brandenburg, Urteil v. 16.02.2011 - 4 Sa 2132/10, NZA-RR 2011, 342, 344.

392 A. A.: LAG Hessen, Urteil v. 21.09.2018 - 10 Sa 601/18, NZA-RR 2019, 130 Rn.82.

393 *Traut*, in: Compliance, § 9 Rn.8, 9.

394 Keylogger-Systeme sind nur in engen datenschutzrechtlichen Grenzen zulässig, vgl. BAG, Urteil v. 27.07.2017 - 2 AZR 681/16, NZA 2017, 1327. Auch die Beteiligungsrechte des Betriebsrats sind zu beachten, vgl. §§ 80, 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG.

395 BAG, Urteil v. 27.07.2017 - 2 AZR 681/16, NZA 2017, 1327.

War der Keylogger-Einsatz datenschutzrechtlich unzulässig, kann aus dem Verstoß gegen das informationelle Selbstbestimmungsrecht des Arbeitnehmers ein Verwertungsverbot in Bezug auf die (Auswertungs-) Daten resultieren, vgl. Art. 1 Abs. 3 GG.[396] Die datenschutzrechtliche Zulässigkeit kann damit Voraussetzung für den Nachweis eines Geheimnisverrats sein.[397]

Auf Gesprächsinhalte darf der Arbeitgeber nur ausnahmsweise zurückgreifen. Das Recht am gesprochenen Wort (Art. 2 Abs. 1, Art. 1 Abs. 1 GG) erfordert in der Regel die Einwilligung des Arbeitnehmers.[398] Zulässig ist die Auswertung von E-Mail-Logfiles oder Telefonverbindungsdaten. Auch hier kann es sich aus Verhältnismäßigkeitsgründen anbieten, den Zugriff lediglich stichprobenartig und in Bezug auf zufällig ausgewählte Beschäftigte durchzuführen. Eine vorübergehende Speicherung und stichprobenartige Kontrolle der Verlaufsdaten eines Internetbrowsers ist regelmäßig zulässig.[399]

Zieht der Arbeitgeber eine Videoüberwachungsmaßnahme in Erwägung, ist zunächst festzustellen, dass § 4 Abs. 1 S. 1 Nr. 2 und Nr. 3 BDSG für Videoüberwachungen im Beschäftigungskontext unbeachtlich ist.[400] Datenverarbeitungen aufgrund eines berechtigten Interesses im Beschäftigungskontext werden durch Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 1 BDSG) legitimiert.[401] Insofern fehlt

---

396 BAG, Urteil v. 27.07.2017 - 2 AZR 681/16, NZA 2017, 1327.

397 Zu der Frage eines Beweisverwertungsverbots datenschutzrechtswidrig erhobener Informationen siehe: Kapitel B) II. 3. c) (2).

398 Vgl. *Thüsing/Traut*, in: Compliance, § 10 Rn.2.

399 Vgl. LAG Berlin-Brandenburg, Urteil v. 14.01.2016 - 5 Sa 657/15, ArbRAktuell 2016, 172.

400 Nach § 4 Abs. 1 S. 1 Nr. 1 bis 3 BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen (Nr. 1), zur Wahrnehmung des Hausrechts (Nr. 2) oder zur Wahrnehmung berechtigter Interessen (Nr. 3) für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen.

401 *Wilhelm-Robertson,* in: BeckOK-DatenschutzR, § 4 BDSG, Rn.19.

es an der für § 4 Abs. 1 S. 1 Nr. 2 und Nr. 3 BDSG nötigen Öffnungsklausel.[402] Der deutsche Gesetzgeber hat für Datenverarbeitungen im Beschäftigungskontext von der Öffnungsklausel in Art. 88 Abs. 1 DS-GVO Gebrauch gemacht und diese in § 26 BDSG geregelt - nicht jedoch in § 4 BDSG.[403] Dieses Verständnis hat das BAG insoweit bestätigt, als es zu Recht darauf hinweist, dass es wenig plausibel erscheine, wenn bezogen auf den Datenschutz von Arbeitnehmern, die in öffentlich zugänglichen Räumen arbeiten, andere Maßstäbe gelten sollten, als für Arbeitnehmer, die dies nicht tun.[404] Dem steht nicht entgegen, dass § 26 Abs. 1 S. 1 BDSG nach hiesiger Auffassung unangewendet bleiben muss.[405] Der Gesetzgeber hat mit der Schaffung des § 26 Abs. 1 S. 1 BDSG deutlich zum Ausdruck gebracht, dass sich Datenverarbeitungen im Beschäftigungskontext nicht an § 4 Abs. 1 S. 1 Nr. 2 und Nr. 3 BDSG auszurichten haben.[406] Dass Datenverarbeitungen im Beschäftigungskontext nunmehr auf Art. 6 Abs. 1 S. 1 lit. f) DS-GVO gestützt werden müssen, ist Folge der EuGH-Rechtsprechung zu einer mit § 26 Abs. 1 S. 1 BDSG im Wesentlichen inhaltsgleichen Regelung.[407] Die Intention des nationalen Gesetzgebers, Datenverarbeitungen im Beschäftigungskontext nicht über § 4 Abs. 1 S. 1 Nr. 2 und Nr. 3 BDSG zu regeln, hat sich in Folge der

---

402 Vgl. *Pötters*, in: Compliance, § 11 Rn.28 m. w. N. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) geht davon aus, dass die Anwendbarkeit des § 4 BDSG stets einzelfallbezogen zu prüfen ist, vgl. DSK, Kurzpapier Nr. 15, 1; bestätigt durch BVerwG, NVwZ, 2019, 1126, 1131.

403 Vgl. BT-Drs. 18/11325, S. 96.

404 Vgl. BAG, Urteil v. 22.09.2016 - 2 AZR 848/15, NZA 2017, 112, 116 zu § 32 Abs. 1 BDSG a. F. Infolge der Entscheidung des EuGH zu § 23 HDSIG ist davon auszugehen, dass Datenverarbeitungen im Beschäftigungskontext jedenfalls auf Art. 6 Abs. 1 lit. f) DS-GVO zu stützen sind, vgl. EuGH, Urteil v. 30.03.2023 - C-34/21. Auch dort findet eine Interessenabwägung statt, sodass die unter § 32 BDSG a. F. entwickelten Grundsätze nunmehr im Rahmen des Art. 6 Abs. 1 lit. f) DS-GVO Beachtung finden.

405 Siehe: Kapitel B) II. 4. b).

406 Vgl. BT-Drs. 18/11325, S. 97.

407 EuGH, Urteil v. 30.03.2023 - C-34/21.

EuGH-Entscheidung nicht verändert. Die Legitimation einer Datenverarbeitung aufgrund eines berechtigten Interesses im Beschäftigungskontext erfolgt daher nach wie vor ausschließlich über Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 1 BDSG).[408]

Nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 1 BDSG) dürfen personenbezogene Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses im Rahmen einer Videoüberwachung verarbeitet werden, wenn dies unter anderem für die Durchführung des Beschäftigungsverhältnisses nach Maßgabe des Verhältnismäßigkeitsgrundsatzes erforderlich ist.[409] Die Eingriffsintensität hängt insbesondere von der Art des Kameraeinsatzes und den weiteren Funktionsweisen der Kamera wie z. B. Tonaufzeichnungen ab. Eine Kamera, die regelmäßig sich selbst überschreibende Standbilder ohne Zoomfunktion anfertigt, greift z. B. nicht so tief in die Persönlichkeitsrechte der Beschäftigten ein, wie eine hochauflösende Kamera mit Zoomfunktion.[410]

Unzulässig und mitunter strafbewehrt (§ 201 StGB) sind insbesondere Videoüberwachungen, die die Intimsphäre des Arbeitnehmers tangieren. Videoaufnahmen der Sanitäranlagen oder Umkleideräume betreffen den „*Kernbereich privater Lebensgestaltung*“ und sind unter keinen Umständen möglich.[411] Bewirken Kameraeinsätze eine psychische Drucksituation, ist die Überwachung regelmäßig unzulässig. Maßgeblich sind die Umstände des jeweiligen Einzelfalls. Zu erwägen ist auch, ob mildere Mittel eine ebenso verhaltens- steuernde Wirkung haben. Möglich sind z. B. Kamera-Attrappen. Entscheidet sich der Arbeitgeber, Videoaufnahmen in Form einer sog. Live-Cam online zu

---

408 Vgl. BAG RDV 2003, 293; ArbG Ludwigshafen RDV 2004, 179; ArbG Düsseldorf RDV 2004, 225; *Bayreuther,* NZA 2005, 1038.

409 Vgl. BT-Drs. 18/11325, S. 97.

410 LAG-Schleswig-Holstein, Beschluss v. 29.08.2013 - 5 TaBV 6/13, NZA-RR 2013, 577; *Pötters*, in: Compliance, § 11 Rn.37.

411 BVerfG, Urteile v. 03.03.2004 - 1 BvR 2378/98 und BvR 1084/99109, NJW 2004, 999.

stellen, bedarf dies einer zusätzlichen Einwilligung des Arbeitnehmers nach § 22 S. 1 KunstUrhG.[412]

bb) Maßnahmen zu repressiven Zwecken

Werden Überwachungsmaßnahmen zur Aufklärung eines Geheimnisverrats eingesetzt (sog. Internal Investigations), hat dies repressiven Charakter. Die Aufklärung eines Geheimnisverrats dient dazu, die bestehenden Sicherheitslücken zu identifizieren und zu schließen sowie den Regelverstoß zu sanktionieren.[413] Dabei ist die außerordentliche Kündigung des Geheimnisverräters nicht nur arbeitsrechtliches Sanktionsmittel, sondern aufgrund ihrer abschreckenden Wirkung zugleich ein geeignetes Mittel, andere Arbeitnehmer auf die besondere Bedeutung der Einhaltung ihrer Verschwiegenheitspflicht aufmerksam zu machen (präventives Element).[414] Datenschutzrechtliche Legitimationsgrundlage repressiver Überwachungsmaßnahmen wird in aller Regel Art. 6 Abs. 1 S. 1 lit. f) DS-GVO sein. Zwar ist davon auszugehen, dass § 26 Abs. 1 S. 2 BDSG, anders als § 26 Abs. 1 S. 1 BDSG,[415] einen eigenen Regelungsgegenstand enthält und damit eine im Vergleich zu Art. 6 Abs 1 S. 1 lit. b) DS-GVO bzw. Art. 6 Abs. 1 S. 1 lit. f) DS-GVO spezifischere Vorschrift im Sinne des Art. 88 Abs. 1 DS-GVO darstellt. Allerdings bestehen nach hiesiger Auffassung Zweifel, ob § 26 Abs. 1 S. 2, Abs. 5 BDSG den Vorgaben des Art. 88 Abs. 2 DS-GVO gerecht wird.[416]

---

412 *Thüsing/Pötters*, in: Compliance, § 11 Rn.35.

413 Arbeitsrechtliche Sanktionsmittel sind aufgrund ihrer abschreckenden Wirkung zugleich ein geeignetes Mittel, andere Arbeitnehmer auf die Bedeutung ihrer eigenen Regeltreue aufmerksam zu machen.

414 Ein Geschäftsgeheimnisverrat sowie der dringende Verdacht eines solchen können wichtige Gründe im Sinne des § 626 Abs. 1 BGB sein, vgl. LAG Köln, Urteil v. 17.08.2001 - 11 Sa 484/00, BeckRS 2001, 30792860; *Fuhlrott/Hiéramente,* DB 2019, 967, 970.

415 Zur Unanwendbarkeit des § 26 Abs. 1 S. 1 BDSG: Kapitel B) II. 4. b).

416 Vgl. EuGH, Urteil v. 30.03.2023 - C-34/21 Rn.71, 74.

Nach Art. 88 Abs. 2 DS-GVO sind geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der von der Datenverarbeitung betroffenen Person in die spezifischere Rechtsvorschrift aufzunehmen.[417] Daraus folgt, dass Rechtsvorschriften, die spezifische Datenverarbeitungen im Beschäftigungskontext regeln, mittels eigener Vorgaben sicherstellen müssen, dass die Rechte der von der Datenverarbeitung betroffenen Person gewahrt bleiben.[418] Dies gilt insbesondere in den Fällen, in denen eine spezifischere Vorschrift zugleich eine Beschränkung der Betroffenenrechte Art. 12 ff. DS-GVO darstellt. Ist dies der Fall, muss die spezifischere Vorschrift mittels eigener Vorgaben sicherstellen, dass die von der Datenverarbeitung betroffene Person - dem Telos des Grundsatzes auf Datentransparenz entsprechend - hinreichend in die Lage versetzt wird, die Rechtmäßigkeit der Datenverarbeitung zu prüfen, um diese ggf. durchsetzen zu können.[419] Insbesondere im Hinblick auf verdeckte Überwachungsmaßnahmen, die nach § 26 Abs.1 S. 2 BDSG grundsätzlich möglich sind, drängt sich nach alledem das Erfordernis weiterer Vorgaben auf, die den Grundsatz der Datentransparenz hinreichend sicherstellen. Möglich wäre beispielsweise ein gegenüber Art. 13 DS-GVO zeitlich verzögertes Informationsrecht nach dem Vorbild des Art. 23 Abs. 1 lit. j) DS-GVO i. V. m. § 32 Abs. 3 BDSG.

Zu beachten ist, dass verdeckt durchgeführte Maßnahmen nur dann verdeckt sind, wenn sie keine Informationspflicht des datenschutzrechtlich Verantwortlichen zum Zeitpunkt der Datenverarbeitung auslösen, vgl. Art. 13 DS-GVO. Das BAG hat in diesem Zusammenhang zu Recht darauf hingewiesen, dass „*die Aufdeckung strafbaren*

---

417 EuGH, Urteil v. 30.03.2023 - C-34/21, Rn.65.

418 Die Grundsätze der Datenverarbeitung sind im Sinne eines Mindestschutzes zu verstehen, der zwingend gewahrt bleiben muss, vgl. EuGH, Urteil v. 30.03.2023 - C-34/21 Rn.71, 74. Zum damaligen Streitstand, ob spezifischere Vorschriften die DS-GVO beschränken können oder die DS-GVO eine vollharmonisierende Wirkung hat, siehe: Kapitel C) I. 3. c) bb) (1) (c), dort: Fn.813.

419 Zum Telos der Datentransparenz siehe auch: Kapitel C, II. 1.

Verhaltens bereits seiner Natur nach auf Heimlichkeit angelegt ist".[420] Da jedoch kein Ausnahmetatbestand in Fällen einer repressiven Überwachungsmaßnahme ersichtlich ist,[421] haben sich im Schrifttum verschiedene Überlegungen herausgebildet, um zur Entbehrlichkeit der Informationspflicht zu gelangen.[422] Diskutiert wird z. B. eine analoge Anwendung des Art. 14 Abs. 5 lit. b) DS-GVO oder des § 33 Abs. 1 Nr. 2a BDSG in Fällen einer verdeckt durchgeführten Videoüberwachung.[423] Teilweise wird auch überlegt, eine Ausnahmeregelung in § 26 Abs. 1 S. 2 BDSG hineinzulesen.[424] Die Entbehrlichkeit der Informationspflicht ergebe sich bereits aus der Zulässigkeit der verdeckt durchgeführten Datenverarbeitung, wobei der Grundsatz der Verhältnismäßigkeit stets zu wahren sei.[425] Eben diese Überlegungen sind Beleg dafür, dass der Grundsatz der Datentransparenz im Rahmen des § 26 Abs. 1 S. 2 BDSG unzureichend sichergestellt ist.

Der nationale Gesetzgeber hat sich mit § 26 Abs. 5 BDSG für eine Regelung entschieden, die den Regelungsauftrag hinsichtlich der Wahrung des Grundsatzes der Datentransparenz an den datenschutzrechtlich Verantwortlichen lediglich weiterreicht. Dies genügt nach hiesiger Auffassung den Anforderungen des Art. 88 Abs. 2 DS-GVO

---

420 BAG, Urteil v. 20.10.2016 - 2 AZR 395/15, NZA 2017, 443, 446.

421 Solange nicht sicher feststeht, durch wen der Geheimnisverrat begangen worden ist, kann die Ausnahme der Informationspflicht nach § 32 Abs. 1 Nr. 4, Abs. 3 BDSG bereits dem Wortlaut nach nicht einschlägig sein. Die Geltendmachung oder Ausübung rechtlicher Ansprüche setzt voraus, dass der Anspruchsgegner hinreichend individualisiert ist, vgl. *Golla*, in: Kühling/Buchner, §32 BDSG Rn.18; *Hennemann*, in: Paal/Pauly, § 32 BDSG Rn.19; *Eßer*, in: Auernhammer, § 32 BDSG Rn.22.

422 *Pötters*, in: Compliance, § 11 Rn.55; *Byers*, NZA 2017, 1086, 1089, 1090.

423 Vgl. BAG, Urteil v. 22.10.2016 - 2 AZR 395/95, NZA 2017, 443 Rn.29; kritisch und das Meinungsspektrum aufzeigend: *Thüsing/Pötters*, in: Compliance, § 11 Rn.55.

424 *Kort,* RdA 2018, 24, 27; in diese Richtung wohl auch *Bäcker*, in: Kühling/Buchner, DS-GVO Art. 13 Rn.14.

425 *Byers*, NZA 2017, 1086, 1090.

nicht. Vor dem Hintergrund des eindeutigen Wortlauts in Art. 88 Abs. 2 DS-GVO, wonach die spezifischere Vorschrift selbst die jeweiligen Maßnahmen zur Wahrung der Datentransparenz festlegen muss, kann der deutsche Gesetzgeber seinen Regelungsauftrag nicht ohne Weiteres an den datenschutz- rechtlich Verantwortlichen delegieren. Mag dies in Fällen denkbar sein, in denen die spezifischere Vorschrift keine Beschränkung der Betroffenenrechte nach sich zieht, weil die allgemeinen Vorgaben der DS-GVO ohnehin uneingeschränkt Anwendung finden, so genügt dies jedenfalls im Fall einer Beschränkung der Betroffenenrechte nicht.[426] Der nationale Gesetzgeber muss den an ihn gerichteten Regelungsauftrag in Art. 88 Abs. 2 DS-GVO im Rahmen der spezifischeren Vorschrift selbst wahrnehmen und für die nötige Datentransparenz im Sinne des Art. 5 Abs. 1 lit. a) DS-GVO sorgen.[427] Erwägungsgrund 8 der DS-GVO erlaubt zwar die Übernahme von Teilen der Verordnung; dies jedoch mit der Maßgabe, dass es sich um Präzisierungen handeln muss. Die nahezu wortgleiche Delegation des verordnungsunmittelbaren Regelungsauftrags stellt jedoch keine Präzisierung der DS-GVO mehr dar.

Nach hiesiger Auffassung ist daher davon auszugehen, dass § 26 Abs. 1 S. 2 BDSG die in Art. 88 Abs. 2 DS-GVO vorgegebenen Voraussetzungen einer spezifischeren Vorschrift nicht erfüllt und

---

[426] In diese Richtung auch: *Thüsing*/*Peisker*, die in diesem Zusammenhang zu Recht in Bezug auf Betriebsvereinbarungen fragen, ob immer explizite Vorgaben nötig seien, vgl. *Thüsing*/*Peisker*, NZA 2023, 213, 214. Nach hiesiger Auffassung sind explizite Vorgaben zumindest bezüglich der Datentransparenz nötig, soweit die spezifischere Vorschrift eine Beschränkung der Betroffenenrechte, respektive des Transparenzgrundsatzes darstellt, vgl. Art. 5 Abs. 1 lit. a) DS-GVO, Art. 12 ff. DS-GVO. Im Übrigen stellen die ohnehin zu beachtenden Betroffenenrechte in Art. 12 ff. DS-GVO den Grundsatz der Datentransparenz sicher. Diese repetitiv zu wiederholen, erscheint auch nach hiesiger Auffassung nicht sachgerecht. Sinnvoll bleibt dagegen eine Bezugnahme in Form eines Hinweises, z. B. im Rahmen der Gesetzesbegründung oder einer Betriebsvereinbarung.

[427] Vgl. EuGH, Urteil v. 30.03.2023 - C-34/21, Rn.65.

infolgedessen unangewendet bleiben muss.[428] Für die Praxis ändert sich dadurch nicht viel.[429] Datenverarbeitungen sind im selben Umfang auf Art. 6 Abs. 1 S. 1 lit. f) DS-GVO zu stützen.[430] Die unter § 26 Abs. 1 S. 2 BDSG entwickelten Maßstäbe beanspruchen insofern weiterhin Geltung, wenn auch unter anderer Vorschrift. Dafür spricht, dass sowohl § 26 Abs. 1 S. 2 BDSG als auch Art. 6 Abs. 1 S. 1 lit. f) DS-GVO die Zulässigkeit der Datenverarbeitung von einer Interessenabwägung abhängig machen, die dem Grundsatz der Verhältnismäßigkeit unterliegt.[431] Insofern sind keine abweichenden Ergebnisse unter Art. 6 Abs. 1 S. 1 lit. f) DS-GVO zu erwarten. Anders sieht dies jedoch mit Blick auf verdeckt durchgeführte Überwachungsmaßnahmen aus - dazu sogleich.

Die vorliegende Arbeit wird Datenverarbeitungen zu Zwecken des § 26 Abs. 1 S. 2 BDSG im Folgenden auf die Legitimationsgrundlage des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO stützen und diese in Zusammenhang mit § 26 Abs. 1 S. 2 BDSG zitieren. Es bleibt abzuwarten, ob auch der EuGH zur Unionsrechtswidrigkeit des § 26 Abs. 1 S. 2 BDSG

---

428 EuGH, Urteil v. 30.03.2023 - C-34/21, Rn.65, 82. In die entgegengesetzte Richtung tendierend: *Thüsing*/*Peisker*, NZA 2023, 213, 215, die davon ausgehen, dass § 26 Abs. 1 S. 2 BDSG weiterhin Anwendung finden dürfte.

429 Zu derselben Einschätzung gelangt das Land Hessen in Bezug auf § 23 HDSIG im Rahmen seiner Handreichung zur Verarbeitung personenbezogener Daten von Beschäftigten in Reaktion auf die Entscheidung des EuGH, Urteil v. 30.03.2023 - C-34/21.

430 Bestätigt wird diese Sichtweise dadurch, dass Art. 6 Abs. 1 S. 1 lit. f) DS-GVO im Beschäftigungskontext anwendbar ist und inhaltlich nicht von § 26 Abs. 1 S. 1 BDSG abweicht. Allg. zum Verhältnis der spezifischeren Vorschriften (Art. 88 Abs. 1 DS-GVO) zu Art. 6 Abs. 1 S. 1 lit. f) DS-GVO: *Franzen*, in: ErfK-ArbR, § 26 BDSG Rn.4, der zu der Zeit noch wie viele andere von der Unionsrechtsmäßigkeit des § 26 Abs. 1 S. 1 BDSG ausging und der Frage einer eigenständigen Anwendbarkeit des Art. 6 Abs. 1 S 1 lit. f) DS-GVO neben § 26 Abs. 1 S. 1 BDSG im Unternehmenskontext nachging.

431 BAG, Urteil v. 07.05.2019 - 1 ABR 53/17, BAGE 166, 309 Rn.42, NZA 2019, 1218; BAG, Urteil v. 27.07.2017 - 2 AZR 681/16, jeweils zu § 32 BDSG a. F.

gelangen wird, sollte er danach gefragt werden. Der EuGH trägt die Auslegungshoheit über die DS-GVO.[432]

Nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 2 BDSG) dürfen personenbezogene Daten von Beschäftigten zur Aufdeckung von Straftaten verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.[433] Unter denselben Voraussetzungen ist auch eine Datenverarbeitung zur Aufklärung eines begründeten Verdachts einer schwerwiegenden Pflichtverletzung zulässig.[434] Dafür spricht, dass die strengeren Voraussetzungen des § 26 Abs. 1 S. 2 BDSG bei Datenverarbeitungen zu repressiven Zwecken unterhalb der Strafbarkeitsschwelle bislang in § 26 Abs. 1 S. 1 BDSG hineinzulesen waren.[435] Laut BAG entfalte § 26 Abs. 1 S. 2 BDSG keine „*Sperrwirkung dergestalt, dass eine anlassbezogene Datenerhebung durch den Arbeitgeber ausschließlich zur Aufdeckung von Straftaten zulässig wäre*“.[436] Das BAG betont in diesem Zusammenhang den Grundsatz der Verhältnismäßigkeit und bestätigt, dass die strengeren Voraussetzungen des § 26 Abs. 1 S. 2 BDSG bei

---

[432] EuGH 02.06.2022 - C-587/20, Rn.25, 26 m. w. N. = NZA 2022, 1183.

[433] Der durch tatsächliche Anhaltspunkte begründete und zu dokumentierende „*Verdacht*“ ist im Sinne eines ein-fachen Verdachts bzw. Anfangsverdachts zu verstehen, vgl. BAG, Urteil v. 20.10.2016 - 2 AZR 395/15, NZA 2017, 443 Rn.25; *Thüsing/Rombey,* NZA 2018, 1105, 1107.

[434] Legitimationsgrundlage ist nunmehr Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 1 und S. 2 BDSG). Auch eine Betriebsvereinbarung eignet sich als datenschutzrechtliche Legitimationsgrundlage, vgl. Art.88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 4 BDSG.

[435] BAG, Urteil v. 29.06.2017 - 2 AZR 597/16, NZA 2017, 1179, Rn.26; *Thüsing*, in: Compliance, § 3 Rn.21, 29; *Thüsing/Rombey,* NZA 2018, 1105, 1107.

[436] BAG, Urteil v. 29.06.2017 - 2 AZR 597/16, NZA 2017, 1179, Rn.26.

repressiven Datenverarbeitungen unterhalb der Strafbarkeitsschwelle in § 26 Abs. 1 S. 1 BDSG hineinzulesen sind.

Weil § 26 Abs. 1 S. 1 BDSG ebenso wie § 26 Abs. 1 S. 2 BDSG nach hiesiger Auffassung jedoch unangewendet bleiben müssen, gelten deren Grundsätze nunmehr unter Art. 6 Abs. 1 S. 1 lit. f) DS-GVO fort. Überwachungsmaßnahmen zu repressiven Zwecken können daher sowohl zur Aufklärung einer Straftat als auch zur Aufklärung einer schwerwiegenden arbeitsvertraglichen Pflichtverletzung datenschutzrechtlich nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 1 und S. 2 BDSG) legitimiert sein. Im Bereich des Geschäftsgeheimnisschutzes wird diese Unterscheidung insoweit relevant, dass nicht jede Verletzungshandlung in § 4 GeschGehG strafbewehrt ist, vgl. § 23 GeschGehG.

Die Frage der datenschutzrechtlichen Zulässigkeit repressiver Überwachungsmaßnahmen läuft auf eine umfassende, auf den Einzelfall bezogene Interessenabwägung hinaus. Der Persönlichkeitsschutz der Arbeitnehmer (Art. 2 Abs. 1, Art. 1 Abs. 1 GG) ist mit dem Interesse des Arbeitgebers, mittels betrieblicher Überwachungsmaßnahmen unternehmensschädigenden Geheimnisverrat zu sanktionieren (Art. 12 und Art. 14 GG), im Wege einer praktischen Konkordanz in einen schonenden Ausgleich zu bringen. Zentrales Kriterium für die Abwägung im Rahmen des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 1 und S. 2 BDSG) ist die Eingriffsintensität der Überwachungsmaßnahme. Je schwerwiegender und umfangreicher der Eingriff, desto höher wiegt der Persönlichkeitsschutz des Verdächtigen. Relevanz haben auch ein erhöhter Verdachtsgrad und inwieweit der Verdächtige mit seinem Verhalten Anlass für die Überwachungsmaßnahme gegeben hat. Grundsätzlich sind repressive Überwachungsmaßnahmen an den Verdächtigen bzw. den Kreis der Verdächtigen zu richten. Im Einzelfall dürfen repressive Überwachungs-

maßnahmen aber auch Unverdächtige erfassen.[437] Voraussetzung ist, dass die Aufklärung ein solches Vorgehen erfordert. Da Unverdächtige jedoch keinen Anlass für die repressive Überwachungsmaßnahme gesetzt haben, muss ein Eingriff in deren Persönlichkeitsrechte „*letztes Mittel*" (sog. ultima ratio) bleiben.[438] Sollte es dabei zu einem „*Zufallsfund*" in Bezug auf einen bislang unverdächtigen Mitarbeiter kommen, sind die Daten im Streitfall verwertbar.[439] Stehen dem Arbeitgeber mehrere Überwachungsmaßnahmen gleicher Eignung zur Verfügung, ist diejenige auszuwählen, die die Persönlichkeitsrechte des Verdächtigen am wenigsten tangiert. Maßgeblich sind die Umstände des jeweiligen Einzelfalls. Aus Verhältnismäßigkeitsgründen sind die jeweiligen Überwachungsmaßnahmen zeitlich zu begrenzen. Zulässig ist in aller Regel der Zugriff auf die betriebliche Kommunikation oder Maßnahmen im Bereich der offenen Videoüberwachung.[440]

Darüber hinaus galt unter § 26 Abs. 1 S. 1 und S. 2 BDSG, dass eine offen durchgeführte Überwachungsmaßnahme gegenüber einer verdeckt durchgeführten Maßnahme grundsätzlich das mildere Mittel ist.[441] Fraglich ist allerdings, ob verdeckt durchgeführte Maßnahmen unter Art. 6 Abs. 1 S. 1 lit. f) DS-GVO zulässig sind. Grundsätzlich beanspruchen die unter § 26 Abs. 1 S. 1 und S. 2 BDSG entwickelten Maßstäbe weiterhin Geltung. Danach war eine verdeckt durchgeführte Videoüberwachung zu repressiven Zwecken angesichts ihrer erhöhten Eingriffsintensität zulässig,[442] sofern ein konkreter Verdacht einer

---

437 BAG, Urteil v. 22.9.2016 - 2 AZR 848/15, NZA 2017, 112, 114; *Pötters*, in: Compliance, § 11 Rn.50.

438 Vgl. BAG, Urteil v. 27.7.2017 - 2 AZR 681/16.

439 BAG, Urteil v. 22.9.2016 - 2 AZR 848/15, NZA 2017, 112, 114.; *Fuhlrott*, GWR 2017, 60 ff.

440 *Thüsing*/*Rombey*, NZA 2018, 1105, 1107.

441 Vgl. *Thüsing*, in: Compliance, § 3 Rn.46 m. w. N.; *Gola*, BB 2017, 1462, 1467 mit dem zutreffenden Hinweis, dass Betroffenen in Fällen einer verdeckt durchgeführten Datenverarbeitung der Rechtsschutz erschwert wird.

442 *Byers*, NZA 2017, 1086, 1090.

strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers bestand, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft waren und die verdeckte Videoüberwachung praktisch das einzig verbleibende Mittel darstellte und Art und Ausmaß der Maßnahme insgesamt nicht unverhältnismäßig waren.[443] Die Kollision mit dem Transparenzgebot einer verdeckt durchgeführten Datenverarbeitung wurde dahingehend gelöst, dass die Entbehrlichkeit der Informationspflicht aus der Zulässigkeit der verdeckt durchgeführten Maßnahme hergeleitet worden war.[444]

Mochte dies unter der spezifischeren Vorschrift des § 26 Abs. 1 S. 2 BDSG nachvollziehbar gewesen sein, muss die Unionsrechtsmäßigkeit des § 26 Abs. 1 S. 2 BDSG nach hiesiger Auffassung jedoch spätestens mit der Entscheidung des EuGH zu § 26 HDSIG auf den Prüfstand gestellt werden.[445] Die Überlegungen zur Entbehrlichkeit der Informationspflicht unter § 26 Abs. 1 S. 2 BDSG lassen sich nicht auf Art. 6 Abs. 1 S. 1 lit. f) DS-GVO übertragen. Um zur Annahme einer Beschränkung der Informationspflicht zu gelangen, braucht es eines Beschränkungstatbestands, der hier im Einzelfall nach Art. 23 Abs. 1 lit. i) DS-GVO i. V. m. § 32 Abs. 1 Nr. 4, Abs. 3 BDSG zur Geltendmachung oder Ausübung zivilrechtlicher Ansprüche gegeben sein kann.[446] Voraussetzung ist, dass der Arbeitgeber die nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO zulässig erhobenen Daten benötigt, um die Beendigung des Arbeitsverhältnisses in Folge eines

---

443 Vgl. BAG, Urteil v. 27.03.2003 - 2 AZR 51/02, NZA 2003, 1193.

444 Der Gesetzgeber geht von der Zulässigkeit verdeckter Maßnahmen aus, da er bewusst kein Verbot im Rahmen des § 26 Abs. 1 S. 2 BDSG in Bezug auf verdeckt durchgeführte Überwachungsmaßnahmen geregelt hat, BT-Drs. 18/11325 S. 97. Dies legt den Schluss nahe, dass sich die Zulässigkeit verdeckt durchgeführter Überwachungsmaßnahmen nach dem Willen des Gesetzgebers direkt aus § 26 Abs. 1 S. 2 BDSG ergeben soll. A. A.: *Herbst*, in: Kühling/Buchner/Herbst, Art. 5 DS-GVO Rn.18.

445 Vgl. EuGH, Urteil v. 30.03.2023 - C-34/21.

446 Es ist umstritten, ob § 32 Abs. 1 Nr. 4 BDSG auf Art. 23 Abs. 1 lit. i) oder lit. j) DS-GVO zurückzuführen ist, vgl. *Golla*, in: Kühling/Buchner, § 32 BDSG Rn.17; *Schmidt-Wudy*, in: BeckOK-DatenschutzR, § 32 BDSG Rn.44 m. w. N.

Geheimnisverrats durchzusetzen.[447] Solange allerdings nicht sicher feststeht, durch wen der Geheimnisverrat begangen worden ist, kann § 32 Abs. 1 Nr. 4, Abs. 3 BDSG bereits seinem Wortlaut nach nicht einschlägig sein. Die Geltendmachung oder Ausübung rechtlicher Ansprüche setzt voraus, dass der Anspruchsgegner hinreichend individualisiert ist.[448] Dies ist in Fällen verdeckter Überwachungsmaßnahmen zur Aufklärung eines Geheimnisverrats gerade nicht gegeben.

Geheimnisinhaber befinden sich damit in einem Dilemma. Einerseits folgt aus der Interessenabwägung des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO, dass verdeckt durchgeführte Maßnahmen nicht absolut unzulässig, sondern zumindest in engen Grenzen möglich sein müssen.[449] Dies steht jedoch in Widerspruch mit der Informationspflicht des Art. 13 DS-GVO. Solange die Informationspflicht uneingeschränkt besteht, kann es faktisch keine verdeckt durchgeführten Überwachungsmaßnahmen zu repressiven Zwecken geben. Der nationale Gesetzgeber ist daher dringend aufgefordert, der bestehenden Rechtsunsicherheit im Rahmen des § 26 Abs. 1 S. 2 BDSG mit einer neuen Regelung zur Gewährleistung der Datentransparenz entgegenzutreten. Dies kann z. B. über eine im Vergleich zu Art. 13 DS-GO zeitlich verzögerte Informationspflicht geschehen. Bis dahin bietet sich der Abschluss einer Betriebsvereinbarung an, die die Zulässigkeit verdeckt durchgeführter Überwachungsmaßnahmen unter hinreichender Verankerung des Transparenzgrundsatzes legitimiert, Art. 88 Abs. 1 und Abs. 2 DS-GVO i. V. m. § 26 Abs. 4 BDSG.[450]

---

447 Vgl. *Franzen*, in: ErfK-ArbR, § 32 BDSG Rn.4.

448 In diese Richtung auch: *Golla*, in: Kühling/Buchner, §32 BDSG Rn.18; *Hennemann*, in: Paal/Pauly, § 32 BDSG Rn.19; *Eßer*, in: Auernhammer, § 32 BDSG Rn.22.

449 *Thüsing/Pötters*, in: Compliance, § 11 Rn.55.

450 Zu den Grenzen einer Betriebsvereinbarung: Kapitel C) I. 3. c) cc) (3).

cc) Beteiligung des Betriebsrats

Bei der Einführung und Anwendung technischer Überwachungsmaßnahmen ist das zwingende Mitbestimmungsrecht des § 87 Abs. 1 Nr. 6 BetrVG zu beachten.[451] Das Mitbestimmungsrecht dient dem präventiven Schutz der Persönlichkeitsrechte der Arbeitnehmer vor den Gefahren, die sich aus der Einführung und der Anwendung technischer Einrichtungen ergeben.[452] Das BAG legt das Mitbestimmungsrecht des § 87 Abs. 1 Nr. 6 BetrVG weit aus.[453] Die Informationen, die die technische Einrichtung über das Verhalten oder die Leistung der Arbeitnehmer erfasst, müssen einem einzelnen Arbeitnehmer zuordbar sein.[454] Ob diese Zuordnung durch die technische Einrichtung selbst erfolgt, ist insofern unbeachtlich. Es genügt, dass die Informationen mittels weiterer Informationen einem bestimmten Arbeitnehmer zugeordnet werden können.[455] Für das Bestehen des Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG bedarf es außerdem einer eigenständigen Überwachungswirkung durch die technische Einrichtung.[456] Laut BAG sei eine technische Einrichtung zur Überwachung „*bestimmt*“, wenn sie objektiv dazu geeignet ist, Informationen über das Verhalten oder die Leistung der Arbeitnehmer zu erheben, verarbeiten oder auszuwerten.[457] Dafür

---

451 Weitere Beteiligungsrechte können sich aus §§ 80 Abs. 2, 87 Abs. 1 Nr. 1 BetrVG ergeben.

452 *Granetzny*, Compliance, § 20 Rn.8 m. w. N.

453 Vgl. BAG, Beschluss v. 13.12.2016 - 1 ABR 7/15, NZA 2017, 657; *Pötters*, in: Gola, § 26 BDSG Rn.83.

454 BAG, Beschluss v. 25.04.2017 - 1 ABR 46/15, NZA 2017, 1205; BAG, Beschluss v. 13.12.2016 - 1 ABR 7/15, NZA 2017, 657 Rn.27; BAG, Beschluss v. 06.12.1983 - 1 ABR 43/81, AP, BetrVG 1972 § 87 Überwachung Nr. 7; *Kania*, in: ErfK-ArbR, § 87 Rn.54 m. w. N.

455 *Kania*, in: ErfK-ArbR, § 87 Rn.53.

456 Exemplarisch: BAG, Beschluss v. 10.12.2013 - 1 ABR 43/12, NZA 2014, 439; *Franzen*, ZfA 2019, 18, 36 m. w. N. Keine technische Einrichtung im Sinne des § 87 Abs. 1 Nr. 6 BetrVG sind dagegen Hilfsmittel wie z. B. Brillen oder Taschenrechner, vgl. *Werner*, in: BeckOK-ArbR § 87 Rn.92.

457 BAG-Rechtsprechung seit: BAG, Beschluss v. 09.09.1975 - 1 ABR 20/74, AP BetrVG 1972 - § 87 Überwachung Nr. 2.

braucht es einer konkreten Funktion des technischen Geräts, von der eine eigenständige Überwachungswirkung ausgeht.[458] Auf eine subjektive Überwachungsabsicht des Arbeitgebers kommt es dagegen nicht an.[459] Lässt der Arbeitgeber die Überwachung durch Dritte durchführen, hat er im Wege der Vertragsgestaltung zu gewährleisten, dass der Betriebsrat weiterhin sein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG ausüben kann.[460]

Vor diesem Hintergrund bietet sich im Rahmen der Einführung und Anwendung technischer Überwachungsmaßnahmen der Abschluss einer Betriebsvereinbarung an. Mithin eignet sich eine Betriebsvereinbarung auch als datenschutzrechtliche Legitimationsgrundlage, Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 4 BDSG. Dabei haben die Betriebsparteien den Persönlichkeitsschutz der Beschäftigten zu wahren. Die betriebsverfassungsrechtlichen Regelungen dürfen außerdem die allgemeinen Grundprinzipien der DS-GVO nicht unterlaufen, Art. 88 Abs. 2 DS-GVO, § 26 Abs. 5 BDSG.[461]

---

458 BAG, Beschluss v. 06.12.1983 - 1 ABR 43/81, AP BetrVG 1972 - § 87 Überwachung Nr. 7.

459 BAG, Beschluss v. 10.12.2013 - 1 ABR 43/12, NZA 2014, 439. Während im Bereich der betrieblichen Überwachungs- und Kontrollmaßnahmen das Mitbestimmungsrecht des § 87 Abs. 1 Nr. 6 BetrVG sinnvoll erscheint, bleibt abzuwarten, wie lange das BAG darüber hinaus an seiner nahezu uferlos daherkommenden Rechtsprechung festhalten wird. Angesichts der rasanten technologischen Entwicklung im betrieblichen Umfeld dürfte mittlerweile jedes digitale Tool im weitesten Sinne dazu geeignet sein, Informationen über das Verhalten oder die Leistung der Arbeitnehmer zu erheben, zu verarbeiten oder auszuwerten. Kritisch ebenfalls: *Pötters*, in: Gola, § 26 BDSG Rn.83 mit dem zutreffenden Hinweis, dass „*quasi jedes IT-System bzw. jede neue Softwareanwendung*“ das Mitbestimmungsrecht auslöse.

460 BAG, Beschluss v. 18.04.2000 - 1 ABR 22/99, AP BetrVG 1972 - § 87 Überwachung Nr. 33.

461 BAG, Beschluss v. 15.04.2014 - 1 ABR 2/13, NZA 2014, 551; *Traut*, in: Compliance, § 4 Rn.10, 26.

dd) Zwischenfazit

Überwachungs- und Kontrollmaßnahmen sind Teil der Geheimnisschutzkonzepte und zählen zu den Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG. Geheimhaltungsmaßnahmen lassen sich in präventive und repressive Geheimhaltungsmaßnahmen kategorisieren. Präventive Überwachungsmaßnahmen dienen der Kontrolle der ordnungsgemäßen Erbringung der Arbeitsleistung, um die Beschäftigten zur Regeltreue anzuhalten. Ihr Ziel ist es, Regelverstöße zu verhindern und sicherzustellen, dass Unberechtigte keinen Zugriff auf die geschützte Information haben. Datenschutzrechtliche Legitimationsgrundlage präventiver Überwachungsmaßnahmen wird in aller Regel Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 1 BDSG) sein. Werden Überwachungsmaßnahmen zur Aufklärung eines Geheimnisverrats eingesetzt (sog. Internal Investigations), hat dies repressiven Charakter. Maßnahmen zu repressiven Zwecken richten sich nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 2 und S. 1 BDSG). Die Aufklärung eines Geheimnisverrats dient dazu, die bestehenden Sicherheitslücken zu schließen sowie den Regelverstoß zu sanktionieren. Dabei ist die außerordentliche Kündigung des Geheimnisverräters nicht nur arbeitsrechtliches Sanktionsmittel, sondern aufgrund ihrer abschreckenden Wirkung zugleich ein geeignetes Mittel, andere Arbeitnehmer auf die besondere Bedeutung der Einhaltung ihrer Verschwiegenheitspflichten aufmerksam zu machen (sog. präventives Element).[462]

Die Frage der datenschutzrechtlichen Zulässigkeit von Überwachungsmaßnahmen im Bereich des Geschäftsgeheimnisschutzes läuft auf eine umfassende Interessenabwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes hinaus. Folglich ist das informationelle Selbstbestimmungsrecht der Arbeitnehmer (Art. 2 Abs. 1 i. V. m.

[462] Ein Geschäftsgeheimnisverrat sowie der dringende Verdacht eines solchen können wichtige Gründe im Sinne des § 626 Abs. 1 BGB sein, vgl. LAG Köln, Urteil v. 17.08.2001 - 11 Sa 484/00, BeckRS 2001, 30792860; *Fuhlrott/Hiéramente,* DB 2019, 967, 970.

Art. 1 Abs. 1 GG) mit dem Interesse des Arbeitgebers, mittels Überwachungsmaßnahmen Geheimnisverrat vorzubeugen und adäquat zu sanktionieren (Art. 12 Abs. 1 und Art. 14 Abs. 1 GG), im Wege einer praktischen Konkordanz in einen schonenden Ausgleich zu bringen. Zentrales Abwägungskriterium ist die Eingriffsintensität der Überwachungsmaßnahme. Je schwerwiegender und umfangreicher der Eingriff ist, desto höher wiegt der Persönlichkeitsschutz. Aus Verhältnismäßigkeitsgründen sind die jeweiligen Überwachungsmaßnahmen zeitlich zu begrenzen. Stehen dem Arbeitgeber mehrere Überwachungsmaßnahmen gleicher Eignung zur Verfügung, ist diejenige auszuwählen, die die Persönlichkeitsrechte des Verdächtigen am wenigsten tangiert. Maßgeblich sind die Umstände des jeweiligen Einzelfalls.

Verdeckte Maßnahmen zu repressiven Zwecken sind zwar grundsätzlich auch weiterhin nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO möglich. Allerdings braucht es für die Heimlichkeit der Maßnahme einer Beschränkung der Informationspflicht, die nur im Wege eines Beschränkungstatbestandes möglich ist. Art. 23 Abs. 1 lit. i) DS-GVO i. V. m. § 32 Abs. 1 Nr. 4, Abs. 3 BDSG hilft nur in begrenzten Einzelfällen weiter. Im Übrigen ist der Gesetzgeber dringend aufgefordert, der bestehenden Rechtsunsicherheit entgegenzutreten und den Grundsatz der Datentransparenz für Fälle verdeckt durchgeführter Überwachungsmaßnahmen zu repressiven Zwecken im Rahmen des § 26 BDSG nach Maßgabe des Art. 88 Abs. 2 DS-GVO hinreichend zu verankern. § 26 Abs. 5 BDSG wird diesem Erfordernis nicht gerecht, weshalb § 26 Abs. 1 S. 2 BDSG nach hiesiger Auffassung unangewendet bleiben muss.[463] Insofern bietet sich der Abschluss einer Betriebsvereinbarung als datenschutzrechtliche Legitimationsgrundlage für verdeckt durchgeführte Überwachungsmaßnahmen an, sofern eine hinreichende Verankerung des Transparenzgrundsatzes

[463] Siehe: Kapitel B) II. 4. b) bb).

durch die Betriebsparteien sichergestellt ist, Art. 88 Abs. 1, Abs. 2 DS-GVO i. V. m. § 26 Abs. 4 BDSG.[464]

Geht es dem Arbeitgeber um die Überwachung der elektronischen Kommunikation, ist das Fernmeldegeheimnis nach § 3 Abs. 1 und Abs. 3 TTDSG unbeachtlich. Dies gilt sowohl im Falle eines Privatnutzungsverbots als auch im Falle einer erlaubten Privatnutzung. Der Arbeitgeber ist nicht als Dienst-anbieter bzw. Mitwirkender eines Anbieters zu qualifizieren. Soll ein E-Mail-Account kontrolliert werden, sind Arbeitnehmer zunächst anzuweisen, private und dienstliche E-Mails getrennt voneinander zu organisieren bzw. die privaten E-Mails als privat zu kennzeichnen. Kommt der Arbeitnehmer dem nicht nach, kann der Arbeitgeber diese Unterscheidung selbst anhand der Betreffzeile vornehmen. Zieht der Arbeitgeber eine Videoüberwachungsmaßnahme im Beschäftigungskontext in Erwägung, ist die Regelung des § 4 BDSG unbeachtlich. Bei der Einführung und Anwendung technischer Überwachungsmaßnahmen ist das zwingende Mitbestimmungsrecht des § 87 Abs. 1 Nr. 6 BetrVG zu beachten. Auch vor diesem Hintergrund bietet sich der Abschluss einer Betriebsvereinbarung an.

c) Bewerberprüfungen

Zu den Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG zählen auch Bewerberprüfungen, insbesondere wenn das Stellenprofil den Umgang mit Geschäftsgeheimnissen vorsieht.[465] Um ein umfassendes Bild von dem jeweiligen Kandidaten zu erhalten, benötigt der Arbeitgeber eine hinreichende Informationsgrundlage. In Betracht kommen insbesondere Bewerbungsgespräche, Hintergrundrecherchen und Arbeitsproben. Dabei geht es beispielsweise um einen lückenlosen Lebenslauf und die Echtheit von Zeugnissen und

[464] Zur Betriebsvereinbarung als datenschutzrechtliche Legitimationsgrundlage: Kapitel C) I. 3. c) cc) (3).

[465] Dies gilt auch für den Einsatz von Fremdpersonal in sensiblen Bereichen des Betriebs.

Zertifikaten, deren Vorlage im Original nötig sein kann. Die folgende Untersuchung befasst sich mit der Reichweite des arbeitgeberseitigen Fragerechts, dem Einsatz von KI-Systemen im Bewerberverfahren sowie der Zulässigkeit elektronischer Datenabgleiche.

Bei der Bestimmung der Reichweite des arbeitgeberseitigen Fragerechts sind insbesondere der Diskriminierungsschutz und die datenschutzrechtlichen Vorgaben zu beachten. Nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 1 BDSG)[466] ist die Datenverarbeitung zulässig, wenn dies für die Entscheidung über die Begründung des Beschäftigungsverhältnisses erforderlich ist.[467] Ein Fragerecht besteht demnach, soweit der Arbeitgeber ein berechtigtes Interesse an der Beantwortung der jeweiligen Frage im Hinblick auf die Begründung des Arbeitsverhältnisses hat.[468] Folgerichtig kann sich das Informationsinteresse des Arbeitgebers nur auf solche Informationen beziehen, die mit der Begründung des Arbeitsverhältnisses in Zusammenhang stehen und für eine sachgerechte Einstellungsentscheidung erforderlich sind. Der Arbeitgeber hat immer dann ein berechtigtes Interesse an der Beantwortung einer Frage, soweit diese dabei hilft, die Eignung und Befähigung des Bewerbers in Bezug auf die offene Stelle zu beurteilen.[469] Zulässig sind z. B. Fragen zum beruflichen Werdegang bzw. nach etwaigen Ausbildungs- und Weiterbildungszeiten. Fragen nach den fachlichen Fähigkeiten bzw. Erfahrungen sind ebenfalls zulässig, soweit sie für den künftigen Arbeitsplatz von

---

466 Zur Unionsrechtswidrigkeit des § 26 Abs. 1 S. 1 BDSG: Kapitel B) II. 4. b).

467 Eine Einwilligung scheidet im Bewerbungsverfahren als datenschutzrechtliche Legitimationsgrundlage in aller Regel aus, vgl. *Höpfner/Daum,* ZfA 2021, 467, 484. Das Machtgefälle zwischen Arbeitgeber und Bewerber steht der Freiwilligkeit einer wirksamen Einwilligung regelmäßig entgegen, vgl. § 26 Abs. 2 und 3 S. 2 BDSG i. V. m. Art. 4 Nr. 11, Art. 7 Abs. 4, Art. 9 Abs. 2 lit. a) DS-GVO.

468 Das BAG verlangt in diesem Kontext ein „*berechtigtes, billigenswertes und schutzwürdiges Interesse*“ des Arbeitgebers an der Beantwortung seiner Fragen, vgl. BAG, Urteil v. 05.10.1995 - 2 AZR 923/94, NZA 1996, 371; BAG, Urteil v. 07.06.1984 - 2 AZR 270/83, NZA 1985, 57.

469 Vgl. BAG, Urteil v. 05.10.1995 - 2 AZR 923/94, NZA 1996, 371.

Bedeutung sind, beispielsweise um herauszufinden, ob ein Arbeitnehmer Vorerfahrungen im Umgang mit Geschäftsgeheimnissen hat.

Demgegenüber ist eine Frage, die nicht im Zusammenhang mit dem Arbeitsverhältnis steht, unzulässig.[470] Fragen nach der familiären Situation gehören zu den persönlichen Lebensumständen eines Bewerbers und sind grundsätzlich ohne Bedeutung für das Arbeitsverhältnis.[471] Ausnahmen bestehen immer dann, soweit der Arbeitgeber ein objektiv berechtigtes Interesse an der Beantwortung der Frage hat. So kann z. B. die Frage nach einer Liebesbeziehung zu Mitarbeitern eines Konkurrenzunternehmens zulässig sein. Maßgeblich bleiben die Umstände des jeweiligen Einzelfalls. Ist eine Frage unzulässig, darf der Bewerber die Frage wahrheitswidrig beantworten, ohne dafür Sanktionen fürchten zu müssen, sollte es zu seiner Einstellung kommen (sog. „*Recht zur Lüge*“).[472]

Besonders entscheidend für den künftigen Umgang mit Geschäftsgeheimnissen ist die Frage, ob der Bewerber über etwaige Vorstrafen verfügt. Fragen nach etwaigen Vorstrafen sind nur in engen Grenzen zulässig, da diese in aller Regel mit dem Resozialisierungsgedanken kollidieren. Laut BAG dürfe ein Bewerber nach einschlägigen Vorstrafen gefragt werden, soweit die Art des zu besetzenden Arbeitsplatzes dies erfordere.[473] Vorstrafen seien für die auszuübende Tätigkeit einschlägig, wenn deren Vorliegen auf Eigenschaften des Bewerbers

---

[470] Besteht Grund zu der Annahme, dass eine Frage auf eine Ungleichbehandlung im Sinne des AGG zielt, ist sie ebenfalls unzulässig. Das AGG zieht die Grenzen des Fragerechts insofern noch einmal enger. Hintergrund ist, dass die Beantwortung einer Frage Grundlage für eine unzulässige Benachteiligung (§ 3 AGG) im Rahmen der Einstellungsentscheidung sein kann.

[471] *Maties*, in: BeckOK-GK, § 66a Rn.621; *Joussen*, in: BeckOK-ArbR, § 611a Rn.107.

[472] Erstmals: BAG, Urteil v. 22.09.1961 - 1 AZR 241/60, NJW 1962, 74. Der Arbeitgeber ist dann nicht berechtigt, den Arbeitsvertrag aufgrund der unrichtigen Information anzufechten, vgl. § 123 Abs. 1 Var. 1 BGB.

[473] BAG, Urteil v. 20.03.2014 - 2 AZR 1071/12, NZA 2014, 1131; BAG, Urteil v. 05.12.1957 - 1 AZR 594/56, NJW 1958, 516.

schließen lasse, die mit der zu besetzenden Stelle in objektiv unmittelbarem Zusammenhang stehen und das Fehlen dieser Eigenschaften für die Erbringung der Arbeitsleistung unerlässlich sei. Zu beachten ist, dass sich ein einschlägig vorbestrafter Bewerber als unbestraft bezeichnen darf, soweit dessen Verurteilung nach §§ 51, 53 BZRG nicht in das Führungszeugnis aufzunehmen oder zu tilgen ist. Laut BAG müsse der Arbeitgeber den Bewerber im Falle einer etwaigen Fragestellung demgemäß darauf hinweisen, dass Strafen, die der Tilgung oder der beschränkten Auskunft unterliegen, nicht zwingend anzugeben sind.[474]

Fragen nach noch anhängigen Straf- oder Ermittlungsverfahren sind zulässig, sofern der bloße Verdacht einer Straftat zu einem Verlust der Integrität führt, deren Bestehen für die zu besetzende Stelle von maßgebender Bedeutung ist.[475] Fragen zu abgeschlossenen Ermittlungsverfahren, die zu keiner Verurteilung des Bewerbers geführt haben, sind dagegen unzulässig.[476] In diesem Zusammenhang kommt auch die Durchführung elektronischer Datenabgleiche in Betracht, ob der Bewerber auf einer Sanktions- oder Antiterrorliste gelistet ist.[477] Der EuGH hält Screenings am Beispiel des Datenabgleichs mit Terrorlisten zu Recht für grundsätzlich möglich.[478] Dafür spricht, dass elektronische Datenabgleiche in der Regel eine geringe Eingriffsintensität haben.[479] Hinzu kommt, dass ein Eingriff in das informationelle Selbstbestimmungsrecht regelmäßig erst dann vorliegt, wenn ein

---

474 BAG, Urteil v. 05.12.1957 - 1 AZR 594/56, NJW 1958, 516.

475 *Thüsing*, in: Richardi, § 94 BetrVG Rn.25, 26 m. w. N.

476 BAG, Urteil v. 15.11.2012 - 6 AZR 339/11, FD-ArbR 2013, 343956.

477 Sanktions- und Anti-Terrorlisten enthalten Informationen zu Personen, mit denen jede wirtschaftliche Kollaboration und insbesondere auch die Zahlung von Arbeitsentgelt untersagt ist. Bei Verstößen gegen diese Listen drohen dem Verantwortlichen teils massive Bußgelder oder andere Sanktionen, vgl. *Kort*, NZA-Beilage 2016, 62, 70; *Byers*/*Fetsch*, NZA 2015, 1364, 1366.

478 EuGH, Urteil v. 03.09.2008 - C-402/05, NJOZ 2008, 4499.

479 *Stück*, CCZ 2020, 77, 78 f.

Treffer erfolgt.[480] Erst im Falle eines Treffers wird eine neue Information über den Bewerber generiert.[481]

Kommen KI-Systeme im Bewerbungsverfahren zum Einsatz, stellen die datenschutzrechtlichen Vorgaben den Persönlichkeitsschutz der Bewerber sicher.[482] Gleicht ein KI-System die öffentlich zugänglichen Informationen eines möglichen Bewerbers mit dem Stellenprofil einer zu besetzenden Stelle ab, ergibt sich die Zulässigkeit der Datenverarbeitung aus Art. 6 Abs. 1 S. 1 lit. f) DS-GVO. Ohne den Einsatz des KI-Systems wäre es dem Arbeitgeber nicht möglich, das Internet innerhalb kürzester Zeit zu durchforsten und mit dem Stellenprofil der zu besetzenden Stelle abzugleichen. Hinzu kommt, dass das KI-System nicht tiefer in die Persönlichkeitsrechte der potenziellen Bewerber eingreift als eine manuelle Internetrecherche durch den Personaler. Wurden die Daten offensichtlich öffentlich zugänglich gemacht, besteht zudem ein verringertes Schutzniveau, vgl. Art. 9 Abs. 2 lit. e) DS-GVO. Darüber hinaus dürfen Bewerberdaten einem KI-System zugeführt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses nach Maßgabe des Verhältnismäßigkeitsgrundsatzes erforderlich ist, Art. 6 Abs. 1 S. 1 lit. f)

---

480 Dies trifft z. B. auf leitende Angestellte zu oder, wenn die auszuübende Tätigkeit ein besonderes Vertrauens-verhältnis voraussetzt, vgl. *Thüsing*/*Granetzny*, in: Compliance, § 8 Rn.6.

481 *Thüsing*/*Granetzny*, in: Compliance, § 8 Rn.6, 5 mit dem Hinweis auf BVerfG, Beschluss v. 17.02.2009 - 2 BvR 1372, 1745/07, NJW 2009, 1405.

482 Z. B. ist eine Datenschutzfolgeabschätzung immer dann durchzuführen, wenn der KI-Einsatz voraussichtlich hohe Risiken für die Rechte und Freiheiten einer Person, deren personenbezogene Daten verarbeitet werden, befürchten lässt, vgl. Art. 35 Abs. 1 S. 1 DS-GVO.

DS-GVO (bzw. § 26 Abs. 1 S. 1 BDSG).[483] Ziel der Datenerhebung ist es, die Bewerberauswahl durch den Einsatz des KI-Systems vorzubereiten, dass die Auswahlentscheidung effizienter und objektiver getroffen werden kann.[484] Das arbeitgeberseitige Interesse an einer effektiven und objektiven Auswahlentscheidung ist mit dem Persönlichkeitsschutz des Bewerbers abzuwägen und in einen angemessenen Ausgleich zu bringen. Ein übermäßiger Eingriff in die Persönlichkeitsrechte der Bewerber kommt immer dort in Betracht, wo die Validität der Ergebnisse des KI-Systems nicht sichergestellt ist, beispielsweise im Bereich der People-Analytics-Anwendungen.[485] Soweit es um die Erstellung eines umfassenden Persönlichkeitsprofils des Bewerbers geht, ist der Einsatz von People-Analytics-Anwendungen

---

[483] Bei der Durchführung eines KI-basierten Bewerbungsverfahrens sind die Beteiligungsrechte des Betriebsrats zu beachten, vgl. etwa § 87 Abs. 1 Nr. 6 und § 90 Abs. 1 Nr. 2, Nr. 3 BetrVG. Ob und inwieweit das Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG im Bewerbungsverfahren Anwendung findet, entscheiden die Einzelfallumstände. Gegen eine Anwendung des Mitbestimmungsrechts aus § 87 Abs. 1 Nr. 6 BetrVG spricht, dass sich der Wortlaut der Regelung ausschließlich auf „*Arbeitnehmer*“, nicht jedoch auf „*Bewerber*“ bezieht*, vgl. Hoffmann*, NZA 2022, 19, 24. *Lang*/*Reinbach*, differenzieren zutreffend danach, ob die Einführung einer KI-Anwendung ausschließlich der Unterstützung und Automatisierung von Bewerbungsverfahren dient (nur unter diesen Voraussetzungen bestehe kein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG) oder ob das KI-System auch darüber hinaus, z. B. während des „*Onboardings*“ genutzt werde oder das System geeignet ist, z. B. Arbeitnehmer der Personalabteilung während des Bewerbungsverfahrens zu überwachen (dann bestehe das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG). Vgl. auch: *Lang*/*Reinbach*, NZA 2023, 1273, 1277. A. A.: *Möllenkamp*, NZA-RR 2021, 76, 81.

[484] *Höpfner/Daum*, ZfA 2021, 467.

[485] Neben erheblichen Manipulationsrisiken ist insbesondere die Validität solcher Methoden und Messergebnisse in Frage zu stellen*,* vgl. *Freyler*, NZA 2020, 284, 285; *Hoffmann,* NZA 2022, 19, 20.

ebenfalls grundsätzlich unzulässig.[486] Maßgeblich bleiben die Umstände des jeweiligen Einzelfalls.

d) Zusammenfassender Überblick

Die Geheimhaltungsmaßnahmen im Beschäftigungskontext sind vielgestaltig. In der Regel wird es auf eine Kombination organisatorischer, rechtlicher und technischer Maßnahmen hinauslaufen, deren Zusammenwirken den betrieblichen Geheimnisschutz sicherstellen. Maßgebliche Richtschnur ist eine Einzelfallabwägung, bei der das Interesse des Unternehmens an der Geheimhaltung der Information mit dem für das Unternehmen möglichen und zumutbaren Aufwand, den das Unternehmen tatsächlich unternommen hat, um die Erkennbarkeit der Geheimhaltung zu erreichen und die Information vor unberechtigtem Zugriff zu schützen, ins Verhältnis zu setzen ist. Daraus ergeben sich insbesondere zwei relevante Zielvorgaben, anhand derer die jeweiligen Geheimhaltungsmaßnahmen auszurichten sind. Einerseits geht es darum, die Geheimhaltung der Information für diejenigen erkennbar zu machen, die mit ihr berechtigterweise in Berührung kommen. Andererseits geht es darum, die Information vor unberechtigtem Zugriff zu schützen.

Damit eine Information unter den Schutz des GeschGehG fällt, muss der Arbeitgeber proaktiv Geheimhaltungsmaßnahmen treffen. Die arbeitsvertragliche Treuepflicht ist für sich genommen ungeeignet, die Geheimhaltung einer Information erkennbar zu machen, da diese ihrerseits das Vorliegen eines erkennbaren berechtigten betrieblichen Interesses an der Geheimhaltung voraussetzt.[487] In aller Regel werden

---

[486] Zu beachten ist auch, dass die Verarbeitung der Bewerberdaten unzulässig ist, wenn dadurch eine finale Auswahlentscheidung des KI-Systems herbeigeführt werden soll, vgl. Art. 22 Abs. 1 DS-GVO. Aus Art. 22 Abs. 1 DS-GVO folgt außerdem, dass KI-Auswertungen in aller Regel nicht ungeprüft übernommen werden dürfen (sog. „*menschliche Letztentscheidungsbefugnis*"), vgl. *Malorny*, JuS 2022, 289, 295; *Höpfner/Daum*, ZfA 2021, 467, 483 m. w. N.

[487] Vgl. *Reinfeld*, in: Hdb-ArbR, § 30 Rn.16, 18.

daher arbeitsvertragliche Regelungen getroffen, die eine Verschwiegenheitspflicht des Arbeitnehmers enthalten. Maßgeblich für die Wirksamkeit arbeitsvertraglicher Verschwiegenheitsvereinbarungen ist die Einhaltung des Transparenzgebots. Darüber hinaus darf die Verschwiegenheitspflicht keine unangemessene Benachteiligung für den Arbeitnehmer bedeuten, vgl. § 307 Abs. 1 BGB. Dazu gilt es, das Bestehen eines berechtigten betrieblichen Interesses im Rahmen einer Einzelfallabwägung zu ermitteln. Enthält eine Verschwiegenheitsvereinbarung eine sog. „*Catch-All-Klausel*", ist diese unwirksam, weil der Arbeitnehmer in unzumutbarer Weise an seinem beruflichen Fortkommen gehindert wird (Art. 12 Abs. 1 GG).[488] Um dem Transparenzgebot des § 307 Abs. 1 S. 2 BGB zu entsprechen, muss aus einer Verschwiegenheitsvereinbarung zudem hinreichend hervorgehen, was im Einzelfall erlaubt, und was verboten ist. Zulässig sind umfassende Rückgabevereinbarungen in Bezug auf die Geschäftsunterlagen bei Beendigung des Arbeitsverhältnisses.[489]

Die arbeitsvertragliche Verschwiegenheitspflicht stellt sicher, dass die arbeitsvertragliche Treuepflicht über das Ende des Arbeitsverhältnisses hinaus in Form einer sog. „*nachwirkenden Verschwiegenheitspflicht*" fortwirken kann.[490] Zwar endet mit der Beendigung des Arbeitsverhältnisses auch die arbeitsvertragliche Verschwiegenheitsklausel. Soweit jedoch die Treuepflicht fortwirkt, gewährleistet die beendete arbeitsvertragliche Verschwiegenheitsklausel, dass das Geheimhaltungsinteresse auf Seiten des ehemaligen Arbeitgebers erkennbar fortbesteht, welches wiederum notwendige Voraussetzung für die „*nachwirkende Verschwiegenheitspflicht*" ist. Die jeweiligen Voraussetzungen für eine nachwirkende Treuepflicht sind jedoch nicht abschließend geklärt. Nach hiesiger Auffassung darf ein ausgeschiedener Arbeitnehmer geheime Informationen immer dann im Rahmen einer neuen Tätigkeit einsetzen, sofern diese zu seinen redlich

---

488 Siehe: Kapitel B) II. 4. a).

489 Vgl. BAG, Urteil v. 14.12.2011 - 10 AZR 283/10, ZD 2012, 385 m. Anm.: *Sörup*; LAG Düsseldorf, Urteil v. 03.06.2020, MMR 2021, 18.

490 Siehe: Kapitel B) II 4. a).

erworbenen Erfahrungen und Fähigkeiten zählen. Dies setzt voraus, dass der Abruf dieser vertraulichen Information ohne Weiteres, also ohne die Zuhilfenahme angefertigter Unterlagen, möglich ist. Um bestehende Rechtsunsicherheiten zu vermeiden, bietet sich der Abschluss einer gesonderten Verschwiegenheitsvereinbarung mit dem ausscheidenden Arbeitnehmer an, wobei die Vereinbarung eines nachvertraglichen Wettbewerbsverbots das höchste Maß an Rechtssicherheit schafft, zugleich jedoch den höchsten Wirksamkeitsanforderungen unterliegt.

Überwachungs- und Kontrollmaßnahmen sind ebenfalls Teil des Geheimnisschutzkonzepts und zählen zu den Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG. Zu den verschiedenen Überwachungs- und Kontrollmaßnahmen im Bereich des Beschäftigungskontexts gehören Maßnahmen, die auf die Regeltreue der Beschäftigten hinwirken und eine effektive Aufarbeitung im Falle eines Geheimnisverrats gewährleisten. Die Aufklärung eines Geheimnisverrats dient dazu, die bestehenden Sicherheitslücken zu identifizieren und zu schließen sowie den Regelverstoß zu sanktionieren. Die daran anknüpfenden arbeitsrechtlichen Maßnahmen wie z. B. Abmahnung und Kündigung demonstrieren Effektivität und Schlagkraft des unternehmerischen Compliance-Systems. Im Hinblick auf die datenschutzrechtlichen Legitimationsgrundlagen des Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 1 S. 1 BDSG und § 26 Abs. 1 S. 2 BDSG muss nach der Entscheidung des EuGH allerdings von deren Unionsrechtswidrigkeit ausgegangen werden. Für § 26 Abs. 1 S. 1 BDSG folgt dies aus dem repetitiven Charakter der Vorschrift im Vergleich zu Art. 6 Abs. 1 S. 1 lit. b) DS-GVO.[491] Darüber hinaus drängt sich nach hiesiger Auffassung auch die Unanwendbarkeit des § 26 Abs. 1 S. 2 BDSG auf.[492] Insbesondere im Hinblick auf verdeckte Überwachungsmaßnahmen, die nach § 26 Abs. 1 S. 2 BDSG

---

[491] EuGH, Urteil v. 30.03.2023 - C-34/21 Rn.65, 71.
Siehe: Kapitel B) II. 4. b).

[492] Siehe: Kapitel B) II. 4. b) bb).

grundsätzlich möglich sind,[493] hätte es weiterer Vorgaben bedurft die den Grundsatz der Datentransparenz hinreichend sicherstellen, vgl. Art. 88 Abs. 2 DS-GVO. § 26 Abs. 5 genügt dafür nicht. Vor dem Hintergrund des eindeutigen Wortlauts in Art. 88 Abs. 2 DS-GVO, wonach die spezifischere Vorschrift selbst die jeweiligen Maßnahmen zur Wahrung der Datentransparenz festlegen muss, kann der deutsche Gesetzgeber seinen Regelungsauftrag nicht ohne Weiteres an den datenschutzrechtlich Verantwortlichen delegieren. Mag dies in Fällen möglich sein, in denen die spezifischere Vorschrift keine Beschränkung der Betroffenenrechte darstellt und die allgemeinen Vorgaben in Art. 12 ff. DS-GVO uneingeschränkt Anwendung finden, so genügt dies im Fall einer Beschränkung der Betroffenenrechte nicht. Der nationale Gesetzgeber muss den an ihn gerichteten Regelungsauftrag in Art. 88 Abs. 2 DS-GVO im Rahmen der spezifischeren Vorschrift selbst wahrnehmen und für die nötige Datentransparenz sorgen, Art. 5 Abs. 1 lit. a) DS-GVO.[494]

Für die Praxis ändert sich dadurch nicht viel.[495] Datenverarbeitungen sind im selben Umfang auf Art. 6 Abs. 1 S. 1 lit. f) DS-GVO zu stützen.[496] Sowohl die unter § 26 Abs. 1 S. 1 BDSG als auch die unter

---

493 BAG, Urteil v. 27.03.2003 - 2 AZR 51/02, NZA 2003, 1193; BAG, Urteil v. 22.09.2016 - 2 AZR 848/15, NZA 2017, 112, 114; vgl. auch: *Thüsing*/*Pötters*, in: Compliance, § 11 Rn.55; *Gola* BB 2017, 1462, 1467.

494 Vgl. EuGH, Urteil v. 30.03.2023 - C-34/21, Rn.65.

495 Zu derselben Einschätzung gelangt das Land Hessen in Bezug auf § 23 HDSIG im Rahmen seiner Handreichung zur Verarbeitung personenbezogener Daten von Beschäftigten in Reaktion auf die Entscheidung des EuGH, Urteil v. 30.03.2023 - C-34/21.

496 Bestätigt wird diese Sichtweise dadurch, dass Art. 6 Abs. 1 S. 1 lit. f) DS-GVO im Beschäftigungskontext anwendbar ist und inhaltlich nicht von § 26 Abs. 1 S. 1 BDSG abweicht. Allg. zum Verhältnis der spezifischeren Vorschriften (Art. 88 Abs. 1 DS-GVO) zu Art. 6 Abs. 1 S. 1 lit. f) DS-GVO: *Franzen*, in: ErfK-ArbR, § 26 BDSG Rn.4, der zu der Zeit noch wie viele andere von der Unionsrechtsmäßigkeit des § 26 Abs. 1 S. 1 BDSG ausging und der Frage einer eigenständigen Anwendbarkeit des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO neben § 26 Abs. 1 S. 1 BDSG im Unternehmenskontext nachging.

§ 26 Abs. 1 S. 2 BDSG entwickelten Maßstäbe beanspruchen weiterhin Geltung, wenn auch nunmehr unter anderer Vorschrift. Anders sieht dies jedoch mit Blick auf verdeckt durchgeführte Überwachungsmaßnahmen aus. Zwar bleiben verdeckt durchgeführte Maßnahmen grundsätzlich auch weiterhin nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO möglich. Allerdings braucht es für die Heimlichkeit der Maßnahme einer Beschränkung der Informationspflicht, die nur im Wege eines Beschränkungstatbestandes möglich ist.

Art. 23 Abs. 1 lit. i) DS-GVO i. V. m. § 32 Abs. 1 Nr. 4, Abs. 3 BDSG hilft nur in begrenzten Einzelfällen weiter. Insofern bietet sich der Abschluss einer Betriebsvereinbarung als datenschutzrechtliche Legitimationsgrundlage für verdeckt durchgeführte Überwachungsmaßnahmen an, sofern die hinreichende Verankerung des Transparenzgrundsatzes durch die Betriebsparteien sichergestellt ist, Art. 88 Abs. 1, Abs. 2 DS-GVO i. V. m. § 26 Abs. 4 BDSG.[497] Im Übrigen ist der Gesetzgeber dringend aufgefordert, der bestehenden Rechtsunsicherheit entgegenzutreten und den Grundsatz der Datentransparenz für Fälle verdeckt durchgeführter Überwachungsmaßnahmen zu repressiven Zwecken im Rahmen des § 26 BDSG nach Maßgabe des Art. 88 Abs. 2 DS-GVO hinreichend zu verankern.

Die Frage der datenschutzrechtlichen Zulässigkeit betrieblicher Überwachungsmaßnahmen im Bereich des Geschäftsgeheimnisschutzes läuft auch weiterhin auf eine umfassende Interessenabwägung zwischen dem Interesse des Arbeitgebers am betrieblichen Geheimnisschutz (Art. 12 Abs. 1 und Art. 14 Abs. 1 GG) und dem Recht des von der Datenverarbeitung betroffenen Arbeitnehmers auf informationelle Selbstbestimmung (Art. 2 Abs. 1 und Art. 1 Abs. 1 GG) nach Maßgabe des Verhältnismäßigkeitsgrundsatzes hinaus. Maßgeblich sind die Umstände des jeweiligen Einzelfalls.

---

[497] Siehe: Kapitel C) I. 3. c) cc) (3).

Zentrales Abwägungskriterium bleibt die Eingriffsintensität einer Überwachungsmaßnahme. Je schwerwiegender und umfangreicher der Eingriff ist, desto höher wiegt der Persönlichkeitsschutz. Aus Verhältnismäßigkeitsgründen sind die jeweiligen Überwachungsmaßnahmen zeitlich zu begrenzen. Stehen dem Arbeitgeber mehrere Überwachungsmaßnahmen gleicher Eignung zur Verfügung, ist diejenige auszuwählen, die die Persönlichkeitsrechte des Verdächtigen am wenigsten tangiert. Geht es dem Arbeitgeber um die Überwachung der elektronischen Kommunikation, ist das Fernmeldegeheimnis gemäß § 3 Abs. 1 und Abs. 3 TTDSG unbeachtlich. Dies gilt sowohl im Falle eines Privatnutzungsverbotes als auch im Falle einer erlaubten Privatnutzung. Bei der Einführung und Anwendung technischer Überwachungsmaßnahmen ist das zwingende Mitbestimmungsrecht des § 87 Abs. 1 Nr. 6 BetrVG zu beachten. Auch vor diesem Hintergrund bietet sich der Abschluss einer Betriebsvereinbarung an.

Zu den Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG zählen auch Bewerberprüfungen, insbesondere wenn das Stellenprofil den Umgang mit Geschäftsgeheimnissen vorsieht.[498] Zulässig ist eine Frage an den Bewerber, soweit der Arbeitgeber ein berechtigtes Interesse an deren Beantwortung im Hinblick auf die Begründung des Arbeitsverhältnisses hat.[499] Fragen nach etwaigen Vorstrafen sind nur erlaubt, sofern es sich dabei um Fragen nach sog. „*einschlägige Vorstrafen*“ handelt. Maßgebend ist, dass ihr Vorliegen auf Eigenschaften des Bewerbers schließen lässt, die mit der zu besetzenden Stelle in objektiv unmittelbarem Zusammenhang stehen und das Fehlen dieser Eigenschaften für die Erbringung der Arbeitsleistung unerlässlich ist. Möglich ist auch die Durchführung elektronischer Datenabgleiche. Kommen KI-Systeme im Bewerbungsverfahren zum Einsatz, ist das arbeitgeberseitige Interesse an einer

---

[498] Siehe: Kapitel B) II. 4. c).

[499] Das BAG verlangt in diesem Kontext ein „*berechtigtes, billigenswertes und schutzwürdiges Interesse*“ des Arbeitgebers an der Beantwortung seiner Fragen, vgl. BAG, Urteil v. 05.10.1995 - 2 AZR 923/94, NZA 1996, 371; BAG, Urteil v. 07.06.1984 - 2 AZR 270/83, NZA 1985, 57.

effektiven und objektiven Auswahlentscheidung mit dem Recht auf informa-tionelle Selbstbestimmungsfreiheit des Bewerbers abzuwägen und in einen angemessenen Ausgleich zu bringen. Ein übermäßiger Eingriff in die Persönlichkeitsrechte der Bewerber kommt immer dort in Betracht, wo die Validität der Ergebnisse des KI-Systems nicht sicher ist, beispielsweise im Bereich der People-Analytics-Anwendungen. Maßgeblich sind die Umstände des jeweiligen Einzelfalls.

III. Weiterungen für das unternehmerische Compliance-System

Der Geschäftsgeheimnisschutz ist Teil des unternehmerischen Compliance-Systems. Vorstand und Geschäftsführung trifft eine Leitungsverantwortung (§ 76 Abs. 1 AktG). Sie sind verpflichtet, das Unternehmen sorgfältig zu führen und die Gesetzestreue des Unternehmens zu überwachen.[500] Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Zu diesen Pflichten zählt unter anderem, das Unternehmen so zu führen, dass diesem keine wirtschaftlichen Nachteile entstehen.[501] Welche Maßnahmen dies im Einzelnen umfasst, entscheiden die Umstände des jeweiligen Einzelfalls. Die Geschäftsleitung ist verpflichtet, eine hinreichende Compliance-Organisation sicherzustellen, in deren konkreter Ausgestaltung sie frei ist.[502] Voraussetzung ist, dass die Compliance-Maßnahmen wirksam und den datenschutzrechtlichen sowie betriebsverfassungsrechtlichen Anforderungen gerecht werden (sog. Legalitätsgrundsatz).[503]

Um wirtschaftliche Nachteile vom Unternehmen fernzuhalten, ist die Geschäftsleitung gesellschaftsrechtlich zur Implementierung betrieb-

---

500 § 93 Abs. 1 S. 1 AktG, § 43 Abs. 1 GmbHG, § 34 Abs. 1 S. 2 GenG.
501 *Thüsing*, in: Compliance, § 2 Rn.20; *Spindler*, in: MüKo-AktG, § 93 Rn.63; *Fleischer*, in: VorstandsR-HdB, § 7 Rn.64.
502 *Reinfeld*, in: Hdb-ArbR, § 35 Rn.9 ff.
503 *Thüsing*, in: Compliance, § 2 Rn.22.

licher Geheimhaltungsmaßnahmen verpflichtet.[504] Dazu sieht das Geheimnisschutzkonzept die Implementierung den Umständen nach angemessenen Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG vor. Andernfalls kann sich das Unternehmen nicht auf das Schutz- und Abwehrsystem der §§ 6 ff. GeschGehG berufen. Welche Geheimnisschutzmaßnahmen zu implementieren sind, ist unternehmensbezogen anhand sämtlicher Umstände des Einzelfalls zu entscheiden.[505] Berücksichtigungsfähig sind insbesondere der Wert und die Bedeutung des Geheimnisses sowie die Größe des Unternehmens, die Art der Kennzeichnung und die Kosten.[506] Für die Festlegung konkreter Geheimhaltungsmaßnahmen bietet sich ein abgestuftes Vorgehen an. In einem ersten Schritt sind die zu schützenden Informationen zu identifizieren.[507] In einem zweiten Schritt sind diese Informationen den Kategorien mit absteigender Wichtigkeit zuzuordnen. Die Wichtigkeit entscheidet darüber, welche Maßnahmen prioritär zu implementieren sind. Sodann empfiehlt sich ein Vorgehen anhand der Erkennbarkeit der Geheimhaltung in Bezug auf die jeweilige Information. Hier gilt es auch zu klären, wer mit der Information üblicherweise in Berührung kommt und wie die geheime Information vor unberechtigten Zugriffen geschützt werden kann, ehe konkrete

---

504 Ist der Arbeitgeber aufgrund seiner gesellschaftsrechtlichen Pflichten zur Einführung betrieblicher Kontrollmaßnahmen verpflichtet, steht dies der Annahme des Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG nicht entgegen. Die gesellschaftsrechtlichen Pflichten begründen eine Handlungspflicht für die Geschäftsleitung, die Regelungsspielraum in Bezug auf die konkrete Ausgestaltung der Kontrollmaßnahmen zulässt, vgl. § 93 Abs. 1 S. 1 AktG, § 43 Abs. 1 GmbHG, § 34 Abs. 1 S. 2 GenG, vgl. *Thüsing/Granetzny*, in: Compliance, § 20 Rn.6.

505 *Reinfeld*, Das neue GeschGehG, § 1 Rn.170.

506 BT-Drs. 19/4724, S. 24, 25; *Apel/Walling*, DB 2019, 891, 895; *Fuhlrott/Hiéramente*, DB 2019, 967, 970; *Ohly,* GRUR 2019, 441, 451.

507 *Scholtyssek*/*Judis*/*Krause*, CCZ 2020, 23, 27; *Dann*/*Markgraf*, NJW 2019, 1774, 1776; *Dumont*, BB 2018, 2441, 2443; *Fuhlrott*, in: BeckOK-GeschGehG, § 2 Rn.23; *Hoppe*/*Oldekop*, Geschäftsgeheimnisse, Rn.129; *Maaßen*, GRUR 2019, 352, 356.

Geheimhaltungsmaßnahmen für die jeweiligen Kategorien zu erwägen sind.[508]

Aus Nachweisgründen sind die implementierten Maßnahmen zu dokumentieren und einer regelmäßigen Überprüfung zu unterziehen. Die Unternehmensleitung hat darüber zu wachen, dass die eingeführten Maßnahmen dem Angemessenheitserfordernis dauerhaft gerecht werden und ist verpflichtet, ggf. notwendige Anpassungen vorzunehmen.[509] Dies gilt auch für den Fall des konkreten Verdachts eines Geheimnisverrats. Geheimnisschutzkonzepte benötige entsprechende Mechanismen, um Sicherheitslücken im konkreten Verdachtsfall identifizieren und sodann schließen zu können. Im Ergebnis wird es daher auf eine Kombination vertraglicher, technischer und organisatorischer Maßnahmen hinauslaufen. Unterlässt ein Unternehmen entsprechende Maßnahmen, drohen nach § 130 OWiG empfindliche Bußgelder.[510] Duldet die Unternehmensleitung pflichtwidrig Verstöße eines Arbeitnehmers gegen das GeschGehG und erleidet das Unternehmen dadurch einen Schaden, kann die Geschäftsleiter-Haftung nach § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG greifen. Gleiches gilt für den Fall, dass erforderliche Mitarbeiterschulungen zum Umgang mit

---

508 *Reinfeld*, in: Hdb-ArbR, § 35 Rn.9 ff.

509 *Apel*/*Walling*, DB 2019, 891, 894; *Maaßen*, GRUR 2019, 352, 360.

510 Verstöße gegen § 76 Abs. 1 AktG i. V. m. § 93 Abs. 1 AktG bzw. § 43 Abs. 1 GmbHG können nach § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG zur Innenhaftung der Unternehmensleitung gegenüber der Gesellschaft führen sowie nach § 30 OWiG, § 81 GWB bußgeldpflichtig und nach §§ 266, 299 StGB strafrechtlich relevant sein. Im Außenverhältnis haftet die Unternehmensleitung nur im Ausnahmefall, beispielsweise für die Inanspruchnahme besonderen Vertrauens im Vorfeld eines Vertragsschlusses nach §§ 280, 311 Abs. 3 BGB. Dafür spricht, dass § 130 OWiG kein Schutzgesetz im Sinne des § 823 Abs. 2 BGB ist und ein Anspruch aus § 826 BGB zumeist an dem nötigen Vorsatz scheitert. Vgl. dazu auch: BGH, Urteil v. 13.04.1994 - II ZR 16/93, BGHZ 125, 366, 371, 373; bestätigend: *Altmeppen*, in: Altmeppen GmbHG, § 43 Rn.66. Laut *Schmidt* ZIP 1994, 841 f. könne § 130 OWiG ein Schutzgesetz sein, wenn das Unterlassen der Aufsichtsmaßnahme zugleich eine andere Schutzgesetzverletzung zur Folge habe.

unternehmenseigenen Geschäftsgeheimnissen pflichtwidrig durch die Unternehmensleitung unterblieben sind und infolgedessen einem Arbeitnehmerregress entgegenstehen, § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG.

Um im Rahmen bestehender Compliance-Systeme Aufwand und Kosten zu sparen, kann es sich anbieten, mögliche Synergien aus Art. 32 DS-GVO und § 2 Nr. 1 lit. b) GeschGehG zu heben. Nach Art. 24 Abs. 1 S. 1 i. V. m. Art. 32 DS-GVO sind Unternehmen verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Anforderungen an die Datensicherheit ähneln den Anforderungen an die angemessenen Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG, obgleich die beiden Regelwerke von einem von einem unterschiedlichen Verständnis des Angemessenheitsbegriffs ausgehen.[511] Dafür spricht, dass im Rahmen der DS-GVO die Regel gilt: Je schutzbedürftiger eine Information ist, desto höher sind die Anforderungen, die an die vom Geheimnisinhaber zu treffenden Schutzmaßnahmen zu stellen sind.[512] Gemeint ist damit der Vorsichtsgrad des für die Datenverarbeitung Verantwortlichen: Mit steigender Wichtigkeit des Datums steigt der gebotene Schutzaufwand. Hintergrund ist, dass die DS-GVO das Verhältnis zwischen dem Verantwortlichen und der von der Datenverarbeitung betroffenen Person regelt. Je schützenswerter das Datum der betroffenen Person ist, desto höher hat der gebotene Schutzaufwand auszufallen, das Datum vor einem unbefugten Zugriff Dritter zu schützen.

Diese Wertung lässt sich dem Grunde nach auf das GeschGehG übertragen: Mit steigender Wichtigkeit der geheimen Information würde der gebotene Schutzaufwand des Geheimnisinhabers steigen. Dies überzeugt jedoch nur bedingt. Zum einen entscheidet nach hiesiger

---

511 *Thüsing*/*Rombey*, ZD 2020, 221, 222; *Weigert*, NZA 2020, 209, 210, 213.

512 *Apel/Walling,* DB 2019, 891, 894; *Dann/Markgraf*, NJW 2019, 1774, 1775; *Naber/Peukert/Seeger*, NZA 2019, 583, 584; *Preis/Seiwerth*, RdA, 2019, 351, 353.

Auffassung die Schutzbedürftigkeit einer Information nicht ausschließlich über das Maß an Sicherheitsvorkehrungen.[513] Denn je wertvoller eine Information ist, desto offensichtlicher kann auch die Erkennbarkeit ihrer Geheimhaltung sein, wodurch das Maß an Sicherheitsvorkehrungen unter Umständen absinken kann.[514] Zum anderen kennt das GeschGehG das Verhältnis zwischen dem Verantwortlichen und der von der Datenverarbeitung betroffenen Person nicht. Das GeschGehG regelt vielmehr das Verhältnis zwischen dem Geheimnisinhaber und dem (potenziellen) Rechtsverletzer und erkennt in diesem Kontext die Schutzwürdigkeit beider an.[515] Würde man die Wertungen der DS-GVO auf das GeschGehG übertragen, so wäre die betroffene Person mit dem Geheimnisinhaber gleichzusetzen, das geschützte Datum wäre das geschützte Geschäftsgeheimnis und der „*unbefugt*" (im Sinne der DS-GVO) auf die Daten Zugreifende, wäre der (potenzielle) Geheimnisbrecher. Im Gegensatz zum GeschGehG berücksichtigt die DS-GVO jedoch nicht die (potenzielle) Schutzwürdigkeit eines unbefugt auf die Daten zugreifenden Dritten, sodass die Wertungen der DS-GVO zumindest nicht in Gänze auf § 2 Nr. 1 lit. b) GeschGehG übertragbar sind.[516] In der Praxis geht es jedoch häufig um dasselbe: Den Schutz sensibler Daten vor unbefugter Einsichtnahme, Nutzung und Offenlegung. Hinzu kommt, dass sowohl der Schutz von personenbezogenen Daten als auch der Schutz von Geschäftsgeheimnissen regel-mäßig einer Kategorisierung von Daten samt Risikobewertung bedarf. Um im Rahmen bestehender Schutzkonzepte Aufwand und Kosten zu sparen, kann es sich daher anbieten, diese Synergien zu realisieren.

---

513 Siehe: Kapitel B) II. 3. c) aa).

514 Sollte sich die Geheimhaltung dagegen auf eine Information beziehen, die auf den ersten Blick eher unbedeutend scheint, bedarf es eines erhöhten Aufwandes, um ihre Geheimhaltung erkennbar zu machen.

515 Vgl. *Thüsing*/*Rombey*, ZD 2020, 221, 222; *Weigert*, NZA 2020, 209, 210, 213.

516 § 3 Abs. 2 GeschGehG i. V. m. §§ 6 Abs. 1, 35 Abs. 2 HinSchG und § 5 GeschGehG. So auch: Vgl. *Thüsing*/*Rombey*, ZD 2020, 221, 222.

Kommt es bei der Erstellung eines „*gemeinsamen Konzepts*“ zur Offenlegung von Geschäftsgeheimnissen gegenüber dem Datenschutzbeauftragten, unterliegt dieser einer Verschwiegenheitspflicht in Bezug auf Geschäftsgeheimnisse und sonstige vertrauliche betriebliche Informationen des Unternehmens. Die Verschwiegenheitspflicht des Datenschutzbeauftragten resultiert aus seiner Rücksichtnahmepflicht gegenüber den (Geheimhaltungs-) Interessen des Verantwortlichen, mit dem der Datenschutzbeauftragte über ein Vertragsverhältnis verbunden ist, vgl. Art. 38 Abs. 5 DS-GVO i. V. m. § 241 Abs. 2 BGB. Diese Verschwiegenheitspflicht gilt auch gegenüber der Aufsichtsbehörde.[517] Dafür spricht, dass ein Geheimnisverrat einen Abberufungsgrund darstellt, soweit dieser geeignet ist, eine fristlose Kündigung aus wichtigem Grund zu rechtfertigen. Der Datenschutzbeauftragte hat daher im Rahmen seiner Zusammenarbeit mit der Aufsichtsbehörde die entsprechenden Passagen vorab zu schwärzen oder anderweitig unkenntlich zu machen. Zu beachten ist allerdings, dass der datenschutzrechtlich Verantwortliche Bereitstellungspflichten gegenüber der Aufsichtsbehörde unterliegt, die auch Geschäftsgeheimnisse umfassen können, vgl. Art. 30 Abs. 4 und Art. 58 Abs. 1 lit. a) DS-GVO. Soweit es in Erfüllung der Bereitstellungspflichten zur Weitergabe von Geschäftsgeheimnissen kommt, unterliegen diese dem besonderen Vertraulichkeitsschutz der Aufsichtsbehörde.[518]

In Teilen der Literatur wird darüber hinaus eine Meldepflicht des Datenschutzbeauftragten gegenüber der Aufsichtsbehörde hinsichtlich etwaiger (gravierender) Datenschutzverstöße diskutiert.[519] Dies ist zweifelhaft. DS-GVO und BDSG sehen keine Meldepflicht des Datenschutzbeauftragten hinsichtlich möglicher Datenschutzverstöße vor. Stimmen in der Literatur ziehen deshalb die Pflicht des

---

[517] Ein Auskunftsverweigerungsrecht steht dem Datenschutzbeauftragten nur in den normierten Fällen zu der §§ 6 Abs. 6, 38 Abs. 2 BDSG.

[518] *Klug*, in: Gola, Art. 31 DS-GVO Rn.2.

[519] *Bergt*, in: Kühling/Buchner, DS-GVO, Art. 39 Rn.9; vgl. *Klug*, in: Gola, Art. 39 DS-GVO Rn.6.

Datenschutzbeauftragten zur Zusammenarbeit mit der Aufsichtsbehörde nach Art. 39 Abs. 1 lit. d) DS-GVO als Rechtsgrundlage heran.[520] Ergänzend dazu wird Art. 39 Abs. 1 lit. e) DS-GVO angeführt, wonach der Datenschutzbeauftragte Anlaufstelle der Aufsichtsbehörde für mit der Datenverarbeitung zusammenhängende Fragen fungieren soll. Die Zusammenschau dieser Funktionsbereiche zeigt, dass der Datenschutzbeauftragte lediglich Ansprechpartner für die Aufsichtsbehörde in datenschutzrechtlichen Angelegenheiten sein soll und keiner Meldeverpflichtung unterliegt. Gegen eine Meldepflicht des Datenschutzbeauftragten spricht außerdem, dass die Entgegennahme von Hinweisen hinsichtlich möglicher Verstöße nicht zu den in Art. 57 DS-GVO gelisteten Aufgabenbereichen der Aufsichtsbehörde zählen. Aus Art. 57 Abs. 3 DS-GVO geht nur hervor, dass der Datenschutzbeauftragte sich in datenschutzrechtlichen Fragestellungen zu Informations- und Beratungszwecken kostenfrei an die Aufsichtsbehörde wenden kann. Im Ergebnis besteht daher keine Meldepflicht des Datenschutzbeauftragten gegenüber der Aufsichtsbehörde. Dem Datenschutzbeauftragten bleibt es insofern jedoch unbenommen, Datenschutzverstöße nach Maßgabe des HinSchG über die entsprechenden Whistleblowing-Kanäle zu melden,[521] wobei eine Meldung von Geschäftsgeheimnissen den hervorgehobenen Vorgaben des § 6 Abs. 1 HinSchG unterfällt.[522]

---

520 *Thüsing/Granetzny*, in: Compliance, § 19 Rn.18; *Bergt*, in: Kühling/Buchner, DS-GVO, Art. 39 Rn.19.

521 Vgl. § 2 Abs. 1 Nr. 3 lit. p) HinSchG.

522 Siehe: Kapitel C) I. 2. a).

IV. Eine erste Sammlung der Erkenntnisse

Anhand der vorstehenden Ausführungen lassen sich folgende Erkenntnisse zu den eingangs aufgezeigten Leitfragen festhalten:

Wann unterfällt eine Information dem GeschGehG-Schutzregime?

1. Das Vorliegen eines Geschäftsgeheimnisses erfordert eine geheime Information von wirtschaftlichem Wert, § 2 Nr. 1 lit. a) GeschGehG. Der Begriff der Informationen ist weit zu verstehen.[523] Der nötige Unternehmensbezug liegt vor, sofern die Information der Sphäre eines bestimmten Unternehmens unmittelbar zuordbar, respektive marktrelevant ist. Auch Informationen aus dem privaten Bereich können marktrelevant sein. Besteht eine Information aus mehreren Bestandteilen, ist sie auch dann geheim, wenn ihre Einzelteile öffentlich zugänglich sind. § 2 Nr. 1 lit. a) GeschGehG ist dahingehend auszulegen, dass die „*weder […] noch*“ - Formulierung im Sinne eines alternativen Verständnisses - *„entweder […] oder*“ - zu verstehen ist. Der Begriff des „*wirtschaftlichen Werts*“ entspricht dem des „*kommerziellen Werts*“ in der GeschGehG-RL. Die Kausalverbindung zwischen Geheimhaltung und Wertigkeit einer Information ist ebenfalls weit auszulegen. Ausreichend ist, dass eine Information durch die Geheimhaltung einen (potenziellen) Wertzuwachs erfährt. Auch rechtswidrige Informationen können einen „*wirtschaftlichen Wert*“ aufweisen.[524]

2. Der Begriff des „*berechtigten Interesses*“ gemäß § 2 Nr. 1 lit. c) GeschGehG entspricht dem des „*legitimen Interesses*“ in Erwägungsgrund 14 GeschGeh-RL und berücksichtigt das Mindestschutzgebot der GeschGeh-RL hinreichend.[525] Das Kriterium des

[523] Siehe: Kapitel B) II. 3. a).
[524] Siehe: Kapitel B) II. 3) a) cc) (6).
[525] Siehe: Kapitel B) II. 3. b).

„*berechtigten Interesses an der Geheimhaltung*“ geht vollständig in dem Erfordernis des „*wirtschaftlichen Werts*“ (§ 2 Nr. 1 lit. a) GeschGehG) auf. Auf Definitionsebene besteht daher die unwiderlegliche Vermutung (sog. Fiktion), dass an einer Information, die wirtschaftlichen Wert aufweist, auch ein berechtigtes Interesse an ihrer Geheimhaltung besteht. Das Kriterium dient nicht des Ausschlusses rechtswidriger Informationen. Diese können dem Schutzregime des GeschGehG unterfallen. Interessengerechte Lösungen lassen sich über § 5 GeschGehG realisieren.[526]

3. Ob den Umständen nach angemessene Geheimhaltungsmaßnahmen getroffen wurden, ist unternehmensspezifisch zu beurteilen. Entscheidend für das Vorliegen angemessener Geheimhaltungsmaßnahmen ist eine Einzelfallabwägung, bei der das Interesse des Unternehmens an der Geheimhaltung der Information mit dem für das Unternehmen möglichen und zumutbaren Aufwand, den das Unternehmen tatsächlich unternommen hat, um die Erkennbarkeit der Geheimhaltung zu erreichen und die Information vor unberechtigtem Zugriff zu schützen, ins Verhältnis zu setzen ist.[527] Die Anforderungen an die angemessenen Geheimhaltungsmaßnahmen dürfen keine abschreckende Wirkung für den Schutz von Geschäftsgeheimnissen entfalten. Soweit die Geltendmachung von Schutzansprüchen angesichts der getroffenen Geheimhaltungsmaßnahmen im Einzelfall unverhältnismäßig erscheint, findet dies sein Korrektiv in § 9 Nr. 2 GeschGehG. Ein Untätigbleiben im Vertrauen darauf, die Information werde nicht entdeckt, reicht nicht aus. Ereignet sich ein Geheimnisverrat, folgt daraus nicht automatisch die Unangemessenheit des Schutzniveaus. In diesem Fall entscheiden die Umstände des Einzelfalls darüber, ob das Unternehmen im Zeitpunkt des Geheimnisverrats berechtigterweise davon ausgehen durfte, die geheime Information sei hinreichend geschützt.

---

526 Siehe: Kapitel B) II. 3. b) ff).
527 Siehe: Kapitel B) II. 3. c) aa) (6).

4. Rechtswidrige Geheimhaltungsmaßnahmen können im Rahmen des § 2 Nr. 1 lit. b) GeschGehG Berücksichtigung finden, sofern dies dem Grundsatz der Verhältnismäßigkeit entspricht. Berücksichtigungsfähig meint in diesem Kontext, dass die jeweiligen Maßnahmen Teil der getroffenen Geheimhaltungsmaßnahmen sind, ohne dass aus deren Rechtswidrigkeit ein Anspruchsausschluss nach § 9 Nr. 2 GeschGehG droht. Dies ist anhand einer eigenständigen Abwägung zu beurteilen, bei der es darauf ankommt, ob der Geheimnisinhaber zum Zeitpunkt des Geheimnisverrats berechtigterweise von der Rechtmäßigkeit der Geheimhaltungsmaßnahme ausgehen durfte.[528] Sollte eine unwirksame arbeitsvertragliche Verschwiegenheitsklausel im Einzelfall nicht berücksichtigungsfähig sein, kann stattdessen die arbeitsvertragliche Treuepflicht des Arbeitnehmers berücksichtigungsfähig sein, sofern die unwirksame Klausel die nötige Erkennbarkeit des Geheimhaltungsinteresses sicherstellt. Die datenschutzrechtliche Unzulässigkeit einer Maßnahme kann dem Nachweis eines Geheimnisverrats entgegenstehen, sofern ein Beweisverwertungsverbot in Bezug auf Informationen, die einer unzulässigen Datenverarbeitung entstammen, besteht.[529]

Welche Besonderheiten gelten im Beschäftigungskontext?

1. Die Geheimhaltungsmaßnahmen im Beschäftigungskontext sind vielgestaltig. In der Regel wird es auf eine Kombination organisatorischer, rechtlicher und technischer Maßnahmen hinauslaufen, deren Zusammenwirken den betrieblichen Geheimnisschutz sicherstellen. Maßgeblich sind die beiden Zielvorgaben, anhand derer die jeweiligen Geheimhaltungsmaßnahmen auszurichten sind. Einerseits geht es darum, die Geheimhaltung der Information für diejenigen erkennbar zu machen, die mit ihr berechtigterweise in Berührung kommen. Andererseits geht es darum, die Information vor unberechtigtem Zugriff zu schützen.

---

528 Siehe: Kapitel B) II. 3. c) bb) (1).
529 Siehe: Kapitel B) II. 3. c) bb) (2).

2. Damit eine Information dem Schutzregime des GeschGehG unterfällt, muss der Arbeitgeber gegenüber den Arbeitnehmern proaktiv Geheimhaltungsmaßnahmen treffen. Zu beachten ist, dass die arbeitsvertragliche Treuepflicht aus dem Arbeitsverhältnis für sich genommen ungeeignet ist, die Geheimhaltung einer Information erkennbar zu machen. Hintergrund ist, dass die arbeitsvertragliche Treuepflicht ihrerseits das Vorliegen eines erkennbaren berechtigten betrieblichen Interesses an der Geheimhaltung voraussetzt. Aus Gründen der Rechtssicherheit werden in der betrieblichen Praxis daher in aller Regel arbeitsvertragliche Verschwiegenheitsvereinbarungen getroffen.[530]

3. Maßgeblich für die Wirksamkeit arbeitsvertraglicher Verschwiegenheitsvereinbarungen ist die Einhaltung des Transparenzgebots. Darüber hinaus darf die Verschwiegenheitspflicht keine unangemessene Benachteiligung für den Arbeitnehmer bedeuten, vgl. § 307 Abs. 1 BGB. Dafür gilt es, das Bestehen eines berechtigten Interesses im Rahmen einer Einzelfallabwägung zu ermitteln. Enthält eine Verschwiegenheitsvereinbarung eine sog. „*Catch-All-Klausel*“, ist diese unwirksam, weil der Arbeitnehmer in unzumutbarer Weise an seinem beruflichen Fortkommen gehindert wird (Art. 12 Abs. 1 GG).[531]

4. Eine arbeitsvertragliche Verschwiegenheitspflicht stellt sicher, dass die arbeitsvertragliche Treuepflicht über das Ende des Arbeitsverhältnisses hinaus in Form einer sog. „*nachwirkenden Verschwiegenheitspflicht*“ fortwirken kann. Zwar endet mit der Beendigung des Arbeitsverhältnisses auch die arbeitsvertragliche Verschwiegenheitsklausel. Soweit jedoch die Treuepflicht fortwirkt, gewährleistet die beendete arbeitsvertragliche Verschwiegenheitsklausel, dass das Geheimhaltungsinteresse auf Seiten des ehemaligen Arbeitgebers erkennbar fortbesteht, welches wie-

---

[530] Siehe: Kapitel B) II. 4.
[531] Siehe: Kapitel B) II. 4. a).

derum notwendige Voraussetzung für die nachwirkende Verschwiegenheitspflicht ist.[532] Die nachwirkende Treuepflicht bezieht sich auf Informationen, die nicht mehr zu den redlich erworbenen Erfahrungen und Fähigkeiten eines Arbeitnehmers zählen, weil ein Abruf beispielsweise nur unter Zuhilfenahme angefertigter Unterlagen möglich ist.

5. Zu den Überwachungs- und Kontrollmaßnahmen im Bereich des Geheimnisschutzes gehören Maßnahmen, die auf die Regeltreue der Beschäftigten hinwirken und eine effektive Aufarbeitung im Falle eines Geheimnisverrats gewährleisten. Begrenzende Wirkung haben insbesondere die datenschutzrechtlichen Vorgaben, wobei von der Unionsrechtswidrigkeit des § 26 Abs. 1 S. 1 BDSG sowie des § 26 Abs. 1 S. 2 BDSG auszugehen ist.[533] Die unter den beiden Vorschriften entwickelten Maßstäbe beanspruchen weiterhin auf der Grundlage des Art. 6 Abs. 1 lit. f) DS-GVO Geltung. Anders sieht dies jedoch mit Blick auf verdeckt durchgeführte Überwachungsmaßnahmen aus. Zwar bleiben verdeckt durchgeführte Maßnahmen grundsätzlich auch weiterhin nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO zulässig. Allerdings braucht es für die Heimlichkeit der Maßnahme einer Beschränkung der Informationspflicht, die nur im Wege eines Beschränkungstatbestandes möglich ist. § 32 Abs. 1 Nr. 4, Abs. 3 BDSG hilft nur in begrenzten Einzelfällen weiter. Insofern bietet sich der Abschluss einer Betriebsvereinbarung als datenschutzrechtliche Legitimationsgrundlage für verdeckt durchgeführte Überwachungsmaßnahmen an, vorausgesetzt die Verankerung des Transparenzgrundsatzes ist durch die Betriebsparteien sichergestellt, vgl. Art. 88 Abs. 2 DS-GVO i. V. m. § 26 Abs. 4 BDSG.

---

[532] Siehe: Kapitel B) II. 4. a).
[533] Siehe: Kapitel B) II. 4. b).

6. Bewerberprüfungen zu Zwecken des Geschäftsgeheimnisschutzes dienen der Integritätsprüfung eines Bewerbers. Ein Fragerecht besteht, soweit der Arbeitgeber ein berechtigtes Interesse an der Beantwortung der Frage hat. Fragen nach etwaigen Vorstrafen sind nur erlaubt, sofern es sich dabei um sog. einschlägige Vorstrafen handelt.[534] Möglich ist auch die Durchführung elektronischer Datenabgleiche. Kommen KI-Systeme zum Einsatz, ist das arbeitgeberseitige Interesse an einer effektiven und objektiven Auswahlentscheidung mit dem Persönlichkeitsschutz des Bewerbers abzuwägen und in einen angemessenen Ausgleich zu bringen.

Was bedeutet das für das unternehmerische Compliance-System?

1. Um wirtschaftliche Nachteile vom Unternehmen fernzuhalten, ist die Geschäftsleitung gesellschaftsrechtlich verpflichtet, geheime Informationen dem Schutzregime des GeschGehG zu unterstellen. Dies umfasst die Implementierung betrieblicher Geheimhaltungsmaßnahmen, vgl. § 2 Nr. 1 lit. b) GeschGehG. Die Unternehmensleitung hat zudem darüber zu wachen, dass die eingeführten Maßnahmen dem Angemessenheitserfordernis dauerhaft gerecht werden und ist verpflichtet, ggf. adäquate Anpassungen vorzunehmen. Unterlässt ein Unternehmen entsprechende Maßnahmen, drohen nach § 130 OWiG empfindliche Bußgelder. Duldet die Unternehmensleitung pflichtwidrig Verstöße eines Arbeitnehmers gegen das GeschGehG und erleidet das Unternehmen dadurch einen Schaden, kann die Geschäftsleiter-Haftung nach § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG greifen.[535]

2. Für die Festlegung konkreter Geheimhaltungsmaßnahmen bietet sich ein abgestuftes Vorgehen an. In einem ersten Schritt sind die zu schützenden Informationen zu identifizieren. In einem zweiten Schritt sind die identifizierten Informationen Kategorien nach

[534] Siehe: Kapitel B) II. 4. c).
[535] Siehe: Kapitel B) III.

absteigender Wichtigkeit zuzuordnen. Die Wichtigkeit entscheidet darüber, welche Maßnahmen prioritär zu implementieren sind. Sodann empfiehlt sich ein Vorgehen anhand der Erkennbarkeit der Geheimhaltung in Bezug auf die jeweilige Information. Geheimnisschutzkonzepte benötigen auch entsprechende Mechanismen, um Sicherheitslücken im konkreten Verdachtsfall identifizieren und sodann schließen zu können. Aus Nachweisgründen sind die implementierten Maßnahmen zu dokumentieren.[536]

3. Die Anforderungen an die Datensicherheit ähneln den Anforderungen an die angemessenen Geheimhaltungsmaßnahmen. Insofern bietet es sich an, mögliche Synergien zu heben.[537] Kommt es dabei zur Offenlegung von Geschäftsgeheimnissen gegenüber dem Datenschutzbeauftragten, unterliegt dieser einer Verschwiegenheitspflicht, die auch gegenüber der Aufsichtsbehörde zu beachten ist, Art. 38 Abs. 5 DS-GVO i. V. m. § 241 Abs. 2 BGB. Eine Meldepflicht des Datenschutzbeauftragten gegenüber der Aufsichtsbehörde bzgl. etwaiger Datenverstöße besteht nicht. Dem Datenschutzbeauftragten bleibt es allerdings unbenommen, Geschäftsgeheimnisse nach Maßgabe des § 6 Abs. 1 HinSchG zu melden.[538]

---

536 Siehe: Kapitel B) III.
537 Siehe: Kapitel B) III.
538 Zu den Voraussetzungen des § 6 Abs. 1 HinSchG siehe ausführlich: Kapitel C) I. 2. a).

C) Der Geschäftsgeheimnisschutz: Reichweite und Grenzen im Beschäftigungskontext

Der Schutz vor unerlaubter Erlangung, Nutzung und Offenlegung von Geschäftsgeheimnissen gilt nicht uneingeschränkt.[539] Nach § 3 Abs. 2 GeschGehG können gesetzliche und rechtsgeschäftliche Sonderregelungen zum Umgang mit Geschäfts-geheimnissen dem Geheimnisschutz nach dem GeschGehG vorgehen. Dazu zählen insbesondere das Recht als Whistleblower Informationen über Verstöße zu melden, die zugleich Geschäftsgeheimnisse sind sowie Auskunfts- und Informationsrechte.[540] Darüber hinaus gibt es Fälle, in denen öffentliche bzw. höherrangige Interessen den Geheimnisschutz überwiegen. § 5 GeschGehG normiert hierfür Tatbestandsausnahmen.[541]

Inwieweit ein Unternehmen im Beschäftigungskontext zur Offenlegung seiner Geschäftsgeheimnisse verpflichtet ist bzw. die Weitergabe oder Offenlegung der geschützten Informationen zu dulden hat, wird die vorliegende Darstellung im Folgenden untersuchen. Schwerpunkte der Analyse bilden dabei das Verhältnis des Geschäftsgeheimnisschutzes zum Hinweisgeberschutz und zu den datenschutzrechtlichen Betroffenenrechten. Sowohl das Spannungsverhältnis zwischen Geschäftsgeheimnisschutz und Whistleblowing als auch das Spannungsverhältnis zwischen Geschäftsgeheimnisschutz und Datenschutz bilden Konflikte widerstreitender Rechtspositionen, die in einen angemessenen Ausgleich zu bringen sind. Abschließend widmet sich die vorliegende Arbeit dem Verhältnis des Geschäftsgeheimnisschutzes zu den Rechten der Arbeitnehmervertretungen.

---

539 *Reinfeld,* Das neue GeschGehG, § 1 Rn.62.

540 Vgl. §§ 81 ff. BetrVG, § 10 Abs. 1 EntgTranspG, § 13 AÜG, § 613a Abs. 5 BGB, § 7 TzBfG, Art. 15 DS-GVO. Erlangt ein Arbeitnehmer durch ein Ausüben seiner Rechte ein Geschäftsgeheimnis, stellt § 3 Abs. 1 Nr. 3 Var. 1 GeschGehG klar, dass das Haftungssystem des GeschGehG keine Anwendung findet.

541 Vgl. §§ 3 Abs. 2, 5 Nr. 1 bis 3 GeschGehG.

I. Geschäftsgeheimnisschutz und Whistleblowing

Whistleblowing war seit jeher ein großes Diskussionsthema.[542] Wurden Whistleblower zunächst vorwiegend des Denunziantentums bezichtigt, wird heute zunehmend die Zivilcourage in den Fokus gerückt.[543] Mit dem am 2. Juli 2023 in Kraft getretenen HinSchG hat der Hinweisgeberschutz eine richtungs-weisende Stärkung erfahren.[544] Unternehmen stehen seitdem vor der Herausforderung, Anreize für eine interne Meldung zu schaffen, auch um darauf hinzuwirken, dass geheimhaltungs-bedürftige Information nicht nach außen gelangen. Sowohl die Implementierung eines wirksamen Hinweisgeberschutzsystems als auch die Schaffung von Anreizen zu dessen Nutzung sind daher spätestens mit Inkrafttreten des HinSchG als Teil des unternehmerischen Geheimnisschutzkonzeptes zu begreifen und fließen in die Beurteilung angemessener Geheimhaltungsmaßnahmen im Sinne des § 2 Nr. 1 lit. b) GeschGehG mit ein.

Die vorliegende Arbeit beleuchtet zunächst die Grundlagen des Whistleblowings. Dafür gilt es, die bestehenden Friktionen zwischen GeschGehG und HinSchG herauszuarbeiten und einer Lösung zuzuführen. Im Zuge der Nachforschungen wird untersucht, unter welchen Voraussetzungen Whistleblower bei der Erlangung und Weitergabe bzw. Offenlegung von Geschäftsgeheimnissen geschützt sind, respektive dem Geheimnisinhaber Schutz- und Abwehransprüche nach dem GeschGehG versagt bleiben müssen. Die vorliegende Arbeit analy-

---

[542] Um nur einige zu nennen: *Chelsea Manning, Julian Assange, Edward Snowden, „Panama Papers*“, „*Cum-Ex-Skandal*“ sowie die Enthüllungen von „*WikiLeaks*“, vgl. *Redder*, Schutz von Whistleblowern, S. 32-35; *Schenkel*, Whistleblowing und Strafbarkeit, S. 1, 2; *Wiedmann*/*Seyfert*, CCZ 2019, 12, 13; *Garden*/*Hiéramente*, BB 2019, 963; *Schmitt*, NZW-Beilage 2020, 50, 54; *Hiéramente*, in: BeckOK-GeschGehG, § 5 Rn.17.

[543] *Beukelmann*, NJW-Spezial 2019, 312; *Szesny*, BB 2019, Heft 16-17, Umschlagteil, I (Die Erste Seite); *Schröder*, ZRP 2020, 212, 213; *Simon*/*Schilling*, BB 2011, 2421, 2422.

[544] Gesetz für einen besseren Schutz hinweisgebender Personen, BGBl. I v. 31.05.2023, Nr. 140.

siert zudem mögliche Anreize für eine vorrangige Nutzung eines internen Meldekanals. Schwerpunkte bilden in diesem Zusammenhang die Fragen, ob und inwieweit Arbeitnehmer zur Abgabe einer (vorrangig) internen Meldung verpflichtet werden können und inwieweit Unternehmen den Identitätsschutz für Whistleblower bei der Nutzung eines internen Meldekanals erhöhen können.

1. Grundlagen des Whistleblowings

Der Begriff „*Whistleblowing*“ findet seinen Ursprung im Anglo-Amerikanischen.[545] Gemeint sind insbesondere Personen aus dem Innenbereich einer Organisation, die Informationen über Missstände, von denen sie im Zusammenhang mit ihrer beruflichen Tätigkeit erfahren haben, an interne oder externe Stellen melden oder diese gegenüber der Öffentlichkeit offenlegen.[546] Dem Whistleblower geht es dabei um die Aufdeckung von Missständen, die aus seiner Sicht im öffentlichen Interesse liegt. Sein Ziel ist es, die Missstände abzustellen und politische Debatten anzustoßen. Alternativ zum Begriff des „*Whistleblowers*“ findet sich häufig der gleichbedeutende Begriff des „*Hinweisgebers*“.[547] Da sich die Begriffe inhaltlich nicht unterscheiden, scheint nach hiesiger Auffassung keiner der Begriffe gegenüber

---

[545] *Müller*, NZA 2002, 424, 425; *Ohly*, in: Harte-Bavendamm/Ohly/Kalbfus GeschGehG, § 5 Rn.30; *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 411; *Sixt*, Whistleblowing im Spannungsfeld, S. 22.

[546] *Aldoney Ramìrez*, Schutz von Geschäfts- und Betriebsgeheimnissen, S. 352-353; *Alexander*, in: Köhler/Born-kamm/Feddersen UWG, § 5 GeschGehG Rn.26; *Azar*, JuS 2017, 930; *Forst,* NJW 2011, 3477; *Hauck*, GRUR-Prax 2019, 223, 225; *Krause*, SR 2019, 138; *Nöbel*/*Veljovic*, CB 2020, 34; *Redder*, Schutz von Whistleblowern, S. 26-28; *Ullrich*, NZWiSt 2019, 65. Vgl. auch Erwägungsgründe 1 und 37 der Whistleblowing-RL.

[547] *Nöbel*/*Veljovic*, CB 2020, 34, 35; *Ohly*, in: Harte-Bavendamm/Ohly/Kalbfus GeschGehG, § 5 Rn.30; *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 411 m. w. N.

dem jeweils anderen vorzugswürdig.[548] Soweit die vorliegende Darstellung überwiegend vom „*Whistleblower*“ spricht, ist dies allein dem Umstand geschuldet, dass es sich hierbei um den historisch gewachsenen Begriff handelt.

Die nachfolgenden Abschnitte beleuchten den Rechtsrahmen des Whistleblowings und wie dieser durch das HinSchG in Umsetzung der Whistleblowing-RL ausgestaltet worden ist. Im Fokus steht dabei das Zusammenspiel von Whistleblowing-RL und GeschGeh-RL sowie HinSchG und GeschGehG.

a) Rechtsrahmen und Funktion

Die Informationsweitergabe eines Whistleblowers an eine interne oder externe Meldestelle sowie die Offenlegung gegenüber der Öffentlichkeit unterfällt dem Schutzbereich der Meinungsfreiheit.[549] Dafür spricht, dass jede Meldung zugleich ein Ausdruck von Kritik ist, die Bedeutung für die Meinungsbildung Dritter haben kann.[550]

Verfassungsrechtlich ist die Meinungsfreiheit im Rahmen des Art. 5 Abs. 1 S. 1 Hs. 1 GG geschützt. Konventionsrechtlich folgt dies aus Art. 10 EMRK und unionsrechtlich aus Art. 11 GR-CH, wobei Schutzbereich und Schranken im Wesentlichen mit denen in Art. 5 Abs. 1 S. 1 Hs. 1 GG übereinstimmen.[551] Zu Recht spricht

---

[548] *Aldoney Ramírez*, Schutz von Geschäfts- und Betriebsgeheimnissen, S. 352; *Ullrich*, NZWiSt 2019, 65; *Thüsing*/*Fütterer*/*Jänsch*, RDV 2018, 133; a. A.: *Nöbel*/*Veljovic*, CB 2020, 34; *Redder*, Schutz von Whistleblowern, S. 28, 29; *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 411, auf eine negative Konnotation in dem Begriff des Whistleblowers hinweisend.

[549] BAGE 107, 36, 44; BAG NJW 2017, 1833, 1834.

[550] Zur Diskussion, inwieweit anonyme Anzeigen von der Meinungsfreiheit geschützt sein können: Kritisch BAGE 107, 36, 44 1191; grundsätzlich bejahend dagegen: BGHZ 181, 328, 241, 342. Ausführlicher dazu: *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Drittes Kapitel, S. 271.

[551] *Schmitt*, RdA, 365, 368, 372.

Dobler in diesem Zusammenhang von *„einem kongruenten Rechtmäßigkeitsmaßstab nach deutschem Recht und Unionsrecht.“*[552] Da die Meinungsfreiheit einen konstitutiven Beitrag für die Demokratie leistet, greift eine Vermutung für die freie Rede, sobald der Whistleblower im öffentlichen Interesse für die öffentliche Meinungsbildung wirkt.[553] Es ist mittlerweile anerkannt, dass Whistleblower entscheidend dazu beitragen, Debatten in der Öffentlichkeit anzustoßen. Diese dienen zugleich der Wahrung des Gemeinwohlinteresses, da Missstände benannt und infolgedessen abgestellt werden können.[554] Dennoch gilt das Recht auf Meinungsfreiheit nicht absolut, obgleich erhöhte Rechtfertigungsanforderungen für eine Beschränkung notwendig sind.[555] Beschränkungen kommen immer dann in Betracht, wenn die Informationsweitergabe in tatsächlicher Hinsicht keinen Mehrwert für die öffentliche Meinungsbildung leistet. Im Übrigen entscheidet eine Interessenabwägung. Zu beachten ist jedoch, dass auch ein gutgläubiger Hinweisgeber geschützt sein muss.[556] Voraussetzung ist, dass dieser zum Zeitpunkt der Meldung bzw. Offenlegung berechtigterweise davon ausgehen durfte, dass ein Missstand besteht und dieser Missstand im Falle seines Bestehens einen Mehrwert für die öffentliche Debatte leistet. Die Meldung vorsätz-licher Falschinformationen ist demzufolge nicht von der Meinungsfreiheit geschützt.[557]

---

[552] *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Drittes Kapitel, S. 271.

[553] BVerfGE 7, 198, 208, 212 - *Lüth*; 61, 1, 11; 11, 116, 150; BVerfG, NJW 2006, 3266, 3267; BGHZ 45, 296.

[554] *Payandeh*, JuS 2016, 690, 694, 695; EGMR, Urteil v. 21.07.2011 - 28274/08 - *Heinisch/Deutschland.*

[555] Vgl. BVerfGE 66, 116, 137-139 - *Springer/Wallraff*, für den Bereich des investigativen Journalismus; BVerfG, NJW 2006, 3266, 3267; ähnlich BVerfG, NJW 2020, 2622, 2623, 2629, 2630-2632, 2636; *Payandeh*, JuS 2016, 690, 694, 695; EGMR, Urteil v. 21.07.2011 - 28274/08 - *Heinisch/Deutschland.*

[556] *Schmitt*, RdA, 365, 365.

[557] *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Drittes Kapitel, S. 271.

b) Die gesetzgeberische Ausgestaltung des Whistleblowings

Am 2. Juli 2023 ist das HinSchG in Umsetzung der Whistleblowing-RL in Kraft getreten. Gab es vor Inkrafttreten des HinSchG nur vereinzelte Regelungen, die Whistleblower vor rechtlichen Sanktionen schützten, sind die Anforderungen seit Inkrafttreten des HinSchG denkbar niedrig.[558] Nach den Vorgaben des HinSchG stehen Whistleblowern interne und externe Meldekanäle zur Verfügung, vgl. §§ 12, 19 ff. HinSchG. Unter den zusätzlichen Voraussetzungen des § 32 HinSchG kann auch eine Offenlegung der Informationen in Betracht kommen. Beschäftigungsgeber ab in der Regel 50 Beschäftigten müssen eine interne Meldestelle einrichten und betreiben, über die Whistleblower Verstöße über Informationen melden können, die dem sachlichen Anwendungsbereich des § 2 HinSchG unterfallen.

Vor dem Inkrafttreten des HinSchG wurde das Whistleblowing maßgebend durch die Rechtsprechung der nationalen Arbeitsgerichte, des BVerfG sowie vom EGMR geprägt.[559] Meist ging es dabei um die Frage der Wirksamkeit einer Kündigung in Folge einer Informationsweitergabe.[560] Anhand der §§ 241 Abs. 2, 242 BGB waren sodann die Grundrechte von Arbeitnehmer und Arbeitgeber in einen angemessenen Ausgleich zu bringen. Dies mündete in eine Einzelfallabwägung

---

[558] Hinweisgeberschutz besteht schon dann, wenn die hinweisgebende Person zum Zeitpunkt der beabsichtigten Meldung oder Offenlegung hinreichenden Grund zu der Annahme hatte, dass die von ihr gemeldeten oder offengelegten Informationen der Wahrheit entsprechen, vgl. § 33 HinSchG Die Anforderungen an die Verifizierung des Wahrheitsgehalts einer Information durch den Hinweisgeber sind denkbar niedrig gehalten, BT-Drs. 20/5992, S. 78, 92. Einschränkend zu Recht: *Siemes,* CCZ 2022, 293, 302, wonach die Befürchtung entdeckt zu werden, nicht rein subjektiv sein darf; ebenso *Thüsing/Musiol,* BB 2022, 2420, 2421.

[559] Insbesondere EGMR, Urteil v. 21.07.2011 - 28274/08 - *Heinisch*/*Deutschland.* Ausführlich: *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse, S. 416-428; *Sixt*, Whistleblowing im Spannungsfeld, S. 55.

[560] *Krause*, SR 2019, 138, 141; *Ohly*, in: Harte-Bavendamm/Ohly/Kalbfus GeschGehG, § 5 Rn.16; *Colneric*/*Gerdemann*, Umsetzung der Whistleblowing-RL, S. 66-74.

zwischen dem Grundrecht auf Meinungsfreiheit und den unternehmerischen Geheimhaltungsinteressen, die ihrerseits grundrechtlich geschützt sind.[561] Mit der Zeit ließen sich aus der nationalen Rechtsprechung Kriterien in Bezug auf den Hinweisgeberschutz ableiten, die mit der Entscheidung des EGMR in der Rechtssache *Heinisch* eine wesentliche Ergänzung erfahren haben.[562] Sämtliche darauffolgende Entscheidungen lassen sich in das durch den EGMR aufgestellte Konstrukt einfügen.[563] Kriterien, die einen Vorrang der Meinungsfreiheit gegenüber den betrieblichen Interessen des Arbeitgebers bedingen können, waren nach der Rechtsprechung des EGMR: das öffentliche Interesse an der Information, die Berechtigung der Vorwürfe, der drohende Schaden in Folge der Informationsweitergabe sowie die Motive des Hinweisgebers.[564] Für eine externe Meldung galt zudem aus Verhältnismäßigkeitsgründen die Maßgabe, dass vor einer externen Meldung bzw. Offenlegung grundsätzlich innerbetriebliche Abhilfe über einen betrieblichen Kanal versucht werden müsse (sog. Eskalationsmodell).[565]

Der nationale Gesetzgeber entschied sich jedoch für eine Stärkung des Hinweisgeberschutzes und verschärfte im Zuge der Umsetzung der Whistleblowing-RL das von der Rechtsprechung entwickelte Eskalationsmodell hin zu einem grundsätzlich zweistufigen Modell. Das

---

561 Etwa: BAG, NJW 2017, 1833, 1834; EGMR, Urteil v. 21.07.2011 - 28274/08 - *Heinisch*/*Deutschland.* Zum grundrechtlichen Schutz unternehmerischer Geheimhaltungsinteressen siehe auch: Kapitel B) I. 3.

562 EGMR, Urteil v. 21.07.2011 - 28274/08 - *Heinisch*/*Deutschland.*

563 Dazu ausführlich: *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Sechstes Kapitel, S. 439 mit umfassenden Rechtsprechungs-Nachweisen.

564 EGMR, Urteil v. 21.07.2011 - 28274/08 - *Heinisch*/*Deutschland;* EGMR, Urteil v. 16.02.2021 - 23922/19, §§ 81-82; BAGE 107, 36, 45, 46; BAG NJW 2017, 1833, 1835; OLG Frankfurt, Urteil v. 17.05.2022 - II U 115/21 Rn.107-109.

565 EGMR, Urteil v. 21.07.2011 - 28274/08 - *Heinisch*/*Deutschland;* EGMR, Urteil v. 16.02.2021 - 23922/19, §§ 81-82; BAGE 107, 36, 45, 46; BAG NJW 2017, 1833, 1835; OLG Frankfurt, Urteil v. 17.05.2022 - II U 115/21 Rn.107-109.

HinSchG normiert nunmehr die allgemeine Möglichkeit einer externen Meldung, ohne dass hiervon einschränkend abgewichen werden kann, §§ 7, 39 HinSchG. Dies ist Beleg dafür, dass es dem nationalen Gesetzgeber im Rahmen der Umsetzung der Whistleblowing-RL vordergründig um die Stärkung des Hinweisgeberschutzes ging, zu deren Gunsten schützenswerte, dem Hinweisgeberschutz gegenläufige unternehmerische (Geheimhaltungs-) Interessen in den Hintergrund gerückt wurden.

Dass es zu dieser Abkehr vom Eskalationsmodell des EGMR kommt, war bis zuletzt nicht sicher absehbar.[566] Das bewährte System hätte in Umsetzung der Whistleblowing-RL jedenfalls weiter Bestand haben können. Doch aufgrund vieler Unstimmigkeiten zwischen den damaligen Koalitionspartnern[567] konnte das Umsetzungsgesetz nicht fristgerecht bis zum 17. Dezember 2021 umgesetzt werden.[568] Ausschlaggebend war auch, dass sich zu dieser Zeit ein Regierungswechsel vollzog. Unter der neuen Legislatur musste sodann unter Hochdruck eine neue Einigung erzielt werden. Diese geriet aufgrund abermaliger Dispute - diesmal zwischen Bund und Ländern - erneut ins Schwanken, konnte jedoch nach einer Anrufung des Vermittlungsausschusses einer Einigung zugeführt werden.[569]

Bemerkenswert ist, dass sich der nationale Gesetzgeber für eine Richtlinien überschießende Umsetzung entschieden hat (sog.

---

566 Die Abkehr vom Eskalationsmodell des EGMR war stark umstritten, vgl. *Schmitt*, NZA-Beilage 2020, 50, 56; *Schröder*, ZRP 2020, 212, 213; BDA-Stellungnahme zum HinSchG-E, August 2022, S. 6.

567 Der Ende 2020 vorgelegte Referentenentwurf eines Hinweisgeberschutzgesetzes fand in der Großen Koalition keine Mehrheit, vgl. *Gerdemann,* ZRP 2021, 37.

568 Die EU-Kommission leitete am 27.01.2022 ein Vertragsverletzungsverfahren gegen Deutschland und 23 weitere EU-Mitgliedstaaten ein, vgl. *Thüsing,* DB 2022, 1066; *Reufels*/*Osmakova,* ArbRB 2022, 147; *Miege/Ahrens,* CCZ 2022, 171, 172. Am 14.03.2023 reichte die EU-Kommission Klage gegen die Bundesrepublik Deutschland beim EuGH zum Az. C-149/23 ein.

569 *Dzida*, NZA-Editorial, 5/2023.

Goldplating).[570] Dies gilt insbesondere im Hinblick auf den sachlichen Anwendungsbereich des HinSchG, § 2 HinSchG. Das HinSchG enthält erstmals eine sektorübergreifende Kodifizierung des Hinweisgeberschutzes. Leider hat der nationale Gesetzgeber die Gelegenheit verpasst, den aus Gründen der Rechtssicherheit gebotenen Gleichlauf zwischen GeschGehG und HinSchG herzustellen. Stattdessen wurde mit § 6 HinSchG eine Erlaubnisnormgeschaffen,[571] die neben den Erlaubnistatbestand des § 5 Nr. 2 GeschGehG tritt.[572] Die erhoffte Rechtssicherheit an der Schnittstelle von Geschäftsgeheimnisschutz und Hinweisgeberschutz blieb damit aus.

c) Das Verhältnis von GeschGehG und HinSchG im Lichte der GeschGeh-RL und der Whistleblowing-RL

Der durch das GeschGehG in Umsetzung der GeschGeh-RL in § 5 Nr. 2 GeschGehG verankerte Hinweisgeberschutz führt zu der Frage seines Verhältnisses zu den Vorgaben des HinSchG in Umsetzung der Whistleblowing-RL. Aus § 3 Abs. 2 GeschGehG folgt, dass § 6 Abs. 1 HinSchG eine gesetzliche Gestattung im Hinblick auf den Geschäftsgeheimnisschutz darstellt. Dies ergibt sich auch aus dem Verweis in Art. 3 Abs. 2 GeschGeh-RL auf die Vorgaben der Whistleblowing-RL. Liegen die Voraussetzungen des HinSchG vor, ergibt sich daraus ein Vorrang des Hinweisgeberschutzes gegenüber dem Geschäftsgeheimnisschutz.[573] Daneben regelt § 5 Nr. 2 GeschGehG, dass die Nutzung oder Offenlegung von Geschäftsgeheimnissen zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens nicht unter die Verbotstatbestände in § 4 GeschGehG fällt, wenn die Erlangung, Nutzung oder Offenlegung geeignet ist, das allgemeine öffentliche Interesse zu schützen. Das Nebeneinander zweier nicht völlig kongruenter Hinweisgeberregelungen in § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG und

---

570 *Dzida*/*Seibt,* NZA 2023, 657.
571 Gemeint ist eine Erlaubnisnorm im Sinne des § 3 Abs. 2 GeschGehG.
572 BT-Drs. 20/5992, S. 55. Siehe ausführlich: Kapitel C) I. c) ee).
573 *Hoppe*/*Oldekop*, Geschäftsgeheimnisse, Rn.366, 462.

§ 5 Nr. 2 GeschGehG lässt Friktionen entstehen, die es aufzulösen gilt.[574] In einem ersten Schritt analysiert die Darstellung, worin die Unterschiede im Einzelnen bestehen. Daran anschließend wird ein Lösungsvorschlag zur Auflösung der bestehenden Friktionen herausgearbeitet.

aa) Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich des HinSchG erfasst Verstöße gegen bestimmtes Unionsrecht sowie sämtliche Verstöße, die straf- oder bußgeldbewehrt sind, wobei bußgeldbewehrte Verstöße nur erfasst sind, soweit die verletzte Vorschrift dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient, § 2 Abs. 1 Nr. 2 HinSchG. Darüber hinaus sind nach § 3 Abs. 2 S. 2 HinSchG auch Meldungen übe missbräuchliche Handlungen oder Unterlassungen, die dem Ziel oder dem Zweck der genannten Regelungen in § 2 HinSchG zuwiderlaufen, erfasst.

Demgegenüber stellt § 5 Nr. 2 GeschGehG auf das Vorliegen einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens ab. Eine Einschränkung auf bestimmte Regelungskomplexe kennt § 5 Nr. 2 GeschGehG nicht. Allerdings bedarf der Begriff der rechtswidrigen Handlung einer einschränkenden Auslegung, dass es eine rechtswidrige Handlung von einigem Gewicht braucht.[575] Dafür spricht Erwägungsgrund 20 GeschGeh-RL, der einen Rechtsverstoß bzw. Fehlverhalten von unmittelbarer Relevanz erwähnt. Auch die Systematik des GeschGehG streitet dafür, § 5 Nr. 2 GeschGehG als Tatbestandsausnahme aufgrund seines Ausnahme-

---

[574] Die Absicherung durch verschiedene Regelungen in zwei eigenständigen RL führt zu Ungereimtheiten und wird deshalb auch als „*Richtlinien-Potpourri*“ bezeichnet, vgl. *Ullrich*, WiJ 2019, 52; *Vogel*/*Poth*, CB 2019, 45, 46.

[575] *Hiéramente*, in: BeckOK-GeschGehG, § 5 Rn.20; *Reinbacher*, KriPoZ 2018, 115, 118, mit Verweis auf Erwägungsgrund 20 GeschGeh-RL.

charakters eng auszulegen. Das Telos des GeschGehG in Umsetzung der GeschGeh-RL deutet in dieselbe Richtung: Im Sinne einer Stärkung des Geschäftsgeheimnisschutzes gilt es, die Tatbestandsausnahme restriktiv zu begreifen. Nach alledem ist daher davon auszugehen, dass § 5 Nr. 2 GeschGehG nicht jede rechtswidrige Handlung erfasst. Vielmehr ist der Begriff im Gesamtzusammenhang zu verstehen. Nach § 5 Nr. 2 GeschGehG muss die Offenlegung einer rechtswidrigen Handlung geeignet sein, das allgemeine öffentliche Interesse zu schützen.[576] Die rechtswidrige Handlung muss also im Zusammenhang mit dem allgemeinen öffentlichen Interesse stehen.[577] Dies bedeutet, dass die Informationsweitergabe einen Mehrwert für die öffentliche Debatte haben muss. Hintergrund ist, dass das Whistleblowing Ausdruck der Meinungsfreiheit ist, die ihrerseits voraussetzt, dass die Informationsweitergabe einen Beitrag für die öffentliche Debatte leistet.[578]

In der Gesetzesbegründung zum GeschGehG heißt es folgerichtig: „*Die Einstufung eines Rechtsverstoßes als straf- oder bußgeldbewehrt ist ein Indiz dafür, dass der Gesetzgeber diesem eine besondere Schwere beimisst.*"[579] Demgemäß ist im Rahmen des § 5 Nr. 2 GeschGehG in Fällen der Offenlegung rechtswidriger Handlungen von einer einzelfallbezogenen Bagatellschwelle auszugehen, die nach Maßgabe des nationalen Gesetzgebers regelmäßig in Fällen eines straf- oder bußgeldbewehrten Verstoßes überschritten ist.[580] Aufgrund der fehlenden Beschränkung auf bußgeldbewehrte Verstöße, die dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dienen (vgl. § 2 Abs. 1 Nr. 2 HinSchG), ist festzuhalten, dass der sachliche Anwendungsbereich des § 5 Nr. 2 GeschGehG hinsichtlich des Kriteriums

---

576 *Hiéramente*, in: BeckOK-GeschGehG, § 5 Rn.20.
577 BT-Drs. 19/8300, S. 14; *Hauck*, AfP 2021, 193, 203.
578 Siehe: Kapitel C) I. 1. a).
579 BT-Drs. 19/4724, S. 40.
580 BT-Drs. 19/4724, S. 29; *Hauck*, AfP 2021, 193, 203; *Hoppe*/*Oldekop*, Geschäftsgeheimnisse, Rn.566, 567.

der rechtswidrigen Handlung weiter ist als der Anwendungsbereich des HinSchG.

Darüber hinaus ist zu prüfen, inwieweit Meldungen über formal rechtmäßige Tatsachen geschützt sind. Im Rahmen des § 5 Nr. 2 GeschGehG könnte formal rechtmäßiges Verhalten unter den Begriff „*eines beruflichen oder sonstigen Fehlverhaltens*“ zu subsumieren sein. Das berufliche Fehlverhalten scheidet jedoch aus. Ein beruf-liches Fehlverhalten meint einen Verstoß gegen berufsständige Normen und geht folgerichtig in dem Begriff der rechtswidrigen Handlung auf.[581] Fraglich ist, ob das auch für die Formulierung des „*sonstigen Fehlverhaltens*“ gilt. Es handelt sich um einen unbestimmten Rechtsbegriff, der einer Auslegung bedarf. Der Begriff „*Fehlverhalten*“ impliziert, dass nicht jedes Verhalten erfasst wird, sondern ein verwerfliches Element erforderlich ist. Der Zusatz „*sonstiges*“ stellt den Bezug zu den vorherigen Varianten „*rechtswidrige Handlung*“ und „*berufliches Fehlverhalten*“ her. Daraus folgt, dass es sich um ein der Schwere nach vergleichbares Verhalten handeln muss, das zwar nicht rechtswidrig ist, dessen verwerfliches Moment dem Unwert einer rechtswidrigen Handlung oder eines beruflichen Fehlverhaltens aber gleichkommt. Gestützt wird dieses Verständnis durch das Telos des GeschGehG, das auf die Stärkung des Geschäftsgeheimnisschutzes zielt. Folgerichtig muss das gemeldete Fehlverhalten von einigem Gewicht sein, um einen Vorrang gegenüber dem Geschäftsgeheimnisschutz zu rechtfertigen.

In der Gesetzesbegründung heißt es dazu: „*Darüber hinaus ist die Erlangung, die Nutzung oder die Offenlegung eines Geschäftsgeheimnisses gerechtfertigt, um ein sonstiges Fehlverhalten aufzudecken. Hiervon können Aktivitäten erfasst sein, die ein unethisches Verhalten darstellen, aber nicht notwendigerweise gegen Rechtsvorschriften verstoßen. Ein Beispiel hierfür könnten Auslandsaktivitäten eines Unternehmens sein, die in den betreffenden Ländern nicht*

[581] *Hiéramente*, in: BeckOK-GeschGehG, § 5 Rn.22.

rechtswidrig sind, aber dennoch von der Allgemeinheit als Fehlverhalten gesehen werden, wie zum Beispiel Kinderarbeit oder gesundheits- oder umweltschädliche Produktionsbedingungen.“[582]

Daraus folgt nach hiesiger Auffassung, dass der nationale Gesetzgeber unter dem Begriff des sonstigen Fehlverhaltens Menschrechtsverletzungen subsumiert wissen will. Dies überzeugt insofern, dass Auslandsaktivitäten eines Unternehmens, die nach dem dort geltenden Recht nicht rechtswidrig sind und menschenrechtliche Verstöße darstellen, von der Allgemeinheit als Fehlverhalten erkannt werden. Menschenrechtsverletzungen entlang der Lieferkette stellen zudem ein Fehlverhalten dar, das dem Unrecht einer rechtswidrigen Handlung gleicht, sodass Wortlaut und Telos der Norm für diese Auslegung streiten.[583] Dem steht nicht entgegen, dass der Gesetzgeber nicht explizit „*Menschenrechtsverletzungen*“ im Rahmen des § 5 Nr. 2 GeschGehG formuliert hat. Ausschlaggebend dürfte die Formulierung im Rahmen der GeschGeh-RL gewesen sein, die ebenfalls vom „*sonstigen Fehlverhalten*“ spricht und die der Gesetzgeber sprachlich nicht verändern wollte. Der Hinweis auf die Umgehung von Steuertatbeständen im Rahmen der Gesetzesbegründung zeigt, dass der Gesetzgeber sich außerdem nicht abschließend auf eine bestimmte Kategorie eines möglichen Fehlverhaltens festlegen wollte.[584] Der Verweis auf die systematische und unredliche Umgehung von Steuertatbeständen als weiterer Fall eines sonstigen Fehlverhaltens läuft allerdings ins Leere.[585] Die Umgehung von Steuertatbeständen stellt bereits für sich genommen eine rechtswidrige Handlung dar, sodass es keines Rückgriffs auf ein „*sonstiges Fehlverhalten*“ braucht.

---

[582] BT-Drs. 19/4724, S. 29.

[583] Diese Lesart ist nach hiesiger Auffassung unionsrechtskonform: Art. 5 lit. b) GeschGeh-RL verlangt ebenfalls ein sonstiges Fehlverhalten, ohne dieses weiter zu spezifizieren.

[584] BT-Drs. 19/4724, S. 29.

[585] BT-Drs. 19/4724, S. 29; dies aufgreifend: *Hauck*, AfP 2021, 193, 203; *Krause*, SR 2019, 138, 147; *Hoppe*/*Oldekop*, Geschäftsgeheimnisse, Rn.564, 565.

Zu beachten ist jedoch, dass seit Inkrafttreten des GeschGehG die Wahrung der Menschenrechte entlang der Lieferkette eine einfachgesetzliche Verankerung durch das LkSG erfahren hat.[586] Mit der Einführung des LkSG hat der Gesetzgeber einen Rechtsrahmen geschaffen, der die unternehmerische Verantwortung für die Einhaltung von Menschenrechten in den globalen Lieferketten regelt und insbesondere den Schutz vor Kinderarbeit sowie den Umweltschutz erfasst, vgl. § 2 LkSG. Unternehmen, die etwaigen Menschenrechtsverstößen entlang ihrer Lieferkette weder angemessen entgegenwirken noch in angemessener Art und Weise Abhilfe leisten, handeln rechtswidrig im Sinne der bußgeldbewehrten Vorgaben der §§ 6, 7 LkSG.

Die Einführung des LkSG hat zur Konsequenz, dass dem sonstigen Fehlverhalten im Sinne des § 5 Nr. 2 GeschGehG kein eigenständiger Anwendungsbereich mehr verbleibt. Verstöße gegen das LkSG sind über die „*rechtswidrige Handlung*“ erfasst. Zum jetzigen Zeitpunkt ist nicht davon auszugehen, dass der Gesetzgeber von seiner Intention, die Achtung der Menschenrechte entlang der Lieferkette legislativ abzusichern, wieder abrücken wird. Im Gegenteil: Der Unionsgesetzgeber hat sich im Trilog mit den europäischen Institutionen am 15. März 2024 auf eine eigene EU-Lieferkettenregelung geeinigt, der sog. CSDDD-RL, die der nationale Gesetzgeber voraussichtlich über eine Fortentwicklung des LkSG umsetzen wird. Vor diesem Hintergrund ist davon auszugehen, dass der Regelung des „*sonstigen Fehlverhaltens*“ auch in Zukunft kein eigener Anwendungsbereich verbleiben wird, weil die Wahrung der Menschenrechte entlang der

[586] Das Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten ist am 01.01.2023 in Kraft getreten, vgl. BGBl. I v. 16.07.2021, S. 2959.

Lieferkette ihre einfach gesetzliche Verankerung beibehalten wird.[587] Sowohl das berufliche Fehlverhalten als auch das sonstige Fehlverhalten gehen folgerichtig vollständig in der „*rechtswidrigen Handlung*“ auf. Dies hat zur Konsequenz, dass § 5 Nr. 2 GeschGehG kein formal rechtmäßiges Handeln (mehr) erfasst.[588]

Für das HinSchG stellt § 3 Abs. 2 S. 2 HinSchG klar, dass auch Meldungen über missbräuchliche Handlungen oder Unterlassungen, die dem Ziel oder dem Zweck der in § 2 HinSchG genannten Regelungen zuwiderlaufen, geschützt sind. Fraglich ist, was das HinSchG mit dem Begriff „*missbräuchlich*“ meint. Der Begriff erinnert an den Einwand des unzulässigen Rechtsmissbrauchs zur Abwehr von Forderungen, vgl. § 242 BGB.[589]

In der Gesetzesbegründung zum HinSchG heißt es: „*Mit dieser Vorschrift sollen Praktiken erfasst werden, die der Gesetzgeber bei der Regelung der betreffenden Fachmaterie nicht im Blick hatte, die er aber miteinbezogen hätte, wenn er eine Vorstellung von den möglichen Umgehungsversuchen gehabt hätte. Mit dieser Regelung werden daher auch missbräuchliche Praktiken im Sinne der EuGH-Rechtsprechung vom Anwendungsbereich umfasst, das heißt solche, die zwar in formaler Hinsicht nicht als rechtswidrig erscheinen, die jedoch mit*

---

[587] Vor Inkrafttreten des LkSG hat das OLG Oldenburg z. B. entschieden, dass der Export von Giftstoffen, die im Empfängerstaat auch zur Vollstreckung der Todesstrafe Verwendung finden, ein ethisch zu missbilligendes Verhalten darstellt, welches nach dem Willen des Gesetzgebers dem Begriff des beruflichen oder sonstigen Fehlverhaltens im Sinne des § 5 Nr. 2 GeschGehG unterfallen soll. Das OLG Oldenburg zog in diesem Zusammenhang unter anderem die Wertung des Art. 102 GG zur Todesstrafe heran, vgl. OLG Oldenburg, Beschluss v. 21.05.2019 - 1 Ss 72/19, NZWiSt, 2021, 30.

[588] Grundlegend zur Kontroverse rund um den Begriff des sonstigen Fehlverhaltens: *Hiéramente*, in: BeckOK-GeschGehG, § 5 Rn.23-26.

[589] So auch: *Hütter-Brungs*, in: Thüsing, HinSchG, § 3 Rn.6 und *Colneric/Gerdeman*, in: BeckOK-HinSchG, § 3 Rn.9, die auf das Verbot des Rechtsmissbrauchs als allgemeinen Grundsatz des Unionsrechts hinweisen.

dem Ziel oder Zweck der einschlägigen Rechtsvorschriften unvereinbar sind. (...) Die Versagung eines Rechts oder Vorteils wegen missbräuchlicher oder betrügerischer Tätigkeiten ist daher nach der Rechtsprechung des EuGH auch nur die bloße Folge der Feststellung, dass im Fall von Betrug oder Rechtsmissbrauch die objektiven Voraussetzungen für die Erlangung des ersuchten Vorteils in Wirklichkeit nicht erfüllt sind und daher für die Versagung keine spezielle Rechtsgrundlage erforderlich ist (EuGH, Rs. C-251/16, Cussens u. a., Rn.32)."[590]

Die Bezugnahme des nationalen Gesetzgebers auf den EuGH bestätigt, dass der Begriff im Sinne des Verbots des Rechtsmissbrauchs zu verstehen ist. Ebenso wie das nationale Recht kennt das europäische Recht das Verbot des Rechtsmissbrauchs, welches durch die Rechtsprechung des EuGH mittlerweile generell anerkannt ist.[591]

Die Formulierung in § 3 Abs. 2 S. 2 HinSchG ist daher so zu verstehen, dass dem Whistleblower auch dann Schutz nach den Vorgaben des HinSchG zu gewähren ist, sofern der Beschäftigungsgeber aufgrund seines treuwidrigen Handelns Anlass für eine Meldung gegeben

---

590 BT-Drs. 20/3442, S. 64.

591 Das Gebot von Treu und Glauben gilt über die Normierungen hinaus: Die „*betrügerische oder missbräuchliche Berufung auf Unionsrecht ist unzulässig*", vgl. etwa EuGH, NJW 2022, 40 Rn.121 - *UK/Volkswagen Bank*; NJW 2016, 2796 Rn.38 - *Kratzer*; EuZW 2007, 641 Rn.38 - *Kofoed*.

hat.[592] Dafür spricht, dass die Interessen des Beschäftigungsgebers nach dem Willen des nationalen Gesetzgebers gegenüber der Meinungsfreiheit des Hinweisgebers zurücktreten sollen, sofern das treuwidrige Verhalten des Beschäftigungsgebers Anlass genug ist, einen Beitrag für den öffentlichen Diskurs zu liefern. Diese Lesart folgt auch aus dem Hinweis, dass der Gesetzgeber Praktiken einbeziehen will, die er selbst noch nicht erblickt hat.[593] Die Information über diese Praktiken ist insofern nötig, damit der Gesetzgeber daran anknüpfend entsprechende gesetzliche Änderungen auf den Weg bringen kann. Hinweisgeberschutz soll also nicht nur bestehen, um Rechtsverstöße abzustellen. Es geht auch darum, im Wege einer Stärkung des Whistleblowings dafür Sorge zu tragen, dass Whistleblower bestehende Rechtslücken aufzeigen können. Erweisen sich Geschäftspraktiken als unredlich oder treuwidrig, ohne dass diese einen Verstoß gegen geltendes Recht darstellen, soll im Wege des Whistleblowings eine Identifizierung dieser Rechtslücken ermöglicht werden, ohne dass der Whistleblower um seinen Hinweisgeberschutz fürchten muss. Diese Lesart stimmt mit der allgemeinen Schutzrichtung des HinSchG in Umsetzung der Whistleblowing-RL überein, die eine Stärkung des Hinweisgeberschutzes bezweckt.

---

[592] *Hütter-Brungs*, in: Thüsing, HinSchG, § 3 Rn.11, spricht in diesem Kontext von einem zweistufigen Prüfprogramm des Whistleblowers: Es sei zu prüfen, ob die Regelung „*zweckwidrig anwendbar oder zweckwidrig unanwendbar*“ sei. Laut *Hütter-Brungs* habe der Hinweisgeber zunächst die Norm zu ermitteln, der die Praktik unterfallen könnte. In einem zweiten Schritt habe er die Norm nach ihrem Telos zu beurteilen, „ob das in Rede stehende Verhalten der Norm unterfallen sollte, wenn es ihr an sich nicht unterfällt, oder ob es ihr nicht unterfallen sollte, wenn es ihr an sich unterfällt“, vgl. *Hütter-Brungs*, in: Thüsing, HinSchG, § 3 Rn.11. Zu Recht verweist *Hütter-Brungs* in diesem Zusammenhang auch darauf, dass der hypothetische Wille des Gesetzgebers zu ermitteln sei, wobei es auf ein subjektives Element des Beschäftigungsgebers nicht ankommen solle. A. A.: *Colneric/Gerdeman*, in: BeckOK-HinSchG, § 3 Rn.6, die auch die subjektiven Voraussetzungen des Rechtsmissbrauchs zum Erfordernis des § 3 Abs. 2 HinSchG erklären.

[593] BT-Drs. 20/5992, S. 49, 64.

Der Whistleblower ist also im Anwendungsbereich des § 2 HinSchG berechtigt, Verstöße und treuwidriges Verhalten, das auf Gesetzeslücken hindeutet, zu melden bzw. offenzulegen. Demgegenüber erfasst § 5 Nr. 2 GeschGehG nach hiesiger Auffassung lediglich rechtswidrige Handlungen, wobei das Erfordernis einer rechtswidrigen Handlung eine gewisse Bagatellschwelle überschreiten muss. Auch hier wird noch einmal deutlich: Der sachliche Anwendungsbereich des § 5 Nr. 2 GeschGehG weicht einzelfallbezogen von dem des § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG ab. Insoweit besteht eine erste Friktion.

bb) Relevanz der subjektiven Motivlage

Zu prüfen ist, ob die subjektive Motivlage des Whistleblowers im Rahmen des § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG und § 5 Nr. 2 GeschGehG in unterschiedlicher Weise zu berücksichtigen ist.[594] § 5 Nr. 2 GeschGehG stellt seinem Wortlaut nach auf keine subjektive Motivlage des Whistleblowers ab. Die Genese des GeschGehG zeigt, dass der Gesetzgeber zunächst die Absicht des Whistleblowers verlangte, das allgemeine öffentliche Interesse zu schützen.[595] Dahinter stand die Regelung des Unionsgesetzgebers in Art. 5 lit. b) GeschGeh-RL, die das Erfordernis der Absicht klar benennt sowie das Anliegen, die Offenbarung von Geschäfts-geheimnissen nicht als Druck- oder Rachemittel gegen den Geheimnisinhaber einsetzen zu können. Nachdem im Rahmen des Gesetzgebungsverfahrens auf die Gefahr einer „*Gesinnungsprüfung*“ hingewiesen worden war, verzichtete der nationale Gesetzgeber im Sinne der Beschlussempfehlung des Ausschusses für Recht und Verbraucherschutz des Deutschen

---

[594] Bisher war die Motivlage des Whistleblowers eines der entscheidenden Kriterien bei der Beurteilung der Rechtmäßigkeit einer Meldung, vgl. EGMR, Urteil v. 21.07.2011 - 28274/08 §§ 69, 82-87 - *Heinisch/Deutschland*; BVerfG, NJW 2001, 3474, 3475, 3476; BAGE 107, 36, 45, 46; BAG, NJW 2017, 1833, 1834, 1835; *Preis*, in: Staudinger, BGB, § 626 Rn.131a.

[595] BT-Drs. 19/4724, S. 10, 29; siehe auch: Kapitel C) I. 1. b).

Bundestags auf die Formulierung.[596] Stattdessen sollte es genügen, dass das Whistleblowing geeignet sei, das allgemeine Interesse zu schützen.

Fraglich ist, wie das objektive Kriterium der Geeignetheit unionsrechtskonform auszulegen ist. Maßgeblich ist, wie der Absichtsbegriff in Art. 5 lit. b) GeschGeh-RL zu verstehen ist. Zu beachten ist, dass andere Sprachfassungen an dieser Stelle Formulierungen wählen, die nicht zwingend im Sinne einer Absicht zu verstehen sind, sondern auch im Sinne einer Zweckrichtung verstanden werden können. Im Englischen findet sich z. B. der Begriff „*Purpose*", der übersetzt „*Zweck*" und „*Absicht*" zugleich sein kann.[597] Es ist jedoch zu beachten, dass auch eine Zweckrichtung ein subjektives Element beinhaltet, da sie von der Person bestimmt wird, die die Informationen meldet.

Für das Verständnis einer Zweckrichtung spricht das praktische Bedürfnis nach einer Überprüfbarkeit der subjektiven Motivlage des Whistleblowers: Der Begriff der Zweckrichtung gewährleistet, dass anhand objektiver Umstände Schlüsse auf die subjektive Motivlage möglich sind.[598] Dahinter steht zugleich das Anliegen, auch den gutgläubigen Hinweisgeber zu schützen, vgl. Erwägungsgrund 20 S. 3 GeschGeh-RL.[599] Die Zweckbestimmung ist daher so zu verstehen, dass eine Meldung immer dann geeignet ist, das allgemeine öffentliche Interesse zu schützen, sofern der Whistleblower im Zeitpunkt der Meldung berechtigterweise vom Vorliegen einer rechtswidrigen Handlung ausgehen durfte.[600] Demgemäß ist die Geeignetheit in

---

596 BT-Drs. 19/8300, S. 14; *Brockhaus*, ZIS 2020, 102, 114; *Dann*/*Markgraf*, NJW 2019, 1774, 1774; *Hauck*, GRUR-Prax 2019, 223, 225.

597 Vgl. Art. 5 lit. b) GeschGehG (englische Sprachfassung). Dies gilt auch für die französische Sprachfassung.

598 Vgl. *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Sechstes Kapitel, S. 454, 455.

599 Dort zwar in Bezug auf die Faktenlage formuliert, dennoch mit der Motivlage eng verbunden.

600 So auch: *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Sechstes Kapitel, S. 454, 455.

§ 5 Nr. 2 GeschGehG unionsrechtskonform im Sinne einer Zweckbestimmung zu verstehen, die zugleich sicherstellt, dass vorsätzliche und grob fahrlässige Falschmeldungen keinen Vorrang gegenüber dem Geschäftsgeheimnisschutz haben. Im Ergebnis sind sowohl die Motivlage als auch die Gutgläubigkeit des Whistleblowers berücksichtigungsfähige Umstände im Rahmen des § 5 Nr. 2 GeschGehG.

Demgegenüber soll die Motivlage im HinSchG in Umsetzung der Whistleblowing-RL nach dem Willen des (Unions-) Gesetzgebers unbeachtlich sein.[601] In der Gesetzesbegründung zum HinSchG heißt es: „*Auf eine bestimmte Motivation der meldenden Person kommt es hingegen nicht an; sie verliert ihren Schutz nicht dadurch, dass sie einen Rechtsverstoß etwa nur aus eigensüchtigen Motiven oder zum eigenen Vorteil meldet (Erwägungsgrund 32)*.“[602] Diese Aussage bedarf jedoch einer Einschränkung.

Aus der Gesamtschau von §§ 9 Abs. 1, 35 Abs. 1 Nr. 2 bis 3 und § 35 Abs. 2 HinSchG folgt, dass Hinweisgeber, die vorsätzlich oder grob fahrlässig Falschinformationen melden, nicht geschützt sind. Darüber hinaus knüpft § 33 Abs. 1 Nr. 2 und Nr. 3 HinSchG hinsichtlich der Faktenlage und hinsichtlich des Schutzbereichs an die Gutgläubigkeit des Hinweisgebers an („*hinreichenden Grund zur Annahme*“).[603] Insofern sind sehr wohl subjektive Kriterien im Rahmen des HinSchG in Umsetzung der Whistleblowing-RL zu berücksichtigen. Auch aus der allgemeinen Zweckbestimmung einer Meldung im Sinne des HinSchG folgt, dass subjektive Motive zu berücksichtigen sind. Zwar formulieren § 6 Abs. 1 und § 35 Abs. 2 HinSchG,

---

601 BT-Drs. 20/5992 S. 31, 33, 55; BT-Drs. 20/3442; Erwägungsgrund 32 Whistleblowing-RL.

602 BT-Drs. 20/3442, S. 33.

603 *Hütter-Brungs* führt in diesem Zusammenhang zutreffend die Legaldefinition des § 3 Abs. 3 HinSchG ins Feld: Danach bedürfen „Informationen“ das Wissen oder begründete Verdachtsmomente über Missstände. Nötig sei also ein gewisser Grad subjektiver Gewissheit, vgl. *Hütter-Brungs*, in: Thüsing, HinSchG, § 3 Rn.15.

dass die Meldung erforderlich sein muss, „*um einen Verstoß aufzudecken*“.

Zu beachten ist jedoch, dass das Whistleblowing Ausdruck der Meinungsfreiheit ist.[604] Das Aufdecken von Verstößen stellt demzufolge keine eigene Zweckrichtung einer Meldung bzw. Offenlegung dar, sondern ist dieser immanent. Erfolgt eine Weitergabe von Informationen über Verstöße, liegt es in der Natur der Sache, dass dabei Verstöße aufgedeckt werden. Das Aufdecken von Verstößen ist daher lediglich probates Mittel zum eigentlichen Ziel: Die Sicherstellung gesetzeskonformen Handelns aller Akteure im beruflichen Zusammenhang durch die Beseitigung etwaiger Missstände. Die Meldung ist vielmehr Ausdruck der Meinungsfreiheit im Sinne eines Mehrwerts für die öffentliche Meinungsbildung. Demnach ist auch im Kontext des HinSchG eine Meldung im allgemeinen öffentlichen Interesse erforderlich. Diese Zweckbestimmung mag zwar objektiv zu bestimmen sein, enthält zugleich aber auch ein subjektives Element. Im Ergebnis sind also subjektive Komponenten im Rahmen des HinSchG berücksichtigungsfähig.

Weder § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG noch § 5 Nr. 2 GeschGehG lassen sich nach hiesiger Auffassung losgelöst von subjektiven Wertungen des Hinweisgebers beurteilen. Nach beiden Regelungen muss die Meldung bzw. Offenlegung im öffentlichen Interesse erfolgen, weshalb Meldungen, die grob fahrlässige oder vorsätzliche Falschinformationen enthalten, in beiden Fällen keinen Schutz genießen. Zusammenfassend lässt sich daher feststellen, dass sich die beiden Regelungen hinsichtlich der Berücksichtigung der subjektiven Motivlage des Whistleblowers nicht unter-scheiden. Insoweit liegt daher keine Friktion vor.

[604] Dazu siehe auch: Kapitel C) I. 1. a).

cc) Auslegungsmaßstab

Der vorherige Abschnitt hat gezeigt, dass die Informationsweitergabe einer Zweckbestimmung unterliegt, die anhand des allgemeinen öffentlichen Interesses auszurichten ist. Dies gilt sowohl für § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG als auch für § 5 Nr. 2 GeschGehG. Nach § 5 Nr. 2 GeschGehG muss die Offenlegung einer rechtswidrigen Handlung geeignet sein, das allgemeine öffentliche Interesse zu schützen. Die rechtswidrige Handlung muss also im Zusammenhang mit dem allgemeinen öffentlichen Interesse stehen. Dies bedeutet, dass die Informationsweitergabe einen Mehrwert für die öffentliche Debatte leistet, auch weil die rechtswidrige Handlung von einigem Gewicht ist (sog. Bagatellschwelle).[605] Hintergrund ist, dass das Whistleblowing Ausdruck der Meinungsfreiheit ist.[606] Für das HinSchG folgt dies aus der Formulierung, dass die Meldung bzw. Offenlegung „*notwendig ist, um einen Verstoß aufzudecken*". Auch hier ist das Whistleblowing Ausdruck der Meinungsfreiheit, bei dem es auf einen Mehrwert für die öffentliche Meinungsbildung ankommt. Demzufolge sind sowohl im Rahmen des § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG als auch im Rahmen des § 5 Nr. 2 GeschGehG obligatorische Verhältnismäßigkeitserwägungen anhand des öffentlichen Interesses anzustellen.[607] Dadurch ist sichergestellt, dass es keinen absoluten Vorrang für die Meinungsfreiheit geben kann, vgl. Art. 52 Abs. 1 GR-CH.[608]

Fraglich ist, ob es einer darüber hinaus gehenden, nachgeschalteten Interessenabwägung bedarf. Dafür spricht zunächst, dass Einschränkungen der Meinungsfreiheit nach Art. 52 Abs. 1 GR-CH

---

605 Siehe: Kapitel C) I. 1. c) aa).

606 Zum Schutzbereich der Meinungsfreiheit siehe: Kapitel C) I. 1. a).

607 Erwägungsgrund 21 Whistleblowing-RL.

608 Die Sicherstellung der Verhältnismäßigkeit von Maßnahmen stellt einen allgemeinen Grundsatz des Unionsrechts dar; ausführlich dazu: *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Sechstes Kapitel, S. 458, sowie Siebtes Kapitel, S. 516, 517.

ausdrücklich nur nach Maßgabe des Verhältnismäßigkeitsgrundsatzes möglich sein sollen. Dagegen spricht jedoch, dass der Grundsatz der Verhältnismäßigkeit bereits hinreichend im Rahmen der § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG und § 5 Nr. 2 GeschGehG verankert ist, sodass es keiner eigenständigen Interessenabwägung mehr bedarf. Im Rahmen des HinSchG wird die Verankerung des Verhältnismäßigkeitsgrundsatzes einerseits durch die Formulierung „*notwendig*“ (§ 6 Abs. 1 HinSchG) deutlich.[609] Zusätzlich ermöglicht das Kriterium des allgemeinen öffentlichen Interesses, gebotene Verhältnismäßigkeitserwägungen einfließen zu lassen. Der Grundsatz der Verhältnismäßigkeit ist demzufolge hinreichend verankert, sodass es keiner nachgeschalteten Interessenabwägung im Rahmen des § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG bedarf. Dasselbe gilt für § 5 Nr. 2 GeschGehG. Auch hier stellt das Kriterium des allgemeinen öffentlichen Interesses die obligatorischen Verhältnismäßigkeitserwägungen sicher. Bestätigt wird dies durch die Formulierung „*geeignet*“, die Ausdruck des Verhältnismäßigkeitsgrundsatzes ist. Darüber hinaus bedarf es keiner eigenständigen Interessenabwägung. § 5 Nr. 2 GeschGehG ist ein benannter Fall des berechtigten Interesses, vgl. Eingangssatz zu § 5 GeschGehG. Liegen die Voraussetzungen des § 5 Nr. 2 GeschGehG vor, erfolgt folgerichtig keine nachgeschaltete Interessenabwägung.[610]

Fraglich ist jedoch, inwieweit sich die jeweiligen Auslegungsmaßstäbe im Rahmen der beiden Regelungen unterscheiden. Zu beachten ist, dass die Regelung in § 6 Abs. 1 HinSchG in Umsetzung der Whistleblowing-RL zuvörderst der Stärkung des Hinweisgeberschutzes dient. Folgerichtig gehen die Hinweisgeberschutzinteressen im Regelwerk des HinSchG in Zweifelsfragen vor, sollten die Geheimhaltungsinteressen den Hinweisgeberschutz im Einzelfall nicht

---

[609] Vgl. der Notwendigkeitsvorbehalts in Art. 21 Whistleblowing-RL; Erwägungsgrund 92 Whistleblowing-RL.

[610] Insofern kann auch von einer unwiderleglichen Vermutungswirkung gesprochen werden, vgl. *Colneric*/*Gerdemann*, Umsetzung der Whistleblowing-RL, S. 58, 59.

überwiegen. Umgekehrtes gilt für das Regelungsregime des Geschäftsgeheimnisschutzes. Die Regelungen des GeschGehG in Umsetzung der GeschGeh-RL dienen zuvörderst dem Geschäftsgeheimnisschutz. Dementsprechend gehen im Regelwerk des GeschGehG die Geheimhaltungsinteressen in Zweifelfragen vor, sollte die Meinungsfreiheit des Whistleblowers den Geschäftsgeheimnisschutz nicht im Einzelfall überwiegen. Hier wird deutlich, dass den Verhältnismäßigkeitserwägungen verschiedene Wertungen zugrunde liegen. Im Ergebnis sind zwar im Rahmen beider Regelungen obligatorische Verhältnismäßigkeitserwägungen anzustrengen. Diese unterscheiden sich allerdings in ihren jeweiligen Maßstäben. Dies führt nach hiesiger Auffassung zur Annahme einer zweiten Friktion.

dd) Haftungsausschluss

Auch auf Rechtsfolgenseite stellt sich die Frage nach bestehenden Friktionen zwischen § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG und § 5 Nr. 2 GeschGehG. Aus § 5 Nr. 2 GeschGehG folgt, dass sowohl die Erlangung, die Nutzung als auch die Offenlegung kein Handlungsverbot im Sinne des § 4 GeschGehG darstellt, sofern die übrigen Voraussetzungen des § 5 Nr. 2 GeschGehG erfüllt sind. In diesem Fall stehen dem Geheimnisinhaber keine Schutz- und Abwehransprüche nach den Vorgaben des GeschGehG zur Verfügung und der Hinweisgeber erfüllt auch nicht den Straftatbestand des § 23 GeschGehG. Im Ergebnis normiert die Regelung des § 5 Nr. 2 GeschGehG in Bezug auf das GeschGehG einen umfassenden Hinweisgeberschutz. Einen solchen kennt auch das HinSchG, allerdings nur in Bezug auf die Meldung bzw. Offenlegung, vgl. § 6 Abs. 1 HinSchG. Für die Erlangung der Informationen ist § 35 Abs. 1 HinSchG zu beachten. Danach kann ein Whistleblower nicht für die Beschaffung von oder den Zugriff auf Informationen, die er gemeldet oder offengelegt hat, rechtlich verantwortlich gemacht werden, sofern die Beschaffung nicht als solche oder der Zugriff nicht als solcher eine eigenständige Straftat darstellt.

Sowohl § 35 Abs. 1 HinSchG als auch § 5 Nr. 2 GeschGehG setzen zunächst voraus, dass die Beschaffung bzw. Erlangung der Information zum Zwecke der Meldung bzw. Offenlegung erfolgt. Während sich dies aus dem Wortlaut des § 35 Abs. 1 HinSchG ableiten lässt, folgt dies für § 5 Nr. 2 GeschGehG aus der Zweckrichtung der Erlangung. § 5 Nr. 2 GeschGehG setzt voraus, dass die Erlangung geeignet sein muss, das allgemeine öffentliche Interesse zu schützen, was wiederum bedeutet, dass eine Meldung bzw. Offenlegung im Anschluss an die Erlangung auch tatsächlich erfolgt sein muss. Die Meldung bzw. Offenlegung ist folgerichtig notwendige Voraussetzung, um der öffentlichen Meinungsbildung zu dienen. Diesbezüglich unterscheiden sich die beiden Regelungen nicht. Setzt sich der Arbeitnehmer über eine Zugriffsbeschränkung hinweg, trägt er das Risiko, dass es im Anschluss an die Informationsbeschaffung auch tatsächlich zu einer Meldung nach Maßgabe der § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG kommt (sog. „*Melderisiko*“).[611]

---

[611] *Rombey* weist in teleologischer Auslegung des § 35 Abs. 1 HinSchG darauf hin, dass der Haftungsausschluss auch für die Erlangung von Informationen gelte, die der Hinweisgeber nicht meldet, weil er erkannt habe, dass sie irrelevant seien, vgl. *Rombey*, in: Thüsing, HinSchG, § 35 Rn.6. Voraussetzung sei, dass die Informationen in einem *„untrennbaren, räumlich-zeitlichen Zusammenhang mit der Informationsbeschaffung“* stünden. *Gerdemann* geht sogar noch weiter hinsichtlich einer möglichen Zusammenarbeit mit den Strafverfolgungsbehörden, vgl. *Gerdemann*, ZRP 2021, 37, 39. Zutreffend ist nach hiesiger Auffassung, dass nur diejenigen Informationen gemeldet werden dürfen, die für die Beseitigung des Missstands erforderlich sind, vgl. § 6 Abs. 1 HinSchG und § 35 Abs. 2 HinSchG. Entscheidend für den Haftungsausschluss nach § 35 Abs. 1 HinSchG ist demnach, dass im Anschluss an die Informationsbeschaffung überhaupt eine rechtmäßige Meldung erfolgt, wenngleich sich die Meldung nicht zwingend auf sämtliche Informationen erstrecken muss, die zuvor ggf. unter Hinwegsetzung von Zugriffsbeschränkungen beschafft worden sind. Offenbleibt, in welcher zeitlichen Nähe die Meldung zu der Informationsbeschaffung bzw. dem Zugriff stehen muss. Auch nach hiesiger Auffassung keine zu hohen Anforderungen an den Whistleblower zu stellen sein dürften (vgl. BT-Drs. 20/5992, S. 78), darf zumindest ein gewisser zeitlicher Zusammenhang erwartet werden. Dies gilt für § 5 Nr. 2 GeschGehG gleichermaßen.

Allerdings ist der Haftungsausschluss des § 35 Abs. 1 HinSchG im Vergleich zu dem in § 5 Nr. 2 GeschGehG enger gesteckt. Während eine „*Informationsbeschaffung*“ oder ein „*Zugriff*“ in § 35 Abs. 1 HinSchG dem Wortlaut nach ein positives Tun voraussetzt, kann die „*Erlangung*“ im Sinne des § 5 Nr. 2 GeschGehG auf jede denkbare, sonstige Weise stattfinden, vgl. §§ 3 Abs. 1, 4 Abs. 1 GeschGehG.[612] Bemerkenswert ist in diesem Zusammenhang, dass nach § 35 Abs. 1 HinSchG die strafrechtliche Verantwortlichkeit bei der Informationsbeschaffung bestehen bleibt, der Hinweisgeber also insoweit nicht von seiner Haftung entlastet wird.[613] Relevanz erlangt dies insbesondere im Hinblick auf die Strafnorm des § 23 GeschGehG. Erfolgt eine Meldung nach Maßgabe des § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG, bleibt nach § 35 Abs. 1 HinSchG die Strafbarkeit gemäß § 23 GeschGehG in Bezug auf die vorherige Informationsbeschaffung bestehen. Dies unterscheidet sich von der Regelung in § 5 Nr. 2 GeschGehG, die den Hinweisgeberschutz in Bezug auf die Strafnorm des § 23 GeschGehG erstreckt. Insofern besteht eine dritte Friktion.

ee) Harmonisierende Auslegung zur Überwindung bestehender Friktionen

Die vorherigen Abschnitte haben zwischen § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG bzw. § 35 Abs. 1 HinSchG und § 5 Nr. 2 GeschGehG drei Friktionen identifiziert.[614] Diese beziehen sich auf den sachlichen Anwendungsbereich,[615] den Auslegungsmaßstab,[616]

---

612 Ebenso: *Rombey*, in: Thüsing, HinSchG, § 35 Rn.4.

613 Umfassend zur möglichen Strafbarkeit eines Whistleblowers in Bezug auf die Erlangung eines Geschäftsgeheimnisses: *Wiedmann*/*Hoppmann*, CCZ 2023, 11.

614 Zu einer ähnlichen Einschätzung gelangt auch *Forst*, der § 5 Nr. 2 GeschGehG einerseits einen weiteren Anwendungsbereich im Vergleich zum HinSchG attestiert, in Teilen aber auch einen engeren Anwendungsbereich erkennt, vgl. *Forst*, in: Thüsing, HinSchG, § 6 Rn.10.

615 Siehe: Kapitel C) I. 1. c) aa).

616 Siehe: Kapitel C) I. 1. c) cc).

und den Umfang des Haftungsausschlusses.[617] Fraglich ist, wie diese Friktionen aufzulösen sind. Entscheidend ist das Konkurrenzverhältnis von GeschGehG in Umsetzung der GeschGeh-RL und HinSchG in Umsetzung der Whistleblowing-RL. Der Unionsgesetzgeber verweist im Rahmen des Art. 3 Abs. 2 GeschGeh-RL auf die Vorgaben der Whistleblowing-RL, um zu betonen, dass die Vorschriften der Whistleblowing-RL eine gesetzliche Gestattung im Hinblick auf den Geschäftsgeheimnisschutz darstellen. Gleiches formuliert auch Erwägungsgrund 98 Whistleblowing-RL.[618] Daraus resultiert ein gewisser Vorrang des HinSchG gegenüber dem GeschGehG.[619] Liegen die Voraussetzungen des § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG bzw. § 35 Abs. 1 HinSchG vor, kommt es folgerichtig auf die Vorgaben des § 5 Nr. 2 GeschGehG nicht mehr an.[620]

Der nationale Gesetzgeber hat die Unterschiede zwischen § 6 Abs. 1 HinSchG bzw. § 35 Abs. 1 HinSchG und § 5 Nr. 2 GeschGehG erkannt und im Rahmen der Gesetzesbegründung zum HinSchG formuliert: *„Die Anforderungen an die Offenlegung nach dem GeschGehG sollen durch diese Bestimmung nicht abgesenkt werden. Vielmehr bleibt § 5 Nummer 2 GeschGehG neben der Neuregelung bestehen (...).“*[621] Der nationale Gesetzgeber geht insofern von einem Nebeneinander der beiden Regelungen aus.[622] Dies entspricht dem Anliegen des Gesetzgebers, den Hinweisgeberschutz zu stärken. Für den Anwendungsbereich gilt demnach: Die Vorgaben des HinSchG sind nicht abschließend in Bezug auf den Hinweisgeberschutz zu verstehen und entfalten keine Sperrwirkung gegenüber § 5 Nr. 2 GeschGehG. Soweit der Anwendungsbereich des § 2 HinSchG nicht eröffnet

---

617 Siehe: Kapitel C) I. 1. c) dd).

618 Erwägungsgrund 98, S. 3-5 Whistleblowing-RL.

619 *Hoppe*/*Oldekop*, Geschäftsgeheimnisse, Rn.462, 366.

620 Im Sinne der Rechtssicherheit und der Einheit der Rechtsordnung ist nicht danach zu unterscheiden, ob die jeweilige Meldung dem Anwendungsbereich der Whistleblowing-RL oder dem Teil des HinSchG, der die Richtlinie überschießend umsetzt, zuzuordnen ist.

621 BT-Drs. 20/3442, S. 71.

622 So auch: *Forst*, in: Thüsing, HinSchG, § 6 Rn.10 m. w. N.

ist, kann Hinweisgeberschutz nach § 5 Nr. 2 GeschGehG bestehen. Bestätigt wird dies durch Erwägungsgrund 98 S. 5 Whistleblowing-RL.

Fraglich ist, wie das Nebeneinander der Regelungen in Bezug auf die unterschiedlichen Auslegungsmaßstäbe zu verstehen ist. Die Einheit der Rechtsordnung streitet aus Gründen der Rechtssicherheit für ein identisches Verständnis. Ungeklärt ist jedoch, welchem Auslegungsmaßstab der Vorrang gebührt. Hervorzuheben ist in diesem Zusammenhang, dass sowohl die Gesetzesbegründung zum GeschGehG als auch die Erwägungsgründe der GeschGeh-RL auf die Whistleblowing-RL Bezug nehmen. Daraus folgt, dass der Gesetzgeber das Verhältnis zwischen Hinweisgeberschutz und Geschäftsgeheimnisschutz durch Inkrafttreten des GeschGehG nicht verschieben bzw. verändern, sondern die Vorgaben des zu dieser Zeit noch ausstehenden HinSchG in Umsetzung der Whistleblowing-RL lediglich ergänzen wollte.[623] Der (Unions-) Gesetzgeber bekennt sich damit abermals dazu, dass den Vorgaben des HinSchG ein gewisser Vorrang gegenüber dem GeschGehG zuteilwird.

Demzufolge ist aus Gründen der Einheit der Rechtsordnung bei Auslegungsfragen im Rahmen des § 5 Nr. 2 GeschGehG der Maßstab des § 6 Abs. 1 HinSchG heranzuziehen. Diese Lesart wird dem Anliegen des nationalen Gesetzgebers gerecht, den Hinweisgeberschutz zu stärken und schafft Rechtssicherheit. Soweit die Regelung des § 5 Nr. 2 GeschGehG im Vergleich zu den Vorgaben des § 6 Abs. 1 HinSchG enger ist, bedarf es also einer harmonisierenden Auslegung, die den

[623] In diese Richtung auch: *Colneric/Gerdemann*, in: BeckOK HinSchG, § 6 Rn.13, die von einer komplementären Schutzfunktion des § 5 Nr. 2 GeschGehG sprechen.

Anforderungen des HinSchG entspricht.[624] Ist die Regelung in § 5 Nr. 2 GeschGehG demgegenüber weiter als die Vorgaben des HinSchG, so verbleibt ihr ein eigenständiger Anwendungsbereich.[625] Im Hinblick auf den Umfang des Haftungsausschlusses bedeutet Letzteres: Dort, wo § 35 Abs. 1 HinSchG keinen Hinweisgeberschutz gewährt, kann der Hinweisgeberschutz ergänzend aus § 5 Nr. 2 GeschGehG greifen. In diesem Fall wird das Nebeneinander der beiden Regelungen deutlich. Während der Hinweisgeberschutz in Bezug auf die Meldung bzw. die Offenlegung nach § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG besteht, ergibt sich die Straffreiheit der vorausgegangenen Erlangung in Bezug auf § 23 GeschGehG aus § 5 Nr. 2 GeschGehG.[626]

d) Zusammenfassender Überblick

Die Informationsweitergabe eines Whistleblowers unterfällt dem Schutzbereich der Meinungsfreiheit. Verfassungsrechtlich ist die Meinungsfreiheit in Art. 5 Abs. 1 S. 1 Hs. 1 GG geschützt. Konventionsrechtlich folgt dies aus Art. 10 EMRK, unionsrechtlich aus Art. 11 GR-CH, wobei Schutzbereich und Schranken im Wesentlichen mit

---

624 Soweit es in der Gesetzesbegründung zum HinSchG heißt, § 5 Nr. 2 GeschGehG sei enger als § 6 Abs. 1 HinSchG, weil er nur eine Erlangung, Nutzung oder Offenlegung vom Verbot der Weitergabe ausnimmt, die geeignet ist, das allgemeine öffentliche Interesse zu schützen, so überzeugt dies nicht, vgl. BT-Drs. 20/3442, S. 71. Informationsweitergaben sind stets Ausdruck der Meinungsfreiheit, deren Schutz ein öffentliches Interesse voraussetzt. Dies gilt für § 5 Nr. 2 GeschGehG und § 6 Abs. 1 HinSchG gleichermaßen. § 5 Nr. 2 GeschGehG ist insoweit nicht enger als § 6 Abs. 1 HinSchG.

625 Zu den Auslegungsmöglichkeiten, über die noch vor Inkrafttreten des HinSchG spekuliert wurden, ausführlich: *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus, Sechstes Kapitel, S. 474 ff. 516.

626 § 5 Nr. 2 GeschGehG gilt in Bezug auf § 23 GeschGehG, mithin nicht rechtsgebietsübergreifend. Relevant wird dies z. B. für § 123 StGB, vgl. exemplarisch: *Naber*/*Peukert*/*Seeger*, NZA 2019, 583, 585; *Nöbel*/*Veljovic*, CB 2020, 34, 38; a. A.: *Trebeck*/*Schulte-Wissermann*, NZA 2018, 1175, 1179.

denen des Grundgesetzes übereinstimmen. Da die Meinungsfreiheit einen konstitutiven Beitrag für die Demokratie leistet, greift eine Vermutung für die freie Rede, sobald der Whistleblower im öffentlichen Interesse einen Beitrag für die öffentliche Meinungsbildung leistet und der Whistleblower zum Zeitpunkt der Meldung bzw. Offenlegung berechtigterweise davon ausgehen durfte, dass ein Missstand besteht. Dennoch gilt das Recht auf Meinungsfreiheit nicht absolut, Art. 52 GR-CH. Beschränkungen kommen in Betracht, wenn die Informationsweitergabe in tatsächlicher Hinsicht keinen Mehrwert für die öffentliche Meinungsbildung leistet. Die Meldung vorsätzlicher Falschinformationen ist folgerichtig nicht geschützt. Im Übrigen entscheidet eine Interessenabwägung.[627]

Am 2. Juli 2023 ist das HinSchG in Umsetzung der Whistleblowing-RL in Kraft getreten. Zuvor wurde das Whistleblowing maßgebend durch die Rechtsprechung der nationalen Arbeitsgerichte, des BVerfG sowie vom EGMR geprägt. Mit der Zeit ließen sich aus der Rechtsprechung Kriterien in Bezug auf den Hinweisgeberschutz ableiten, die mit der Entscheidung des EGMR in der Rechtssache *Heinisch* eine wesentliche Ergänzung erfahren haben.[628] Für den Fall einer externen Meldung galt aus Verhältnismäßigkeitsgründen grundsätzlich die Maßgabe, dass vorrangig innerbetriebliche Abhilfe über einen betrieblichen Kanal versucht werden müsse (sog. Eskalationsmodell). Hiervon ist der nationale Gesetzgeber nun abgerückt, vgl. §§ 7, 39 HinSchG. Bemerkenswert ist auch, dass sich der nationale Gesetzgeber für eine Richtlinien überschießende Umsetzung entschieden hat (sog. Goldplating). Dies gilt insbesondere mit Blick auf den sachlichen Anwendungsbereich, § 2 HinSchG. Darüber hinaus hat der nationale Gesetzgeber die Gelegenheit verpasst, den aus Gründen der Rechtssicherheit gebotenen Gleichlauf zwischen GeschGehG und HinSchG herzustellen. Das Nebeneinander zweier nicht völlig kongruenter

---

627 Zum Rechtsrahmen des Whistleblowings siehe auch: Kapitel C) I. 1. a).

628 Etwa: BAG, NJW 2017, 1833, 1834; EGMR, Urteil v. 21.07.2011 - 28274/08 - *Heinisch/Deutschland.*

Hinweisgeberregelungen in § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG und § 5 Nr. 2 GeschGehG lässt Friktionen entstehen, die es aufzulösen gilt.

Eine erste Friktion bezieht sich auf den sachlichen Anwendungsbereich.[629] Der Whistleblower ist im Anwendungsbereich des § 2 HinSchG berechtigt, Verstöße und treuwidriges Verhalten, das auf Gesetzeslücken hindeutet, zu melden bzw. offenzulegen. Demgegenüber erfasst § 5 Nr. 2 GeschGehG die Offenlegung rechtswidriger Handlungen, wobei diese von einigem Gewicht sein müssen. Anzumerken ist, dass das Kriterium der „*rechtswidrigen Handlung*“ in § 5 Nr. 2 GeschGehG die beiden weiteren Kriterien des „*beruflichen oder sonstigen Fehlverhaltens“* erfasst.[630]

Keine Friktion besteht hingegen mit Blick auf die Relevanz der subjektiven Motivlage.[631] Weder § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG noch § 5 Nr. 2 GeschGehG lassen sich losgelöst von subjektiven Wertungen des Whistleblowers beurteilen. Nach beiden Regelungen muss die Meldung bzw. Offenlegung im öffentlichen Interesse liegen (sog. Zweckbestimmung). Für § 5 Nr. 2 GeschGehG ergibt sich dies im Wege einer unionsrechtskonformen Auslegung der Formulierung: „*geeignet, das allgemeine öffentliche Interesse zu schützen*“. Für § 6 Abs. 1 HinSchG folgt dies aus dem Umstand, dass auch subjektive Kriterien Relevanz haben, beispielsweise bei der Bestimmung der Gutgläubigkeit im Rahmen des § 33 Abs. 1 Nr. 2 und Nr. 3 HinSchG. Die Meldung ist Ausdruck der Meinungsfreiheit und hat im Kontext des HinSchG im allgemeinen öffentlichen Interesse zu erfolgen. Diese Zweckbestimmung mag zwar objektiv zu bestimmen sein, enthält aber zugleich ein subjektives Element.

---

629 Siehe: Kapitel C) I. 1. c) aa).
630 Siehe: Kapitel C) I. 1. c) aa).
631 Siehe: Kapitel C) I. 1. c) bb).

Eine weitere Friktion bezieht sich auf die verschiedenen Auslegungsmaßstäbe, die im Rahmen der obligatorischen Verhältnismäßigkeitserwägungen anzustrengen sind.[632] Während § 6 Abs. 1 HinSchG in Zweifelsfällen von einem grundsätzlichen Vorrang des Hinweisgeberschutzes ausgeht, besteht im Rahmen des § 5 Nr. 2 GeschGehG in ebendiesen Zweifelsfällen ein Vorrang des Geschäftsgeheimnisschutzes. Den Verhältnismäßigkeitserwägungen liegen insofern verschiedene Wertungen zugrunde. Anzumerken ist, dass beide Vorschriften keiner eigenständigen Interessenabwägung unterliegen, die über die obligatorischen Verhältnismäßigkeitserwägungen im Hinblick auf die Zweckbestimmung der Meldung hinausgeht.

Eine dritte Friktion bezieht sich sodann auf den Umfang des Haftungsausschlusses im Falle einer Meldung bzw. Offenlegung.[633] Erfolgt eine Meldung nach Maßgabe des § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG, bleibt nach § 35 Abs. 1 HinSchG die Strafbarkeit des Whistleblowers in Bezug auf die vorherige Informationsbeschaffung bestehen. Dies unterscheidet sich von der Regelung in § 5 Nr. 2 GeschGehG, die den Whistleblower bei erfolgter Offenlegung auch hinsichtlich der Informationserlangung von der straffrechtlichen Verantwortung nach § 23 GeschGehG ausnimmt. Festzuhalten ist, dass der Hinweisgeberschutz in Bezug auf die Erlangung einer Information nach beiden Vorschriften nur besteht, sofern eine Meldung bzw. Offenlegung nach Maßgabe des § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG auch tatsächlich erfolgt ist. Die Meldung bzw. Offenlegung ist notwendige Voraussetzung, um dem Schutzbereich der Meinungsfreiheit zu unterfallen.

Es gilt, die bestehenden Friktionen zu überwinden. Der nationale Gesetzgeber geht von einem Nebeneinander der beiden Regelungen aus. Die Vorgaben des HinSchG sind demzufolge nicht abschließend

---

632 Siehe: Kapitel C) I. 1. c) cc).
633 Siehe: Kapitel C) I. 1. c) dd).

in Bezug auf den Hinweisgeberschutz und entfalten keine Sperrwirkung gegenüber § 5 Nr. 2 GeschGehG. Ist der Anwendungsbereich des § 2 HinSchG nicht eröffnet, kann folgerichtig Hinweisgeberschutz nach § 5 Nr. 2 GeschGehG bestehen. Hinsichtlich der unterschiedlichen Auslegungsmaßstäbe im Rahmen der Verhältnismäßigkeitserwägungen gebietet die Einheit der Rechtsordnung aus Gründen der Rechtssicherheit ein identisches Verständnis.[634] Dies stimmt auch mit dem Willen des (Unions-) Gesetzgebers überein, der mit der Regelung in § 5 Nr. 2 GeschGehG das Verhältnis zwischen Hinweisgeberschutz und Geschäftsgeheimnisschutz nicht verschieben wollte, sondern die Vorgaben des zu dieser Zeit noch ausstehenden HinSchG lediglich ergänzen wollte. Vor diesem Hintergrund ist der Maßstab des § 6 Abs. 1 HinSchG vorzugwürdig. Das bedeutet: Soweit die Regelung des § 5 Nr. 2 GeschGehG im Vergleich zu den Vorgaben des § 6 Abs. 1 HinSchG enger ist, bedarf es einer harmonisierenden Auslegung, die den Anforderungen des HinSchG entspricht. Ist § 5 Nr. 2 GeschGehG jedoch weiter als die Vorgaben des HinSchG, so verbleibt § 5 Nr. 2 GeschGehG ein eigenständiger Anwendungsbereich. Mit Blick auf die dritte Friktion bedeutet dies: Dort, wo § 35 Abs. 1 HinSchG keinen Hinweisgeberschutz gewährt, kann der Hinweisgeberschutz ergänzend aus § 5 Nr. 2 GeschGehG greifen. Während der Hinweisgeberschutz in Bezug auf die Meldung bzw. die Offenlegung nach § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG besteht, ergibt sich die Straffreiheit der vorausgegangenen Erlangung in Bezug auf § 23 GeschGehG aus § 5 Nr. 2 GeschGehG.

2. Hinweisgeberschutz bei der Weitergabe von Geschäftsgeheimnissen durch Whistleblower

Die folgenden Abschnitte untersuchen die Voraussetzungen einer zulässigen Weitergabe bzw. Offenlegung von Geschäftsgeheimnissen durch Whistleblower. Da sich gezeigt hat, dass § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG gegenüber § 5 Nr. 2 GeschGehG faktisch

[634] Siehe: Kapitel C) I. 1. c) ee).

vorrangig ist,[635] wird die Untersuchung zunächst die Vorgaben des § 6 Abs. 1 HinSchG analysieren. Dabei wird der Frage nachgegangen, inwieweit ein interner Meldekanal vorrangig zu nutzen ist. Der nationale Gesetzgeber hat sich zwar für ein grundsätzlich zweistufiges Eska-lationsmodell im HinSchG entschieden. Da Geschäfts-geheimnisse jedoch besonders schutzbedürftig sind, könnte dies Anlass für eine differenziertere Betrachtungsweise geben. Die gefundenen Ergebnisse werden sodann auf § 5 Nr. 2 GeschGehG angewandt.

a) Die zulässige Weitergabe von Geschäftsgeheimnissen nach § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG

Nach § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG ist die Weitergabe eines Geschäftsgeheimnisses an eine interne oder externe Meldestelle oder dessen Offenlegung erlaubt, sofern der Whistleblower hinreichenden Grund zu der Annahme hat, dass die Weitergabe oder Offenlegung notwendig ist, um einen Verstoß aufzudecken und die Voraussetzungen des § 33 Abs. 1 Nr. 2 und Nr. 3 HinSchG erfüllt sind.[636] Eine zulässige Weitergabe bzw. Offenlegung eines Geschäftsgeheimnisses setzt zum einen voraus, dass die gemeldeten Informationen Verstöße betreffen, die in den Anwendungsbereich des § 2 HinSchG fallen oder der Hinweisgeber zum Zeitpunkt der Meldung oder Offenlegung hinreichenden Grund zu der Annahme hatte, dass dies der Fall sei, § 33 Abs. 1 Nr. 3 HinSchG. Für die Frage der zulässigen Weitergabe bzw. Offenlegung eines Geschäftsgeheimnisses ist ferner entscheidend, dass der Whistleblower zum Zeitpunkt der Meldung oder Offenlegung hinreichenden Grund zu der Annahme hat, dass die gemeldeten oder offengelegten Informationen der Wahrheit entsprechen, § 33 Abs. 1 Nr. 2 HinSchG. Es bedarf daher begründeter Verdachtsmomente über Verstöße oder Wissen über tatsächliche oder

---

635 Siehe: Kapitel C) I. 2. b) ee).

636 BT-Drs. 20/5992, S. 80. In Fällen einer Offenlegung (§ 3 Abs. 5 HinSchG) sind zudem die zusätzlichen Voraussetzungen des § 32 HinSchG zu beachten. Dasselbe gilt für Informationen, die einer vertraglichen oder gesetzlichen Verschwiegenheitspflicht unterliegen, § 6 Abs. 2 HinSchG.

mögliche Verstöße, die bereits begangen wurden oder sehr wahrscheinlich erfolgen werden.[637] Ob dies der Fall ist, ist im Rahmen einer Gesamtwürdigung aller maßgebenden Einzelfallumstände zu entscheiden.

Hervorzuheben ist, dass § 6 Abs. 1 Nr. 1 HinSchG in diesem Kontext das Kriterium der Notwendigkeit aufstellt. Die Formulierung sorgt für die nötige Verankerung des Verhältnismäßigkeitsgrundsatzes und bedarf einer Konturierung. In der Gesetzesbegründung zum HinSchG heißt es: „*Im Hinblick auf die Erforderlichkeit der Weitergabe von Geschäftsgeheimnissen kommt es nicht allein darauf an, ob die Weitergabe überhaupt notwendig ist, sondern auch darauf, in welchem Umfang sie notwendig ist. Die hinweisgebende Person hat damit darauf zu achten, dass nur solche Geheimnisse weitergegeben werden, deren Inhalt für die Aufdeckung des Verstoßes erforderlich ist.*“[638] Auffällig ist, dass der Gesetzgeber im Rahmen seiner Begründung zu § 6 Abs. 1 HinSchG das Kriterium der Erforderlichkeit mittels des Begriffs der Notwendigkeit erläutert. Beide Begriffe dienen dem Verhältnismäßigkeitsgrundsatz als Einfallstor. Die Formulierung des Gesetzgebers betont insofern die besondere Bedeutung des Verhältnismäßigkeitsgrundsatzes im Rahmen des § 6 Abs. 1 HinSchG.

Da sich § 35 Abs. 2 HinSchG in seinem Anwendungsbereich mit dem des § 6 Abs. 1 HinSchG überschneidet, sind die Ausführungen der Gesetzesbegründung zu § 33 Abs. 1 Nr. 2 HinSchG auf § 6 Abs. 1 HinSchG übertragbar. In der Gesetzesbegründung zu § 35 Abs. 2 HinSchG heißt es: „*Um einer Verantwortlichkeit zu entgehen, wird eine hinweisgebende Person daher zu prüfen haben, ob die Weitergabe der Informationen für die von ihr gemachte Meldung notwendig ist. Dazu, welche Anforderungen an den hinreichenden Grund zu der Annahme, dass die Meldung oder Offenlegung erforderlich war, zu stellen sind, wird auf die Ausführungen in der Begründung*

[637] Vgl. dazu auch: *Lüneborg*, in: Thüsing, HinSchG, § 33 Rn.13-15.
[638] BT-Drs. 20/3442, S. 71.

zu § 33 Absatz 1 Nummer 2 verwiesen.“[639] Aus der Gesetzesbegründung zu § 33 Abs. 1 Nr. 2 HinSchG geht außerdem hervor, dass eine Meldung nicht „*leichtfertig ohne ein Bemühen um Verifizierung erfolgen darf, sofern diese Bemühen zumutbar ist*“.[640] Daraus ergibt sich, dass der Whistleblower in Bezug auf den Inhalt und die Form der Weitergabe eines Geschäftsgeheimnisses einer Prüfpflicht unterliegt, deren Anforderungen derjenigen hinsichtlich des Wahrheitsgehaltes entsprechen, § 33 Abs. 1 Nr. 2 HinSchG.[641]

Vor diesem Hintergrund gilt es zu klären, was mit dem Begriff der Leichtigkeit gemeint ist. Der Begriff ist einerseits aus dem Strafrecht bekannt (§ 251 StGB) und beschreibt „*ein Verhalten, das einen hohen Grad an Fahrlässigkeit aufweist*“ (§ 15 StGB).[642] Sein zivilrechtliches Pendant findet sich im Begriff der groben Fahrlässigkeit, vgl. § 276 Abs. 2 BGB. Grobe Fahrlässigkeit meint den höchsten Grad einer Fahrlässigkeit und wird als eine Verletzung der gebotenen Sorgfalt „*in besonders schwerem Maße*“ beschrieben, mithin als „*das, was im gegebenen Falle jedem einleuchten musste, (und) nicht beachtet wird*“.[643] Darüber hinaus hat der BGH die Kategorie des „*leichtfertigenden Verhaltens*“ als Kriterium für die Schlussfolgerung auf eine gleichgültige und gewissenlose Haltung gegenüber den Interessen

---

639 BT-Drs. 20/3442, S. 94.

640 BT-Drs. 20/5992, S. 78.

641 Bestätigend: *Forst*, in: Thüsing, HinSchG, § 6 Rn.15, wonach der Bezugspunkt der Gutgläubigkeit im Rahmen des § 6 Abs. 1 HinSchG die Erforderlichkeit sei.

642 *Wittig*, in: BeckOK-StGB, § 251 Rn.7; vgl. auch OLG Nürnberg, NStZ 1986, 556.

643 Etwa: BGH, BeckRS 2022, 35146 Rn.55; 2020, 40730 Rn.270; NJW-RR 2011, 1055 Rn.10; NJW 2009, 681 Rn.35; 2003, 1118, 1119; 2001, 2092, 2093; NJW-RR 1998, 34, 35; NJW 1992, 3235, 3236.

anderer aufgestellt, das zur Annahme eines vorsätzlichen Handelns im Rahmen des § 826 BGB gereichen soll.[644]

Daraus folgt, dass der Whistleblower vor der Meldung eines Geschäftsgeheimnisses einer Prüfpflicht zumindest im Sinne einer Bemühenspflicht unterliegt.[645] Diese Bemühenspflicht dient der Sicherstellung, dass der Whistleblower nur diejenigen Geschäftsgeheimnisse meldet bzw. offenlegt, die ihrem Inhalt und ihrer Form nach notwendig, respektive verhältnismäßig sind, um bestehende Missstände zu beseitigen und Rechtskonformität herzustellen. Dafür streitet auch die Rechtsprechung des EuGH zu Art. 10 EMRK: „*Von jemandem, der Anzeige in gutem Glauben erstattet hat, kann vernünftigerweise nicht erwartet werden, vorherzusehen, ob die Ermittlungen zu einer Anklage führen oder eingestellt werden. Unter solchen Umständen muss aber der Informant seiner Pflicht genügt haben, nach den Umständen möglichst sorgfältig zu prüfen, ob die Information genau und zuverlässig ist*.“[646]

Zu prüfen ist nach hiesiger Auffassung also, ob der Whistleblower zum Zeitpunkt seiner Meldung berechtigterweise davon ausgehen durfte, dass es zum Zeitpunkt der beabsichtigten Meldung auch der Weitergabe des Geschäftsgeheimnisses bedurfte, um Rechtskonformität zu erreichen. Insofern darf eine gewisse Aufklärung durch den

---

644 Vgl. BGHZ 176, 281 Rn.46, NJW 2008, 2245; BGHZ 184, 365 Rn.39, ZIP 2010, 786, WM 2010, 749; BGH NJW-RR 1986, 1158, 1159. In der gerichtlichen Praxis spielt das Kriterium der Leichtfertigkeit unter § 826 BGB bei der Ermittlung vorsätzlichen Handelns eine tragende Rolle. Dabei geht es zumeist um Haftungsfragen in Bezug auf Auskunftspersonen, Kreditinstituten, Sachverständigen, Steuerberatern sowie Wirtschaftsprüfern.

645 Das Schrifttum spricht ebenfalls davon, keine überhöhten Anforderungen zu stellen: *Fuhlrott*/*Henckel*, ArbRAktuell 2022, 441, 444; *Pielow*/*Volk*, CB 2021, 232, 234; *Vitt*, BB 2022, 1844, 1847; *Bruns,* NJW 2023, 1609, 1611. Gegen eine Nachforschungspflicht: *Siemes,* CCZ 2022, 293, 300.

646 EGMR, Urteil v. 16.02.2021 - 23922/19, Rn.75, NJW 2021, 2343.

Whistleblower erwartet werden.[647] Entscheidend ist, was einem vernünftigen Dritten in der Person des Whistleblowers sofort hätte einleuchten müssen, um die Geheimhaltungsinteressen des Beschäftigungsgebers nicht über Gebühr zu belasten.[648]

Hinsichtlich des Umfangs der Meldung darf der Whistleblower nicht mehr als das unbedingt notwendige Maß an geheimen Informationen weitergeben.[649] Dies zielt auf die Einhaltung des Übermaßverbotes ab und wird in der Regel darauf hinauslaufen, dass der Whistleblower vor der Weitergabe eines Geschäftsgeheimnisses einen Anwalt zu konsultieren hat. Dies ist zumutbar, da die Geheimhaltungsbedürftigkeit der Information erkennbar ist. Andernfalls läge schon per Definition kein Geschäftsgeheimnis vor (§ 2 Nr. 1 GeschGehG).[650] Die Einholung eines vorherigen Rechtsrats kann einzelfallbezogen unzumutbar sein, soweit eine begründete und erhebliche Gefahr für das Leben oder die Gesundheit anderer besteht, sodass eine anwaltliche Konsultation nicht mehr abgewartet werden kann. Maßgeblich sind die Umstände des jeweiligen Einzelfalls. In der Regel kann von einem Whistleblower erwartet werden, vor der Meldung bzw. Offenlegung eines Geschäftsgeheimnisses Rechtsrat hinsichtlich des Umfangs der beabsichtigten Meldung einzuholen, um dem Erfordernis der Notwendigkeit in § 6 Abs. 1 HinSchG gerecht zu werden.

In Bezug auf die Form der Informationsweitergabe ist zu prüfen, ob der Whistleblower zum Zeitpunkt der beabsichtigten Meldung berechtigterweise davon ausgehen durfte, dass es der Weitergabe des Geschäftsgeheimnisses in der von ihm gewählten Form bedurfte, um Rechtskonformität zu erreichen. Dazu gehört auch eine Prüfung

---

647 Ebenso: *Thüsing*, Stellungnahme zum RegE eines Hinweisgerbeschutzgesetzes, S. 3.

648 *Lüneborg* formuliert z. B. zutreffend zu § 33 HinSchG, dass die Meldung „*verantwortungsvoll*“ sein müsse, vgl. *Lüneborg*, in: Thüsing, HinSchG § 33 Rn.29.

649 BT-Drs. 20/5992, S. 80; Erwägungsgründe 91, 97 Whistleblowing-RL.

650 Zur Definition des Geschäftsgeheimnisses siehe: Kapitel B) II. 3.

alternativer Mittel, die in gleicher Weise dazu geeignet sind, Rechtskonformität herzustellen. Beispielsweise muss eine Schwärzung oder anderweitige Unkenntlichmachung der geheimhaltungsbedürftigen Passagen in Erwägung gezogen werden. Darüber hinaus stellt sich die Frage, ob ein vorhandener interner Meldekanal als ein weniger eingriffsintensives Mittel gegenüber einem externen Meldekanal im Rahmen des § 6 Abs. 1 HinSchG Vorrang genießt. Dies beleuchtet der nächste Abschnitt.

b) Problemaufriss: Ist ein interner Meldeweg bei der Weitergabe eines Geschäftsgeheimnisses vorrangig zu nutzen?

Das Notwendigkeitskriterium des § 6 Abs. 1 HinSchG führt zu der Frage, ob und inwieweit ein Whistleblower einen vorhandenen internen Meldeweg bei der Weitergabe eines Geschäftsgeheimnisses vorrangig zu nutzen hat. Die Weitergabe eines Geschäftsgeheimnisses muss sowohl hinsichtlich des Umfangs der mitgeteilten Informationen als auch mit Blick auf die Form der Informationsweitergabe verhältnismäßig sein. Eine Weitergabe eines Geschäftsgeheimnisses ist verhältnismäßig, sofern die Weitergabe das zum Zeitpunkt der beabsichtigten Meldung mildeste Mittel darstellt, das geeignet ist, bestehende Missstände zu beseitigen und Rechtskonformität zu erreichen.[651] Dafür gilt es zunächst zu klären, welche Form der Meldung das mildeste Mittel darstellt, das die Geheimhaltungsinteressen des Beschäftigungsgebers am wenigsten tangiert.

Das HinSchG kennt die interne und die externe Meldung sowie die Offenlegung. Entscheidet sich der Whistleblower für eine Offenlegung eines Geschäftsgeheimnisses, stellt dies die eingriffsintensivste Art der Informationsweitergabe mit Blick auf die Geheimhaltungs-

[651] Vgl. BVerfG, Beschluss v. 27.04.2022 - 1 BvR 2649/21, NJW 2022, 1999, Rn.215; BVerfG, Beschluss v. 09.02.2022 - 2 BvL 1/20, NJW 2022, 1160, Rn.126; BVerfG, Beschluss v. 19.11.2021 - 1 BvR 781/21, NJW 2022, 139, Rn.211; BGH, Urteil v. 15.05.2018 - VI ZR 233/17, NJW 2018, 2883, Rn.25.

interessen des Beschäftigungsgebers dar. Die Offenlegung eines Geschäftsgeheimnisses hat zur Folge, dass die geschützten Informationen gegenüber der Öffentlichkeit zugänglich gemacht werden, § 3 Abs. 5 HinSchG. Dem Beschäftigungsgeber drohen dadurch irreparable Wettbewerbsnachteile. Eine Nutzung der geschützten Informationen durch Konkurrenten kann für den Beschäftigungsgeber unter Umständen sogar existenzvernichtende Wirkung haben.

Entscheidet sich der Hinweisgeber für einen externen Meldeweg, drohen dem Arbeitgeber ebenfalls irreparable Wettbewerbsnachteile. Zwar darf die externe Meldestelle die gemeldeten Informationen, die sich auf Geschäftsgeheimnisse beziehen, nach § 6 Abs. 4 HinSchG nur insoweit verwenden oder weitergeben, wie dies für das Ergreifen von Folgemaßnahmen erforderlich ist.[652] Dies setzt jedoch voraus, dass die für die Meldung zuständige Person auch Kenntnis darüber hat, dass es sich bei den gemeldeten Informationen um ein Geschäftsgeheimnis im Sinne des § 2 Nr. 1 GeschGehG handelt.

Der Whistleblower ist aufgrund seiner arbeitsvertraglichen Rücksichtnahmepflicht gegenüber den Interessen des Arbeitgebers dazu verpflichtet, im Rahmen seiner externen Meldung die Meldestelle darauf hinzuweisen, ob und inwieweit sich die gemeldeten Informationen auf ein Geschäftsgeheimnis im Sinne des § 2 Nr. 1 GeschGehG beziehen, §§ 241 Abs. 2, 242 BGB.[653] Kommt der Whistleblower dieser Pflicht nicht hinreichend nach, besteht die Gefahr, dass die geschützten Informationen insbesondere in den Fällen des § 29 Abs. 2 Nr. 2 und Nr. 4 HinSchG an öffentliche oder andere zuständige Stellen gelangen und infolgedessen an die Öffentlichkeit durchsickern. Hinzu kommt,

---

[652] Die Regelung des § 6 Abs. 4 HinSchG normiert eine eigenständige Geheimhaltungspflicht derjenigen, die für die externe Meldestelle tätig sind. Der Umfang der Geheimhaltungspflicht richtet sich nach dem Umfang der zugrundeliegenden Verschwiegenheits- oder Geheimhaltungspflicht, vgl. BT-Drs. 20/5992, S. 56.

[653] Dasselbe gilt für Informationen, die einer vertraglichen Verschwiegenheitspflicht unterliegen, § 6 Abs. 5 HinSchG. Hier hat der Gesetzgeber das Problem der fehlenden Kenntnis erkannt, vgl. BT-Drs. 20/5992, S. 57.

dass es immer Situationen geben kann, in denen eine externe Meldestelle (wenn auch nur vorübergehend) nicht ordnungsgemäß funktioniert. In diesen Fällen droht dem Beschäftigungsgeber erneut die Offenlegung der Informationen durch den Whistleblower, § 32 Abs. 1 Nr. 1 HinSchG. Der Beschäftigungsgeber hat aufgrund der fehlenden Kenntnis über die externe Meldung weder die Möglichkeit, auf ein ordnungsgemäßes Verfahren der externen Meldestelle hinzuwirken, noch den gemeldeten Missstand selbst zu beseitigen.

Entscheidet sich der Whistleblower für einen internen Meldeweg, führt dies dazu, dass die für die interne Meldung zuständige Person Kenntnis über das Geschäftsgeheimnis erlangt. Auch hier gilt die Regelung des § 6 Abs. 4 HinSchG. Die interne Meldestelle darf die Informationen, die sich auf Geschäftsgeheimnisse beziehen nur insoweit verwenden oder weitergeben, wie dies für das Ergreifen von Folgemaßnahmen erforderlich ist.[654] Der Whistleblower ist aufgrund seiner arbeitsvertraglichen Rücksichtnahmepflicht gegenüber den Interessen des Arbeitgebers verpflichtet, die Meldestelle darauf hinzuweisen, ob und inwieweit sich die gemeldeten Informationen auf ein Geschäftsgeheimnis im Sinne des § 2 Nr. 1 GeschGehG beziehen, §§ 241 Abs. 2, 242, 611a BGB. Kommt der Arbeitnehmer dieser Pflicht unzureichend nach, besteht für den Beschäftigungsgeber eine geringe Gefahr, dass die Informationen ungeschützt an andere Stellen gelangen und infolgedessen an die Öffentlichkeit durchsickern. Im Gegensatz zu einer externen Meldestelle wird die interne Meldestelle den Beschäftigungsgeber vor einer geplanten Abgabe eines Verfahrens darüber informieren, § 18 Nr. 2 und Nr. 4 lit. b) HinSchG. Der Beschäftigungsgeber hat sodann die Möglichkeit zu prüfen, ob die Informationen, die an eine andere Stelle gelangen sollen, hinreichend als schutzbedürftig ausgewiesen sind. Das interne Meldeverfahren ist

[654] § 18 HinSchG beschreibt keine bestimmten Folgemaßnahmen. Sofern keine Möglichkeit besteht, den gemeldeten Verstoß intern weiter zu überprüfen oder abzustellen, kann der Vorgang unter Beachtung der Vertraulichkeit (u. a. § 9 Abs. 3 und Abs. 4 HinSchG) an eine zuständige Behörde oder eine interne Ermittlungseinheit abgegeben werden.

damit diejenige Form der Meldung, die die Geheimhaltungsinteressen des Arbeitgebers am wenigsten beeinträchtigt (sog. mildestes Mittel).

Soweit ein interner Meldekanal zur Beseitigung bestehender Missstände geeignet ist, streiten die Verhältnismäßigkeitserwägungen im Rahmen des § 6 Abs. 1 HinSchG dafür, dem internen Meldekanal einen Vorrang zu gewähren. Allerdings spricht § 7 Abs. 1 S. 1 HinSchG dem Whistleblower ein Wahlrecht zwischen einem internen und externen Meldeweg zu. Es bedarf daher einer Untersuchung, inwieweit das Wahlrecht in § 7 Abs. 1 S. 1 HinSchG der Annahme eines vorrangig zu nutzenden internen Meldekanals im Rahmen des § 6 Abs. 1 HinSchG entgegensteht oder ob § 6 Abs. 1 HinSchG eine gegenüber § 7 Abs. 1 S. 1 HinSchG eigenständige Regelung bildet. Stimmen in der Literatur beurteilen diese Frage unterschiedlich. Während *Greiner* die Fortführung der Rechtsprechung des EMRK in der Rechtssache Heinisch unter § 6 Abs. 1 HinSchG andeutet und von einer „*spezifischen Verhältnismäßigkeitsbindung*“ spricht,[655] scheinen andere einen Vorrang des internen Meldewegs unter § 6 Abs. 1 HinSchG abzulehnen.[656]

---

655 *Greiner*, in: ErfK-ArbR, § 6 Rn.1.

656 *Bruns* geht anhand des § 7 Abs. 1 S. 1 HinSchG davon aus, dass es keinen internen Vorrang im Rahmen des § 6 Abs. 1 HinSchG geben kann, vgl. *Bruns*, in: BeckOK-ArbR, § 6 Rn.2-8. *Colneric*/*Gerdeman* sprechen zwar von einem „*besonderen Notwendigkeitsvorbehalt*“, halten diesen jedoch für klarstellend, ohne dass daraus Besonderheiten im Rahmen des § 6 Abs. 1 HinSchG ableitbar wären, vgl. *Colneric*/*Gerdeman*, in: BeckOK-HinSchG, §6 Rn.10. In diese Richtung auch: *Forst*, in: Thüsing, HinSchG § 6 Rn.15, 17, der zunächst richtig feststellt, dass Bezugspunkt der Gutgläubigkeit die Erforderlichkeit sei. Eine eigenständige Angemessenheitsprüfung im Rahmen des § 6 Abs. 1 HinSchG sei laut *Forst* allerdings nur auf Extremfälle beschränkt und komme allenfalls in Bezug auf die Geheimhaltungsinteressen Dritter in Betracht. Nach hiesiger Auffassung sind die Geheimhaltungsinteressen Dritter im Rahmen des § 6 Abs. 1 HinSchG insoweit berücksichtigungsfähig, als § 6 Abs. 1 HinSchG für jeden Geheimnisinhaber gesondert zu prüfen ist. Dafür spricht, dass § 6 Abs. 1 HinSchG einen allgemeinen Interessenausgleich zwischen Geheimnisinhaber und Whistleblower schafft, sodass die Norm

aa) Eine Betrachtung des Wortlauts

Maßgeblich für die Frage eines vorrangig internen Meldekanals ist, ob das Rangverhältnis des § 7 Abs. 1 S. 1 HinSchG im Rahmen des § 6 Abs. 1 HinSchG zu berücksichtigen ist. Nach dem Wortlaut des § 6 Abs. 1 HinSchG stehen zunächst sämtliche Meldewege gleichrangig nebeneinander, ohne dass sich daraus ein Rangverhältnis ableiten lässt. Für eine eigenständige Beurteilung der Meldekanäle im Rahmen des § 6 Abs. 1 HinSchG spricht, dass § 6 Abs. 1 HinSchG keinen Hinweis auf § 7 Abs. 1 S. 1 HinSchG enthält. Aus diesem Umstand kann jedoch nicht geschlossen werden, dass dem Whistleblower das Wahlrecht nach § 7 Abs. 1 S. 1 HinSchG nicht zustehen soll. Keine der Regelungen im HinSchG nimmt direkt Bezug auf § 7 Abs. 1 S. 1 HinSchG. Aus der fehlenden Bezugnahme lassen sich daher keine Schlussfolgerungen ableiten. Auch der Wortlaut der Whistleblowing-RL hilft bei der Frage, ob bei der Weitergabe von Geschäftsgeheimnissen ein Rangverhältnis zu beachten ist, nicht weiter. Es blieb den Mitgliedstaaten überlassen, ein dreistufiges oder zweistufiges Eskalationsmodell in Umsetzung der Whistleblowing-RL einzuführen. Folgerichtig trifft der Unionsgesetzgeber in Erwägungsgrund 98 Whistleblowing-RL keine ausdrückliche Aussage zum Rangverhältnis der Meldekanäle im Falle der Weitergabe eines Geschäftsgeheimnisses.

Demgegenüber streitet der Wortlaut des § 7 Abs. 1 S. 1 HinSchG dafür, dass dieser auch für die Weitergabe von Geschäftsgeheimnissen gilt. Dafür spricht, dass § 7 Abs. 1 S. 1 HinSchG nicht bezüglich der Art der Information unterscheidet. Die Zusammenschau mit § 7 Abs. 1 S. 2 HinSchG und § 7 Abs. 2 HinSchG deutet außerdem darauf hin, dass es keinen Vorrang eines internen Meldekanals geben

---

auch auf Dritte in ihrer Eigenschaft als Geheimnisinhaber Anwendung findet. Anknüpfungspunkt des § 6 Abs. 1 HinSchG ist demnach die Geheimnisinhaberschaft. Sollte es sich um ein Geschäftsgeheimnis eines Dritten handeln, ist § 6 Abs. 1 HinSchG daher für diesen mit Blick auf etwaige Schutz- und Abwehransprüche nach dem GeschGehG gesondert zu prüfen.

soll. § 7 Abs. 1 S. 2 HinSchG enthält lediglich eine allgemeine Empfehlung an den Whistleblower für die vorrangige Nutzung eines internen Meldekanals.[657] Dazu enthält § 7 Abs. 2 HinSchG spiegelbildlich eine allgemeine Aufforderung an den Beschäftigungsgeber, darauf hinzuwirken, dass ein interner Meldekanal vorrangig genutzt wird.[658] Ein solches Verständnis kollidiert jedoch mit dem im Notwendigkeitsvorbehalt des § 6 Abs. 1 HinSchG verankerten Verhältnismäßigkeitsgrundsatz, der sicherstellt, dass den Geheimhaltungsinteressen des Beschäftigungsgebers hinreichend Rechnung getragen wird. Dies gelingt jedoch nur, wenn von einem gewissen Vorrang des internen Meldewegs als dem mildesten Mittel auszugehen ist - vorausgesetzt der interne Meldeweg ist zur Beseitigung des Missstands geeignet und dem Whistleblower drohen in Folge der Meldung keine Repressalien.

Im Ergebnis hilft die Wortlautauslegung von § 6 Abs. 1 und § 7 HinSchG daher nichtweiter. Während § 7 HinSchG gegen einen Vorrang eines internen Meldekanals spricht, scheint dieser nach § 6 Abs. 1 HinSchG aus Gründen der Verhältnismäßigkeit geboten.

bb) Eine Betrachtung der Systematik

Aus der Systematik des HinSchG folgt, dass die Weitergabe von Geschäftsgeheimnissen eine hervorgehobene Stellung einnimmt. Mit § 6 Abs. 1 HinSchG wurde eine eigene Norm geschaffen, die zu den allgemeinen Vorschriften in Abschnitt 1 des HinSchG zählt. Daraus folgt, dass die Vorschrift „*vor die Klammer*“ gezogen wurde und den nachfolgenden Vorschriften als „*Allgemeiner Teil*“ vorgeht. Demgegenüber ist das Wahlrecht des § 7 Abs. 1 S. 1 HinSchG in Abschnitt 2 geregelt und zählt damit nicht zu den allgemeinen Vorschriften des HinSchG. Stattdessen gehört § 7 Abs. 1 S. 1 HinSchG zu den

---

[657] Die Rede ist auch von einem „*Appell*“ ohne rechtliche Verbindlichkeit, vgl. *Thüsing*, in: Thüsing, HinSchG, § 7 Rn.8; vgl. auch: *Dzida*/*Seibt,* NZA 2023, 657, 660.

[658] Die Orientierung wurde erst auf Betreiben des Vermittlungsausschusses eingefügt, BT-Drs. 20/6700, S. 2.

„*Grundsätzen der Meldung*“, die sich vorrangig an die Meldestelle richten. Beispielsweise sind es die Meldestellen, die das Vertraulichkeitsgebot wahren (§§ 8, 9 HinSchG), die datenschutzrechtlichen Vorgaben einhalten (§ 10 HinSchG) und die Meldungen dokumentieren müssen (§ 11 HinSchG). Insofern verwundert es, dass auch § 7 HinSchG Eingang in diesen Abschnitt gefunden hat. Denn dieser richtet sich an den Whistleblower und den Beschäftigungsgeber, nicht jedoch an die Meldestelle. Dass der Gesetzgeber sich für eine Verortung des § 7 HinSchG im Rahmen der Grundsätze zur Arbeitsweise der Meldestelle entschieden hat, spricht dafür, dass dies bewusst geschah, weil § 7 Abs. 1 S. 1 HinSchG keine Wirkkraft in Bezug auf § 6 Abs. 1 HinSchG ausstrahlen soll. Andersherum lässt die systematische Stellung des § 6 Abs. 1 HinSchG ebenfalls darauf schließen, dass diese der Regelung in § 7 Abs. 1 S. 1 HinSchG vorgehen soll. Im Ergebnis streitet die systematische Auslegung daher für eine von § 7 Abs. 1 S. 1 HinSchG losgelöste Betrachtungsweise des § 6 Abs. 1 HinSchG.

cc) Eine Betrachtung der Historie

Besondere Bedeutung hatte vor Inkrafttreten des HinSchG in Umsetzung der Whistleblowing-RL die Rechtsprechung des EGMR in der Rechtssache *Heinisch* erlangt.[659] Der EGMR ging in seiner Entscheidung von einem grundsätzlichen Vorrang der innerbetrieblichen Abhilfe aus. Dieser sei Ausfluss einer umfassenden Verhältnismäßigkeitsprüfung. Im Rahmen der gebotenen Verhältnismäßigkeitsprüfung seien unter anderem das öffentliche Interesse an der Information, deren Wahrheitsgehalt, Handlungsalternativen des Arbeitnehmers, aber auch die Gründe für dessen Handeln zu berücksichtigen. Die Interessenabwägung ergebe sodann, dass Arbeitnehmer aufgrund ihrer Loyalitätspflicht gegenüber ihrem Arbeitgeber in der Regel dazu verpflichtet seien, zunächst auf innerbetrieblichem Weg für Abhilfe zu sorgen. Nur wenn die Umstände des Einzelfalls eindeutig zu erkennen

---

[659] EGMR, Urteil v. 21.07.2011 - 28274/08, NJW 2011, 3501.
Siehe auch: Kapitel C) I. 1. a) und b).

geben, dass eine innerbetriebliche Abhilfe nicht möglich sei, könne der Arbeitnehmer die Informationen als letztes Mittel an die Öffentlichkeit geben, vgl. Art. 10 der EMRK. Dieses Verständnis stimmt mit der Rechtsprechung des BAG überein: Auch das BAG war bislang von einem grundsätzlichen Vorrang der internen Aufklärung ausgegangen.[660]

Mit dem Inkrafttreten des HinSchG ist die Rechtsprechung des BAG weitestgehend obsolet geworden, kann aber dennoch in Auslegungsfragen herangezogen werden. Voraussetzung ist, dass Auslegungsspielraum besteht. Dafür spricht, dass die Vorgaben des HinSchG die Rechtsprechung des EGMR in nationales Recht überführen.[661] Insofern bedarf es zwar keines unmittelbaren Rückgriffs mehr, dennoch kann in Auslegungsfragen des HinSchG auf die Rechtsprechung des EGMR zurückgegriffen werden. Zieht man die Maßstäbe der EGMR heran, ist davon auszugehen, dass bei der Weitergabe eines Geschäftsgeheimnisses grundsätzlich von einem Vorrang des internen Meldeweges auszugehen ist. Die Rücksichtnahme auf die Geheimhaltungsinteressen des Beschäftigungsgebers gebietet es, diesem zunächst die Gelegenheit zu geben, für innerbetriebliche Abhilfe zu sorgen. Nur wenn entgegenstehende Anhaltspunkte zum Zeitpunkt der beabsichtigten Meldung vorliegen, dass dem Missstand z. B. nicht wirksam abgeholfen werden könne, kann eine interne Meldung entbehrlich sein und die Informationen an eine andere Stelle gegeben werden. Auch die historische Auslegung deutet damit auf einen grundsätzlichen Vorrang des internen Meldekanals hin.

---

[660] BAG, Urteil v. 15.12.2016 - 2 AZR 42/16, NZA 2017, 703; BAG, Urteil v. 14.12.2011 - 10 AZR 283/10, NZA 2012, 501; BAG, Urteil v. 07.12.2006 - 2 AZR 400/05, FD-ArbR 2007, 219939; BAG, Urteil v. 03.07.2003 - 2 AZR 235/02, NZA 2004, 427.

[661] BT-Drs. 20/5992, S. 28-29, 55.

dd) Eine Betrachtung des Telos

Mit Blick auf das Telos ist festzuhalten, dass das HinSchG in Umsetzung der Whistleblowing-RL der Stärkung des Hinweisgeberschutzes dient und für Rechtskonformität sorgen will.[662] Koinzident hat der Gesetzgeber in § 6 HinSchG den Interessenkonflikt mit den Geheimhaltungsinteressen des Beschäftigungsgebers adressiert. Die Bezugnahmen des (Unions-) Gesetzgebers im Rahmen des GeschGehG und der GeschGeh-RL auf die Whistleblowing-RL belegen, dass der Interessenausgleich im Rahmen des HinSchG gefunden werden soll.[663] Demnach ist davon auszugehen, dass das HinSchG neben der Stärkung des Hinweisgeberschutzes auch einen angemessenen Interessenausgleich zwischen dem Hinweisgeberschutz und dem Geschäftsgeheimnisschutz bezwecken will. Diese Sichtweise streitet dafür, die Geheimhaltungsinteressen des Beschäftigungsgebers im Rahmen des § 6 Abs. 1 HinSchG hinreichend zu berücksichtigen. Insofern ist es zutreffend, wenn von einer „*spezifischen Verhältnismäßigkeitsbindung*“ im Rahmen des § 6 Abs. 1 HinSchG die Rede ist.[664] Die Interessenkollision zwischen Geschäftsgeheimnis- und Hinweisgeberschutz ist - dem Telos des § 6 Abs. 1 HinSchG entsprechend - anhand sämtlicher Einzelfallumstände aufzulösen.

Da § 7 Abs. 1 S. 1 HinSchG ausschließlich den Hinweisgeberschutz adressiert, ohne die gegenläufigen Geheimhaltungsinteressen des Beschäftigungsgebers in den Blick zu nehmen, muss die Verhältnismäßigkeitsprüfung anhand des Notwendigkeitskriteriums im Rahmen des § 6 Abs. 1 HinSchG folgerichtig eigenständig vorgenommen werden, um einseitige Verzerrungen zu Gunsten des Hinweisgeberschutzes zu vermeiden. Ungeachtet dessen streitet die allgemeine Verortung innerhalb des HinSchG weiterhin dafür, in Zweifelsfragen dem

662 BT-Drs. 20/5992, S. 38.
663 Siehe: Kapitel C) I. 1. c) ee).
664 *Greiner*, in: ErfK-ArbR, § 6 Rn.1

Hinweisgeberschutz den Vorrang im Rahmen des § 6 Abs. 1 HinSchG einzuräumen.[665]

ee) Gesamtbetrachtung:
Weshalb im Rahmen des HinSchG eine (Prüf-) Obliegenheit zur vorrangigen Nutzung eines internen Meldewegs besteht

Die Wortlautauslegung hilft bei der Frage nicht weiter, ob ein Vorrang eines internen Meldekanals im Rahmen des § 6 Abs. 1 HinSchG bestehen kann. Während § 7 HinSchG gegen einen Vorrang eines internen Meldekanals spricht, ist dieser aus Gründen der Verhältnismäßigkeit anhand des Notwendigkeitsvorbehalts geboten. Aus der Systematik folgt, dass die Weitergabe von Geschäftsgeheimnissen eine hervorgehobene Stellung einnimmt. Der nationale Gesetzgeber hat das Wahlrecht bei den Grundsätzen zur Arbeitsweise der Meldestelle verortet, weshalb aus systematischer Sicht davon auszugehen ist, dass die Regelung des § 7 Abs. 1 S. 1 HinSchG nach dem Willen des Gesetzgebers keine Wirkkraft auf die allgemeine Vorschrift des § 6 Abs. 1 HinSchG entfalten soll. Das Telos streitet ebenfalls für eine eigenständige Auslegungsweise des § 6 Abs. 1 HinSchG, ohne dass es auf die Vorgabe des § 7 Abs. 1 S. 1 HinSchG ankommt. Der nationale Gesetzgeber verfolgt mit den Vorgaben des HinSchG in Umsetzung der Whistleblowing-RL einerseits das Ziel, den Hinweisgeberschutz zu stärken. Darüber hinaus soll im Rahmen des § 6 Abs. 1 HinSchG ein angemessener Interessenausgleich zwischen dem Hinweisgeberschutz und dem Geschäftsgeheimnisschutz geschaffen werden. § 7 Abs. 1 S. 1 HinSchG lässt jedoch die gegenläufigen Geschäftsgeheimnisinteressen des Beschäftigungsgebers außen vor. Es ist daher richtig, von einer „*spezifischen Verhältnismäßigkeitsbindung*“[666] im Rahmen des § 6 Abs. 1 HinSchG zu sprechen. Systematik und Telos geben den Ausschlag dafür, dass die Interessenkollision anhand sämtlicher Einzelfallumstände innerhalb des § 6 Abs. 1 HinSchG aufzu-

665 Siehe: Kapitel C) I. 1. c) ee).
666 *Greiner*, in: ErfK-ArbR, § 6 Rn.1.

lösen ist, ohne dass es auf die Vorgabe des § 7 Abs. 1 S. 1 HinSchG ankommt.

Das Wahlrecht des § 7 Abs. 1 S. 1 HinSchG ist daher so zu verstehen, dass sich dieses auf Informationen bezieht, die keine Geschäftsgeheimnisse sind. Dies steht auch dem Bestreben nach mehr Rechtssicherheit im Bereich des Hinweisgeberschutzes nicht entgegen. Aufgrund der besonderen Stellung des § 6 Abs. 1 HinSchG ist es für den Whistleblower deutlich erkennbar, dass § 6 Abs. 1 HinSchG eine gesonderte Rolle einnimmt und von den übrigen Vorschriften losgelöst zu betrachten ist. Da das Rangverhältnis des § 7 Abs. 1 HinSchG folgerichtig im Rahmen des § 6 Abs. 1 HinSchG keine Anwendung findet, kann die historische Auslegung nach dem Maßstab des EGMR in die Auslegung des Notwendigkeitskriteriums mit einfließen. Nach den vom EGMR entwickelten Maßstäben ist davon auszugehen, dass bei der Weitergabe eines Geschäftsgeheimnisses grundsätzlich ein Vorrang des internen Meldeweges besteht, soweit das interne Hinweisgebersystem wirksam ist und dem Whistleblower keine Repressalien infolge der Meldung drohen. Die Rücksichtnahme auf die Geheimhaltungsinteressen des Beschäftigungsgebers gebietet es, diesem zunächst die Gelegenheit zu geben, für innerbetriebliche Abhilfe zu sorgen. Nur wenn entgegenstehende Anhaltspunkte vorliegen, dass dem Missstand nicht wirksam abgeholfen wird, kann eine zunächst interne Meldung entbehrlich sein und die Information an andere Stelle gemeldet werden.

Hat der Whistleblower zum Zeitpunkt der beabsichtigten Meldung hinreichenden Grund zu der Annahme, der interne Meldeweg sei zur Beseitigung des möglichen Missstands geeignet, resultiert daraus konsequenterweise ein Vorrang des internen Meldekanals im Rahmen des § 6 Abs. 1 HinSchG. Hintergrund ist, dass der interne Meldeweg gegenüber einer externen Meldung bzw. Offenlegung das mildere Mittel im Hinblick auf die Geheimhaltungsinteressen des Beschäftigungsgebers ist. Der Whistleblower hat zum Zeitpunkt seiner beabsichtigten Meldung zu beurteilen, ob Anhaltspunkte vorliegen, die gegen die

Wirksamkeit des internen Hinweisgeberschutzsystems sprechen, wobei ihm dabei nichts Unzumutbares abverlangt werden darf. Gründe, die gegen ein wirksames Hinweisgebersystem sprechen, sind z. B. die häufige Nichterreichbarkeit der internen Meldestelle oder Äußerungen von Vorgesetzten bzw. Führungskräften, die Ankündigungen oder Andeutungen enthalten, internen Meldungen werde nicht hinreichend nachgegangen. Unzumutbar könnte die Nutzung sein, wenn dem Whistleblower infolge der Nutzung des internen Meldekanals Repressalien drohen. In Zweifelfragen ist dem Hinweisgeberschutz Vorrang zu gewähren. Dies folgt aus der allgemeinen Verortung der Norm im Regelungsgefüge des HinSchG.

Setzt sich der Whistleblower über den Vorrang der internen Meldung im Rahmen des § 6 Abs. 1 HinSchG hinweg, erfolgt die Weitergabe des Geschäftsgeheimnisses nicht erlaubt im Sinne des § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 GeschGehG und das Haftungssystem des GeschGehG greift.[667] Dies gilt auch für den Ausnahmetatbestand des § 5 Nr. 2 GeschGehG, der im Sinne der Einheit der Rechtsordnung denselben Grundsätzen wie § 6 Abs. 1 HinSchG unterliegt.[668] Darüber hinaus drohen dem Whistleblower nach § 6 Abs. 2 HinSchG auch arbeits- rechtliche Konsequenzen. Die Anforderungen des § 6 Abs. 2 HinSchG entsprechen denen des § 6 Abs. 1 HinSchG, soweit es um die Weitergabe von Geschäftsgeheimnissen geht.[669] Darüber hinaus bleibt der Identitätsschutz nach §§ 8, 9 HinSchG bestehen. Der Hinweisgeber verliert nach Maßgabe des § 33 Abs. 1 HinSchG i. V. m § 35 Abs. 2 HinSchG auch nicht seinen Schutz vor einer

[667] Das Haftungssystem des GeschGehG greift, sofern weder § 3 Abs. 2 GeschGehG noch § 5 Nr. 2 GeschGehG einschlägig sind. Siehe: Kapitel C) I. 2. c).

[668] Siehe: Kapitel C) I. 1. c) ee).

[669] *Forst*, in: Thüsing, HinSchG, § 6 Rn.21.

weitergehenden Haftung vor Schäden Dritter.[670] Auch das Verbot von Repressalien nach § 36 HinSchG bleibt bestehen.[671] Dieses Ergebnis ist interessengerecht, weil es der Funktion des § 6 Abs. 1 HinSchG als Kollisionsvorschrift von Hinweisgeberschutz und Geschäftsgeheimnisschutz gerecht wird und zugleich dafür sorgt, dass der Hinweisgeberschutz im Übrigen fortbesteht.

Es entspricht dem obligatorischen Grundsatz der Verhältnismäßigkeit, an den Ausschluss der rechtlichen Verantwortlichkeit eines Whistleblowers für eine Weitergabe bzw. Offenlegung eines Geschäftsgeheimnisses erhöhte Anforderungen zu stellen. Die Geheimhaltungsbedürftigkeit der Information gebietet es, dass die Weitergabe eines Geschäftsgeheimnisses mit der nötigen Rücksichtnahme auf die Unternehmensinteressen erfolgt. Da der Whistleblower seines Hinweisgeberschutzes bei Missachtung des Notwendigkeitsvorbehalts in § 6 Abs. 1 HinSchG im Übrigen nicht verlustig geht, trifft den Whistleblower weniger eine Prüfpflicht in Bezug auf Umfang und Form der Weitergabe eines Geschäftsgeheimnisses, sondern vielmehr eine Prüfobliegenheit, aus der ein Vorrang des internen Meldewegs resultieren kann. Voraussetzung ist, dass der Whistleblower zum Zeitpunkt der beabsichtigten Meldung bei objektiver Betrachtung hinreichenden Grund zu der Annahme hat, der interne Meldeweg sei zur Beseitigung des möglichen Missstands geeignet, weil ein funktionsfähiges und wirksames Hinweisgeberschutzsystem vorhanden ist.

---

[670] Soweit es um die Weitergabe bzw. Offenlegung eines Geschäftsgeheimnisses eines Dritten geht, bestimmt sich die Frage des Haftungsaus-schlusses gegenüber diesem in seiner Eigenschaft als Geheimnisinhaber gesondert nach § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG. *Forst* geht von einer Berücksichtigungsfähigkeit der Geheimhaltungsinteressen Dritter im Rahmen der Verhältnismäßigkeitserwägung aus, vgl. *Forst*, in: Thüsing, HinSchG, § 6 Rn.21.

[671] BT-Drs. 20/3442, S. 94.

c) Die zulässige Weitergabe von Geschäftsgeheimnissen nach den Vorgaben des § 5 Nr. 2 GeschGehG

Ist der Anwendungsbereich des HinSchG nicht eröffnet, kann Hinweisgeberschutz nach § 5 Nr. 2 GeschGehG bestehen. § 5 Nr. 2 GeschGehG ist nach dem Willen des (Unions-) Gesetzgebers neben § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG anwendbar und ergänzt diesen.[672] Die Vorgaben des HinSchG entfalten demzufolge keine Sperrwirkung gegenüber § 5 Nr. 2 GeschGehG. Die Einheit der Rechtsordnung gebietet aus Gründen der Rechtssicherheit, dass § 5 Nr. 2 GeschGehG dem gleichen Auslegungsmaßstab folgt, dem § 6 Abs. 1 HinSchG unterliegt. Insofern bedarf es einer harmonisierenden Auslegung des § 5 Nr. 2 GeschGehG nach Maßgabe des § 6 Abs. 1 HinSchG.[673] Diese Lesart wird dem Anliegen des nationalen Gesetzgebers gerecht, den Hinweisgeberschutz zu stärken und schafft Rechtssicherheit im Gefüge zwischen Geschäftsgeheimnisschutz und Hinweisgeberschutz. Dementsprechend sind die zuvor anhand des Notwendigkeitskriteriums gefundenen Maßstäbe auch im Rahmen des § 5 Nr. 2 GeschGehG anhand der obligatorischen Verhältnismäßigkeitsprüfung zu beachten.[674] Dies gilt insbesondere mit Blick auf die (Prüf-) Obliegenheit, aus der ein Vorrang des internen Meldewegs resultieren kann.[675]

3. Weiterungen für das unternehmerische Compliance-System

Zu den Sorgfaltspflichten eines ordentlichen und gewissenhaften Geschäftsleiters zählt, das Unternehmen so zu führen, dass diesem keine wirtschaftlichen Nachteile entstehen, § 93 Abs. 1 AktG,

---

672 Etwa: Art. 3 Abs. 2 GeschGeh-RL verweist auf die Vorgaben der Whistleblowing-RL, Erwägungsgrund 98 Whistleblowing-RL für den Unionsgesetzgeber.

673 Zur harmonisierenden Auslegung: Kapitel C) I. 1. c) ee).

674 Zur Verhältnismäßigkeitsprüfung im Rahmen des § 5 Nr. 2 siehe auch: Kapitel C) I. 1. c) cc).

675 Siehe: Kapitel C). I. 2. b) ee).

§ 43 Abs. 1 GmbHG.[676] Um das Unternehmen vor einem Reputationsverlust und weiteren Schäden in Folge des Bekanntwerdens von Geschäftsgeheimnissen hinreichend zu schützen, ist die Geschäfts-leitung verpflichtet, darauf hinzuwirken, dass ein Whistleblower sich für einen internen Meldeweg entscheidet.

In der Beschlussempfehlung des Vermittlungsausschusses heißt es: „*Ob und inwieweit Beschäftigungsgeber Anreize für Beschäftigte schaffen, zunächst interne Meldeverfahren zu nutzen, wird bewusst nicht vorgegeben*“.[677] Das HinSchG biete „*Motivation für Beschäftigungsgeber zur selbständigen Optimierung der internen Meldewege*“.[678] Im gleichen Zuge lässt es sich der Vermittlungsausschuss jedoch nicht nehmen, allgemeine Hinweise zu geben, die für ein wirksames Hinweisgebersystem sprechen: „*So sollen eine gute Kommunikationskultur und soziale Verantwortung gefördert werden. Wenn hinweisgebende Personen der Meinung sind, dass innerhalb der Organisation wirksam gegen den Verstoß vorgegangen werden kann und keine Repressalien drohen, dürfte dies die Bereitschaft fördern, zunächst interne Meldekanäle zu nutzen*.“[679]

Die vorstehenden Ausführungen haben gezeigt, dass im Rahmen des § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG eine (Prüf-) Obliegenheit des Whistleblowers besteht, aus der ein Vorrang des internen Meldewegs resultieren kann.[680] Die Geschäftsleitung ist daher gesellschaftsrechtlich verpflichtet, sicherzustellen, dass aus der Prüfobliegenheit im Rahmen des § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG ein Vorrang des internen Meldewegs resultiert. Dies gelingt durch die Implementierung eines wirksamen Hinweisgebersystems, von dem der Whistleblower hinreichenden Grund zu der

---

676 *Reinfeld*, in: Hdb-ArbR, § 35 Rn.9 ff.; *Thüsing*, in: Compliance, § 2 Rn.20 m. w. N.
677 BT-Drs. 20/4909, S. 53.
678 BT-Drs. 20/4909, S. 53.
679 BT-Drs. 20/4909, S. 53.
680 Siehe: Kapitel C). I. 2. b) ee).

Annahme hat, dass dieses zur Beseitigung des Missstands geeignet ist, ohne dass ihm durch die Meldung Repressalien drohen. Dafür gilt es, insbesondere häufige Nichterreichbarkeiten der internen Meldestelle zu vermeiden und Äußerungen von Vorgesetzten bzw. Führungs-kräften, die Ankündigungen oder Andeutungen enthalten, internen Meldungen werde nicht hinreichend nach-gegangen, zu unterbinden und adäquat zu korrigieren. In Zweifelsfragen ist dem Hinweisgeberschutz Vorrang zu gewähren. Dies folgt aus der allgemeinen Verortung der Norm im Regelungsgefüge des HinSchG. Die Implementierung eines wirksamen Hinweisgeberschutzsystems ist damit Teil des Geheimnisschutzkonzepts, vgl. § 2 Nr. 1 lit. b) GeschGehG.[681]

Um das Unternehmen vor Schäden und Reputationsverlusten zu bewahren, steht die Geschäftsleitung außerdem vor der Herausforderung, sicherzustellen, dass Informationen über Missstände, die (noch) keine Geschäftsgeheimnisse sind, vorrangig intern gemeldet werden. Das Unternehmen wird die Missstände beseitigen und mittels den Umständen nach angemessenen Geheimhaltungsmaßnahmen dafür Sorge tragen, dass die Informationen nicht nach außen dringen.[682] Dafür hat die Unternehmensleitung Anreize zu schaffen, dass Whistleblower einen internen Meldekanal bevorzugen. Neben der Schaffung anonymer Meldekanäle und Maßnahmen zur Erhöhung des Identitätsschutzes kommen insbesondere berufliche und finanzielle Anreize in Betracht.[683] Darüber hinaus sind auch interne Meldever-

---

[681] Bei der Einführung interner Meldeverfahren sind unter Umständen die Beteiligungsrechte des Betriebsrats zu beachten. Bestimmt der Arbeitgeber ein standardisiertes Meldeverfahren, ist das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG in Erwägung zu ziehen. Die Implementierung digitaler Meldesysteme kann auch ein Mitbestimmungsrecht nach § 87 Abs.1 Nr. 6 BetrVG auslösen. Ausführlicher zu den Beteiligungsrechten des Betriebsrats bei der Einführung einer Meldestelle: *Zimmer*/*Millfahrt*, BB 2023, 1269, 1271.

[682] Auch rechtswidrige Informationen sind schutzfähig nach dem GeschGehG. Siehe: Kapitel B) II. 3. a) (6) und Kapitel B) II. 3. b).

[683] Vgl. *Colneric/Gerdemann*, in: BeckOK HinSchG, § 7 Rn.31-33 m. w. N.

pflichtungen zu erwägen.[684] Sämtliche Anreize bilden einen notwendigen Zwischenschritt, um die sensiblen Informationen in den Schutzbereich des GeschGehG zu überführen. Zugleich ist die Förderung von Hinweisen aus der eigenen Belegschaft probates Mittel, um sicherzustellen, dass das Unternehmen im Einklang mit der geltenden Rechtsordnung handelt (sog. Legalitätspflicht).[685]

a) Verpflichtung zur vorrangigen Nutzung eines internen Meldewegs

Zweifelhaft ist, ob die Geschäftsleitung Whistleblower in Bezug auf Informationen, die keine Geschäftsgeheimnisse sind, zu einer vorrangigen Nutzung eines internen Meldewegs verpflichten kann.[686] § 7 Abs. 1 S. 1 HinSchG gewährt dem Hinweisgeber das Recht, zwischen einer internen Meldung und einer externen Meldung zu wählen. Interner und externer Meldeweg stehen dabei gleichwertig nebeneinander. Flankierend dazu stellt § 7 Abs. 2 HinSchG klar, dass es verboten ist, Meldungen zu behindern oder dies zu versuchen. Der nationale Gesetzgeber weist in diesem Zusammenhang ausdrücklich darauf hin, dass es nicht mit den Vorgaben des HinSchG vereinbar wäre, den Zugang zu externen Meldestellen durch interne Vorschriften oder Vereinbarungen einzuschränken.[687] Eine Pflicht zur vorrangigen Nutzung eines internen Meldewegs hätte jedoch zur Folge, dass dem Hinweisgeber der Weg zur externen Meldestelle verwehrt bliebe. Darin liegt eine unzulässige Beschränkung des Wahlrechts, deren Unwirksamkeit § 39 HinSchG anordnet. Die Geschäftsleitung darf den Whistleblower daher nicht zur vorrangigen Nutzung eines internen Meldewegs verpflichten. Vereinbarungen, die eine solche Pflicht vorsehen, sind nach §§ 7 Abs. 1 S. 1, Abs. 2 Var. 1, 39 HinSchG i. V. m. § 134 BGB unwirksam. Das gesellschaftsrechtliche Pflichtenprogramm der Ge-

684 Kritisch: *Lüneborg*, in: Thüsing, HinSchG, § 7 Rn.25 m. w. N.
685 *Thüsing*, in: Compliance, § 2 Rn.6, 10 m. w. N.
686 Zur Obliegenheit der vorrangigen Nutzung eines internen Meldewegs bei der Weitergabe von Geschäftsgeheimnissen siehe: Kapitel C) I. 2. b) ee).
687 BT-Drs. 20/5992, S. 57.

schäftsleitung kann sich nicht über das gesetzliche Verbot hinwegsetzen.

Ein Vorrang einer internen Meldung ergibt sich auch nicht aus § 17 Abs. 2 S. 1 ArbSchG. Zwar heißt es in § 17 Abs. 2 S. 1 ArbSchG, dass ein Arbeitnehmer, der auf Grund konkreter Anhaltspunkte der Auffassung ist, dass die vom Arbeitgeber getroffenen Maßnahmen und bereitgestellten Mittel nicht ausreichen, um die Sicherheit und den Gesundheitsschutz bei der Arbeit zu gewährleisten, erst dann berechtigt ist, sich an die zuständige Behörde zu wenden, wenn der Arbeitgeber zuvor einer darauf gerichteten arbeitnehmerseitigen Beschwerde nicht abgeholfen hat. Allerdings stellt § 17 Abs. 2 S. 3 ArbSchG klar, dass die Vorschriften des HinSchG unberührt bleiben. Der Arbeitnehmer hat daher die Wahl, ob er sich für ein Vorgehen im Sinne des § 17 Abs. 2 S. 1 ArbSchG entscheidet oder als Whistleblower im Sinne des HinSchG agiert. Ihm bleibt der Weg zu einer externen Meldestelle nicht verwehrt.

b) Verpflichtung zur Abgabe einer internen Meldung

Es stellt sich die Frage, ob die Geschäftsleitung den Arbeitnehmer zu einer internen Meldung verpflichten kann. Eine Pflicht zur internen Meldung ist sowohl der *„Legalitätskontrollpflicht*“ als auch der Pflicht zur sorgfältigen Unternehmensführung zuordbar.[688]

Aus § 7 Abs. 2 Var. 1 HinSchG i. V. m. § 134 BGB folgt, dass es der Geschäftsleitung verboten ist, Meldungen zu behindern oder dies zu versuchen. Ergänzend stellt § 39 HinSchG klar, dass die Schutzvorschriften des HinSchG zwingend sind. Abweichende Vereinbarungen zuungunsten des Hinweisgebers sind folgerichtig nicht möglich. Der nationale Gesetzgeber weist in diesem Zusammenhang ausdrücklich darauf hin, dass es nicht mit den Vorgaben des HinSchG vereinbar

[688] Vgl. § 93 Abs. 1 S. 1 AktG, § 43 Abs. 1 GmbHG, § 34 Abs. 1 S. 2 GenG. Siehe auch: *Thüsing*, in: Compliance, § 2 Rn.6, 10.

wäre, den Zugang zu externen Meldestellen durch interne Vorschriften oder Vereinbarungen einzuschränken: „*Unwirksam sind danach alle Vereinbarungen, die in diesem Gesetz vorgesehene Rechte beschränken oder ausschließen. Dies gilt insbesondere für den freien Zugang zu externen Meldestellen oder die Zulässigkeit einer Offenlegung unter den Voraussetzungen dieses Gesetzes*."[689] Zu beachten ist demnach, dass eine interne Meldepflicht den Whistleblower nicht davon abhalten darf, eine externe Meldung zu tätigen. Dass eine interne Meldepflicht zu einer Art „*Gleichzeitigkeit*" mit der externen Meldung führt, ist insofern unerheblich.

Wortlaut und Gesetzesmaterialien zeigen, dass das Telos des Wahlrechts ist, den externen Meldeweg nicht zu versperren. Der Whistleblower soll stets eine Zugangsmöglichkeit zu einer externen Meldestelle haben. Dies geht auch aus § 7 Abs. 1 S. 3 HinSchG hervor. Dazu heißt es in der Gesetzesbegründung: „*Satz 3 stellt klar, dass es nicht mit den Vorgaben dieses Gesetzes vereinbar wäre, den Zugang zu externen Meldestellen einzuschränken, etwa durch interne Vorschriften oder Vereinbarungen.*"[690] § 7 Abs. 1 S. 1, Abs. 2 HinSchG ist daher ausschließlich im Sinne eines unabdingbaren Zugangsrechts zu einer externen Meldestelle zu verstehen.

Für diese Lesart streitet auch die Whistleblowing-RL. In Erwägungsgrund 33 der Whistleblowing-RL heißt es: „*Zugleich sollte der Hinweisgeber den Meldekanal wählen können, der sich angesichts der fallspezifischen Umstände am besten eignet. Zudem ist es erforderlich, im Einklang mit den von der Rechtsprechung des EGMR aufgestellten Kriterien die Offenlegung von Informationen unter Berücksichtigung demokratischer Grundsätze wie Transparenz und Verantwortlichkeit und Grundrechten wie die Freiheit der Meinungsäußerung und die Freiheit und die Pluralität der Medien zu schützen und gleichzeitig das Interesse der Arbeitgeber an der Verwaltung ihrer Unternehmen*

[689] BT-Drs. 20/5992, S. 83.
[690] BT-Drs. 20/5992, S. 57, 58.

und dem Schutz ihrer Interessen einerseits mit dem Interesse der Öffentlichkeit am Schutz vor Schaden andererseits abzuwägen." Daraus ergibt sich, dass der Unionsgesetzgeber ebenfalls von einem Wahlrecht des Whistleblowers ausgeht. Der zusätzliche Hinweis auf die vom EGMR aufgestellten Kriterien, die ein grundsätzlich dreistufiges Eskalationsmodell vorsehen, belegt, dass der Unionsgesetzgeber sogar einen Vorrang für einen internen Meldekanal für zulässig erachtet hätte. Aus Sicht des Unionsgesetzgebers soll lediglich sichergestellt sein, dass dem Hinweisgeber in Fällen, in denen ein Whistleblower berechtigte Zweifel an der Wirksamkeit eines internen Meldewegs hegt, auch eine externe Meldestelle sowie die Möglichkeit einer Offenlegung zur Verfügung stehen, wobei die Offenlegung sog. „*ultima ratio*" ist.[691] Die Whistleblowing-RL steht einer internen Meldepflicht folgerichtig nicht entgegen. Voraussetzung ist, dass dem Whistleblower der Weg zu einer externen Meldestelle erhalten bleibt. Der Unionsgesetzgeber geht somit ebenfalls von einem unabdingbaren Zugangsrecht zu einer externen Meldestelle aus.

Im Ergebnis ist eine interne Meldepflicht daher grundsätzlich möglich. Maßgeblich ist, dass dem Whistleblower der Zugang zum externen Meldeweg erhalten bleibt.[692] Aus Transparenzgründen ist der Whistleblower auf diesen Umstand hinzuweisen, § 307 Abs. 1 S. 2 BGB. Eine Pflicht zur internen Meldung stellt keine unzulässige Abweichung zuungunsten des Hinweisgebers im Sinne der §§ 7 Abs. 1 S. 1, Abs. 2 Var. 1, 39 HinSchG dar, unterliegt allerdings einer strengen Wirksamkeitskontrolle.[693] Insbesondere muss die Klausel hinreichend bestimmt sein und darf den Arbeitnehmer in seiner Eigenschaft als Whistleblower nicht unangemessen benachteiligen, § 307 Abs. 1 S. 1 und S. 2 BGB. Dies setzt die Implementierung eines wirksamen Hinweisgeberschutzsystems voraus. Ein Arbeitnehmer, der infolge einer Meldung Repressalien zu fürchten hat, wäre unan-

---

691 Vgl. EGMR, Urteil v. 21.07.2011 - 28274/08 - *Heinisch/Deutschland.*
692 Gleiches gilt mit Blick auf das Recht zur Offenlegung, § 32 HinSchG.
693 Begrenzende Wirkung entfalten u. a. die §§ 134, 138, 242, 307 ff. BGB.

gemessen benachteiligt, wäre er arbeitsvertraglich verpflichtet, sich diesen Repressalien auszusetzen, § 307 Abs. 1 S. 1 BGB. Gleiches gilt mit Blick auf den Identitätsschutz, vgl. §§ 8, 9 HinSchG.

Darüber hinaus ist zu bedenken, dass eine interne Meldepflicht den Arbeitnehmer in seinem Recht, keine Meldung zu tätigen, tangiert (sog. „*Recht auf negative Meinungsfreiheit*“).[694] Eine interne Meldepflicht nimmt dem Whistleblower das Recht, selbst darüber zu entscheiden, ob er Informationen über mögliche Verstöße meldet oder nicht. Dies ist im Rahmen der Wirksamkeitskontrolle unter dem Gesichtspunkt der unangemessenen Benachteiligung (§ 307 Abs. 1 S. 1 BGB) zu bedenken. Maßgeblich ist ein Interessenausgleich zwischen dem Interesse des Beschäftigungsgebers an der Aufdeckung des Missstands und der negativen Meinungsfreiheit des Whistleblowers.

Der Arbeitgeber hat ein berechtigtes Interesse daran, sicherzustellen, dass das Unternehmen im Einklang mit der geltenden Rechtsordnung handelt und, dass das Unternehmen vor den mit einem Reputationsverlust einhergehenden Wettbewerbsnachteilen in Folge des Bekanntwerdens von Informationen über mögliche Verstöße geschützt ist.[695] Demgegenüber tangieren Anzeigepflichten auf Seiten des Arbeitnehmers das Recht, über mögliche Verstöße (als Ausdruck der negativen Meinungsfreiheit) zu schweigen. Auch mögliche Gewissenskonflikte sind mitzudenken. Darüber hinaus können auch die Interessen Dritter zum Tragen kommen, beispielsweise über die Fürsorgeverantwortung des Arbeitgebers. Die interne Meldung ermöglicht es dem Arbeitgeber, seiner Fürsorgeverantwortung nachzukommen und die Beschäftigten vor Gefahren zu schützen, von denen er ohne die interne Meldung keine Kenntnis hätte. Maßgeblich sind die Umstände des Einzelfalls.

---

694 Vgl. *Reinfeld*, in: Hdb-ArbR, § 35 Rn.145.

695 Dies entspricht der sog. „*Legalitätskontrollpflicht*“ der Geschäftsleitung, § 93 Abs. 1 S. 1 AktG, § 43 Abs. 1 GmbHG, § 34 Abs. 1 S. 2 GenG, vgl. auch: *Thüsing*, in: Compliance, § 2 Rn.10.

Nach alledem kann ein Arbeitnehmer jedenfalls nicht pauschal, beispielsweise zu denselben Vorgaben, wie das HinSchG sie aufstellt, zur Abgabe einer internen Meldung verpflichtet werden. Nötig sind Konkretisierungen, u. a. hinsichtlich des objektiven Verdachtsgrads und des Schweregrads eines Missstands, die es vermögen, den Eingriff in das Recht auf negative Meinungsfreiheit zu rechtfertigen. Die Rechtsprechung und das überwiegende Schrifttum sind bislang zu Recht davon ausgegangen, dass eine Anzeigepflicht in Bezug auf bestimmte erhebliche Rechtsverstöße, die im betrieblichen Zusammenhang stehen, nach Maßgabe einer umfassenden Interessenabwägung möglich ist (§§ 241 Abs. 2, 242, 611a BGB).[696]

Hinsichtlich des Schweregrads des Missstands gilt die Regel: Je schwerer und gewichtiger der Missstand, desto eher überwiegen die Interessen des Unternehmens an dessen Beseitigung gegenüber der negativen Meinungsfreiheit des Arbeitnehmers, auch weil die Beseitigung des Missstands zugleich im öffentlichen Interesse liegt. Hier bietet sich beispielsweise eine enumerative Auflistung von Straf- oder Bußgeldtatbeständen an. Orientierung bietet auch § 16 Abs. 1 ArbSchG. Danach sind Arbeitnehmer verpflichtet, ihrem Arbeitgeber bzw. dem zuständigen Vorgesetzten jede von ihnen festgestellte unmittelbare erhebliche Gefahr für die Sicherheit und Gesundheit sowie jeden an den Schutzsystemen festgestellten Defekt unverzüglich zu melden.[697] Der Arbeitnehmer ist ohnehin bereits aus § 16 Abs. 1 ArbSchG zur internen Meldung verpflichtet, sobald dieser einen Defekt an den Schutzsystemen feststellt oder eine unmittelbare erhebliche Gefahr für die Sicherheit und Gesundheit besteht. Hinsichtlich der Konkretisierung des objektiven Verdachtsgrads kommen

---

[696] BAG, Urteil v. 18.06.1970 - 1 AZR 520/69, NJW 1970, 1861 f.; LAG Düsseldorf, Beschluss v. 12.12.2005 - 10 TaBV 46/05, BeckRS 2006, 40003; *Reinfeld*, in: Hdb-ArbR, § 35 Rn.145; *Forst*, in: Compliance, § 6 Rn.53; DAV-Stellungnahme zum HinSchG-E, S. 34.

[697] Dafür spricht, dass die Regelung des § 16 Abs. 1 ArbSchG eine „*echte Rechtspflicht*“ i. S. einer öffentlich-rechtlichen Pflicht darstellt, die zugleich die arbeitsvertragliche Rücksichtnahmepflicht aus § 241 Abs. 2 BGB konkretisiert, vgl. auch *Roloff*, in: ErfK-ArbR, § 15 ArbSchG Rn.1.

umschreibende Formulierungen wie „*bergründete Verdachtsmomente*“, „*hohe Wahrscheinlichkeit*“ oder „*objektive Anhaltspunkte*“ in Betracht. Dagegen dürfte die Formulierung eines „*einfachen Verdachts*“ aufgrund ihrer Unbestimmtheit und der besonderen Interessenlage regelmäßig nicht ausreichen, § 307 Abs. 1 BGB. Maßgeblich sind die Umstände des Einzelfalls.

Zu beachten ist, dass sich Unternehmen auch im Falle einer internen Meldepflicht nicht sicher sein können, dass die Informationen intern bleiben. Soweit der nationale Gesetzgeber den Beschäftigungsgeber auf Anreize verweist, bleiben diese auch im Falle einer internen Meldepflicht möglich und nötig, § 7 Abs. 3 S. 1 HinSchG. Anreize meint in diesem Kontext ein „*darauf-Hinwirken*“ des Beschäftigungsgebers, dass den Whistleblower dazu veranlassen soll, sich freiwillig für eine interne Meldung zu entscheiden und zugleich von einer externen Meldung abzusehen. Unternehmen sind demzufolge weiterhin aufgefordert, Anreize dafür zu schaffen, dass ein Whistleblower so viel Vertrauen in den internen Meldekanal hegt, dass er aus eigener Entscheidung von einer externen Meldung absieht, § 7 Abs. 3 S. 1 HinSchG. Neben der Schaffung anonymer Meldekanäle kommen insbesondere Maßnahmen zur Erhöhung des Identitätsschutzes in Betracht.

c) Zusätzlicher Identitätsschutz als Anreiz für eine interne Meldung

Die vorstehenden Ausführungen haben gezeigt, dass dem Whistleblower der Zugang zu einer externen Meldestelle nicht versperrt werden kann. Die §§ 7 Abs. 1 S. 1, Abs. 2, 39 HinSchG normieren ein unabdingbares Zugangsrecht zu einer externen Meldestelle für den Whistleblower. Unternehmen können sich daher nicht sicher sein, dass Informationen über Missstände intern bleiben. Dies gilt auch im Falle einer internen Meldepflicht. Unternehmen bleiben daher weiterhin aufgefordert, Anreize dafür zu schaffen, dass ein Whistleblower so viel Vertrauen in die Funktionsfähigkeit und Wirksamkeit des internen Meldekanals hegt, dass er freiwillig von einer externen

Meldung absieht, vgl. § 7 Abs. 3 S. 1 HinSchG. Ein möglicher Anreiz für das Vertrauen des Whistleblowers in die Funktionsfähigkeit der internen Meldestelle bildet der Identitätsschutz. Sowohl die Whistle blowing-RL als auch der nationale Gesetzgeber betonen fortwährend die Bedeutung des Identitätsschutzes im Bereich des Whistleblowings und stellen diesen als dasjenige Kriterium dar, das mitausschlaggebend für eine interne Meldung sein kann.[698]

Für Rechtsunsicherheit sorgt in diesem Zusammenhang das Spannungsverhältnis zwischen Identitätsschutz und datenschutzrechtlichen Betroffenenrechten der von der Meldung betroffenen Personen.[699] Datenschutzrechtliche Informationspflichten (Art. 14 DS-GVO) und Auskunftsrechte (Art. 15 DS-GVO) können dazu führen, dass die von der Datenverarbeitung betroffene Person Kenntnis von der Identität des Hinweisgebers erhält.[700] Damit geht die Gefahr einer nachhaltigen Störung des Betriebsfriedens einher, insbesondere wenn die von der Meldung betroffene Person als (Mit-) Täter einer Straftat bzw. Ordnungswidrigkeit und nicht bloß als Zeuge im Kontext eines möglichen betrieblichen Vorfalles benannt worden ist und der Whistleblower ein Kollege der von der Meldung betroffenen Person ist. Es ist daher richtig, dass der nationale Gesetzgeber den Identitätsschutz als ein für die interne Meldung ausschlaggebendes Kriterium nennt. Diesbezüglich kann der Identitätsschutz auch als Ausprägung des informationellen Selbstbestimmungsrechts des Hinweisgebers verstanden werden. Schließlich entscheidet der Hinweisgeber, unter welchen Voraussetzungen er ein Hinweisgebersystem nutzt und Informationen meldet, die gegebenenfalls Rückschlüsse auf seine Identität ermöglichen.

Die folgende Darstellung wird zunächst die Reichweite des gesetzlichen Identitätsschutzes untersuchen und sich daran anschließend der

---

698 Etwa: BT-Drs. 20/3442, S. 33, 99.

699 *Stille*, in: Thüsing, HinSchG, § 8 Rn.27 m. w. N.

700 BT-Drs. 20/3442, S. 74; *Dzida*/*Seibt*, NZA 2023, 657, 665; *Paal*/*Nikol,* CB 2022, 466, 469.

Frage widmen, ob und inwieweit dieser zu Gunsten des Whistleblowers durch den Beschäftigungsgeber erhöht werden kann. In Betracht kommen beispielsweise ein Verzicht auf die Betroffenenrechte, die Einschaltung einer externen Ombudsperson sowie der Abschluss einer Betriebsvereinbarung.[701]

aa) Identitätsschutz nach den Vorgaben des HinSchG

Das HinSchG normiert den Identitätsschutz in den §§ 8, 9 HinSchG, die dem Abschnitt 2 des HinSchG unterfallen, der wiederum die Arbeitsweise der internen Meldestelle regelt. Die Vorgaben des Identitätsschutzes in §§ 8, 9 HinSchG richten sich daher zuvörderst an diejenigen, die für die eingehenden Meldungen zuständig sind und diese im Sinne des HinSchG bearbeiten. Nach § 8 Abs. 1 S. 1 Nr. 1 HinSchG besteht der Identitätsschutz, wenn die gemeldeten Informationen Verstöße betreffen, die in den Anwendungsbereich des HinSchG fallen oder der Whistleblower zum Zeitpunkt der beabsichtigten Meldung hinreichenden Grund zu der Annahme hatte, dass dies der Fall sei. Das Vertraulichkeitsgebot des § 8 Abs. 1 S. 1 Nr. 1 HinSchG greift auch in den Fällen, in denen der Hinweisgeber Informationen meldet, die öffentlich verfügbar sind.

Die einschränkende Auslegung des § 33 Abs. 1 Nr. 1 HinSchG, wonach laut Gesetzesbegründung kein Identitätsschutz besteht, soweit Informationen gemeldet werden, deren Inhalt bereits in vollem Umfang öffentlich verfügbar ist, ist nicht auf § 8 Abs. 1 S. 1 Nr. 1, Abs. 2 HinSchG übertragbar.[702] Eine solche Lesart stünde dem Willen des (Unions-) Gesetzgebers entgegen, den Identitätsschutz so umfassend wie nur möglich zu gewähren.[703] Dagegen sind Whistleblower, die Informationen über privates Fehlverhalten melden, von denen sie zwar im beruflichen Kontext erfahren haben, das jedoch ohne

[701] Vgl. *Mohn*, NZA 2022, 1159, 1161, 1164.
[702] BT-Drs. 20/5992, S. 78; Erwägungsgrund 43 der Whistleblowing-RL.
[703] BT-Drs. 20/5992, S. 58; Art. 16 Abs. 1 Whistleblowing-RL.

weiteren Bezug zur beruflichen Tätigkeit steht, nicht von § 8 Abs. 1 S. 1 Nr. 1 HinSchG geschützt, vgl. § 3 Abs. 2 HinSchG.[704]

Ob eine Meldung hinreichend begründete Verdachtsmomente über Verstöße enthält, entscheiden die Umstände des jeweiligen Einzelfalls. Maßgeblich ist, ob der Hinweisgeber zum Zeitpunkt der beabsichtigten Meldung (sog. „*ex-ante*"-Sicht) hinreichenden Grund zu der Annahme eines Verstoßes hatte, weil z. B. objektive Anhaltspunkte dafür bestanden.[705] In diesem Kontext darf eine gewisse Aufklärung durch den Hinweisgeber erwartet werden.[706] In der Gesetzesbegründung zum HinSchG heißt es dementsprechend, dass eine Meldung jedenfalls nicht „*leichtfertig*" erfolgen dürfe.[707] Allerdings heißt es auch wiederum einschränkend, dass es einem Whistleblower schon dann unzumutbar sei, sich zu bemühen, sofern er fürchte, dadurch entdeckt zu werden. Ob der Whistleblower seiner Validierungspflicht hinreichend nachgekommen ist, entscheiden die Umstände des jeweiligen Einzelfalls.

Erfolgt eine interne Meldung in dem Wissen, dass die gemeldeten Informationen nicht in den Anwendungsbereich des HinSchG fallen bzw. hatte der Hinweisgeber zum Zeitpunkt der Meldung keinen hinreichenden Grund zu der Annahme, dass der Anwendungsbereich des HinSchG eröffnet ist, regelt § 8 Abs. 2 HinSchG, dass der Identitätsschutz gleichwohl greift. Die Formulierung des § 8 Abs. 2 HinSchG, wonach es für den Identitätsschutz gerade nicht darauf ankommt, ob die Meldestelle für die eingehende Meldung zuständig ist, zeigt, dass der Gesetzgeber den Identitätsschutz unabhängig von der Gutgläubigkeit des Hinweisgebers in Bezug auf die Eröffnung des Anwendungs-

---

704 Vgl. BT-Drs. 20/5992, S. 39. Der Hinweisgeber ist darauf vor seiner Meldung hinzuweisen, Art. 13 DS-GVO. Gleiches gilt für die Ausnahmen des § 9 HinSchG.

705 BT-Drs. 20/5992, S. 76, 82, mit dem Hinweis, dass an die Anhaltspunkte keine überhöhten Anforderungen zu stellen sind.

706 *Thüsing,* Stellungnahme zum HinSchG-E, S. 3.

707 BT-Drs. 20/5992, S. 78.

bereichs des HinSchG regeln wollte. Andernfalls hätte der Gesetzgeber auf die Regelung des § 8 Abs. 2 HinSchG verzichten können, so wie er es z. B. im Rahmen des § 33 HinSchG in Bezug auf die Schutzmaßnahmen im 4. Abschnitts des HinSchG getan hat. Für diese Lesart spricht auch, dass der Gesetzgeber dem Identitätsschutz einen besonders hohen Stellenwert beimisst.[708] In der Gesetzesbegründung zum HinSchG heißt es: „*Daher ist (...) die Identität der hinweisgebenden Person im Regelfall und so weitgehend wie möglich vor einem Bekanntwerden zu schützen.*“[709] Für das Bestehen des Identitätsschutzes nach § 8 Abs. 1 S. 1 Nr. 1, Abs. 2 HinSchG kommt es daher nicht darauf an, ob der Hinweisgeber hinreichenden Grund zu der Annahme hatte, dass die von ihm gemeldeten Informationen in den Anwendungsbereich des HinSchG fallen.

Der Identitätsschutz besteht unabhängig von der Motivation des Whistleblowers; maßgeblich ist jedoch, dass die Meldung im öffentlichen Interesse liegt.[710] Der Whistleblower geht seines Identitätsschutzes nach § 8 Abs. 1 S. 1 Nr. 1, Abs. 2 HinSchG nicht dadurch verlustig, dass er einen anonymen Meldekanal nutzt.[711] Zu beachten ist, dass der Identitätsschutz auch in Fällen einer anonymen Meldung relevant werden kann, sobald die Meldung Informationen enthält, aus denen die Identität des Hinweisgebers ableitbar ist.[712] Sollte der Arbeitgeber neben einem anonymen Meldekanal auch einen nicht-anonymen Meldekanal vorhalten, ist ein Hinweisgeber, der sich für die Nutzung des nicht-anonymen Meldekanals entscheidet, nicht weniger schutzwürdig als ein Hinweisgeber, der den anonymen Meldekanal nutzt. Das HinSchG normiert insofern keine Pflicht zur vorrangigen Nutzung eines anonymen Meldekanals.

---

708 BT-Drs. 20/5992, S. 58; Art. 16 Abs. 1 Whistleblowing-RL.

709 BT-Drs. 20/5992, S. 58.

710 BT-Drs. 20/5992, S. 31; Erwägungsgrund 32 Whistleblowing-RL. Siehe auch: Kapitel C) I. 1. a).

711 Vgl. BT-Drs. 20/5992, S. 34. Nach § 16 Abs. 1 HinSchG besteht keine Pflicht des Beschäftigungsgebers anonyme Meldekanäle zu ermöglichen.

712 BT-Drs. 20/5992, S. 34.

Darüber hinaus greift der Identitätsschutz des Whistleblowers nach § 8 Abs. 1 S. 1 Nr. 1, Abs. 2 HinSchG unabhängig davon, ob die Einrichtung der internen Meldestelle freiwillig oder in Erfüllung einer gesetzlichen Pflicht erfolgt ist.[713] Der Wortlaut des § 8 Abs. 1 S. 1 Nr. 1, Abs. 2 HinSchG differenziert nicht danach, auf welcher Grundlage die interne Meldestelle eingerichtet worden ist. Hält der Arbeitgeber eine interne Meldestelle vor und liegen die Voraussetzungen des § 8 Abs. 1 S. 1 Nr. 1, Abs. 2 HinSchG vor, besteht Identitätsschutz, sofern keine Ausnahme nach § 9 HinSchG greift.

Demgegenüber ist die Identität des Hinweisgebers nach § 9 Abs. 1 HinSchG nicht geschützt, wenn der Hinweisgeber vorsätzlich oder grob fahrlässig unrichtige Informationen über Verstöße meldet. Hintergrund ist, dass die von der Meldung betroffene Person in diesen Fällen ein berechtigtes Interesse an der Kenntnis der Identität des Hinweisgebers hat, um z. B. Schadensersatzansprüche geltend zu machen oder Strafanzeige zu erstatten.[714] Die Vorschrift des § 9 Abs. 1 HinSchG korrespondiert mit der Regelung des § 33 Abs. 1 Nr. 2 HinSchG. Den Hinweisgeber trifft daher keinen Vorwurf der groben Fahrlässigkeit, sofern er zum Zeitpunkt der Meldung hinreichenden Grund zu der Annahme hatte, dass die von ihm gemeldeten Informationen der Wahrheit entsprechen, vgl. § 33 Abs. 1 Nr. 2 HinSchG. Ob die Ausnahme nach § 9 Abs. 1 HinSchG greift, kann demzufolge nur im Rahmen einer Gesamtwürdigung anhand aller maßgebenden Umstände des jeweiligen Einzelfalls entschieden werden. Maßgeblich ist, ob ein objektiver Dritter von der Wahrheit der Information zum

---

[713] Nach § 12 Abs. 1 HinSchG müssen Beschäftigungsgeber ab in der Regel 50 Beschäftigten eine interne Meldestelle einrichten und betreiben, über die Whistleblower Verstöße über Informationen melden können, die dem sachlichen Anwendungsbereich des § 2 HinSchG unterfallen. Im Übrigen kann eine Pflicht zur Einrichtung einer Meldestelle sektorspezifisch (§ 12 Abs. 3 HinSchG) oder in Erfüllung des gesellschaftsrechtlichen Pflichtenprogramms erfolgen, vgl. § 93 Abs. 1 S. 1 AktG, § 43 Abs. 1 GmbHG.

[714] BT-Drs. 20/5992, S. 59.

Zeitpunkt der Meldung (sog. „*ex-ante Sicht*“) ausgegangen wäre.[715] Widersprechen sich die gemeldeten Informationen z. B. in einer Weise, dass es einem objektiven Dritten in der Gestalt des Hinweisgebers zum Zeitpunkt der Meldung sofort hätte einleuchten müssen, dass die Informationen falsch sind, liegt es nahe, dem Whistleblower den Identitätsschutz über § 9 Abs. 1 HinSchG zu versagen.

In der Praxis dürfte die Ausnahme des § 9 Abs. 1 HinSchG nur in eng begrenzten Ausnahmekonstellationen eine Rolle spielen. Zwar heißt es in der Gesetzesbegründung zum HinSchG, dass Meldungen nicht „*leichtfertig ohne Bemühen um eine Verifizierung erfolgen*“ dürfen.[716] Allerdings sei es dem Hinweisgeber schon dann unzumutbar, einem Verdacht weiter nachzugehen, sobald dieser fürchtet, dabei entdeckt zu werden. Der Gesetzgeber weist zusätzlich darauf hin, dass an den Whistleblower in diesem Zusammenhang keine überhöhten Anforderungen zu stellen sind.[717] Hinzu kommt, dass die Regelung des § 9 Abs. 1 HinSchG einer einschränkenden Auslegung bedarf.[718] Dies hat zur Konsequenz, dass nach dem Sinn und Zweck des Vertraulichkeitsgebots nicht jede vorsätzliche bzw. grob fahrlässige Falschinformation zum Ausschluss des Vertraulichkeitsgebots führen kann. Vielmehr ist § 9 Abs. 1 HinSchG nach seinem Schutzzweck so zu verstehen, dass nur solche Falschinformationen zum Ausschluss des Vertraulichkeitsgebots führen können, soweit diese geeignet sind, Schadensersatzansprüche der von der Meldung betroffenen Person auszulösen oder die gemeldeten Falschinformationen von strafrechtlicher Relevanz für diese sind. Dafür spricht, dass der Identitätsschutz nur insoweit entfallen kann, als dies zum Schutz der berechtigten Interessen der von der Meldung betroffenen Person erforderlich ist.

---

715 BT-Drs. 20/5992, S. 77.
716 EGMR, Urteil v. 16.02.2021 - 23922/19, NJW 2021, 2343, Rn.75; BT-Drs. 20/5992, S. 78.
717 BT-Drs. 20/5992, S. 78.
718 BT-Drs. 20/5992, S. 78.

Gestützt wird dieses Verständnis durch die grundlegende Bedeutung des Identitätsschutzes für einen wirksamen Hinweisgeberschutz.[719]

Im Übrigen betreffen die in § 9 Abs. 2 und 3 HinSchG geregelten Ausnahmen Fälle, in denen es nicht um eine Weitergabe der Identität des Hinweisgebers an die von der Meldung betroffene Person geht. § 9 Abs. 2 HinSchG regelt ausschließlich Ausnahmen vom Vertraulichkeitsgebot in Straf- und Ordnungswidrigkeitenverfahren, in denen eine Weitergabe der Identität des Hinweisgebers an die dort genannten öffentlichen Stellen erfolgen darf. Die Ausnahme des § 9 Abs. 3 S. 1 HinSchG regelt den Fall, dass die Weitergabe der Identität des Hinweisgebers für Folgemaßnahmen erforderlich ist, vgl. §§ 3 Abs. 7, 13 Abs. 1, 17 Abs. 1 Nr. 6, 18 HinSchG. Beide Fallkonstellationen gehören nicht zum Untersuchungsgegenstand der vorliegenden Arbeit und bleiben daher außen vor.

bb) Identitätsschutz im Rahmen der DS-GVO

Eine Meldung fällt in den Anwendungsbereich der DS-GVO, soweit die jeweilige Meldung personenbezogene Daten enthält.[720] Dies dürfte

---

[719] BT-Drs. 20/5992, S. 58; Art. 16 Abs. 1 Whistleblowing-RL; BRAK, Stellungnahme zum HinSchG-E, S. 5.

[720] Legitimationsgrundlage für die Verarbeitung personenbezogenen Daten durch die Meldestelle bildet Art. 6 Abs. 1 S. 1 lit. c) DS-GVO i. V. m. § 10 HinSchG, sofern eine Pflicht zur Einrichtung besteht; *Weidmann,* DB 2019, 2393 f. und *Nikol*, CB 2023, 351, 352. Das Schrifttum diskutiert darüber hinaus die Frage, ob § 10 HinSchG eine „*spezifischere Vorschrift*" im Sinne des Art. 88 Abs. 1 DS-GVO sei, vgl. grundlegend dazu: *Musiol*, Hinweisgeberschutz und Datenschutz, S. 182 f., 250, 336 m. w. N. Nach der Entscheidung des EuGH zu § 23 HDSIG ist nach hiesiger Auffassung davon auszugehen, dass § 10 HinSchG keine spezifischere Vorschrift nach Art. 88 Abs. 1 DS-GVO sein kann, vgl. EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.85. § 10 HinSchG wiederholt lediglich die Legitimationsgrundlage des Art. 6 Abs. 1 S. 1 lit. b) DS-GVO und ist folgerichtig - mangels eigenen Regelungsgegenstands - nicht „*spezifischer*". In die gleiche Richtung zu § 23 Abs. 1 S. 1 BDSG: *Thüsing/Peisker*, NZA 2023, 213, 214 f. und *Wünschelbaum*, NZA 2023, 542 545.

im Bereich des Whistleblowings regelmäßig der Fall sein. Auch wenn der Hinweisgeber einen anonymen Meldekanal nutzt und die gemeldeten Informationen keine Rückschlüsse auf dessen Identität zulassen, wird die Meldung in aller Regel personenbezogene Daten insbesondere derjenigen Personen enthalten, die Gegenstand der Meldung bzw. von ihr Betroffene sind.

Der Identitätsschutz des Whistleblowers ist im Rahmen der datenschutzrechtlichen Betroffenenrechte über Ausnahmetatbestände und Beschränkungen berücksichtigungsfähig. Dies bedeutet, dass die datenschutzrechtlichen Betroffenenrechte im Grundsatz von einer Informationspflicht oder Auskunftspflicht des datenschutzrechtlich Verantwortlichen hinsichtlich der Identität des Whistleblowers ausgehen, diese aber im Einzelfall beschränkt sein können. Für die Informationspflicht folgt dies aus Art. 14 Abs. 2 lit. f) DS-GVO. Die Identität des Whistleblowers ist Teil der „*Quelle*“ der Daten.[721] Daneben erstreckt sich das datenschutzrechtliche Auskunftsrecht in Art. 15 Abs. 1 Hs. 2 Var. 2 lit. g) DS-GVO auf die „*Herkunft*“ der

[721] Telos dieser Informationspflicht ist, den Ursprung der Datenverarbeitung nachvollziehen zu können, vgl. *Kamlah*, in: Plath, DS-GVO, Art. 18 Rn.13; *Bäcker*, in: Kühling/Buchner, DS-GVO, Art. 14 Rn.19. Während Art. 13 DS-GVO die Informationspflichten des Arbeitgebers in Fällen der Direkterhebung regelt, erfasst Art. 14 DS-GVO den Fall, dass die Daten in sonstiger Weise, also ohne Mitwirkung oder Wissen der von der Datenverarbeitung betroffenen Person verarbeitet werden (sog. Dritterhebung). Soweit sich die Meldung eines Hinweisgebers auf andere Personen bezieht, handelt es sich demgemäß um eine Dritterhebung im Sinne des Art. 14 DS-GVO, vgl. *Mohn*, NZA 2022, 1159, 1160; *Franzen*, in: EuArbRK, Art. 14 DS-GVO Rn.1, vgl. auch BGH, Urteil v. 22.02.2022 - VI ZR 14/21, ZD 2022, 326.

Daten, zu der die Identität des Whistleblowers zählt.[722] Die Begriffe Herkunft und Quelle sind insofern deckungsgleich.[723]

Voraussetzung für eine Informationspflicht bzw. ein Auskunftsrecht in Bezug auf die Identität des Whistleblowers ist, dass dem datenschutzrechtlich Verantwortlichen dessen Identität bekannt ist, wobei sich die Identität auch aus Rückschlüssen einer anonymen Meldung ergeben kann.[724] Der Identitätsschutz ist sodann auf Ebene der Ausnahme- bzw. Beschränkungstatbestände zu berücksichtigen. Sowohl Verstöße gegen die Betroffenenrechte der DS-GVO (Art. 83 Abs. 5 lit. b) DS-GVO), als auch Verstöße gegen den Identitätsschutz (vgl. § 40 Abs. 3 und Abs. 4 HinSchG) sind bußgeldbewehrt. Arbeitgeber befinden sich damit in einem Spannungsverhältnis, das es im Folgenden aufzulösen gilt.

(1) Ausnahmen von der Informationspflicht

Nach Art. 14 Abs. 1 lit. c) und lit. d) DS-GVO teilt der Arbeitgeber als die für die Datenverarbeitung verantwortliche Stelle der von der Meldung betroffenen Person die Zwecke, für die die personenbezogenen Daten verarbeitet werden und die Rechtsgrundlage für die Verarbeitung sowie die Kategorien der personenbezogenen Daten mit. Zusätzlich informiert der Arbeitgeber die von der Meldung betroffene Person

---

[722] *Jacksch*/*Hoffmann*, ZD 2022, 605, 607 ff; vgl. auch: *Franck*, in: Gola/Heckmann, DS-GVO, Art. 13 Rn.4; *Ingold*, in: Sydow/Marsch, DS-GVO, Art. 13 Rn.7 m. w. N. Es kommt nicht darauf an, ob der datenschutzrechtlich Verantwortliche die Daten selbst beschafft oder ein Whistleblower diese eigeninitiativ meldet, BGH, Urteil v. 22.02.2022 - VI ZR 14/21, BeckRS 2022, 5496 Rn.13.

[723] Der Blick in die anderen Sprachfassungen der DS-GVO bestätigt, dass dort ebenfalls nicht zwischen Quelle und Herkunft unterschieden wird. Stattdessen heißt es dort einheitlich „*source*“ (englische Sprachfassung) bzw. „*bron*“ (niederländische Sprachfassung), vgl. *Däubler*, in: DWWS, Art. 15 DS-GVO Rn.27; *Dix*, in: NK-DSGVO, Art. 15 Rn.24; *Mohn*, NZA 2022, 1159.

[724] Aus §§ 11, 17 HinSchG folgt eine Speicherpflicht, auch hinsichtlich der Identität des Whistleblowers.

nach Art. 14 Abs. 2 lit. f) Var. 1 DS-GVO darüber, aus welcher Quelle die personenbezogenen Daten stammen. Zur Informationsquelle gehören in diesem Zusammenhang grundsätzlich auch Informationen zum Hinweisgebersystem sowie zur Identität des Hinweisgebers.[725] Ausnahmen von der Informationspflicht enthalten Art. 14 Abs. 5 DS-GVO und Art. 23 Abs. 1 lit. i) DS-GVO i. V. m. §§ 29 Abs. 1 S. 1, 33 BDSG. Zur Bestimmung der Bedeutung des Identitätsschutzes im Rahmen der Informationspflicht kommen insbesondere die Ausnahmetatbestände der Art. 14 Abs. 5 lit. b) und lit. c) DS-GVO sowie Art. 23 Abs. 1 lit. i) DS-GVO i. V. m. § 33 Abs. 1 Nr. 2 lit. a) BDSG in Betracht.[726]

(a) Art. 14 Abs. 5 lit. b) DS-GVO

Nach der verordnungsunmittelbaren Ausnahmeregelung des Art. 14 Abs. 5 lit. b) DS-GVO besteht die Informationspflicht unter anderem nicht, wenn und soweit die Erteilung der Information voraussichtlich die Verwirklichung der Ziele der Datenverarbeitung unmöglich macht oder ernsthaft beeinträchtigt. Dieser Ausnahmetatbestand gilt folgerichtig für die Fälle, in denen die von der Meldung betroffene Person als (Mit-) Täter einer Straftat benannt worden ist und die begründete Annahme besteht, die Kenntnis von der Identität des Whistleblowers werde dazu genutzt, um auf ihn als möglichen Zeugen einzuwirken, seine Meldung zu revidieren. Maßgeblich sind wie so oft die Umstände des jeweiligen Einzelfalls. Dabei kommt es auch darauf an, ob die Kenntnis über die Identität des Whistleblowers den Zweck einer internen Untersuchung gefährden würde, weil Beweismittel

---

[725] BGH, Urteil v. 22.02.2022 - VI ZR 14/21, ZD 2022, 326; *Mohn*, NZA 2022, 1159, 1160. Soweit in einem Hinweisgebersystem allerdings keine Informationen über die Identität des Whistleblowers vorhanden sind, weil der Whistleblower einen anonymen Meldekanal nutzt und die Informationen keine Rückschlüsse auf dessen Identität zulassen, sind diese nicht Gegenstand der Informationspflicht nach Art. 14 Abs. 2 lit. f) DS-GVO.

[726] *Franzen*, in: ErfK-ArbR, § 26 BDSG Rn.26; BT-Drs. 20/5992, S. 59.

drohen, verlustig zu gehen oder die begründete Annahme besteht, die Erhebung weiterer Beweismittel werde gefährdet.[727]

Zu beachten ist, dass Art. 14 Abs. 5 lit. b) S. 2 DS-GVO dahingehend einschränkend auszulegen ist, dass in diesen Fällen eine Information für die Öffentlichkeit nicht bereitzustellen ist.[728] Eine solche Vorgabe würde dem Ausnahmetatbestand als solches zuwiderlaufen, wenn die von der Meldung betroffene Person zwar nicht von dem datenschutzrechtlich Verantwortlichen, dafür aber im Wege einer allgemeinen Veröffentlichung von der Identität des Hinweisgebers erfahren könnte.[729] Gleiches muss dementsprechend auch für die Ausnahmeregelung des Art. 23 Abs. 1 lit. i) DS-GVO in Verbindung mit § 33 Abs. 1 Nr. 2 lit. a) BDSG gelten, die ebenfalls laufende Ermittlungen erfasst.

(b) Art. 14 Abs. 5 lit. c) DS-GVO

Nach Art. 14 Abs. 5 lit. c) DS-GVO besteht die Informationspflicht ferner nicht, soweit die Erlangung der Information durch Rechtsvorschriften der Europäischen Union oder der Mitgliedstaaten, denen der Arbeitgeber unterliegt, ausdrücklich geregelt ist und diese geeignete Maßnahmen zum Schutz der berechtigten Interessen der von der Meldung betroffenen Personen vorsehen.

Fraglich ist, ob die Vorschriften des HinSchG zu den Rechtsvorschriften im Sinne des Art. 14 Abs. 5 lit. c) DS-GVO zählen. Dafür spricht zunächst, dass die Regelungen im HinSchG auch Regelungen zum Schutz der berechtigten Interessen der von der Meldung betroffenen

---

[727] DSK, Orientierungshilfe zu Whistleblowing-Hotlines, S. 10; vgl. auch: *Schmidt-Wudy*, in: BeckOK-DatenschutzR, Art. 14 DS-GVO Rn.99.1; *Altenbach*/*Dierkes*, CCZ 2020, 126, 128; *Fehr*, ZD 2022, 256, 258; *Mohn*, NZA 2022, 1159, 1160.

[728] *Bongers*, in: Kramer, IT-Arbeitsrecht, Kapitel B Rn.794.

[729] *Bongers*, in: Kramer, IT-Arbeitsrecht, Kapitel B Rn.794, 796.

Person enthalten.[730] §§ 8 Abs. 1 S. 2, 16 Abs. 2 HinSchG schützen die von der Meldung betroffene Person vor falschen Verdächtigungen und Verleumdungen, indem der Kreis derjenigen Personen, die Kenntnis über die Identität der von der Meldung betroffenen Person haben, möglichst gering gehalten wird.[731] Kenntnis von der Identität der von der Meldung betroffenen Person erhalten demnach - neben den für die Meldung zuständigen Personen - ausschließlich diejenigen, die diese bei ihrer Arbeit unterstützen, soweit dies für die Unterstützungstätigkeit notwendig ist, sowie diejenigen, die für das Ergreifen von Folgemaßnahmen (§§ 3 Abs. 7, 18 HinSchG) zuständig sind. Die Regelung schützt dabei nicht nur die Identität der von der Meldung betroffenen Personen als solches. Zum Identitätsschutz der von der Meldung betroffenen Personen zählen auch alle anderen Informationen, aus denen die Identität abgeleitet werden kann.[732] Darüber hinaus ist die von der Meldung betroffene Personen vor falschen Verdächtigungen und Verleumdungen im Wege der strafprozessualen Verfahrensrechte geschützt (§ 9 Abs. 4 HinSchG).[733] Ebenfalls zum Schutz vor falschen Verdächtigungen und Verleumdungen der von der Meldung betroffenen Person besteht nach § 9 Abs. 1 HinSchG kein Identitätsschutz des Hinweisgebers, wenn der Hinweisgeber vorsätzlich oder grob fahrlässig unrichtige Informationen über Verstöße meldet. Die Regelung berücksichtigt das berechtigte Interesse der von der Meldung betroffenen Person an der Kenntnis der Identität des Hinweisgebers, um z. B. Schadensersatzansprüche geltend zu machen oder Strafanzeige gegen den Hinweisgeber zu erstatten. Auch dies zeigt, dass das HinSchG die berechtigten Interessen der von der Meldung betroffenen Personen schützt.

---

730 §§ 1 Abs. 2 und Abs. 4, 8 Abs. 1 S. 1 Nr. 2 und Nr. 3, sowie Abs. 1 S. 2, 9 Abs. 1 HinSchG, vgl. *Franzen*, in: ErfK-ArbR, § 26 BDSG Rn.6.

731 BT-Drs. 20/5992, S. 58.

732 BT-Drs. 20/5992, S. 58.

733 § 4 Abs. 4 HinSchG stellt klar, dass die Regelungen des HinSchG die strafprozessualen Verfahrensrechte nicht beschränken.

Zu beachten ist jedoch, dass Art. 14 Abs. 5 lit. d) DS-GVO im Kontext der Einschränkung der datenschutzrechtlichen Informationspflicht auszulegen ist. Es geht im Rahmen einer Rechtsvorschrift im Sinne des Art. 14 Abs. 5 lit. c) DS-GVO daher nicht um den Identitätsschutz der von der Meldung betroffenen Person oder ihren Schutz vor falscher Verdächtigung und Verleumdung, sondern um die Gewährleistung ihrer informationellen Selbstbestimmungsfreiheit, derer Art. 14 Abs. 1 und 2 DS-GVO Ausdruck verschafft. Die Informationspflicht konkretisiert den datenschutzrechtlichen Transparenzgrundsatz (Art. 5 Abs. 1 lit. a) DS-GVO) und verfolgt das Telos, die von einer Datenverarbeitung betroffene Person in Kenntnis über die Datenverarbeitung zu setzen, damit diese die Datenverarbeitung auf Rechtmäßigkeit prüfen und ggf. durchsetzen kann.[734] Soweit Art. 14 Abs. 5 lit. c) DS-GVO auf andere Rechtsvorschriften verweist, die geeignete Maßnahmen zum Schutz der berechtigten Interessen der von der Meldung betroffenen Personen zu treffen haben, sind damit Vorschriften gemeint, die ihrerseits Regelungen enthalten, um sicherzustellen, dass die von der Datenverarbeitung betroffene Person hinreichend Kenntnis über die Datenverarbeitung erlangt, um deren Rechtmäßigkeit zu prüfen und ggf. durchsetzen zu können.

Das HinSchG kennt keine Vorgabe, die dem Beschäftigungsgeber beispielsweise eine im Vergleich zu Art. 14 Abs. 3 DS-GVO zeitlich verzögerte Informationspflicht gegenüber der von der Meldung betroffenen Person auferlegt. Stattdessen gehen die §§ 8, 9 HinSchG pauschal und einseitig zu Lasten der von der Meldung betroffenen Person von einem Vorrang des Identitätsschutzes aus, ohne deren informationelles Selbstbestimmungsrecht im Rahmen einer Interessenabwägung einzubeziehen. Erschwerend kommt hinzu, dass der Beschäftigungsgeber in den Fällen, in denen nach § 9 Abs. 1 HinSchG kein Identitätsschutz besteht, zu der Einschätzung einer grob fahrlässigen oder vorsätzlichen Falschmeldung gelangt sein muss, ehe die von der

[734] Siehe: Kapitel C) I. 1. a).

Meldung betroffene Person auch nur die Möglichkeit hat, diese Einschätzung nachzuvollziehen.

Die vorherigen Ausführungen haben außerdem gezeigt, dass die Annahme einer grob fahrlässigen oder vorsätzlichen Falschmeldung nur sehr selten eintreten wird.[735] Einer von der Datenverarbeitung betroffenen Person ist es nach dem Regelungswerk des HinSchG folgerichtig nicht möglich, sich der Datenverarbeitung ihrer personenbezogenen Daten bewusst zu werden, sollten §§ 8, 9 HinSchG Rechtsvorschriften im Sinne des Art. 14 Abs. 5 lit. c) DS-GVO sein. Aufgrund der fehlenden Berücksichtigung der Interessen der von der Datenverarbeitung betroffenen Personen, sind die Regelungen des HinSchG daher nicht als Rechtsvorschriften im Sinne des Art. 14 Abs. 5 lit. c) DS-GVO zu bewerten.

Dieses Verständnis stimmt mit der Auffassung des Gesetzgebers überein. Der Gesetzgeber verweist in der Gesetzesbegründung zum HinSchG auf die Ausnahmetatbestände des BDSG: „*Die für den Hinweisgeberschutz notwendigen Ausnahmetatbestände sind bereits im Bundesdatenschutzgesetz (BDSG) enthalten*.“[736] Sodann heißt es an anderer Stelle weiter: „*Die notwendigen Ausnahmetatbestände haben indes bereits Eingang in das BDSG gefunden. Über die im Rahmen des § 29 Absatz 1 BDSG geforderte Interessenabwägung lässt sich der erforderliche Gleichlauf zwischen dem Vertraulichkeitsschutz und datenschutzrechtlichen Informationspflichten und Auskunftsrechten herstellen. Nach § 29 Absatz 1 Satz 1 BDSG treffen den datenschutzrechtlich Verantwortlichen keine Informationspflichten, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach geheim gehalten werden müssen.*“[737] Dementsprechend geht auch der nationale Gesetzgeber davon aus, dass der Identitätsschutz im Rahmen der Informationspflicht nicht über Art. 14 Abs. 5 lit. c) DS-GVO

[735] Siehe: Kapitel C) I. 3. c) aa).
[736] BT-Drs. 20/5992, S. 36.
[737] BT-Drs. 20/5992, S. 59.

i. V. m. § 8 HinSchG besteht, sondern dieser aus § 29 Abs. 1 S. 1 BDSG folgt. Demgemäß ist weiter zu prüfen, ob § 29 Abs. 1 S. 1 BDSG den Identitätsschutz des Whistleblowers dergestalt schützt, dass eine Ausnahme von der Informationspflicht besteht.

(c) § 29 Abs. 1 S. 1 BDSG

Um als Ausnahmetatbestand die Informationspflicht in Art. 14 Abs. 1 und Abs. 2 DS-GVO einschränken zu können, braucht es eine Öffnungsklausel.[738] In Betracht kommt zunächst Art. 23 Abs. 1 lit. i) DS-GVO. Bemerkenswert ist, dass § 29 Abs. 1 S. 1 BDSG keine Ausführungen hinsichtlich des Schutzes der von der Datenverarbeitung betroffenen Person bereit hält, obwohl diese nach Art. 23 Abs. 2 lit. g) DS-GVO notwendige Voraussetzung für eine Beschränkung der Informationspflicht sind. § 29 Abs. 1 S. 1 BDSG kann daher nicht auf die Öffnungsklausel des Art. 23 Abs. 1 lit. i) DS-GVO zurückgeführt werden.[739] § 29 Abs. 1 S. 1 BDSG kann auch nicht auf die Öffnungsklausel in Art. 88 Abs. 1 DS-GVO gestützt werden.[740] § 29 Abs. 1 S. 1 BDSG ist schon keine spezifischere Vorschrift des Beschäftigungskontexts, sondern regelt dem Wortlaut nach eine allgemein gehaltene, Art. 14 Abs. 5 DS-GVO ergänzende Ausnahme von der Informationspflicht, ohne einen konkreten Bezug zum Beschäftigungskontext herzustellen. Auch der nationale Gesetzgeber geht davon aus, dass § 29 Abs. 1 S. 1 BDSG keine spezifischere Vorschrift im Beschäftigungskontext ist: Die Gesetzesbegründung zu § 29 Abs. 1 S. 1 BDSG bezieht sich ausdrücklich auf die Öffnungsklausel des Art. 23 Abs. 1 lit. i) DS.GVO.[741]

---

738 *Bäcker*, in: Kühling/Buchner, Einführung Rn.98 ff.; *Ehmann*, in: Ehmann/Selmayr, Einführung Rn.81 ff.

739 A. A.: *Lang,* ZD 2024, 17, 20.

740 Vgl. EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.85 zu § 23 HDSIG. In die gleiche Richtung zu § 23 Abs. 1 S. 1 BDSG: *Thüsing*/*Peisker,* NZA 2023, 213, 214 f.; *Wünschelbaum,* NZA 2023, 542, 545.

741 BT-Drs. 18/11325, S. 100.

Selbst bei unterstelltem Beschäftigungskontext genügt die Regelung in § 29 Abs. 1 S. 1 BDSG den Anforderungen der Öffnungsklausel nicht. Dafür gilt es zunächst festzustellen, dass Art. 88 Abs. 1 DS-GVO nicht auf spezifischere Vorschriften begrenzt ist, deren Regelungsgegenstand eine Rechtsgrundlage für eine Datenverarbeitung ist.[742] Dafür spricht, dass auch die Erfüllung der Informationspflicht eine Datenverarbeitung (Art. 4 Nr. 2 DS-GVO) ist.[743] Geht es beispielsweise darum, die Identität des Whistleblowers offenzulegen, handelt es sich um eine Weitergabe eines personenbezogenen Datums, die folgerichtig eine Datenverarbeitung darstellt.[744] Hinzu kommt, dass spezifischere Vorschriften die einer jeden Datenverarbeitung immanenten Grundsätze der Datenverarbeitung (Art. 5 DS-GVO) stets mit umfassen.[745] Der Grundsatz der Datentransparenz wohnt jeder Datenverarbeitung inne, vgl. Art. 5 Abs. 1 lit. a) DS-GVO. Die Betroffenenrechte sind damit „*Bestandteil einer transparenten Verarbeitung*“.[746] Dementsprechend können spezifischere Vorschriften im Sinne des Art. 88 Abs. 1 DS-GVO auch Transparenzvorgaben hinsichtlich der Betroffenenrechte sein.

Allerdings können spezifischere Vorschriften nur solche sein, die die Vorgaben des Art. 88 Abs. 2 DS-GVO wahren. Dies hat der EuGH

---

742 A. A.: *Lembke*, in: HWK, Art. 88 DS-GVO Rn.6; *Lembke*, NJW 2020, 1841, 1845 f.; *Schulte*/*Welge*, NZA 2019, 1110, 1115.

743 BGH, Urteil v. 22.02.2022 - VI ZR 14/21, BeckRS 2022, 5496 Rn.19; OLG Köln, Urteil v. 14.07.2022 - 15 U 137/21, GRUR-RS 2022, 17897 Rn.14; *Bienemann*, in: Sydow/Marsch, DS-GVO, Art. 15 Rn.42.

744 In Bezug auf die Datenauskunft nach Art. 15 DS-GVO: BGH, Urteil v. 22.02.2022 - VI ZR 14/21, BeckRS 2022, 5496 Rn.19; OLG Köln, Urteil v. 14.07.2022 - 15 U 137/21, GRUR-RS 2022, 17897 Rn.14; *Bienemann,* in: Sydow/Marsch, DS-GVO, Art. 15 Rn.42; *Arens*, NJW 2021, 3417, 3418; *Paal*/*Nikol*, CB 2022, 466, 469; a. A.: LG Bonn, Urteil v. 01.07.2021 - 16 O 128/20 Rn.35.

745 *Peisker* zu Art. 15 DS-GVO: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 152.

746 *Peisker* zu Art. 15 DS-GVO: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 152.

jüngst bestätigt.[747] Art. 88 Abs. 1 DS-GVO ist daher in Zusammenhang mit Art. 88 Abs. 2 DS-GVO zu verstehen. Laut EuGH sei Art. 88 Abs. 1 DS-GVO dahingehend auszulegen, dass eine nationale Rechtsvorschrift keine „*spezifischere Vorschrift*" sein könne, wenn sie nicht die Vorgaben des Art. 88 Abs. 2 DS-GVO erfülle.[748] Nötig sei, dass die spezifischere Vorschrift geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung enthalte.[749] Gemeint sind Vorgaben, die die Rechte der von der Datenverarbeitung betroffenen Person achtet und sicherstellt, dass der Grundsatz der Datentransparenz (Art. 5 Abs. 1 lit. a) DS-GVO) hinreichend besteht.[750]

Demzufolge darf eine spezifischere Vorschrift nach Art. 88 Abs. 1 DS-GVO nicht die allgemeinen Grundsätze einer Datenverarbeitung unterlaufen (Art. 5 und Art. 6 DS-GVO).[751] Die Grundsätze bilden

---

747 EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.85.

748 EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.85.

749 *Franzen*, NZA 2020, 1593 dort: Fn.33; *Thüsing*/*Traut*, in: SJTK, Art. 88 DS-GVO Rn.35; *Wybitul*, ZD 2016, 203, 207.

750 *Thüsing*/*Peisker* fragen in diesem Zusammenhang zu Recht in Bezug auf Betriebsvereinbarungen, ob stets explizite Vorgaben nötig seien, *Thüsing*/*Peisker*, NZA 2023, 213, 214. Nach hiesiger Auffassung sind explizite Vorgaben zumindest hinsichtlich der Datentransparenz nötig, soweit die spezifischere Vorschrift eine Beschränkung der Betroffenenrechte, respektive des Transparenzgrundsatzes darstellt, Art. 5 Abs. 1 lit. a) DS-GVO, Art. 12 ff. DS-GVO. Im Übrigen stellen die ohnehin zu beachtenden Betroffenenrechte in Art. 12 ff. DS-GVO den Grundsatz der Datentransparenz hinreichend sicher. Diese repetitiv zu wiederholen, erscheint nicht sachgerecht. Sinnvoll, wenn auch nicht zwingend, scheint dagegen eine Bezugnahme in Form eines Hinweises, z. B. im Rahmen der Gesetzesbegründung, respektive der Betriebsvereinbarung.

751 Vgl. EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.85. Damit hat der EuGH Frage beantwortet, inwieweit „*spezifischere Vorschriften*" nach Art. 88 Abs. 1 DS-GVO das Schutzniveau der DS-GVO absenken dürfen: Spezifischere Vorschriften müssen demnach mindestens die Grundsätze der Art. 5, Art. 6 DS-GVO wahren und die Vorgaben des Art. 88 Abs. 2

einen Mindestschutz für die Verarbeitung personenbezogener Daten im Beschäftigungskontext, wobei der nationale Gesetzgeber in ihrer konkreten Ausgestaltung frei bleibt. Dieses Verständnis überzeugt, weil mittels Art. 88 Abs. 2 DS-GVO ein einheitliches Datenschutzniveau innerhalb der Europäischen Union gewährleistet ist, ohne dass den Mitgliedstaaten der gebotene Handlungsspielraum genommen wird, den es insbesondere im Beschäftigungskontext braucht.[752]

DS-GVO enthalten. So auch: *Thüsing*/*Granetzny*, in: Compliance, § 4 Rn.15, die darauf hinweisen, dass die Grundprinzipien der DS-GVO nicht unterlaufen werden dürfen. Dazu auch: *Wünschelbaum,* BB 2019, 2102, 2106. Die Frage, ob und inwieweit Abweichungen vom Schutzniveau der DS-GVO über Art. 88 Abs. 1, Abs. 2 DS-GVO möglich sind, war bislang hoch umstritten. Einige Stimmen gingen davon aus, dass Verschärfungen der DS-GVO allgemein möglich seien, vgl. exemplarisch: *Pauly*, in: Paal/Pauly, Art. 88 DS-GVO Rn.4; *Tiedemann*, in: Sydow/Marsch, Art. 88 DS-GVO Rn.3; *Düwell*/*Brink*, NZA 2016, 665, 666; *Jerchel*/*Schubert*, DuD 2016, 782, 783; *Körner*, NZA 2016, 1383 ff; *Klösel*/*Mahnhold*, NZA 2017, 1428, 1430; *Kort*, ZD 2016, 555, 557; *Wurzberger*, ZD 2017, 258, 263. Andere Stimmen sprachen sich gegen Abweichungen nach unten aus, da der DS-GVO eine vollharmonisierende Wirkung zukäme, vgl. exemplarisch: *Däubler*, in: DWWS, Art. 88 DS-GVO Rn.13ff; *Franzen*, in: EuArbRK, Art. 88 DS-GVO Rn.10; *Maschamnn*, in: Kühling/Buchner, Art. 88 DS-GVO Rn.30ff.; *Pötters*, in: Gola/Heckmann, Art. 88 DS-GVO Rn.23 ff.; *Dzida*/*Grau*, DB 2018, 189, 193; *Franck*, ZD 2017, 509, 511; *Wybitul*, ZD 2016, 203, 208 ff. Eine dritte Argumentationslinie hielt eine Abweichung nach unten für dem Grunde nach möglich, schränkte diese jedoch dahingehen ein, dass der durch Art. 88 Abs. 2 DS-GVO vermittelte Mindestschutz gewahrt bleiben müsse; vgl. exemplarisch: *Thüsing*/*Granetzny*, in: Compliance, § 4 Rn.15; *Wünschelbaum,* BB 2019, 2102, 2106; *Forst*, in: Auernhammer, Art. 88 DS-GVO Rn.17; *Riesenhuber*, in: BeckOK-DatenschutzR, Art. 88 DS-GVO Rn.66ff.; *Thüsing*/*Traut*, in: SJTK, Art. 88 DS-GVO Rn.7 ff.; *Zöll*, in: Taeger/Gabel, Art. 88 DS-GVO Rn.21; *Benkert*, NJW-Spezial 2018, 562. Letzterer Auffassung hat sich nunmehr der EuGH angeschlossen. Ein differenzierter Überblick zum bisherigen Streitstand findet sich u. a. bei: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 153 f. und *Wünschelbaum*, Kollektivautonomer Datenschutz, S. 44 ff.

[752] EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.40 - mit Anm. *Meinecke*; vgl. EuGH, NZA 2022, 1183 Rn.25.

Vor diesem Hintergrund sind eigenständige Vorschriften in Bezug auf den Identitätsschutz des Whistleblowers möglich, soweit sie die Grundsätze der Datenverarbeitung in Art. 5 und Art. 6 DS-GVO nicht unterlaufen. Erwägungsgrund 11 der DS-GVO formuliert in diesem Zusammenhang übereinstimmend, dass ein unionsweiter wirksamer Schutz eine präzise Festlegung der Rechte der betroffenen Person erfordert. Dem Telos der Datentransparenz entsprechend kommt es also darauf an, ob die spezifischere Vorschrift Maßnahmen vorsieht, die sicherstellen, dass die von der Meldung betroffene Person über die Datenverarbeitung hinreichend Kenntnis erlangt, um die Rechtmäßigkeit der Datenverarbeitung zu überprüfen und diese ggf. durchzusetzen. Eine Orientierung, wie das in Bezug auf eine mögliche Beschränkung der Betroffenenrechte rechtssicher gelingen kann, bieten die Mindestvorgaben in Art. 23 Abs. 2 DS-GVO.[753] Nötig dürfte insbesondere eine Bezugnahme auf diejenigen Betroffenenrechte sein, die durch die Vorschrift eine Beschränkung erfahren.[754]

Da § 29 Abs. 1 S. 1 BDSG jedoch keinerlei Vorgaben dazu enthält, wie den mit der bezweckten Ausnahme der Informationspflicht einhergehenden Risiken für das informationelle Selbstbestimmungsrecht

---

[753] Vor diesem Hintergrund ist es nicht fernliegend, Art. 88 Abs. 1 DS-GVO als lex specialis zu Art. 23 Abs. 1 DS-GVO anzusehen. Diese Frage kann jedoch dahinstehen, da beide Öffnungsklauseln sicherstellen, dass die datenschutzrechtlichen Grundsätze in Art. 5 und Art. 6 DS-GVO im Sinne eines Mindestschutzes nicht unterlaufen werden dürfen. Richtig ist, dass Art. 23 DS-GVO eine Beschränkung der Betroffenenrechte in den Blick nimmt, während Art. 88 DS-GVO Beschränkungen im Beschäftigungskontext regelt, zu denen auch Transparenzvorgaben zählen können. Grundsätzlich ist daher von einem Nebeneinander der Öffnungsklauseln auszugehen. So auch: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 152; *Bienemann*, in: Sydow/Marsch, DS-GVO, Art. 15 Rn.86; *Franzen*, in: EuArRK, Art. 15 DS-GVO Rn.8; *Riesenhuber*, in: BeckOK-DatenschutzR, Art. 88 DS-GVO Rn.98; *Stollhoff*, in: Auernhammer, DS-GVO, Art. 15 Rn.50; *Thüsing*/*Traut*, in: SJTK, Art. 88 DS-GVO Rn.34 ff.; *Franzen*, NZA 2020, 1593 ff.; *Schantz*, NJW 2016, 1841, 1842; *Wünschelbaum*, BB 2019, 2102 ff. und LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, 242 Rn.172.

[754] Vgl. *Sörup,* ArbRAktuell 2016, 207, 208 f.; *Wybitul,* ZD 2016, 203, 207.

der von der Datenverarbeitung betroffenen Person begegnet wird, genügt § 29 Abs. 1 S. 1 BDSG den Vorgaben in Art. 88 Abs. 1 und Abs. 2 DS-GVO nicht und kann folgerichtig nicht auf die Öffnungsklausel gestützt werden.[755] § 29 Abs. 1 S. 1 BDSG muss demgemäß - mangels Öffnungsklausel - unangewendet bleiben. Der nationale Gesetzgeber hat es sich mit seinem pauschalen Hinweis auf § 29 Abs. 1 S. 1 BDSG zu leicht gemacht.[756] Der Unionsgesetzgeber hat in Erwägungsgrund 85 Whistleblowing-RL ausdrücklich darauf hingewiesen, dass die Mitgliedstaaten mittels gesetzgeberischer Maßnahmen die datenschutzrechtlichen Betroffenenrechte einschränken sollen. Dass solche Vorschriften mehr als nur die pauschale Verankerung des Identitätsschutzes in §§ 8, 9 HinSchG beinhaltet, liegt auf der Hand.

(d) §§ 8, 9 HinSchG

Fraglich ist, ob die Vorgaben des Identitätsschutzes in §§ 8, 9 HinSchG möglicherweise auf die Öffnungsklausel in Art. 23 Abs. 1 lit. i) DS-GVO gestützt werden können und eine Ausnahme der datenschutzrechtlichen Informationspflicht begründen können. Zu beachten ist jedoch, dass die §§ 8, 9 HinSchG keine Ausführungen hinsichtlich der spezifischen Vorgaben, die Art. 23 Abs. 2 DS-GVO verlangt, bereithalten. Auffällig ist insbesondere, dass keine Vorgaben in Bezug auf die mit dem Identitätsschutz des Whistleblowers einhergehenden Risiken für das informationelle Selbstbestimmungsrecht der von der Datenverarbeitung betroffenen Person getroffen werden. Das HinSchG kennt keine Vorgabe, die es der von der Datenverarbeitung

---

[755] Der EuGH formuliert in diesem Zusammenhang zutreffend: „*Art. 88 I und II VO (EU) 2016/679 ist dahin auszulegen, dass nationale Rechtsvorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten von Beschäftigten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext unangewendet bleiben müssen, wenn sie nicht die in ebendiesem Art. 88 I und II vorgegebenen Voraussetzungen und Grenzen beachten.*“, EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.89.

[756] BT-Drs. 20/5992, S. 36, 59.

betroffenen Person ermöglicht, Kenntnis von der Verarbeitung ihrer personenbezogenen Daten zu erlangen, um diese sodann auf Rechtmäßigkeit zu prüfen.[757] § 8, 9 HinSchG sehen keine Interessenabwägung vor, sondern gehen pauschal und einseitig zu Lasten der von der Meldung betroffenen Person von einem Vorrang des Identitätsschutzes aus. Der von der Datenverarbeitung betroffenen Person ist es daher nicht möglich, sich der Datenverarbeitung ihrer personenbezogenen Daten im Rahmen des HinSchG bewusst zu werden. §§ 8, 9 HinSchG können folgerichtig nicht auf die Öffnungsklausel des Art. 23 Abs. 1 lit. i) DS-GVO gestützt werden.

Gleiches gilt mit Blick auf die Öffnungsklausel des Art. 88 Abs. 1 DS-GVO. Ungeachtet der Frage, ob das HinSchG eine spezifischere Vorschrift im Beschäftigungskontext darstellt,[758] enthalten die §§ 8, 9 HinSchG jedenfalls keine Maßnahmen, die das informationelle

---

[757] Siehe ausführlich: Kapitel C) I. 3. c) bb) (1) (b).

[758] *Fischer*, in: Thüsing, HinSchG, § 10 Rn.1, 2. *Baade*/*Hößl,* DStR 2023, 1265, 1267 halten § 10 HinSchG richtigerweise für rein deklaratorisch. Die Zulässigkeit der Datenverarbeitung in Bezug auf eine eingehende Meldung ergibt sich bereits aus Art. 6 Abs. 1 S. 1 lit. c) DS-GVO. Anders die Gesetzesbegründung: BT-Drs. 20/3442, S. 76: Der Gesetzgeber misst § 10 HinSchG offenbar konstitutive Bedeutung bei, obwohl Art. 17 Whistleblowing-RL dazu keinen Regelungsauftrag enthält, vgl. *Rüdiger*/*Adelberg,* K&R 2023, 172, 177. Inwieweit § 10 HinSchG auf eine Öffnungsklausel rückführbar ist, kann jedoch dahinstehen, da jedenfalls Art. 6 Abs. 1 S. 1 lit. c) DS-GVO Datenverarbeitungen im Zusammenhang mit einer eingehenden Meldung hinreichend legitimiert. Ausführlich dazu: *Musiol*, Hinweisgeberschutz und Datenschutz, S. 233 ff. Sollten im Anschluss an die Meldung Folgemaßnahmen erforderlich sein (§ 18 HinSchG), weist *Fischer* darauf hin, dass § 10 HinSchG konstitutive Bedeutung zuteilwerde, vgl. *Fischer*, in: Thüsing, HinSchG § 10 Rn.1. Für eine konstitutive Bedeutung spricht insbesondere die Unanwendbarkeit des § 26 Abs. 1 S. 1 BDSG infolge der Entscheidung des EuGH zu dem im Vergleich zu § 26 Abs. 1 S. 1 BDSG nahezu identischen § 23 HDSIG, vgl. EuGH, Urteil v. 30.03.2023 - C-34/21 Rn.65, NZA 2023, 487 - m. Anm. *Meinecke.* Da Datenverarbeitungen zu Zwecken von Folgemaßnahmen jedenfalls über Art. 6 Abs. 1 S. 1 lit. f) DS-GVO legitimiert sind, kann die Frage der geeigneten Öffnungsklausel für § 10 HinSchG allerdings abermals dahinstehen.

Selbstbestimmungsrecht der von der Meldung betroffenen Person hinreichend berücksichtigt und dem Transparenzgebot die notwendige Geltung verleiht, die Art. 88 Abs. 2 DS-GVO im Sinne eines Mindestschutzes der DS-GVO verlangt.[759]

Es bleibt daher dabei, dass die Informationspflicht zu Gunsten des Identitätsschutzes zumindest nach Art. 14 Abs. 5 lit. b) DS-GVO ausgeschlossen sein kann.[760] Darüber hinaus steht es den Betriebsparteien frei, eine Betriebsvereinbarung zu schließen, dazu später.[761]

(2) Beschränkung der Datenauskunft

Nach Art. 15 Abs. 1 Hs. 1 DS-GVO hat eine von der Datenverarbeitung betroffene Person das Recht, von der für die Datenverarbeitung verantwortlichen Stelle eine Bestätigung darüber zu verlangen, ob diese sie betreffende personenbezogene Daten verarbeitet.[762] Ist dies der Fall, hat die von der Datenverarbeitung betroffene Person ein Recht auf Auskunft über diese personenbezogenen Daten (Art 15 Abs. 1 Hs. 2 Var. 1 DS-GVO) sowie die in Art. 15 Abs. 1 Hs. 2 Var. 2 DS-GVO gelisteten Metainformationen einer Datenverarbeitung. Werden die personenbezogenen Daten nicht bei der betroffenen Person erhoben, erstreckt Art. 15 Abs. 1 Hs. 1 Var. 2 lit. g) DS-GVO das Auskunftsrecht auf alle verfügbaren Informationen über die Herkunft der personenbezogenen Daten.[763] Dazu gehören auch Informationen zum Hinweisgebersystem sowie zur Identität des Hinweisgebers.[764] Der Begriff der „*Herkunft*“ stimmt insofern mit dem

---

759 Vgl. EuGH, Urteil v. 30.03.2023 - C-34/21 Rn.65.
760 Ebenso: *Lühning*, ZD 2023, 136, 139, 140.
761 Siehe: Kapitel C) I. 3. c) cc) (3).
762 Dies umfasst auch das Recht auf Erhalt einer sog. „*Negativauskunft*“, vgl. *Gola*/*Franck,* Art. 15 DS-GVO Rn.5; *Pötters*, in: Compliance, § 18 Rn.30.
763 *Mohn*, NZA 2022, 1159 m. w. N.
764 BGH, Urteil v. 22.2.2022 - VI ZR 14/21, ZD 2022, 326; *Mohn*, NZA 2022, 1159 m. w. N.

der „*Quelle*“ in Art. 14 Abs. 2 lit. f) DS-GVO überein.[765] Sollten in einem Hinweisgebersystem keine Informationen über die Identität des Hinweisgebers vorhanden sein, weil der Hinweisgeber einen anonymen Meldekanal nutzt und die gemeldeten Informationen keine Rückschlüsse auf dessen Identität zulassen, können diese folgerichtig nicht Gegenstand des Auskunftsrechts nach Art. 15 Abs. 1 Hs. 2 Var. 2 lit. g) DS-GVO sein.

Beschränkungen erfährt das Auskunftsrecht durch Art. 15 Abs. 4 DS-GVO sowie über Art. 23 Abs. 1 lit. i) DS-GVO i. V. m. §§ 27 Abs. 2, 28 Abs. 2, 29 Abs. 1 S. 2 und § 34 Abs. 1 BDSG. Für die Berücksichtigung des Identitätsschutzes im Rahmen der Datenauskunft kommen die Beschränkungsmöglichkeiten der Art. 15 Abs. 4 DS-GVO und Art. 23 Abs. 1 lit. i) DS-GVO in Verbindung mit § 29 Abs. 1 S. 2 BDSG in Betracht. Diese werden im Folgenden näher beleuchtet.

Der Gesetzgeber geht davon aus, dass der Identitätsschutz des Whistleblowers in Bezug auf das Auskunftsrecht über § 29 Abs. 1 S. 2 BDSG gewährleistet wird.[766] In der Gesetzesbegründung zum HinSchG heißt es: „*Die notwendigen Ausnahmetatbestände haben indes bereits Eingang in das BDSG gefunden. Über die im Rahmen des § 29 Absatz 1 BDSG geforderte Interessenabwägung lässt sich der erforderliche Gleichlauf zwischen dem Vertraulichkeitsschutz und datenschutzrechtlichen Informationspflichten und Auskunftsrechten herstellen. (...) Nach § 29 Absatz 1 Satz 2 BDSG besteht das Recht zur Auskunft der betroffenen Person nicht, soweit durch die Auskunft Informationen offenbar würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines*

[765] Ein Blick in die anderen Sprachfassungen der DS-GVO bestätigt, dass dort ebenfalls nicht zwischen „*Quelle*“ und „*Herkunft*“ unterschieden wird. Stattdessen heißt es einheitlich „*source*“ (englische Sprachfassung) bzw. „*bron*“ (niederländische Sprachfassung), vgl. *Däubler*, in: DWWS, Art. 15 DS-GVO Rn.27; *Dix*, in: NK-DSGVO, Art. 15 Rn.24; *Mohn*, NZA 2022, 1159; *Bäcker*, in: Kühling/Buchner, DS-GVO, Art. 14 Rn.20; *Kamlah*, in: Plath, DS-GVO, Art. 15 Rn.13.

[766] BT-Drs. 20/5992, S. 59.

Dritten (was regelmäßig hinsichtlich der hinweisgebenden Person - auch nach Abschluss der Ermittlungen - anzunehmen ist) geheim gehalten werden müssen. Soweit Informationen dem Vertraulichkeitsgebot unterliegen, sind diese nach § 29 Absatz 1 BDSG grundsätzlich geheim zu halten."[767] Der Gesetzgeber geht demgemäß von einem Vorrang des Identitätsschutzes nach Maßgabe der §§ 8, 9 HinSchG aus.

Zu beachten ist jedoch, dass § 29 Abs. 1 S. 2 BDSG auf eine Öffnungsklausel gestützt werden muss, um eine Beschränkung der Datenauskunft zu bewirken. Nach Art. 23 Abs. 1 lit. i) DS-GVO kann der nationale Gesetzgeber die Datenauskunft durch Rechtsvorschriften beschränken, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die den Schutz der von der Datenverarbeitung betroffenen Person oder die Rechte und Freiheiten anderer Personen sicherstellt. Zusätzlich sind die in Art. 23 Abs. 2 DS-GVO genannten spezifischen Vorgaben aufzunehmen.

Hervorzuheben ist zunächst, dass die Vorgaben des § 29 Abs. 1 S. 2 BDSG denen des Art. 23 Abs. 1 lit. i) DS-GVO ähneln. Nach § 29 Abs. 1 S. 2 BDSG besteht das Recht auf Datenauskunft nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift (Var. 1) oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten (Var. 2), geheim gehalten werden müssen.[768] Der direkte Vergleich beider Vorschriften verdeutlicht, dass § 29 Abs. 1 S. 2 BDSG dem Grunde nach eine Wiederholung dessen beinhaltet, was Art. 23 Abs. 1 lit. i) DS-GVO vorgibt, wenn auch mit anderem Satzbau. § 29 Abs. 1 S. 2 Var. 1 BDSG stellt insofern eine überflüssige Zwischenstation dar, die suggeriert, § 29 Abs. 1 S. 2 Var. 1 BDSG

---

[767] BT-Drs. 20/5992, S. 59.

[768] §§ 29 Abs. 1 S. 2, 34 BDSG beruhen auf der Öffnungsklausel des Art. 23 Abs. 1 lit. i) DS-GVO, vgl. BT-Drs. 18/11325, S. 100 f; *Steinrötter*, in: BeckOK-IT-Recht, § 29 BDSG Rn.2.

entfalte die Berechtigung für eine Beschränkung der Datenauskunft, wenngleich sich diese erst aus der weiteren Rechtsvorschrift (in diesem Fall §§ 8, 9 HinSchG) ergibt. Dies verschleiert in unionsrechtswidriger Weise die unmittelbare Geltung des Art. 23 Abs. 1 lit. i) DS-GVO. Im Übrigen enthält § 29 Abs. 1 S. 2 BDSG keine Vorgaben hinsichtlich des Schutzes der von der Datenverarbeitung betroffenen Person, obwohl diese nach Art. 23 Abs. 2 lit. g) DS-GVO notwendige Voraussetzung für eine Beschränkung der Datenauskunft sind. § 29 Abs. 1 S. 2 BDSG kann daher nicht auf die Öffnungsklausel des Art. 23 DS-GVO gestützt werden. Vielmehr drängt sich nach hiesiger Auffassung die Unionsrechtswidrigkeit des § 29 Abs. 1 S. 2 BDSG auf.[769] Entgegen der Annahme des nationalen Gesetzgebers muss § 29 Abs. 1 S. 2 BDSG unangewendet bleiben und kann nicht als Beschränkung für die Datenauskunft herangezogen werden.

Die Vorschriften des HinSchG können ebenso wenig als Rechtsvorschriften im Sinne des Art. 23 Abs. 1 lit. i) DS-GVO herangezogen werden. §§ 8, 9 HinSchG enthalten keine Interessenabwägung, sondern gehen einseitig zu Lasten der von der Meldung betroffenen Person von einem Vorrang des Identitätsschutzes aus, ohne deren informationelles Selbstbestimmungsrecht einzubeziehen.[770]

§§ 8, 9 HinSchG enthalten keine spezifischen Vorgaben, die Art. 23 Abs. 2 lit. g) DS-GVO verlangt. Im Ergebnis können die Vorgaben des HinSchG daher nicht auf die Öffnungsklausel des Art. 23 Abs. 1 lit. i) DS-GVO zurückgeführt werden. Gleiches gilt mit Blick auf die Öffnungsklausel des Art. 88 Abs. 1 DS-GVO. Ungeachtet der Frage, ob das HinSchG eine spezifischere Vorschrift im

---

769 Die Unionsrechtmäßigkeit des § 29 Abs. 1 S. 2 BDSG nicht weiter prüfend, stellt das überwiegende Schrifttum fest, dass der Verweis des Gesetzgebers auf § 29 BDSG nicht genügt, um zum Ausschluss der Betroffenenrechte zu gelangen, vgl. *Thüsing*, in: Thüsing, HinSchG § 8 Rn.28; *Bayreuther* DB 2023, 1537, 1541. Folgerichtig wird eine Interessenabwägung gefordert: *Dzida*/*Granetzny*, NZA 2022, 1201, 1206; *Fehr*, DB 2023, 180, 185. Vgl. auch BGH, Urteil vom 22.2.2022 - VI ZR 14/21.

770 Siehe ausführlich: Kapitel C) I. 3. c) bb) (1) (d).

Beschäftigungskontext darstellt,[771] enthalten die Vorgaben jedenfalls keine Maßnahmen, die das informationelle Selbstbestimmungsrecht der von der Meldung betroffenen Person hinreichend berücksichtigt, und die dem Transparenzgebot die nach Art. 88 Abs. 2 DS-GVO notwendige Geltung verleihen.[772]

Damit verbleibt lediglich die allgemeine Möglichkeit der Beschränkung der Datenauskunft über Art. 15 Abs. 4 DS-GVO. Nach Art. 15 Abs. 4 DS-GVO dürfen die Rechte und Freiheiten anderer Personen das Recht auf Erhalt einer Kopie gemäß Art. 15 Abs. 3 DS-GVO nicht beeinträchtigen. Zu beachten ist jedoch, dass Art. 15 Abs. 4 DS-GVO seinem Wortlaut nach ausschließlich auf Art. 15 Abs. 3 DS-GVO verweist.

Dies führt zu der Frage, ob die überwiegenden Rechte und Freiheiten anderer Personen ausschließlich im Rahmen des Art. 15 Abs. 3 DS-GVO berücksichtigungsfähig sind, nicht jedoch im Rahmen des Art. 15 Abs. 1 Hs. 2 DS-GVO, der die Beauskunftung der Identität des Whistleblowers umfasst. Der EuGH hat zutreffend klargestellt, dass das Recht auf Kopie kein eigenständiges Recht neben dem Auskunftsrecht sei, sondern lediglich dessen „*praktische(n) Modalitäten*“ festlege, weshalb Art. 15 Abs. 1 und Abs. 3 DS-GVO im Sinne eines

[771] Siehe ausführlich: Kapitel C) I. 3. c) bb) (1) (d), dort: Fn.659.
[772] Vgl. EuGH, Urteil v. 30.03.2023 - C-34/21 Rn.65.

einheitlichen Rechts auf Datenauskunft zu verstehen seien.[773] Dies hilft jedoch nur bedingt weiter, denn Art. 15 Abs. 3 DS-GVO beziehe sich laut EuGH ausschließlich auf die Beauskunftung der personenbezogenen Daten nach Art. 15 Abs. 1 Hs. 2 Var. 1 DS-GVO, weil „*Informationen*" nach Art. 15 Abs. 3 S. 3 DS-GVO lediglich „*perso-*

[773] Zuvor wurde im Schrifttum darüber diskutiert, ob Art. 15 Abs. 1 und Abs. 3 DS-GVO rechtsdogmatisch im Sinne eines einheitlichen Auskunftsrechts zu verstehen seien oder ob es sich um zwei eigenständige Ansprüche handele, die gesondert voneinander zu betrachten seien. Da der EuGH die Auslegungshoheit innehält, ist diese Frage nunmehr geklärt und die Datenauskunft im Sinne eines einheitlichen Rechts zu verstehen, wobei die Kopie in Art. 15 Abs. 3 DS-GVO die Erfüllungsmodalität der Datenauskunft nach Art. 15 Abs. 1 Hs. 2 Var. 1 DS-GVO vorgibt, EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.31, 32, euzw 2023, 575, entsprechend den Schlussanträgen des *GA Pitruzzella*, GRUR-RS 2022, 36103 Rn.8. Zu den Vertretern dieser Sichtweise gehörten schon vor der EuGH-Entscheidung: *Pötters*, in: Compliance: § 18 Rn.32, 37; *Pauly*, in: Paal/Pauly, DS-GVO, Art. 15 Rn.33, 41; *Dausend*, ZD 2019, 103, 106 f.; *Wybitul*/*Neu*/*Strauch,* ZD 2018, 202, 203; *Wybitul*/*Brams,* NZA 2019, 672, 676; *Zikesch*/*Sörup*, ZD 2019, 239, 240; tendenziell auch: *Pauly*/*Mende,* CCZ 2022, 28, 31; *Zschieschack,* ZWE 2023, 244, 250; *Franck*, in: Gola, DS-GVO, Art. 15 Rn.35 m. w. N. In diese Richtung wohl auch: BGH, Urteil v. 15.06.2021 - VI ZR 576/19, NJW 2021, 2726 sowie BGH, FG Berlin-Brandenburg, Urteil v. 16.01.2022 - 16 K 1059/21, BeckRS 2022, 6615 Rn.78; DSK-Kurzpapier Nr. 6, S. 2. Dagegen zwei eigenständige Ansprüche bejahend: *Bäcker,* in: Kühling/Buchner, DS-GVO, Art. 15 Rn.39; *Schmidt-Wudy*, in: BeckOK-Datenschutzrecht, Art. 15 DS-GVO Rn.85; *Kremer,* CR 2018, 560, 563 f.; *Franck*, in: Gola/Heckmann, DS-GVO, Art. 15 Rn.28; *Härting,* CR 2019, 219 221; *Dix*, in: NK-DatenschutzR, Rn.28; *König,* CR 2019, 295 ff.; *Riemer*, ZD 2019, 413, 414; *Riemer,* DSB 2019, 223; *Korch*/*Chatard,* NZA 2020, 893, 895; *Koreng,* NJW 2021, 2692, 2693; *Lembke*/*Fischels,* NZA 2022, 513, 516; *Maschmann*, NZA-Beilage 2022, 50, 52; *Winterhagen*, ZD-Aktuell 2022, 01066 und *Däubler*, in: DWWS, Art. 15 DS-GVO Rn.27. In diese Richtung auch: BAG, Urteil v. 16.12.2021 - VI ZR 576/19, NJW 2021, 2726. Zum damaligen Streitstand ausführlich: *Leibold*, ZD-Aktuell 2021, 05313. *Peisker* weist darüber hinaus zutreffend darauf hin, dass in Teilen des Schrifttums Rechtsdogmatik und inhaltliche Reichweite nicht hinreichend getrennt beleuchtet worden seien und spricht sich nach umfassender Analyse in überzeugender und mit dem EuGH in übereinstimmender Weise für das Verständnis der Kopie als eine Vorgabe auf Rechtfolgenseite aus: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 94 ff.

nenbezogene Daten“ im Sinne des Art. 15 Abs. 3 S. 1 DS-GVO seien.[774] Die Kopie beziehe sich daher nur auf Art. 15 Abs. 1 Hs. 2 Var. 1 DS-GVO. Dies führt abermals zu der Frage, ob Art. 15 Abs. 4 DS-GVO mit seinem Verweis auf Art. 15 Abs. 3 DS-GVO die Beauskunftung der Metainformationen nach Art. 15 Abs. 1 Hs. 2 Var. 2 DS-GVO überhaupt miterfassen kann.[775]

Anzumerken ist, dass sich die Kopie in Art. 15 Abs. 3 DS-GVO nur deshalb auf die personenbezogenen Daten in Art. 15 Abs. 1 Hs. 2 Var. 1 DS-GVO bezieht, weil über diese ohne Weiteres per Kopie Auskunft erteilt werden kann. Dies erweist sich hinsichtlich der Metainformationen schwieriger. Hinsichtlich der Metainformationen bleibt der Verantwortliche nach Maßgabe des Art. 12 DS-GVO in der Art und Weise seiner Auskunftserteilung im Übrigen frei. Aus Art. 52 GR-CH folgt außerdem, dass das Recht auf Datenauskunft nicht absolut gilt.[776] Die gebotene charta-rechtliche Auslegung des Art. 15 Abs. 1 Hs. 2 Var. 2 DS-GVO führt daher zwingend zu der Annahme, dass kollidierende grundrechtlich geschützte Positionen in der Lage sein müssen, die Beauskunftung der Metainformationen zu beschränken. Diese Wertung gilt es im Rahmen des Art. 15 Abs. 4 DS-GVO zu beachten.[777] Folgerichtig ist davon auszugehen, dass sich der Verweis in Art. 15 Abs. 4 DS-GVO in charta-konformer Auslegung auf das Auskunftsrecht insgesamt erstreckt, also auf das Auskunftsrecht mitsamt der dazugehörigen Metainformationen in

---

774 EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.49.

775 EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.49.

776 Vgl. *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 409 f.; *Jarass*, in: Jarass, GR-CH, Art. 8 Rn.21. Siehe auch: Kapitel C) I. 1. a).

777 *GA Kokott* bezeichnet das Sekundärrecht als den Hebel für eine Drittwirkung der Grundrechte der GR-CH: *GA Kokott*, Schlussanträge v. 18.07.2007 - C-275/06 - *Promusicae*, BeckRS 2007, 70553 Rn.57. Zur Berücksichtigungsfähigkeit der GR-CH in Auslegungsfragen siehe auch: Kapitel B) I.

Art. 15 Abs. 1 Hs. 2 DS-GVO.[778] Die Frage der Beschränkung des Auskunftsrechts muss demgemäß losgelöst vom Bezugspunkt der Erfüllungsmodalität beantwortet werden. Insofern wäre es sinnvoll, Art. 15 Abs. 4 DS-GVO an den Wortlaut seines dazugehörigen Erwägungsgrundes 63 DS-GVO sprachlich anzupassen. Anders als Art. 15 Abs. 4 DS-GVO unterscheidet Erwägungsgrund 63 DS-GVO nicht zwischen „*personenbezogenen Daten*" und „*Informationen*", sondern formuliert allgemein „*Auskunftsrecht*" bzw. „*Recht*".

Im Rahmen des Art. 15 Abs. 4 DS-GVO entscheidet sodann eine umfassende Interessenabwägung zwischen dem Identitätsschutz des Whistleblowers und dem informationellen Selbstbestimmungsrecht der von der Meldung betroffenen Person, wobei der Identitätsschutz nur insoweit zu berücksichtigen ist, als nach den Vorgaben der §§ 8, 9 HinSchG tatsächlich Identitätsschutz besteht, der Whistleblower mithin ein berechtigtes Interesse an der Geheimhaltung seiner Identität hat. Maßgeblich sind die Umstände des jeweiligen Einzelfalls. Kein berechtigtes Interesse des Whistleblowers besteht in Fällen einer grob fahrlässigen oder vorsätzlichen Meldung von Falschinformationen, vgl. § 9 Abs. 1 HinSchG. Da die subjektive Komponente der groben Fahrlässigkeit bzw. des Vorsatzes im Rahmen des § 9 Abs. 1 HinSchG für den Beschäftigungsgeber jedoch nur schwer festzustellen ist, ist zu fragen, ob dem Whistleblower das berechtigte Interesse am Identitätsschutz fehlt, sollte dieser objektiv unrichtige Informationen melden, die persönlichkeitsverletzende Äußerungen enthalten und infolgedessen verschuldensunabhängige Rechtsansprüche (§ 823 Abs. 1 BGB i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG) begründen. Wäre dies der Fall, bestünde kein berechtigtes Interesse im Sinne des Art. 15 Abs. 4 DS-GVO, sodass es auf die Interessenabwägung nicht

---

[778] Ebenso im Ergebnis: *Peisker*, der „*von der (analogen) Anwendung des Art. 15 Abs. 4 DS-GVO auf sämtliche Auskunftsbestandteile ausgeht*": *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 415. So im Ergebnis auch: LAG Baden-Württemberg, Urteil v. 17.03.2021 - 21 Sa 43/20, NZA-RR 2021, 410 Rn.39; LG Stuttgart, Urteil v. 04.11.2020 - 18 O 333/19, BeckRS 2020, 38735 Rn.34.

mehr ankäme.[779] Für ein solches Verständnis spricht, dass das Auskunftsrecht darauf zielt, die von der Datenverarbeitung betroffene Person zu befähigen, sich der Datenverarbeitung bewusst zu werden, um deren Rechtmäßigkeit zu überprüfen und diese durch die Wahrnehmung ihrer Rechte durchzusetzen.[780] Fraglich ist insofern, ob es sich bei diesen Rechten auch um verschuldensunabhängige Rechtsansprüche gegen den Whistleblower handeln kann.

Der EuGH hat klargestellt, dass das Auskunftsrecht „*im Sinne der Ermöglichung der Rechte auf Berichtigung, Löschung, Einschränkung der Datenverarbeitung sowie des Rechts auf Widerspruch*“ auszulegen sei, weil das Auskunftsrecht „*die datenschutzrechtlichen Grundsätze der Transparenz und der fairen und transparenten Verarbeitung*“ effektuiere.[781] Daraus geht hervor, dass die Datenauskunft die von der Datenverarbeitung betroffene Person lediglich zur Durchsetzung der Rechtmäßigkeit der Datenverarbeitung als solches befähigen will, nicht jedoch zur Durchsetzung ihrer weiteren Rechte gegenüber Dritten. Diese Lesart überzeugt auch vor dem Hintergrund, dass das Transparenzgebot den mit der Datenverarbeitung einhergehenden Eingriff in die informationelle Selbstbestimmungsfreiheit in seiner Intensität absenken soll.[782] Die Betroffenenrechte beziehen sich in ihrer Funktion als Konkretisierung des Transparenzgebots ausschließlich darauf, die von der Datenverarbeitung betroffene Person zu befähigen, auf die Rechtmäßigkeit der Datenverarbeitung hinzuwirken.[783] Die objektive Unrichtigkeit einer Information, losgelöst von der subjektiven Motivlage des Whistleblowers (vgl. § 9 Abs. 1 HinSchG), ist daher weder geeignet, dem Whistleblower ein berechtigtes Interesse an der Geheimhaltung abzusprechen, noch dem Auskunftsinteresse

---

779 Vgl. BGH, Urteil v. 22.02.2022 - VI ZR 14/21, BeckRS 2022, 5496 Rn.26; BGH, Urteil v. 18.06.2019 - VI ZR 80/18, NJW 2020, 45 Rn.12.

780 Siehe: Kapitel C) I. 1. a).

781 EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.35, 38.

782 Siehe ebenfalls: Kapitel C) I. 1. a).

783 *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 88; *Plath*, in: Plath, DS-GVO, Art. 5 Rn.5; *Pötters*, in: Gola/Heckmann, DS-GVO, Art. 5 Rn.12; sowie Erwägungsgründe 39 S. 5 und 63 S. 1 DS-GVO.

einen pauschalen Vorrang zu gewähren. Dies gilt auch dann, wenn die Meldung Informationen enthält, die persönlichkeitsverletzende Äußerungen darstellen und infolgedessen verschuldensunabhängige Rechtsansprüche begründet werden.[784] Es bleibt in diesen Fällen bei einer einzelfallbezogenen Interessenabwägung, wobei aufgrund der allgemeinen Konzeption des Art. 15 DS-GVO im Zweifel davon auszugehen ist, dass das Recht auf Datenauskunft überwiegt.

Besteht nach den Vorgaben des HinSchG Identitätsschutz, so folgt daraus ein im Rahmen des Art. 15 Abs. 4 DS-GVO berücksichtigungsfähiges berechtigtes Interesse des Whistleblowers. Dies ist nicht gleichbedeutend mit einem pauschalen Überwiegen zu Gunsten des Identitätsschutzes,[785] und gilt umso mehr, soweit der jeweilige Identitätsschutz auf Vorgaben fußt, die keine eigenen Regelungen zur Datentransparenz treffen. In diesen Fällen ist dem Grundsatz der Datentransparenz im Rahmen des Art. 15 Abs. 4 DS-GVO hinreichend Geltung zu verschaffen. Andernfalls droht die fehlende Überprüfbarkeit der Datenverarbeitung durch die von der Meldung betroffene Person, um deren Rechtmäßigkeit durchsetzen zu können. Ein pauschales Überwiegen des Identitätsschutzes nach Maßgabe der §§ 8, 9 HinSchG wäre demgemäß zweckwidrig.[786] Aus dem Vorliegen

---

[784] Für ein Überwiegen des Auskunftsinteresses „*in aller Regel*“: *Schmidt-Wudy*, in: BeckOK-DatenschutzR, Art. 15 DS-GVO Rn.85.1; *Mohn*, NZA 2022, 1159, 1164; *Engelhardt*, RDi 2022, 298, 304.

[785] In diese Richtung, wenngleich etwas enger: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 456 ff., der den Identitätsschutz nach §§ 8, 9 HinSchG als rechtliche Pflicht des datenschutzrechtlich Verantwortlichen einordnet, die zu einem regelmäßigen Überwiegen seiner berechtigten Interessen führe. Ähnlich: *Brobeil*, Die Auswirkungen der Richtlinie (EU) 2019/1937 auf Arbeitnehmer-Hinweisgeber, S. 285; vgl. auch: *Gerdemann*/*Spindler*, ZIP 2020, 1896, 1904.

[786] Ein pauschales Überwiegen läuft auf eine Beschränkung der DS-GVO hinaus, für die es eine Öffnungsklausel braucht, vgl. Art. 23 Abs. 1 lit. i) DS-GVO bzw. Art. 88 Abs. 1 DS-GVO. Andernfalls droht eine Umgehung der Art. 23 Abs. 2 DS-GVO bzw. Art. 88 Abs. 2 DS-GVO, die den Mindestschutz durch die DS-GVO sicherstellen, vgl. EuGH, Urteil v. 30.03.2023 - C-34/21, Rn.71-73.

der Voraussetzungen in §§ 8, 9 HinSchG kann noch kein Überwiegen zu Gunsten des Identitätsschutzes resultieren.[787] Die Interessenabwägung im Rahmen des Art. 15 Abs. 4 DS-GVO ist richtigerweise eigenständig durchzuführen. Aus dem Regel-Ausnahme-Verhältnis des Art. 15 DS-GVO folgt lediglich, dass in Zweifelsfragen das Recht auf Datenauskunft überwiegt.[788] Darüber können sich die §§ 8, 9 HinSchG nicht hinwegsetzen.

Inwieweit der Identitätsschutz tatsächlich überwiegt, ist einzelfallbezogen zu entscheiden. Ein pauschaler Hinweis auf den Identitätsschutz des Whistleblowers genügt nicht.[789] Für ein Überwiegen des Identitätsschutzes spricht beispielsweise, dass der Whistleblower Repressalien durch die von der Meldung betroffene Person ausgesetzt wäre. Auch eine Gefährdung des Untersuchungszweckes interner Ermittlungen kann zu einem Überwiegen des Identitätsschutzes führen.[790] Dies überzeugt insbesondere vor dem Hintergrund, dass damit ein Gleichlauf mit Art. 14 Abs. 5 lit. b) DS-GVO geschaffen wäre.

Fraglich ist, ob eine Vertraulichkeitszusage für ein Überwiegen des Identitätsschutzes im Rahmen des Art. 15 Abs. 4 DS-GVO genügt. Das LAG Baden-Württemberg hat entschieden, dass ein berechtigtes Interesse an der Geheimhaltung der Quelle bestehen könne, wenn der Arbeitgeber zu Aufklärungszwecken Anonymität zusichere.[791] Das Vorliegen eines berechtigten Interesses sagt jedoch noch nichts darüber aus, ob dieses das informationelle Selbstbestimmungsrecht der

---

[787] Siehe dazu mit etwas anderem Einschlag: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 456 ff. Ähnlich dazu auch: *Brobeil*, Die Auswirkungen der Richtlinie (EU) 2019/1937 auf Arbeitnehmer-Hinweisgeber, S. 285; vgl. auch: *Gerdemann*/*Spindler*, ZIP 2020, 1896, 1904.

[788] Vgl. *Brobeil*, Die Auswirkungen der Richtlinie (EU) 2019/1937 auf Arbeitnehmer-Hinweisgeber, S. 285.

[789] BGH, Urteil v. 22.02.2022 - VI ZR 14/21, BeckRS 2022, 5496 Rn.26.

[790] *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 455; vgl. auch: *Altenbach*/*Dierkes*, CCZ 2020, 126, 129; *Fehr*, ZD 2022, 256, 258.

[791] LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, 242 Rn.181.

von der Meldung betroffenen Person überwiegt. Insofern mag es stimmen, dass eine Vertraulichkeitszusage ein berechtigtes Interesse des Whistleblowers auf Identitätsschutz begründen kann. Dennoch ist zu beachten, dass eine Vertraulichkeitszusage den Identitätsschutz des Whistleblowers nicht erhöht. Das berechtigte Interesse des Whistleblowers folgt bereits aus §§ 8, 9 HinSchG, unabhängig vom Vorliegen einer Vertraulichkeitszusage. Hinzu kommt, dass auch nach Ansicht des LAG Baden-Württemberg Falschinformationen auszunehmen sind, die der Whistleblower leichtfertig oder wider besseres Wissen getätigt hat.[792] Insofern kann sich eine Vertraulichkeitszusage auch nicht über § 9 Abs. 1 HinSchG hinwegsetzen. Dies auch zu Recht nicht, denn diese Informationen sind nicht mehr Teil der Meinungsfreiheit. Vor diesem Hintergrund ist es daher zutreffend, wenn der BGH formuliert, eine Vertraulichkeitszusage begründe noch kein Auskunftsverweigerungsrecht.[793] Aus dem Bestehen eines berechtigten Interesses, das die Vertraulichkeitszusage zu begründen vermag, folgt kein pauschales Überwiegen zu Gunsten des Identitätsschutzes. Für ein Überwiegen des Identitätsschutzes bedarf es vielmehr eines berechtigten Schutzbedürfnisses dahingehend, dass die zugesicherte Vertraulichkeit auch tatsächlich besteht, weil die Meldung andernfalls nicht erfolgt wäre. Auch hier genügt kein pauschaler Hinweis.

Ist das Auskunftsrecht aus Gründen des Identitätsschutzes zu beschränken, darf dies nicht dazu führen, dass der von der Meldung betroffenen Person jegliche Auskunft verweigert wird, vgl. Erwägungsgrund 63 S. 6 der DS-GVO.[794] Stattdessen erfolgt eine Beschränkung des Auskunftsrechts. Arbeitgeber haben die entsprechenden Passagen zu schwärzen bzw. anderweitig unkenntlich zu

---

792 LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, 242 Rn.181.

793 BGH, Urteil v. 22.02.2022 - VI ZR 14/21, BeckRS 2022, 5496 Rn.25.

794 Vgl. *Thüsing/Pötters*, in: Compliance, § 18 Rn.37; *Franzen*, NZA 2020, 1593, 1596.

machen, ehe sie dem Auskunftsverlangen im Übrigen entsprechen.[795] Maßgeblich sind sämtliche Umstände des Einzelfalls.

(3) Zwischenfazit

Dem nationalen Gesetzgeber ist die Auflösung des Spannungsverhältnisses zwischen dem Identitätsschutz des Whistleblowers und den datenschutzrechtlichen Betroffenenrechte der von der Meldung betroffenen Person missglückt. Ein pauschaler Hinweis im Rahmen der Gesetzesbegründung ignoriert den eindeutigen Regelungsauftrag des Unionsgesetzgebers, für die nötige Rechtssicherheit in diesem Bereich zu sorgen. Erschwerend kommt hinzu, dass sich der Hinweis des nationalen Gesetzgebers auf Normen des BDSG bezieht, deren Unionsrechtswidrigkeit sich - nach hiesiger Auffassung - aufdrängt.

Im Einzelnen: Der Identitätsschutz des Whistleblowers ist im Rahmen der datenschutzrechtlichen Betroffenenrechte über Ausnahmetatbestände der Informationspflicht bzw. Beschränkungen des Auskunftsrechts berücksichtigungsfähig. Nach Art. 14 Abs. 5 lit. b) DS-GVO besteht die Informationspflicht nicht, soweit die Erteilung der Information die Verwirklichung der Ziele der Datenverarbeitung voraussichtlich unmöglich macht oder ernsthaft beeinträchtigt. Dabei kommt es einzelfallbezogen darauf an, ob die Kenntnis über die Identität des Whistleblowers den Zweck der internen Untersuchung gefährden würde, weil Beweismittel drohen verlustig zu gehen oder die begründete Annahme besteht, die Erhebung weiterer Beweismittel werde gefährdet.[796] Im Übrigen besteht die Informationspflicht fort. §§ 8, 9 HinSchG sind keine Rechtsvorschriften im Sinne des Art. 14 Abs. 5 lit. c) DS-GVO. Sie enthalten keine Vorgaben, die sicherstellen, dass der von der Datenverarbeitung betroffene Person

---

795 *Schmidt-Wudy*, in: BeckOK-DatenschutzR, Art. 15 DS-GVO Rn.99.2.

796 DSK, Orientierungshilfe zu Whistleblowing-Hotlines, S. 10; vgl. auch *Schmidt-Wudy*, in: BeckOK-DatenschutzR, Art. 14 DS-GVO Rn.99.1; *Altenbach*/*Dierkes*, CCZ 2020, 126, 128; *Fehr*, ZD 2022, 256, 258; *Mohn*, NZA 2022, 1159, 1160.

eine hinreichende Überprüfungsmöglichkeit in Bezug auf die Rechtmäßigkeit der Datenverarbeitung eingeräumt wird. §§ 8, 9 HinSchG gehen von einem Vorrang des Identitätsschutzes aus, ohne das informationelle Selbstbestimmungsrecht der von der Meldung betroffenen Person zu berücksichtigen.

Aus denselben Gründen können die §§ 8, 9 HinSchG auch nicht auf die Öffnungsklausel des Art. 23 Abs. 1 lit. i) DS-GVO oder Art. 88 Abs. 1, Abs. 2 DS-GVO gestützt werden. Ungeachtet der Frage, ob das HinSchG eine spezifischere Vorschrift im Beschäftigungskontext darstellt, enthalten die Vorgaben jedenfalls keine Maßnahmen, die das informationelle Selbstbestimmungsrecht der von der Meldung betroffenen Person hinreichend berücksichtigen und dem datenschutzrechtlichen Transparenzgebot die notwendige Geltung verleihen, vgl. Art. 88 Abs. 2 DS-GVO.[797] Gleiches gilt hinsichtlich Art. 23 Abs. 2 lit. g) DS-GVO.

Ein Ausschluss der Informationspflicht aus Gründen des Identitätsschutzes folgt auch nicht aus § 29 Abs. 1 S. 1 BDSG. Es fehlt bereits an der dafür nötigen Öffnungsklausel. § 29 Abs. 1 S. 1 BDSG hält keine Ausführungen hinsichtlich des Schutzes der von der Datenverarbeitung betroffenen Person bereit, obwohl diese nach Art. 23 Abs. 2 lit. g) DS-GVO notwendige Voraussetzung für eine Beschränkung der Informationspflicht ist. § 29 Abs. 1 S. 1 BDSG kann daher nicht auf die Öffnungsklausel des Art. 23 Abs. 1 lit. i) DS-GVO gestützt werden. Gleiches gilt für die Öffnungsklausel des Art. 88 Abs. 1 DS-GVO. Festzuhalten ist zunächst, dass spezifischere Vorschriften im Sinne des Art. 88 Abs. 1 DS-GVO auch Transparenzvorgaben hinsichtlich der Betroffenenrechte sein können.[798]

Allerdings genügt § 29 Abs. 1 S. 1 BDSG den Anforderungen des Art. 88 Abs. 2 DS-GVO nicht, auch nicht bei unterstelltem Beschäfti-

[797] Siehe: Kapitel C) I. 3. c) bb) (1) (d) dort: Fn.659.
[798] Vgl. EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.71-73.

gungskontext. § 29 Abs. 1 S. 1 BDSG enthält keinerlei Vorgaben dazu, wie den mit der bezweckten Ausnahme einhergehenden Risiken für das informationelle Selbstbestimmungsrecht der von der Datenverarbeitung betroffenen Person begegnet wird. § 29 Abs. 1 S. 1 BDSG muss deshalb unangewendet bleiben.

Im Hinblick auf die Datenauskunft (Art. 15 Abs. 1, Abs. 3 DS-GVO) geht der Gesetzgeber davon aus, dass der Identitätsschutz des Whistleblowers über § 29 Abs. 1 S. 2 BDSG gewährleistet sei.[799] Zu beachten ist jedoch, dass § 29 Abs. 1 S. 2 BDSG auf keine Öffnungsklausel der DS-GVO gestützt werden kann. Der direkte Vergleich mit Art. 23 Abs. 1 lit. i) DS-GVO verdeutlicht, dass § 29 Abs. 1 S. 2 BDSG dem Grunde nach eine Wiederholung dessen beinhaltet, was Art. 23 Abs. 1 lit. i) DS-GVO ohnehin vorgibt, wenn auch mit anderem Satzbau. § 29 Abs. 1 S. 2 Var. 1 BDSG stellt insofern eine überflüssige Zwischenstation dar, die suggeriert, § 29 Abs. 1 S. 2 Var. 1 BDSG entfalte die Berechtigung für eine Beschränkung der Datenauskunft, wenngleich sich diese erst aus der weiteren Rechtsvorschrift (in diesem Fall §§ 8, 9 HinSchG) ergeben soll. Dies verschleiert die unmittelbare Geltung des Art. 23 Abs. 1 lit. i) DS-GVO in unionsrechtswidriger Weise. Im Übrigen enthält § 29 Abs. 1 S. 2 BDSG ebenfalls keine Vorgaben zum Schutz der von der Datenverarbeitung betroffenen Person, obwohl diese nach Art. 23 Abs. 2 lit. g) DS-GVO notwendige Voraussetzung für eine Beschränkung der Datenauskunft sind. § 29 Abs. 1 S. 2 BDSG muss unangewendet bleiben und kann nicht als Beschränkung für die Datenauskunft herangezogen werden.

Es verbleibt die allgemeine Möglichkeit der Beschränkung der Datenauskunft aus Gründen des Identitätsschutzes über Art. 15 Abs. 4 DS-GVO. Der Verweis auf Art. 15 Abs. 3 DS-GVO bezieht sich auf das Auskunftsrecht insgesamt, mitsamt der Metainformationen in Art. 15 Abs. 1 Hs. 2 DS-GVO. Die gebotene charta-rechtliche Auslegung des Art. 15 DS-GVO führt zu der zwingenden Annahme, dass

[799] BT-Drs. 20/5992 S. 59.

kollidierende grundrechtlich geschützte Positionen die Beauskunftung der Metainformationen beschränken können. Im Rahmen des Art. 15 Abs. 4 DS-GVO entscheidet sodann eine umfassende Interessenabwägung zwischen dem Identitätsschutz des Whistleblowers und dem informationellen Selbstbestimmungsrecht der von der Meldung betroffenen Person, wobei der Identitätsschutz nur insoweit zu berücksichtigen ist, als nach den Vorgaben der §§ 8, 9 HinSchG tatsächlich Identitätsschutz besteht, der Whistleblower mithin ein berechtigtes Interesse an der Geheimhaltung seiner Identität hat. Maßgeblich sind die Umstände des jeweiligen Einzelfalls. Ein berechtigtes Interesse besteht auch in Fällen einer Meldung objektiv unrichtiger Informationen, die persönlichkeitsverletzende Äußerungen enthält und infolgedessen verschuldensunabhängige Rechtsansprüche begründet. Nach dem Telos der Datenauskunft soll die von der Datenverarbeitung betroffene Person lediglich zur Durchsetzung der Rechtmäßigkeit der Datenverarbeitung befähigt werden, nicht jedoch zur Durchsetzung ihrer weiteren Rechte gegenüber Dritten. Es bleibt daher in diesen Fällen bei einer einzelfallbezogenen Interessenabwägung.

Die Interessenabwägung im Rahmen des Art. 15 Abs. 4 DS-GVO ist eigenständig durchzuführen. Aus dem Vorliegen der §§ 8, 9 HinSchG ist kein pauschales Überwiegen zu Gunsten des Identitätsschutzes ableitbar. Im Gegenteil: Aus dem Regel-Ausnahme-Verhältnis des Art. 15 DS-GVO folgt, dass in Zweifelsfragen das Recht auf Datenauskunft überwiegt. Darüber können sich die Vorgaben des HinSchG nicht hinwegsetzen. Eine Vertraulichkeitszusage führt nur ausnahmsweise zu einem Überwiegen des Identitätsschutzes. Zu beachten ist, dass das berechtigte Interesse des Whistleblowers bereits aus §§ 8, 9 HinSchG, unabhängig vom Vorliegen einer Vertraulichkeitszusage, besteht und sich die Vertraulichkeitszusage auch nicht über § 9 Abs. 1 HinSchG hinwegsetzen kann. Für ein Überwiegen des Identitätsschutzes kann im Einzelfall sprechen, dass die Meldung ohne die zugesicherte Vertraulichkeit nicht erfolgt wäre und der Arbeitgeber den Whistleblower nachweislich zur Meldung überredet hat. Maßgeblich sind die Umstände des Einzelfalls. Überwiegt der

Identitätsschutz, sind die entsprechenden Passagen zu schwärzen bzw. anderweitig unkenntlich zu machen.

cc) Möglichkeiten zur Erhöhung des Identitätsschutzes

Ein möglicher Anreiz für das Vertrauen des Whistleblowers in die Funktionsfähigkeit der internen Meldestelle bildet der Identitätsschutz. Sowohl der Unionsgesetzgeber als auch der nationale Gesetzgeber betonen die Bedeutung des Identitätsschutzes im Bereich des Whistleblowings und stellen es zu Recht als dasjenige Kriterium dar, das mitausschlaggebend für die Meldung sein kann.[800] Die vorherigen Ausführungen haben jedoch gezeigt, dass die Informationspflicht nur eingeschränkt entfällt. Voraussetzung ist, dass die von der Meldung betroffene Person als (Mit-) Täter einer Straftat benannt worden ist und die begründete Annahme besteht, die Kenntnis von der Identität des Whistleblowers werde dazu genutzt, um auf ihn als möglichen Zeugen einzuwirken, seine Meldung zu revidieren.[801] Auch mit Blick auf das Auskunftsrecht besteht eine große Rechtsunsicherheit. Die Vorgaben der §§ 8, 9 HinSchG können keinen pauschalen Vorrang des Identitätsschutzes im Rahmen der Interessenabwägung gemäß Art. 15 Abs. 4 DS-GVO bewirken. Der nationale Gesetzgeber hat es sich insofern mit seinem pauschalen Hinweis auf § 29 Abs. 1 S. 1 und S. 2 BDSG im Rahmen der Gesetzesbegründung zu leicht gemacht und ist seinem eindeutigen Regelungsauftrag in Erwägungsgrund 85 Whistleblowing-RL nicht nachgekommen.[802] Dies ist besonders misslich, da die Vorgaben der §§ 8, 9 HinSchG dem Whistleblower suggerieren, es bestünde nahezu schrankenloser Identitätsschutz. Stellt sich dann jedoch heraus, dass dem gar nicht so ist, kann die

---

800 BT-Drs. 20/5992, S. 58; BRAK, Stellungnahme zum HinSchG-E, S. 5.

801 Vgl. Art. 14 Abs. 5 lit. b) DS-GVO bzw. Art. 23 Abs. 1 DS-GVO i. V. m. § 33 Abs. 1 Nr. 2 lit. a) BDSG.

802 Die Whistleblowing-RL führt den Erwägungsgrund 153 DS-GVO fort: „*Die Mitgliedstaaten sollten daher Gesetzgebungsmaßnahmen zur Regelung der Abweichungen und Ausnahmen erlassen, die zum Zwecke der Abwägung zwischen diesen Grundrechten notwendig sind. Gemeint ist u. a. das Recht auf freie Meinungsäußerung*“.

Streuwirkung eines einzigen Falls andere Whistleblower dazu veranlassen, von einer internen Meldung abzusehen.

Vor diesem Hintergrund stellt sich die Frage, inwieweit es Beschäftigungsgebern möglich ist, Whistleblowern zusätzlichen Identitätsschutz zu gewähren, um die Versäumnisse des nationalen Gesetzgebers aufzuholen. Zur Erhöhung des Identitätsschutzes kommen ein Verzicht auf die Betroffenenrechte, die Einschaltung einer externen Ombudsperson sowie der Abschluss einer Betriebsvereinbarung zum Identitätsschutz des Whistleblowers in Betracht.[803] Die Einrichtung eines anonymen Meldekanals hilft in der Regel nicht viel weiter, als nach wie vor Rückschlüsse auf die Identität möglich bleiben.

(1) Verzicht auf die Betroffenenrechte

Fraglich ist, ob sich der Arbeitgeber zur Erhöhung des Identitätsschutzes eine Verzichtserklärung seiner Beschäftigten einholen kann, in denen diese auf ihre Betroffenenrechte in Bezug auf Datenverarbeitungen innerhalb des Hinweisgeberschutzsystems verzichten. Zu beachten ist, dass die DS-GVO keine Dispositionsbefugnis über die Betroffenenrechte kennt. Darüber hinaus würde eine Verzichtserklärung dem Telos der DS-GVO zuwiderlaufen.[804] Sinn und Zweck der DS-GVO ist es, den von einer Datenverarbeitung betroffenen Personen die Überprüfung der Datenverarbeitung zu ermöglichen. Hintergrund ist, dass die Datenverarbeitung das Recht der informationellen Selbstbestimmungsfreiheit (Art. 2 Abs. 1, Art. 1 Abs. 1 GG) der von der Datenverarbeitung betroffenen Person tangiert und daher nur gerechtfertigt ist, soweit die Datenverarbeitung unter Einhaltung der in Art. 5 DS-GVO normierten Grundsätze erfolgt. Die Betroffenenrechte in Art. 12 ff. DS-GVO stellen insofern eine Ausprägung des Transparenzgrundsatzes dar (Art. 5 Abs. 1 lit. a) DS-GVO). Sie sollen - in Gestalt der Informationspflicht und dem Auskunftsrecht - der von

[803] Vgl. *Mohn*, NZA 2022, 1159, 1161, 1164.
[804] Rechtsrahmen und Funktion der Datenauskunft siehe: Kapitel C) I. 1. a).

der Datenverarbeitung betroffenen Person ermöglichen, von der Datenverarbeitung zu erfahren, um diese auf Rechtmäßigkeit zu prüfen und ggf. daran anschließend weitere Rechte geltend machen zu können.[805] Ohne Kenntnis von der Datenverarbeitung ist die Frage der Rechtmäßigkeit jedoch nicht beantwortbar, respektive durchsetzbar. Damit ist die Kenntnis von der Datenverarbeitung notwendige Voraussetzung zur Gewährleistung des informationellen Selbstbestimmungsrechts.

Nicht entschieden ist weiterhin, ob eine von der Datenverarbeitung betroffene Person auf ihre Betroffenenrechte verzichten kann. Die Situation erinnert an die Einwilligung in eine Datenverarbeitung als datenschutzrechtliche Legitimationsgrundlage Art. 6 Abs. 1 lit. a) DS-GVO, wobei im Beschäftigtenkontext Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 2 BDSG zu beachten sind. Hervorzuheben ist, dass die Einwilligung in eine Datenverarbeitung einer Wirksamkeitsprüfung anhand des Kriteriums der Freiwilligkeit unterliegt, Art. 7 Abs. 4 DS-GVO, § 26 Abs. 2 BDSG. Eine solche Freiwilligkeit kann im Beschäftigungskontext aufgrund des hierarchischen Machtgefälles zwischen Arbeitgeber und Arbeitnehmer nur in Ausnahmefällen angenommen werden.[806] Bittet der Arbeitgeber den Arbeitnehmer um eine Verzichtserklärung, kommt diese Bitte aufgrund des Machtungleichgewichts in ihrer Wirkung einer Aufforderung an den Arbeitnehmer gleich. Dies spricht gegen die Freiwilligkeit einer Verzichtserklärung im Sinne der Art. 7 Abs. 4 DS-GVO, § 26 Abs. 4 BDSG. Zu beachten ist ferner, dass sich die Einwilligung in eine Datenverarbeitung und die Verzichtserklärung in Bezug auf die Betroffenenrechte in einem wesentlichen Punkt unterscheiden: Während die Einwilligung in eine Datenverarbeitung dem Arbeitnehmer zugleich offenbart, dass eine Datenverarbeitung stattfinden soll, bleibt die Datenverarbeitung - sollte sie vorgenommen werden - dem Arbeitnehmer im Falle einer

---

805 Siehe ebenfalls: Kapitel C) I. 1. a).

806 *Riesenhuber*, in: BeckOK-DatenschutzR, § 26 BDSG Rn.47; vgl. auch: *Schulz*, in: Gola/Heckmann, DS-GVO, Art. 7 Rn.35; *Buchner*/*Kühling*; in: Kühling/Buchner, DS-GVO, Art. 7 Rn.31.

Verzichtserklärung verborgen. Die von der Datenverarbeitung betroffene Person kann nicht abschätzen, ob und inwieweit ihre Daten verarbeitet werden. Vor diesem Hintergrund sind an die Voraussetzungen einer Verzichtserklärung höhere Anforderungen zu stellen, als die Wirksamkeit einer Einwilligung erfordert. Da jedoch schon die Voraussetzungen der Freiwilligkeit einer Einwilligung in Bezug auf die Abgabe einer Verzichtserklärung nicht vorliegen, kann der Verzicht eines Arbeitnehmers den damit einhergehenden Eingriff in die informationelle Selbstbestimmungsfreiheit (erst-recht) nicht rechtfertigten. Nach alledem ist eine Verzichtserklärung hinsichtlich der Betroffenenrechte im Beschäftigungskontext nach hiesiger Auffassung nicht möglich.[807]

(2) Einschaltung einer externen Ombudsperson

Die Einschaltung einer externen Ombudsperson, insbesondere in Form eines externen Rechtsanwalts, ist zur Erhöhung des Identitätsschutzes geeignet.[808] Aufgrund des anwaltlichen Berufsgeheimnisses (§ 43a Abs. 2 BRAO sowie § 203 StGB) wird die Ausnahmeregelung des Art. 14 Abs. 5 lit. d) DS-GVO aktiviert.[809] Zu beachten ist jedoch, dass dies nur so lange gilt, wie die externe Ombudsstelle die Daten bei sich behält. Erfordern etwaige Folgemaßnahmen die Übermittlung der Identität des Hinweisgebers an den Beschäftigungsgeber, verbleibt es bei den oben gefundenen Ergebnissen. Maßgeblich ist auch, dass die externe Ombudsstelle nach den Vorgaben der DS-GVO als

807 Ebenso: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 373 f.; *Franck*, in: Gola/Heckmann, DS-GVO, Art. 15 Rn.27; *Burger*, öAT 2021, 221, 222; *Sorber*, BC 2021, 342, 345.

808 BT-Drs. 20/3442, S. 79.

809 *Henssler*, in: Henssler/Prütting, BRAO, § 43 Rn.48; *Buchert*/*Buchert*, ZWH 2019, 212, 214; *Baranowski*/ *Pant*, CCZ 2018, 250, 251 ff.

datenschutzrechtlich Verantwortlicher gilt.[810] Ist der Beschäftigungsgeber nicht selbst datenschutzrechtlich verantwortlich, unterliegt er dementsprechend auch nicht der Informationspflicht bzw. dem Recht auf Datenauskunft. Dies gilt jedoch nur, soweit keine gemeinsame Verantwortlichkeit (Art. 26 DS-GVO) oder Auftragsverarbeitung (Art. 28 DS-GVO) vorliegt.[811]

(3) Betriebsvereinbarung zur Erhöhung des Identitätsschutzes

Es bedarf einer Klärung, ob sich die Betriebsparteien zur Erhöhung des Identitätsschutzes des Whistleblowers auf eine Betriebsvereinbarung einigen können, die z. B. eine Beschränkung der datenschutzrechtlichen Betroffenenrechte nach Maßgabe der §§ 8, 9 HinSchG vorsieht. Anknüpfungspunkte für eine solche Beschränkung bilden Art. 14 Abs. 5 lit. c) DS-GVO und Art. 23 Abs. 1 lit. i) DS-GVO sowie Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 4 BDSG, die im Folgenden analysiert werden.

Hinsichtlich der Beschränkung der Informationspflicht ist zunächst zu bedenken, dass Betriebsvereinbarungen keine „*Rechtsvorschriften*“ im Sinne des Art. 14 Abs. 5 lit. c) DS-GVO sind. Im Gegensatz zu Rechtsvorschriften der Union oder der Mitgliedstaaten haben Betriebsvereinbarungen kein formales, parlamentarisches Gesetzgebungsverfahren durchlaufen. Ihnen wird daher auch keine Einschätzungsprärogative zuteil, wie sie dem (Unions-) Gesetzgeber zugesprochen wird. Gleiches gilt in Bezug auf eine Beschränkung der Betrof-

---

[810] Zur Abgrenzung der datenschutzrechtlich verantwortlichen Stelle zur Auftragsverarbeitung und Gemeinsamen Verantwortlichkeit: *Haak*/*Spittka*, CB 2023, 356-360, die zutreffend darauf hinweisen, dass die Abgrenzung anhand der DS-GVO erfolgt. Vgl. auch: BT-Drs. 20/3442, S. 79 f.; *Rüdiger*/*Adelberg*, K&R 2023, 172.

[811] Von einer Auftragsverarbeitung ist auszugehen, wenn die Ombudsperson lediglich als externes Postfach eingerichtet ist und sämtliche Meldungen ungeprüft an den Beschäftigungsgeber weiterleitet, vgl. *Schröder*, in: Forgó/Helfrich/Schneider, Teil VI, Kapitel 3 Rn.63; *Plath*, in: Plath, DS-GVO, Art. 28 Rn.56.

fenenrechte über die Öffnungsklausel des Art. 23 Abs. 1 lit. i) DS-GVO. Auch Art. 23 Abs. 1 lit. i) DS-GVO setzt eine „*Rechtsvorschrift*“ voraus.

Die Betriebsvereinbarung kann mangels planwidriger Regelungslücke auch nicht in analoger Anwendung in Art. 23 Abs. 1 lit. i) DS-GVO hineingelesen werden. Zwar könnte sich eine vergleichbare Interessenlage daraus ableiten lassen, dass Betriebsvereinbarungen als Vereinbarungen zwischen den Betriebsparteien normative Wirkkraft zuteilwird und demnach - ähnlich wie ein Gesetz - normativ auf das Arbeitsverhältnis einwirken, § 77 Abs. 4 S. 1 BetrVG. Es fehlt jedoch an der Regelungslücke: Art. 88 Abs. 1 DS-GVO enthält bereits eine Öffnungsklausel für spezifischere Vorgaben im Beschäftigungskontext, die neben Rechtsvorschriften auch Kollektivvereinbarungen sein können. Es ist anerkannt, dass Betriebsvereinbarungen zu den Kollektivvereinbarungen im Sinne des Art. 88 Abs. 1 DS-GVO zählen.[812] Der Unionsgesetzgeber hat daher der besonderen Bedeutung der Betriebsvereinbarung als paritätische Vereinbarung mit normativer Wirkkraft im Beschäftigungskontext über Art. 88 Abs. 1 DS-GVO Geltung verliehen. Die Verortung innerhalb des Art. 88 Abs. 1 DS-GVO überzeugt, da Betriebsvereinbarungen dem Beschäftigungskontext zuordbar sind. Insofern ist es nachvollziehbar, dass der Unionsgesetzgeber diese nicht im Rahmen der allgemeinen Regelungen aufführt.[813] Folgerichtig kommt es darauf an, ob es den Betriebs-

---

[812] Vgl. Erwägungsgrund 155 DS-GVO; *Riesenhuber*, in: BeckOK-DatenschutzR, Art. 88 Rn.51; *Kort*, DB 2016, 711; *Taeger*/*Rose,* BB 2016, 819, 821 f.; *Wybitul*/*Sörup*/*Pötters*, ZD 2015, 559, 561.

[813] Grundsätzlich ist von einem Nebeneinander der Öffnungsklauseln auszugehen. So auch: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 152; *Bienemann*, in: Sydow/Marsch, DS-GVO, Art. 15 Rn.86; *Franzen*, in: EuArRK, Art. 15 DS-GVO Rn.8; *Riesenhuber*, in: BeckOK-DatenschutzR, Art. 88 DS-GVO Rn.98; *Stollhoff*, in: Auernhammer, DS-GVO, Art. 15 Rn.50; *Thüsing*/*Traut*, in: SJTK, Art. 88 DS-GVO Rn.34 ff.; *Franzen*, NZA 2020, 1593 ff.; *Schantz*, NJW 2016, 1841, 1842; *Wünschelbaum*, BB 2019, 2102 ff. und LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, 242 Rn.172.

parteien nach Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 4 BDSG möglich ist, eine Beschränkung der datenschutzrechtlichen Betroffenenrechte nach Maßgabe der §§ 8, 9 HinSchG zu regeln.

Zunächst ist festzustellen, dass Art. 88 Abs. 1 DS-GVO nicht auf spezifischere Vorschriften begrenzt ist, deren Regelungsgegenstand eine Rechtsgrundlage für eine Datenverarbeitung bildet.[814] Dafür spricht, dass auch die Erfüllung der Informationspflicht bzw. der Datenauskunft eine Datenverarbeitung (Art. 4 Nr. 2 DS-GVO) darstellt.[815] Geht es beispielsweise darum, die Identität des Whistleblowers offenzulegen, handelt es sich um eine Weitergabe eines personenbezogenen Datums, die eine Datenverarbeitung darstellt.[816] Hinzu kommt, dass spezifischere Vorschriften hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten die einer jeden Datenverarbeitung immanenten Grundsätze der Datenverarbeitung (Art. 5 DS-GVO) stets mit umfassen.[817] Der Grundsatz der Datentransparenz wohnt jeder Datenverarbeitung inne, Art. 5 Abs. 1 lit. a) DS-GVO. Vor diesem Hintergrund sind die Betroffenenrechte „*Bestandteil einer transparenten Verarbeitung*“.[818] Folgerichtig können spezifischere Vorschriften im Sinne des Art. 88 Abs. 1 DS-GVO auch Transparenzvorgaben hinsichtlich der Betroffenenrechte sein.

---

[814] A. A.: *Lembke*, in: HWK, Art. 88 DS-GVO Rn.6; *Lembke*, NJW 2020, 1841, 1845 f.; *Schulte*/*Welge*, NZA 2019, 1110, 1115. Siehe auch: Kapitel C) I. 3. a) bb) (1).

[815] BGH, Urteil v. 22.02.2022 - VI ZR 14/21, BeckRS 2022, 5496 Rn.19; OLG Köln, Urteil v. 14.07.2022 - 15 U 137/21, GRUR-RS 2022, 17897 Rn.14; *Bienemann*, in: Sydow/Marsch, DS-GVO, Art. 15 Rn.42.

[816] In Bezug auf die Datenauskunft nach Art. 15 DS-GVO: BGH, Urteil v. 22.02.2022 - VI ZR 14/21, BeckRS 2022, 5496 Rn.19; OLG Köln, Urteil v. 14.07.2022 - 15 U 137/21, GRUR-RS 2022, 17897 Rn.14; *Bienemann,* in: Sydow/Marsch, DS-GVO, Art. 15 Rn.42; *Arens*, NJW 2021, 3417, 3418; *Paal*/*Nikol*, CB 2022, 466, 469; a. A.: LG Bonn, Urteil v. 01.07.2021 - 16 O 128/20 Rn.35.

[817] *Peisker* zu Art. 15 DS-GVO: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 152.

[818] *Peisker* zu Art. 15 DS-GVO: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 152.

Allerdings können spezifischere Vorschriften nur solche sein, die die Vorgaben des Art. 88 Abs. 2 DS-GVO wahren.[819] Dies geht auch aus dem Verweis in § 26 Abs. 4 S. 2 BDSG hervor. Art. 88 Abs. 1 DS-GVO ist daher in Zusammenhang mit Art. 88 Abs. 2 DS-GVO zu verstehen. Dies hat der EuGH jüngst bestätigt.[820] Laut EuGH sei Art. 88 Abs. 1 DS-GVO dahingehend auszuglegen, dass eine nationale Rechtsvorschrift keine „*spezifischere Vorschrift*" sei, wenn sie nicht die Vorgaben von Art. 88 Abs. 2 DS-GVO erfülle.[821] Dieses Verständnis ist auf Kollektivvereinbarungen respektive Betriebsvereinbarungen übertragbar. Nötig ist, dass die Betriebsvereinbarung als spezifischere Vorschrift geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Datenverarbeitung enthält. Gemeint sind damit Vorgaben, die die Rechte der von der Datenverarbeitung betroffenen Person achtet und sicherstellt, dass der Grundsatz der Datentransparenz nach Art. 5 Abs. 1 lit. a) DS-GVO hinreichend besteht. Eine Betriebsvereinbarung darf richtigerweise die allgemeinen Grundsätze der Datenverarbeitung nicht unterlaufen (Art. 5 und Art. 6 DS-GVO).[822]

Die Grundsätze der Datenverarbeitung bilden folgerichtig einen Mindestschutz für die Verarbeitung personenbezogenen Daten im Beschäftigungskontext, wobei die Betriebsparteien in ihrer konkreten Ausgestaltung frei bleiben, diesen Mindestschutz im Rahmen der Betriebsvereinbarung zu verankern. Maßgeblich ist, dass das Schutzniveau, welches durch die Grundsätze der Datenverarbeitung vorge-

---

819 EuGH, Urteil v. 30.03.2023 - C-34/21 Rn.81-83.

820 EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.85.

821 EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.85.

822 Vgl. EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.85. Damit hat der EuGH die bis dahin im Schrifttum viel diskutierte Frage beantwortet, inwieweit „*spezifischere Vorschriften*" nach Art. 88 Abs. 1 DS-GVO das Schutzniveau der DS-GVO absenken dürfen. So bereits: *Thüsing*/*Granetzny*, in: Compliance, § 4 Rn.15 und *Wünschelbaum,* BB 2019, 2102, 2106.

ben wird, nicht unterlaufen wird.[823] Dieses Verständnis überzeugt, weil auf die Art ein einheitliches Datenschutzniveau innerhalb der Europäischen Union gewährleistet ist, ohne dass den Betriebsparteien der gebotene Handlungsspielraum genommen wird, den es insbesondere im Beschäftigungskontext braucht.[824]

Unter Berücksichtigung der soeben aufgezeigten Maßgaben, sind eigenständige Regelungen der Betriebsparteien in Bezug auf den Identitätsschutz des Whistleblowers möglich. Voraussetzung ist, dass die Grundsätze der Datenverarbeitung in Art. 5 und Art. 6 DS-GVO nicht unterlaufen werden. Erwägungsgrund 11 DS-GVO formuliert in diesem Zusammenhang, dass ein unionsweiter wirksamer Schutz eine präzise Festlegung der Rechte der betroffenen Person erfordert. Dem Telos der Datentransparenz entsprechend kommt es folgerichtig darauf an, ob die Betriebsvereinbarung Maßnahmen vorsieht, die sicherstellen, dass die von der Meldung betroffene Person hinreichend Kenntnis über die Datenverarbeitung ihrer personenbezogenen Daten erlangt, um die Rechtmäßigkeit der Datenverarbeitung zu prüfen und ggf. durchzusetzen, sollte diese nicht gegeben sein.[825] Eine Orientierung, wie dies in Bezug auf eine mögliche Beschränkung der Betroffenenrechte rechtssicher gelingen kann, bieten die Mindestvorgaben

---

[823] Vgl. *Thüsing/Granetzny*, in: Compliance, § 4 Rn.15, die darauf hinweisen, dass die Grundprinzipien der DS-GVO nicht unterlaufen werden dürfen. Vgl. auch: *Wünschelbaum,* BB 2019, 2102, 2106.

[824] Zu der im Schrifttum breit diskutierten Frage, ob und inwieweit Abweichungen vom Schutzniveau der DS-GVO über Art. 88 Abs. 1, Abs. 2 DS-GVO möglich sind. Siehe ausführlicher: Kapitel C) I. 3. c) bb) (1) (c), dort: Fn.716.

[825] Zur Funktion der Datenauskunft siehe auch: Kapitel C) I. 1. a).

in Art. 23 Abs. 2 DS-GVO.[826] Nötig dürfte insbesondere eine Bezugnahme auf diejenigen Betroffenenrechte sein, die durch die Betriebsvereinbarung eine Beschränkung erfahren.[827] Möglich wäre z. B. auch eine zeitlich verzögerte Informationspflicht bzw. Datenauskunft. Soweit eine Betriebsvereinbarung die vorstehenden Maßstäbe wahrt, ist eine Beschränkung der datenschutzrechtlichen Betroffenenrechte auch nach Maßgabe der §§ 8, 9 HinSchG möglich. Eine pauschale Regelung, wonach die Betroffenenrechte nicht bestehen sollen, sobald der Identitätsschutz nach §§ 8, 9 HinSchG greift, genügt allerdings nicht.

dd) Zwischenergebnis

Unternehmen können sich auch im Falle einer internen Meldepflicht nicht sicher sein, dass Informationen über Missstände intern bleiben. Sie bleiben deshalb weiterhin aufgefordert, Anreize dafür zu schaffen, dass ein Whistleblower so viel Vertrauen in die Funktionsfähigkeit und Wirksamkeit eines internen Meldekanals hegt, dass er freiwillig von einer externen Meldung absieht. Ein möglicher Anreiz für das Vertrauen des Whistleblowers in die Funktionsfähigkeit der internen

---

826 Es ist nicht fernliegend, Art. 88 Abs. 1 DS-GVO als lex specialis zu Art. 23 Abs. 1 DS-GVO anzusehen. Diese Frage kann jedoch dahinstehen, da beide Öffnungsklauseln sicherstellen, dass die datenschutzrechtlichen Grundsätze in Art. 5 und Art. 6 DS-GVO im Sinne eines Mindestschutzes nicht unterlaufen werden dürfen. Richtig ist, dass Art. 23 DS-GVO die Beschränkungen der Betroffenenrechte in den Blick nimmt, während Art. 88 DS-GVO Beschränkungen im Beschäftigungskontext regelt, zu denen auch Transparenzvorgaben zählen können. Grundsätzlich ist daher von einem Nebeneinander der Öffnungsklauseln auszugehen. So auch: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 152; *Bienemann*, in: Sydow/Marsch, DS-GVO, Art. 15 Rn.86; *Franzen*, in: EuArbRK, Art. 15 DS-GVO Rn.8; *Riesenhuber*, in: BeckOK-DatenschutzR, Art. 88 DS-GVO Rn.98; *Stollhoff*, in: Auernhammer, DS-GVO, Art. 15 Rn.50; *Thüsing/Traut*, in: SJTK, Art. 88 DS-GVO Rn.34 ff.; *Franzen*, NZA 2020, 1593 ff.; *Schantz*, NJW 2016, 1841, 1842; *Wünschelbaum*, BB 2019, 2102 ff.; LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, 242 Rn.172.

827 Vgl. *Sörup,* ArbRAktuell, 2016, 207, 208 f.; *Wybitul,* ZD 2016, 203, 207.

Meldestelle bildet der Identitätsschutz. Datenschutzrechtliche Informationspflichten und Auskunftsrechte können allerdings dazu führen, dass die von der Datenverarbeitung betroffene Person Kenntnis von der Identität des Hinweisgebers erhält. Damit geht die Gefahr einer nachhaltigen Störung des Betriebsfriedens einher, insbesondere wenn die von der Meldung betroffene Person als (Mit-) Täter einer Straftat bzw. Ordnungswidrigkeit und nicht bloß als Zeuge im Kontext eines möglichen betrieblichen Vorfalles benannt worden ist und der Hinweisgeber ein Kollege der von der Meldung betroffenen Person ist. Es ist daher richtig, dass der nationale Gesetzgeber den Identitätsschutz als ein für eine interne Meldung ausschlaggebendes Kriterium nennt. In diesem Kontext kann der Identitätsschutz als Ausprägung des informationellen Selbstbestimmungsrechts des Hinweisgebers verstanden werden. Der Hinweisgeber entscheidet, unter welchen Voraussetzungen er ein Hinweisgebersystem nutzt und Informationen meldet, die gegebenenfalls Rückschlüsse auf seine Identität ermöglichen.

Aus Unternehmenssicht kommen verschiedene Möglichkeiten in Betracht, den Identitätsschutz zu erhöhen. Eine Verzichtserklärung in Bezug auf die Betroffenenrechte scheidet im Beschäftigungskontext jedoch aus. Bittet der Arbeitgeber den Arbeitnehmer um eine Verzichtserklärung, kommt diese Bitte aufgrund des Machtungleichgewichts in ihrer Wirkung einer Aufforderung an den Arbeitnehmer gleich. Dies spricht gegen die Freiwilligkeit einer Verzichtserklärung, zieht man die Maßstäbe der Einwilligung heran. Zu beachten ist allerdings, dass die Anforderungen an eine Verzichtserklärung höhere sind als diejenigen, die an die Wirksamkeit einer Einwilligung zu stellen sind. Da es jedoch schon an den Wirksamkeitsvoraussetzungen einer Einwilligung scheitert, folgt daraus erst-recht die Unzulässigkeit eines Verzichts auf die datenschutzrechtlichen Betroffenenrechte im Beschäftigungskontext.

Dagegen ist die Einschaltung einer externen Ombudsperson, insbesondere in Form eines externen Rechtsanwalts, zur Erhöhung des

Identitätsschutzes geeignet. Aufgrund des anwaltlichen Berufsgeheimnisses (§ 43a Abs. 2 BRAO sowie § 203 StGB) wird die Ausnahmeregelung des Art. 14 Abs. 5 lit. d) DS-GVO aktiviert. Dies gilt allerdings nur bis zu dem Zeitpunkt, bis die externe Ombudsstelle die Daten an den Arbeitgeber für etwaige Folgemaßnahmen weiterleitet. Maßgeblich ist auch, dass die externe Ombudsstelle nach den Vorgaben der DS-GVO selbst datenschutzrechtlich Verantwortlicher sein muss.

Daneben kommen Betriebsvereinbarungen zur Erhöhung des Identitätsschutzes in Betracht. Öffnungsklausel hierfür ist Art. 88 Abs. 1 und Abs. 2 DS-GVO i. V. m. § 26 Abs. 4 BDSG. Eine Betriebsvereinbarung darf die allgemeinen Grundsätze der Datenverarbeitung nicht unterlaufen (Art. 5, Art. 6 DS-GVO). Diese bilden einen Mindestschutz für die Verarbeitung personenbezogener Daten im Beschäftigungskontext, wobei die Betriebsparteien in ihrer konkreten Ausgestaltung frei bleiben, diesen Mindestschutz im Rahmen der Betriebsvereinbarung zu verankern. Dem Telos der Datentransparenz entsprechend kommt es darauf an, ob die Betriebsvereinbarung Maßnahmen vorsieht, die sicherstellen, dass die von einer Meldung betroffene Person die Rechtmäßigkeit der Datenverarbeitung hinreichend prüfen und ggf. durchsetzen kann. Soweit eine Betriebsvereinbarung die vorstehenden Maßstäbe wahrt, ist eine Beschränkung der datenschutzrechtlichen Betroffenenrechte auch nach Maßgabe der §§ 8, 9 HinSchG möglich. Eine pauschale Regelung, wonach die Betroffenenrechte nicht bestehen, sobald der Identitätsschutz nach §§ 8, 9 HinSchG greift, genügt jedoch nicht.

d) Zusammenfassender Überblick

Die Geschäftsleitung ist gesellschaftsrechtlich dazu verpflichtet, sicherzustellen, dass bei der Meldung von Geschäftsgeheimnissen im Rahmen des § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG aus der

Prüfobliegenheit ein Vorrang des internen Meldewegs resultiert.[828] Dies gelingt durch die Implementierung eines wirksamen Hinweisgeberschutzsystems, von dem der Whistleblower hinreichenden Grund zu der Annahme hat, dass dieses zur Beseitigung des Missstands geeignet ist, ohne dass ihm durch die Meldung Repressalien drohen. Insofern ist die Implementierung eines wirksamen Hinweisgeberschutzsystems auch als Geheimhaltungsmaßnahme im Sinne des § 2 Nr. 1 lit. b) GeschGehG werten.

Um das Unternehmen vor einem Reputationsverlust und weiteren Schäden in Folge des Bekanntwerdens sensibler Informationen hinreichend zu schützen, die noch keine Geschäftsgeheimnisse sind, ist die Geschäftsleitung ebenfalls verpflichtet, darauf hinzuwirken, dass ein Whistleblower sich für einen internen Meldeweg entscheidet. Das Unternehmen wird die Missstände beseitigen und die dazugehörigen Informationen mittels den Umständen nach angemessenen Geheimhaltungsmaßnahmen in den Schutzbereich des GeschGehG überführen, um dessen erhöhten Schutz nach § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG zu erreichen. Dafür hat die Unternehmensleitung Anreize zu schaffen, dass Whistleblower einen internen Meldekanal bevorzugen. Zugleich ist die Förderung von Hinweisen aus der eigenen Belegschaft probates Mittel, um sicherzustellen, dass das Unternehmen im Einklang mit der geltenden Rechtsordnung handelt (sog. „*Legalitätspflicht*“).

Neben der Schaffung anonymer Meldekanäle und Maßnahmen zur Erhöhung des Identitätsschutzes kommen insbesondere berufliche und finanzielle Anreize in Betracht. Die Geschäftsleitung darf den Whistleblower allerdings nicht zur vorrangigen Nutzung eines internen Meldewegs verpflichten.[829] Vereinbarungen, die eine solche Pflicht vorsehen, sind unwirksam, § 39 HinSchG, § 134 BGB. Hintergrund ist, dass § 7 Abs. 1 S. 1 HinSchG dem Hinweisgeber das Recht gewährt,

---

[828] Zur Herleitung der (Prüf-) Obliegenheit siehe: Kapitel C) I. 2. b).
[829] Siehe: Kapitel C) I. 3. a).

zwischen einer internen Meldung und einer externen Meldung zu wählen. Dieses Recht ist im Sinne eines unabdingbaren Zugangsrechts zu den externen Meldestellen zu verstehen. Darüber kann sich das gesellschaftsrechtliche Pflichtenprogramm der Geschäftsleitung nicht hinwegsetzen. Ein Vorrang einer internen Meldung ergibt sich auch nicht aus § 17 Abs. 2 S. 1 ArbSchG. Auch danach bleibt dem Whistleblower der Weg zu den externen Meldestellen nicht verwehrt.

Im Ergebnis ist eine interne Meldepflicht in Bezug auf Informationen, die (noch) keine Geschäftsgeheimnisse sind, nur möglich, sofern dem Whistleblower der Zugang zum externen Meldeweg erhalten bleibt.[830] Aus Transparenzgründen ist der Whistleblower auf diesen Umstand hinzuweisen, § 307 Abs. 1 S. 2 BGB. Eine Pflicht zur internen Meldung unterliegt einer strengen Wirksamkeitskontrolle. Insbesondere muss die Klausel hinreichend bestimmt sein und darf den Whistleblower nicht unangemessen benachteiligen, § 307 Abs. 1 BGB. Voraussetzung ist die Implementierung eines wirksamen Hinweisgeberschutzsystems. Ein Whistleblower, der infolge einer Meldung Repressalien zu fürchten hätte, wäre unangemessen benachteiligt, wäre er verpflichtet, sich diesen Repressalien auszusetzen, § 307 Abs. 1 S. 1 BGB. Gleiches gilt mit Blick auf den Identitätsschutz, vgl. §§ 8, 9 HinSchG. Eine interne Meldepflicht tangiert den Whistleblower in seinem Recht auf negative Meinungsfreiheit. Maßgeblich ist deshalb ein Interessenausgleich zwischen dem Interesse des Beschäftigungsgebers an der Aufdeckung des Missstands und der negativen Meinungsfreiheit des Whistleblowers. Auch mögliche Gewissenskonflikte sind mitzudenken. Darüber hinaus können Interessen Dritter zum Tragen kommen, beispielsweise wenn es darum geht, andere vor Gefahren zu schützen. Nötig sind Konkretisierungen hinsichtlich des objektiven Verdachtsgrads und des Schweregrads eines Missstands, die es vermögen, den Eingriff in das Recht auf negative Meinungsfreiheit zu rechtfertigen. Hinsichtlich des Schweregrads des Missstands gilt die Regel: Je schwerer und gewichtiger der Missstand, desto eher

[830] Gleiches gilt im Hinblick auf das Recht zur Offenlegung, § 32 HinSchG.

überwiegen die Interessen des Unternehmens an dessen Beseitigung. Hier bietet sich beispielsweise eine enumerative Auflistung von Straf- oder Bußgeldtatbeständen an. Orientierung bietet auch § 16 Abs. 1 ArbSchG. Hinsichtlich der Konkretisierung des objektiven Verdachtsgrads kommen umschreibende Formulierungen wie „*bergründete Verdachtsmomente*“, „*hohe Wahrscheinlichkeit*“ oder „*objektive Anhaltspunkte*“ in Betracht. Dagegen dürfte die Formulierung eines „*einfachen Verdachts*“ aufgrund deren Unbestimmtheit und der besonderen Interessenlage regelmäßig nicht ausreichen. Maßgeblich sind die Umstände des Einzelfalls.[831]

Da Unternehmen auch in Fällen einer internen Meldepflicht nicht abgesichert sind, dass Informationen über Missstände intern bleiben und nicht extern gemeldet werden, müssen sie Anreize dafür schaffen, dass ein Whistleblower so viel Vertrauen in die Funktionsfähigkeit und Wirksamkeit der internen Meldestelle hegt, dass er freiwillig von einer externen Meldung absieht. Ein möglicher Anreiz für das Vertrauen des Whistleblowers in die Funktionsfähigkeit der internen Meldestelle bildet der Identitätsschutz. Das HinSchG normiert dem Grunde nach einen weitreichenden Identitätsschutz, vgl. §§ 8, 9 HinSchG. In der Praxis dürfte die Ausnahme des § 9 Abs. 1 HinSchG nur in eng begrenzten Ausnahmekonstellationen greifen.[832] Kommt es allerdings zu einer Kollision des Identitätsschutzes mit den datenschutzrechtlichen Betroffenenrechten, sehen sich Unternehmen mit einer hohen Rechtsunsicherheit konfrontiert. Die Auflösung der mehrdimensionalen Interessenkonflikte birgt ein fortwährendes Risiko.

Kommt der Arbeitgeber den Betroffenenrechten nur unzureichend nach, drohen empfindliche Bußgelder nach Art. 83 Abs. 5 lit. b) DS-GVO. Offenbart er hingegen in unzulässiger Weise die Identität des Hinweisgebers, drohen ebenfalls Bußgelder, vgl. § 40 Abs. 3 HinSchG. Darüber hinaus besteht die Gefahr, dass potenzielle

831 Siehe: Kapitel C) I. 3. b).
832 Siehe: Kapitel C) I. 3. c) aa).

Whistleblower von einer internen Meldung Abstand nehmen, sobald sie von den tatsächlichen Rechtsunsicherheiten im Bereich des Identitätsschutzes erfahren. Ursache dafür ist, dass dem nationalen Gesetzgeber die Auflösung dieses Spannungsverhältnisses missglückt ist. Ein pauschaler Hinweis im Rahmen der Gesetzesbegründung auf Normen des BDSG, die nach hiesiger Auffassung unionsrechtswidrig sind, setzt sich über den eindeutigen Regelungsauftrag des Unionsgesetzgebers hinweg, für die nötige Rechtssicherheit in diesem Bereich zu sorgen.[833]

Nach Art. 14 Abs. 5 lit. b) DS-GVO besteht die Informationspflicht nicht, soweit die Kenntnis über die Identität des Whistleblowers den Zweck interner Untersuchungen gefährden würde, weil Beweismittel drohen verlustig zu gehen oder die begründete Annahme besteht, die Erhebung weiterer Beweismittel werde gefährdet. Im Übrigen besteht die Informationspflicht fort. §§ 8, 9 HinSchG sind keine Rechtsvorschriften im Sinne des Art. 14 Abs. 5 lit. c) DS-GVO. Sie enthalten keine Vorgaben, die sicherstellen, dass der von der Datenverarbeitung betroffenen Person eine hinreichende Überprüfungsmöglichkeit in Bezug auf die Rechtmäßigkeit der Datenverarbeitung eingeräumt wird.[834] Aus denselben Gründen können die §§ 8, 9 HinSchG auch nicht auf die Öffnungsklausel des Art. 23 Abs. 1 lit. i) DS-GVO oder Art. 88 Abs. 1 DS-GVO gestützt werden. Ungeachtet der Frage, ob das HinSchG eine spezifischere Vorschrift im Beschäftigungskontext darstellt, enthalten die Vorgaben jedenfalls keine Maßnahmen, die das informationelle Selbstbestimmungsrecht der von der Meldung betroffenen Person hinreichend berücksichtigt und dem Transparenzgebot die notwendige Geltung verleiht, die Art. 88 Abs. 2 DS-GVO verlangt. Ein Ausschluss der Informationspflicht aus Gründen des Identitätsschutzes folgt auch nicht aus § 29 Abs. 1 S. 1 BDSG. Auch § 29 Abs. 1 S. 1 BDSG enthält keine Ausführungen hinsichtlich des Schutzes der von der Datenverarbeitung betroffenen Person, obwohl

---

833 Siehe: Kapitel C) I. 3. c) bb) (1).
834 Siehe: Kapitel C) I. 3. c) bb) (1) (b) bis (d).

diese nach Art. 23 Abs. 2 lit. g) DS-GVO notwendige Voraussetzung für eine Beschränkung sind. Dasselbe gilt mit Blick auf die Öffnungsklausel des Art. 88 Abs. 1 DS-GVO. Es fehlt an den für Art. 88 Abs. 2 DS-GVO nötigen Vorgaben zur Wahrung der Datentransparenz.

Mit Blick auf die Datenauskunft (Art. 15 Abs. 1, Abs. 3 DS-GVO) ist ebenfalls zu beachten, dass § 29 Abs. 1 S. 2 BDSG auf keine Öffnungsklausel der DS-GVO gestützt werden kann.[835] Der repetitive Charakter des § 29 Abs. 1 S. 2 Var. 1 BDSG verschleiert in unionswidriger Art und Weise die unmittelbare Geltung des Art. 23 Abs. 1 lit. i) DS-GVO. Im Übrigen enthält § 29 Abs. 1 S. 2 BDSG keine Vorgaben bzgl. des Schutzes der von der Datenverarbeitung betroffenen Person, obwohl diese nach Art. 23 Abs. 2 lit. g) DS-GVO notwendige Voraussetzung für eine Beschränkung der Datenauskunft sind. § 29 Abs. 1 S. 2 BDSG muss daher unangewendet bleiben und kann nicht als Beschränkung für die Datenauskunft herangezogen werden. Insofern verbleibt die allgemeine Möglichkeit der Beschränkung der Datenauskunft aus Gründen des Identitätsschutzes über Art. 15 Abs. 4 DS-GVO.

Der Verweis in Art. 15 Abs. 4 DS-GVO bezieht sich auf das Auskunftsrecht, mitsamt der Metainformationen in Art. 15 Abs. 1 Hs. 2 DS-GVO.[836] Die Frage der Beschränkung des Auskunftsrechts ist losgelöst vom Bezugspunkt der Erfüllungsmodalität zu beantworten. Aus Art. 52 GR-CH folgt, dass das Recht auf Datenauskunft nicht absolut gilt. Die gebotene charta-rechtliche Auslegung des Art. 15 DS-GVO führt daher zwingend zu der Annahme, dass kollidierende grundrechtlich geschützte Positionen die Beauskunftung der Metainformationen beschränken können. Im Rahmen des Art. 15 Abs. 4 DS-GVO entscheidet sodann eine umfassende Interessenabwägung zwischen dem Identitätsschutz des Whistleblowers und dem informationellen Selbstbestimmungsrecht der von der Meldung betroffenen Person, wobei

[835] Siehe: Kapitel C) I. 3. c) bb) (2).
[836] Siehe: Kapitel C) I. 3. c) bb) (2).

der Identitätsschutz nur insoweit zu berücksichtigen ist, als er nach den Vorgaben der §§ 8, 9 HinSchG auch tatsächlich besteht, der Whistleblower mithin ein berechtigtes Interesse an der Geheimhaltung seiner Identität hat.

Die objektive Unrichtigkeit einer Information ist für sich genommen nicht geeignet, dem Whistleblower sein berechtigtes Interesse am Identitätsschutz abzusprechen.[837] Nach dem Telos der Datenauskunft, soll die von der Datenverarbeitung betroffene Person lediglich zur Durchsetzung der Rechtmäßigkeit der Datenverarbeitung befähigt werden, nicht jedoch zur Durchsetzung ihrer weiteren Rechte gegenüber Dritten.

Der Identitätsschutz nach §§ 8, 9 HinSchG führt nicht automatisch zu einer Beschränkung der Datenauskunft, Art. 15 Abs. 1, Abs. 3 DS-GVO. Die Interessenabwägung im Rahmen des Art. 15 Abs. 4 DS-GVO ist eigenständig durchzuführen. Aus dem Regel-Ausnahme-Verhältnis des Art. 15 DS-GVO folgt, dass in Zweifelsfragen das Recht auf Datenauskunft überwiegt. Darüber können sich die Vorgaben des HinSchG nicht hinwegsetzen. Überredet der Arbeitgeber den Whistleblower unter Zusage der Vertraulichkeit zur Meldung, kann dies für ein Überwiegen des Identitätsschutzes sprechen. Arbeitgeber haben die entsprechenden Passagen zu schwärzen bzw. anderweitig unkenntlich zu machen, ehe sie dem Auskunftsverlangen im Übrigen entsprechen.

Aufgrund der großen Rechtsunsicherheit in diesem Bereich stellt sich die Frage, inwieweit Arbeitgebern Mechanismen zur Verfügung stehen, den Identitätsschutz des Whistleblowers zu erhöhen. Eine Verzichtserklärung in Bezug auf die Betroffenenrechte scheidet im Beschäftigungskontext aus.[838] Ungeachtet dessen, dass die Anforderungen an eine Verzichtserklärung höhere sind als diejenigen, die an

[837] Siehe: Kapitel C) I. 3. c) bb) (2).
[838] Siehe: Kapitel C) I. 3. c) cc) (1).

die Wirksamkeit einer Einwilligung zu stellen sind, weil die Datenverarbeitung im Verborgenen bleibt, fehlt es aufgrund des hierarchischen Machtungleichgewichts schon an der Freiwilligkeit des Verzichts nach Maßgabe der Einwilligung, Art. 4 Nr. 4 DS-GVO, § 26 Abs. 2 BDSG.

Demgegenüber eignet sich die Einschaltung einer externen, anwaltlichen Ombudsperson zur Erhöhung des Identitätsschutzes.[839] Aufgrund des anwaltlichen Berufsgeheimnisses (§ 43a Abs. 2 BRAO sowie § 203 StGB) wird die Ausnahmeregelung des Art. 14 Abs. 5 lit. d) DS-GVO aktiviert. Dies gilt allerdings nur, bis die externe Ombudsstelle die Daten an den Arbeitgeber für etwaige Folgemaßnahmen weiterleitet. Maßgeblich ist auch, dass die externe Ombudsstelle nach den Vorgaben der DS-GVO selbst als datenschutzrechtlich verantwortliche Stelle anzusehen ist.

Daneben kommt der Abschluss einer Betriebsvereinbarung zur Erhöhung des Identitätsschutzes in Betracht, wobei diese die allgemeinen Grundsätze der Datenverarbeitung nicht unterlaufen (Art. 5, Art. 6 DS-GVO) darf.[840] Die Grundsätze der Datenverarbeitung bilden folgerichtig einen Mindestschutz für die Verarbeitung personenbezogenen Daten im Beschäftigungskontext. Die Betriebsparteien bleiben in ihrer konkreten Ausgestaltung frei, diesen Mindestschutz im Rahmen einer Betriebsvereinbarung zu verankern. Dem Telos der Datentransparenz entsprechend kommt es darauf an, ob die Betriebsvereinbarung Maßnahmen vorsieht, die sicherstellen, dass die von der Meldung betroffene Person die Rechtmäßigkeit der Datenverarbeitung hinreichend prüfen und erforderlichenfalls durchsetzen kann.

---

[839] Siehe: Kapitel C) I. 3. c) cc) (2).

[840] Art. 88 Abs. 1, Abs. 2 DS-GVO i. V. m. § 26 Abs. 4 BDSG. Siehe: Kapitel C) I. 3. c) cc) (3).

II. Geschäftsgeheimnisschutz und das Recht auf Datenauskunft

Das Spannungsverhältnis zwischen Geschäftsgeheimnisschutz und datenschutzrechtlichem Auskunftsrecht bildet einen weiteren Konflikt widerstreitender Rechtspositionen, die jeweils grundrechtliche, unionsrechtliche und völkerrechtliche Verankerung erfahren haben und notwendigerweise in einen angemessenen Ausgleich zu bringen sind.[841] Beruft sich ein Arbeitnehmer auf das datenschutzrechtliche Auskunftsrecht nach Art. 15 Abs. 1 und Abs. 3 DS-GVO, sind die berechtigten Geheimhaltungsinteressen des Arbeitgebers über Art. 15 Abs. 4 DS-GVO berücksichtigungsfähig.[842] Die nachfolgenden Abschnitte beleuchten das Verhältnis zwischen dem Geschäftsgeheimnisschutz und dem Recht auf Datenauskunft. Dazu werden zunächst die Grundlagen der Datenauskunft herausgearbeitet, ehe auf deren Konzeption und inhaltliche Reichweite eingegangen wird. Daran anschließend untersucht die vorliegende Darstellung die Berücksichtigungsfähigkeit der unternehmerischen Geheimhaltungsinteressen im Rahmen der Datenauskunft. Abschließend wird es um die Frage gehen, ob und inwieweit das personalaktenrechtliche Einsichtsrecht die Datenauskunft verdrängt und inwieweit auch dort Geheimhaltungsinteressen Berücksichtigung finden.

---

[841] Für die betrieblichen Geheimhaltungsinteressen folgt dies u. a. aus Art. 12 Abs. 1 GG und Art. 14 Abs. 1 GG sowie Art. 16, 17 GR-CH, siehe: Kapitel B) I. Das Recht auf Datenauskunft ist demgegenüber in Form eines subjektiven Rechts in Art. 8 Abs. 2 GR-CH verankert und verfassungsrechtlich als Teil des informationellen Selbstbestimmungsrechts anerkannt, siehe auch: Kapitel C) I. 1. a).

[842] Vgl. LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, 242.

1. Grundlagen des datenschutzrechtlichen Auskunftsrechts

Das Recht auf Datenauskunft ist charta-rechtlich in Form eines subjektiven Rechts in Art. 8 Abs. 2 GR-CH verankert.[843] Danach dürfen personenbezogene Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden (Satz 1). Darüber hinaus hat jede Person das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken (Satz 2). Es handelt sich folgerichtig um ein „*normgeprägtes*" Grundrecht mit einem eigenen Schutzgehalt, dessen Beschränkungsmöglichkeiten sich aus Art. 52 Abs. 1 GR-CH ergeben.[844] Telos der Datenauskunft ist, die von der Datenverarbeitung betroffene Person in die Lage zu versetzen, die Rechtmäßigkeit der Verarbeitung ihrer personenbezogenen Daten zu prüfen, um ggf. weitere Rechte geltend zu machen.[845] Auf die Art stellt die Datenauskunft zugleich sicher, dass die Eingriffsintensität der Datenverarbeitung in die informationelle Selbstbestimmungsfreiheit der von der Datenverarbeitung betroffenen Person abgesenkt wird.[846] Einschränkungen sind nach Art. 52 Abs. 1 GRCH möglich, sofern sie gesetzlich vorgesehen sind, den Wesensgehalt der gewährleisteten Rechte achten und den Grundsatz der Verhältnismäßigkeit wahren.[847] Das Grund-

---

[843] *Bernsdorff*, in: Meyer/Hölscheidt, GR-CH, Art. 8 Rn.30; *Marsch*, Das europäische Datenschutzgrundrecht, S. 230; *Jarass*, in: Jarass, GR-CH, Art. 8 Rn.20; *Knecht*, in: Schwarze, GR-CH, Art. 8 Rn.9; *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, Rn.83; *Roßnagel*, in: NK-DSGVO, Art. 5 DS-GVO Rn.49.

[844] Zur dogmatischen Verortung grundlegend: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 66 ff.

[845] Vgl. EuGH, Gutachten v. 26.07.2017 - C-1/15, BeckEuRS 201, 513522 Rn.219; *Frenz*, Handbuch Europarecht, Bd. 4 Rn.1392; *Marsch*, Das europäische Datenschutzgrundrecht, S. 230 und Erwägungsgrund 63 S. 1 DS-GVO für die Sekundärrechtsebene.

[846] Siehe: Kapitel C) I. 1. a).

[847] *Jarass*, in: Jarass, GR-CH, Art. 8 Rn.21; *Marsch*, Das europäische Datenschutzgrundrecht, S. 235 ff.; *Kingreen*, in: Calliess/Ruffert, GR-CH, Art. 21 Rn.59 m. w. N.

gesetz enthält ebenfalls ein verfassungsunmittelbares Auskunftsrecht mit vergleichbarem Telos.[848] Dies ist nach der Rechtsprechung des BVerfG mittlerweile anerkannt und Teil des informationellen Selbstbestimmungsrechts.[849]

Der Unionsgesetzgeber hat sich seines Regelungsauftrags in Art. 8 Abs. 2 GR-CH angenommen und mit der am 24. Mai 2016 in Kraft getretenen DS-GVO eine Verordnung geschaffen, die ein einheitliches Schutzniveau in der Europäischen Union in Bezug auf die Datenauskunft festsetzt und zugleich unmittelbare Geltung beansprucht, vgl. Art. 288 AEUV. Verordnungsunmittelbare Beschränkungen der Datenauskunft enthalten die Art. 15 Abs. 4 DS-GVO und Art. 12 Abs. 5 DS-GVO. Im Bereich des Geschäftsgeheimnisschutzes ist Art. 15 Abs. 4 DS-GVO relevant. Darüber hinaus sind Abweichungen durch das nationale Rechte möglich, wenn und soweit diese auf eine Öffnungsklausel der DS-GVO zurückzuführen sind. Einschränkungsmöglichkeiten des nationalen Gesetzgebers bestehen über die Öffnungsklausel des Art. 23 DS-GVO und Art. 88 DS-GVO unter Beachtung der dort genannten Voraussetzungen. Zu beachten ist, dass das Recht auf Datenauskunft den Grundsatz der Transparenz (Art. 5 Abs. 1 lit. a) DS-GVO) konkretisiert, den jede Datenverarbeitung im Sinne eines allgemeinen Grundsatzes zu wahren hat und Ausdruck des informationellen Selbstbestimmungsrechts der von der Datenverarbeitung betroffenen Person ist.[850] Das Auskunftsrecht stellt sicher, dass die von der Datenverarbeitung betroffene Person hin-

---

[848] BVerfG, Beschluss v. 10.03.2008 - 1 BvR 2388/03; BVerfGE 120, 351, 360; *Dreier*, in: Dreier, GG, Art. 2 Abs. 1 Rn.95 f.; *Rixen*, in: Sachs, GG, Art. 2 Rn.72.

[849] BVerfG, Urteil v. 15.12.1983 - 1 BvR 209/83, BVerfGE 65, 1, 43; *Globig*, in: FS-Rudolf, S. 445 ff.; a. A.: *Ehmann*, CR 1988, 575, 576; kritisch: *Simitis*/*Fuckner*, NJW 1990, 2713, 2717; offenlassend: BVerwG, Urteil v. 20.02.1990 - 1 C 42/83, NJW 1990, 2761, 2762.

[850] Vgl. Erwägungsgrund 39 S. 4 DS-GVO; *Herbst*, in: Kühling/Buchner, DS-GVO, Art. 5 Rn.19; *Roßnagel*, in: NK-DSGVO, Art. 5 DS-GVO Rn.5; *Thüsing*/*Pötters*, in: Compliance, § 18 Rn.6.

reichend Kenntnis über die Datenverarbeitung erlangt, die es ihr sodann ermöglicht, die Datenverarbeitung auf Rechtmäßigkeit zu überprüfen und ggf. weitere rechtliche Schritte in Erwägung zu ziehen.[851] Anders als die Informationspflichten in Art. 13 und Art. 14 DS-GVO setzt das Recht auf Datenauskunft einen Antrag voraus.[852] Der Antrag auf Datenauskunft ist damit notwendige Voraussetzung zur Rechtsausübung, vgl. Erwägungsgrund 63 S.1 DS-GVO.[853] Die Modalitäten der Datenauskunft regelt insbesondere Art. 12 DS-GVO und gewährleistet, dass die von der Datenverarbeitung betroffene Person die Auskunft in einer leicht verständlichen und transparenten Art und Weise erhält.

a) Die Konzeption des Art. 15 DS-GVO

Nach Art. 15 Abs. 1 Hs. 1 DS-GVO hat die von der Datenverarbeitung betroffene Person das Recht, von der für die Datenverarbeitung verantwortliche Stelle eine Bestätigung darüber zu verlangen, ob diese sie betreffende personenbezogene Daten verarbeitet (sog. „*Ob*“ der Datenverarbeitung).[854] Ist dies der Fall, hat die von der Datenverarbeitung betroffene Person zugleich ein Recht auf Auskunft über diese personenbezogenen Daten (Art 15 Abs. 1 Hs. 2 Var. 1 DS-GVO) sowie die in Art. 15 Abs. 1 Hs. 2 Var. 2 DS-GVO gelisteten Metainformationen der Datenverarbeitung.[855] Das „*Ob*“ der Datenverarbeitung geht der weiteren Auskunft demgemäß zeitlich vor. Beschränkungen erfährt die Datenauskunft verordnungsunmittelbar durch die Rechte

---

851 *Pötters*, in: Gola/Heckmann, DS-GVO, Art. 5 Rn.12; vgl. auch Erwägungsgründe 39 S. 5 und 63 S.1 DS-GVO.

852 Etwa: *Specht*, in: Sydow, DS-GVO, Art. 15 Rn.2.

853 BGH, Urteil, v. 22.02.2022 - VI ZR 14/21, BeckRS 2022, 5496 Rn.24; BGH, Urteil v.15.06.2021 - VI ZR 576/19, NJW 2021, 2726 Rn.23; *Bäcker*, in: Kühling/Buchner, DS-GVO, Art. 15 Rn.1; *Ehmann*, in: Selmayr/Ehmann, DS-GVO, Art. 15 Rn.3.

854 Dies umfasst auch das Recht auf Erhalt einer sog. Negativauskunft, vgl. *Franck*, in: Gola, Art. 15 DS-GVO Rn.5; *Thüsing*/*Pötters*, in: Compliance, § 18 Rn.30.

855 Findet keine Datenverarbeitung statt, erfolgt eine sog. Negativauskunft.

und Freiheiten anderer, vgl. Art. 15 Abs. 4 DS-GVO. Nach Art. 15 Abs. 4 DS-GVO dürfen die Rechte und Freiheiten anderer Personen das Recht auf Erhalt einer Kopie gemäß Art. 15 Abs. 3 DS-GVO nicht beeinträchtigen. Zu beachten ist, dass Art. 15 Abs. 4 DS-GVO seinem Wortlaut nach ausschließlich auf Art. 15 Abs. 3 DS-GVO verweist. Dies führt zu der Frage, ob die überwiegenden Rechte und Freiheiten anderer Personen lediglich im Rahmen des Art. 15 Abs. 3 DS-GVO berücksichtigungsfähig sind, nicht jedoch im Rahmen des Art. 15 Abs. 1 DS-GVO.

Der EuGH hat zutreffend klargestellt, dass das Recht auf Kopie kein eigenständiges Recht neben dem Auskunftsrecht gewähre, sondern lediglich dessen „*praktische(n) Modalitäten*“ festlege.[856] Die Kopie-Verpflichtung bildet demnach die Erfüllungsmodalität der Auskunft, wenn es auf Rechtsfolgenseite darum geht, auf welche Art und Weise die Datenauskunft nach Art. 15 Abs. 1 Hs. 2 Var. 1 DS-GVO zu erfüllen ist. Art. 15 Abs. 4 DS-GVO ist deshalb als eine Erweiterung des Art. 12 DS-GVO zu verstehen, der ebenfalls Modalitäten in Bezug auf die Datenauskunft regelt. Der BGH wurde richtigerweise bestätigt, einen Klageantrag auf „*Datenauskunft durch Überlassen in Kopie*“ nicht weiter zu beanstanden.[857] Demgegenüber bedarf die Entscheidung des BAG, die zwischen einem vorrangigen Anspruch auf Auskunft und einem nachrangigen Anspruch auf die Zurver-

---

[856] Zuvor wurde im Schrifttum darüber diskutiert, ob Art. 15 Abs. 1 und Abs. 3 DS-GVO rechtsdogmatisch im Sinne eines einheitlichen Auskunftsrechts zu verstehen sind, oder ob es sich um zwei eigenständige Ansprüche handelt, die gesondert voneinander zu betrachten sind. Da der EuGH die Auslegungshoheit innehält, ist diese Frage nunmehr geklärt und die Datenauskunft im Sinne eines einheitlichen Rechts zu verstehen, wobei die Kopie in Art. 15 Abs. 3 DS-GVO die Erfüllungsmodalität der Datenauskunft nach Art. 15 Abs. 1 Hs. 2 Var. 1 DS-GVO vorgibt, EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.31, 32, EuZW 2023, 575; entsprechend den Schlussanträgen des GA *Pitruzzella,* GRUR-RS 2022, 36103 Rn.8 - *Österreichische Datenschutzbehörde.* Zum damaligen Streitstand siehe: Kapitel C) I. 3. c) bb) (2), dort: Fn.738.

[857] BGH, Urteil v. 15.06.2021 - VI ZR 576/19, NJW 2021, 2726.

fügungstellung einer Kopie unterscheidet, einer Überholung.[858] Art. 15 Abs. 3 DS-GVO kann nicht über das Auskunftsrecht hinausgehen.

Zu beachten ist allerdings, dass sich die Erfüllungsmodalität der Kopie in Art. 15 Abs. 3 S. 1 DS-GVO dem Wortlaut nach ausschließlich auf die Beauskunftung der „*personenbezogenen Daten*“, nicht jedoch auf die Beauskunftung der „*Informationen*“ in Art. 15 Abs. 1 Hs. 2 Var. 2 DS-GVO bezieht. Der EuGH hat dies nunmehr ebenfalls bestätigt und klargestellt, dass der Begriff "*Informationen*" in Art. 15 Abs. 3 S. 3 DS-GVO ausschließlich auf die „*personenbezogenen Daten*“ in Art. 15 Abs. 3 S. 1 Bezug nimmt.[859] Dies ist vor dem Hintergrund der Kopie in ihrer Eigenschaft als Erfüllungsmodalität zu verstehen. Die Kopie bezieht sich auf die personenbezogenen Daten in Art. 15 Abs. 1 Hs. 2 Var. 1 DS-GVO, weil über diese ohne Weiteres in Form einer Kopie Auskunft erteilt werden kann. Dagegen erweist sich eine Kopie-Erteilung in Bezug auf die Metainformationen in aller Regel schwierig. Zu Recht bleibt der Verantwortliche daher in Bezug auf die Beauskunftung der Metainformationen in der Art und Weise seiner Auskunftserteilung weitestgehend frei. Maßgebend bleiben die Modalitäten in Art. 12 DS-GVO. [860] Auch dies hat der EuGH festgestellt: „*Das Auskunftsrecht (…) erstreckt sich nicht nur auf die personenbezogenen Daten, sondern auf sämtliche Informationen i. S. v. Art. 15 I Buchst. a-h DS-GVO. Diese Informationen müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt werden.“*[861]

Gleichwohl ist zu bedenken, dass sich die Beschränkungsmöglichkeit in Art. 15 Abs. 4 DS-GVO - trotz des Verweises auf die Kopie - auf das Auskunftsrecht mitsamt der Metainformationen in

858 BAG, Urteil v. 16.12.2021 - 2 AZR 235/21, NZA 2022, 362 Rn.26, 29.
859 Vgl. EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.49.
860 Vgl. EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.38.
861 Vgl. EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.38.

Art. 15 Abs. 1 Hs. 2 DS-GVO erstreckt.[862] Die Frage der Beschränkung des Auskunftsrechts ist losgelöst vom Bezugspunkt der Erfüllungsmodalität zu beantworten. Aus Art. 52 GR-CH folgt, dass das Recht auf Datenauskunft nicht absolut gilt.[863] Die gebotene chartarechtliche Auslegung des Art. 15 DS-GVO führt daher zwingend zu der Annahme, dass kollidierende grundrechtlich geschützte Positionen die Beauskunftung der Metainformationen beschränken können müssen. Dies gilt es, im Rahmen des Art. 15 Abs. 4 DS-GVO zu beachten. Folgerichtig ist davon auszugehen, dass sich der Verweis in Art. 15 Abs. 4 DS-GVO auf das Auskunftsrecht insgesamt, mitsamt der Metainformationen bezieht.[864] Vor diesem Hintergrund wäre es sicherlich sinnvoll, Art. 15 Abs. 4 DS-GVO an den Wortlaut seines dazugehörigen Erwägungsgrundes 63 DS-GVO sprachlich anzupassen. Anders als Art. 15 Abs. 4 DS-GVO unterscheidet Erwägungsgrund 63 DS-GVO nicht zwischen „*personenbezogenen Daten*“ und „*Informationen*“, sondern formuliert allgemein: „*Auskunftsrecht*“ bzw. „*Recht*“.

b) Inhaltliche Reichweite der Datenauskunft

Für viel Diskussion im Schrifttum hat auch die Frage nach der inhaltlichen Reichweite der Datenauskunft gesorgt.[865] Aus Sicht des Geschäftsgeheimnisschutzes ist zu beachten: Je umfassender die Beauskunftung, desto höher die Wahrscheinlichkeit, dass dabei auch Geschäftsgeheimnisse offengelegt werden. Der EuGH hat in seiner

---

862 Siehe: Kapitel C) I. 3. c) bb) (2).

863 Vgl. *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 409 f.; *Jarass*, in: Jarass, GR-CH, Art. 8 Rn.21. Siehe auch: Kapitel C) I. 1. a).

864 Ebenso im Ergebnis: *Peisker*, der „*von der (analogen) Anwendung des Art. 15 Abs. 4 DS-GVO auf sämtliche Auskunftsbestandteile“* ausgeht, vgl. *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 415; im Ergebnis auch: LAG Baden-Württemberg, Urteil v. 17.03.2021 - 21 Sa 43/20, NZA-RR 2021, 410 Rn.39; LG Stuttgart, Urteil v. 04.11.2020 - 18 O 333/19, BeckRS 2020, 38735 Rn.34.

865 Grundlegend dazu und zum Streitstand: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 265 ff.

Entscheidung vom 22. Juni 2023 nicht nur klargestellt, dass die Kopie eine Modalität des Auskunftsrechts darstellt, sondern darüber hinaus zur inhaltlichen Reichweite des Auskunftsrechts Stellung bezogen.[866] Laut EuGH verlange das Recht auf Kopie zwar nicht zwingend die Reproduktion von Auszügen aus Dokumenten oder gar von ganzen Dokumenten. Einzelfallbezogen könne dies aber sein. Maßgeblich sei, ob sich die verarbeiteten Daten nur in ihrem jeweiligen Kontext erschließen lassen. Der EuGH formuliert dazu: „*So kann es sein, dass eine verständliche Darstellung und transparente Auskunft nur gewährleistet ist, wenn die verarbeiteten personenbezogenen Daten im Zusammenhang als originalgetreue Kopie übermittelt werden. Dies ist insbesondere der Fall, wenn personenbezogene Daten aus anderen Daten, beispielsweise Metadaten, generiert werden.*“[867] Entscheidend ist also, ob die nach Art. 12 Abs. 1 DS-GVO obligatorische

---

[866] Indem der EuGH Art. 15 Abs. 3 DS-GVO als Rechtsfolgenregelung des Art. 15 Abs. 1 Hs. 1 DS-GVO einordnet, kann Art. 15 Abs. 3 DS-GVO folgerichtig nicht über das Auskunftsrecht in Art. 15 Abs. 1 DS-GVO hinausgehen, vgl. EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.31 ff. Der EuGH hat mit dieser Entscheidung zugleich eine grundlegende Richtschnur hinsichtlich des Detaillierungsgrads der Datenauskunft vorgegeben, an der sich aufgrund seiner Auslegungshoheit zwingend zu orientieren ist. Zuvor war der Detaillierungsgrad der Datenauskunft hoch umstritten. Teile des Schrifttums vertraten eine umfassende Beauskunftung, wenngleich diese These mitunter zu Unrecht auf der Annahme fußte, Art. 15 Abs. 3 DS-GVO bilde eine eigenständige Anspruchsgrundlage, vgl. *Riemer*, ZD 2019, 413, 414; *Kremer*, CR 2018, 560, 563 f.; *Härting*, CR 2019, 219, 221; *Dix*, in: NK-DatenschutzR, Rn.28; *König*, CR 2019, 295 ff.; *Riemer*, ZD 2019, 413, 414; *Riemer*, DSB 2019, 223; *Korch/Chatard*, NZA 2020, 893, 895; *Koreng*, NJW 2021, 2692, 2693. Andere Teile des Schrifttums legten die inhaltliche Reichweite des Art. 15 Abs. 3 DS-GVO restriktiver aus, vgl. *Dausend,* ZD 2019, 103, 106 f.; *Paal*, in: Paal/Pauly, Rn.33; *Wybitul/Neu/Strauch,* ZD 2018, 202, 203; *Wybitul/Brams,* NZA 2019, 672, 676; ähnlich: *Pauly/Mende*, CCZ 2022, 28, 31. Vertreter des restriktiveren Verständnisses ließen z. B. eine Übersicht im Sinne einer Auflistung der verschiedenen personenbezogenen Daten genügen. Dieser Auffassung hat der EuGH nunmehr eine Absage erteilt, da die Informationen zu sämtlichen Datenverarbeitungen originalgetreu zu übermitteln sind, vgl. EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.42.

[867] EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.42.

Verständlichkeit und Transparenz der Datenauskunft eine „*Kontextualisierung*“ der verarbeiteten Daten erfordert.[868] Demzufolge kann die Datenauskunft auch „*eine Kopie der Auszüge aus Dokumenten oder gar eine Kopie von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die unter anderem diese Daten enthalten*“ sein, sofern „*die originalgetreue Kopie unerlässlich für die wirksame Ausübung der Betroffenenrechte ist*.“[869] Eine bloße Auflistung oder Beschreibung der verarbeiteten personenbezogenen Daten werde dem - laut EuGH - nicht gerecht. Darüber hinaus betont der EuGH, dass sich die Grundsätze der transparenten Datenauskunft auch auf die Metainformationen in Art. 15 Abs. 1 Hs. 2 Var. 2 DS-GVO erstreckt: Auch diese seien „*in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache*“ zu übermitteln.[870]

Die Frage, wann eine Kontextualisierung erforderlich oder unerlässlich ist, lässt der EuGH hingegen unbeantwortet. Maßgeblich sind die Umstände des jeweiligen Einzelfalls. Richtschnur ist das Telos der Datenauskunft, das der von der Datenverarbeitung betroffenen Person ermöglichen will, Kenntnis von der Datenverarbeitung zu erlangen, um sodann deren Rechtmäßigkeit prüfen und ggf. durchsetzen zu können.[871] Dies hat zur Folge, dass die Datenauskunft im Einzelfall sehr weit gehen kann. Um die unternehmerische Praxis zu entlasten, fordern einige Stimmen in der Literatur zu Recht ein ausgleichendes Gegengewicht im Sinne einer einschränkenden Lesart auf der Rechtsfolgenseite.[872] Inwieweit eine einschränkende Lesart gelingen kann, bleibt abzuwarten. Es spricht Vieles dafür, dass der EuGH auch im Falle eines Auskunftsersuchens zu datenschutzfremden Zwecken zu

---

868 Vgl. EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.49.
869 EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.45.
870 EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.38.
871 Siehe: Kapitel C) I. 1. a).
872 Vgl. *Schreiber*/*Brinke*, RDi 2023, 232; *Suchan*, ZD 2021, 198; *Riemer,* DSB 2019, 223.

der Annahme eines Auskunftsrechts gelangen wird.[873] Richtig ist, dass auf einen „*Durchschnittsadressaten*“ abzustellen ist und nicht individuell auf die jeweilige auskunftsersuchende Person.[874] Dies ergibt sich aus Art. 12 Abs. 1 S. 1 Hs. 2 DS-GVO, der Kinder nur beispielhaft und infolgedessen stellvertretend für andere Empfängergruppen nennt. Aus dem Wort „*insbesondere*“ folgt, dass diese objektive Betrachtung auch für andere Empfängergruppen, wie z. B. Beschäftigte gilt.[875]

2. Beschränkung der Datenauskunft nach Maßgabe des Geschäftsgeheimnisschutzes

Eine Beschränkung der Datenauskunft aufgrund gegenläufiger Geheimhaltungsinteressen des datenschutzrechtlich Verantwortlichen kann sich auf verschiedene Weisen ergeben. Art. 15 Abs. 4 DS-GVO sieht eine verordnungsunmittelbare Beschränkungsmöglichkeit vor. Daneben sind Beschränkungen möglich, sofern diese auf eine Öffnungsklausel der DS-GVO rückführbar sind. In Betracht kommt insbesondere Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 4 BDSG für Betriebsvereinbarungen. Hinsichtlich der Öffnungsklausel in Art. 23 Abs. 1 lit. i) DS-GVO i. V. m. § 29 Abs. 1 S. 2 BDSG gilt es zu bedenken, dass § 29 Abs. 1 S. 2 BDSG nach hiesiger Auffassung unionsrechtswidrig ist und deshalb unangewendet bleiben muss.[876] Die weitere Untersuchung wird sich daher auf die Beschränkung der Datenauskunft nach Art. 15 Abs. 4 DS-GVO aufgrund entgegenstehender Geheimhaltungsinteressen des datenschutzrechtlich Verantwortlichen konzentrieren.

---

873 Vgl. GA *Emiliou*, Schlussantrag v. 20.04.2023 - C-307/22, BeckRS 2023, 7659, Rn.84; ebenso der dazu vorausgegangene BGH, Beschluss v. 29.03.2022 - VI ZR 1352/20, ZD 2022, 497, Rn.19; OLG Köln, Urteil v. 13.05.2022 - 20 U 295/21, ZD 2022, 619, Rn.54.

874 *Quaas*, in: BeckOK-DatenschutzR, Art. 12 DS-GVO, Rn.12.

875 *Quaas*, in: BeckOK-DatenschutzR, Art. 12 DS-GVO, Rn.12; so auch *Bäcker*, in: Kühling/Buchner/Bäcker, DS-GVO, Art. 12 Rn.11.

876 Siehe: Kapitel C) I. 3.c) bb) (2).

Wie bereits aufgezeigt, bezieht sich die Beschränkungsmöglichkeit trotz des Verweises auf Art. 15 Abs. 3 DS-GVO auf das Auskunftsrecht mitsamt der Metainformationen.[877] Im Rahmen des Art. 15 Abs. 4 DS-GVO entscheidet sodann eine umfassende Interessenabwägung zwischen dem informationellen Selbstbestimmungsrecht der von der Verarbeitung betroffenen Person und den berechtigten Geheimhaltungsinteressen des datenschutzrechtlich Verantwortlichen.[878] Im Bereich des Geschäftsgeheimnisschutzes ist davon auszugehen, dass ein berechtigtes Geheimhaltungsinteresse besteht, soweit es sich um ein Geschäftsgeheimnis im Sinne des GeschGehG handelt. Dies geht aus Erwägungsgrund 63 S. 5 DS-GVO hervor, der unter anderem Geschäftsgeheimnisse als Beispiele für ein berechtigtes Geheimhaltungsinteresse anführt.[879] Ein berechtigtes Geheimhaltungsinteresse kann darüber hinaus beispielsweise auch an der Geheimhaltung der Korrespondenz des datenschutzrechtlich Verantwortlichen mit seinem Rechtsanwalt bestehen.[880] Inwieweit der Geschäftsgeheimnisschutz den informationellen Selbstbestimmungsrecht der von der Verarbeitung betroffenen Person überwiegt, ist sodann einzelfallbezogen zu entscheiden.

Aus dem Vorliegen eines berechtigten Geheimhaltungsinteresses folgt noch keine Beschränkung der Datenauskunft. Vielmehr erfordert Art. 15 Abs. 4 DS-GVO eine eigenständige Interessenabwägung.[881]

---

877 Siehe: Kapitel C) I. 3. c) bb) (2).

878 Vgl. *Bienemann*, in: Sydow/Marsch, DS-GVO, Art. 15 Rn.60; *Schmidt-Wudy*, in: BeckOK-DatenschutzR, Art. 15 DS-GVO, Rn.96.

879 Vgl. *Wybitul*/*Brams*, NZA 2019, 672, 673. Zu der Frage, ob eine Erheblichkeitsschwelle in Art. 15 Abs. 4 DS-GVO hineinzulesen ist, grundlegend: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 417 f., der zu dem zutreffenden Ergebnis gelangt, dass jedenfalls die Interessenabwägung dafür sorge, dass nur solche Interessen das informationelle Selbstbestimmungsrecht der von der Datenverarbeitung betroffenen Person überwiegen, die von einigem Gewicht seien. Dies gelte auch mit Blick auf rein wirtschaftliche und ideelle Interessen.

880 *Korch*/*Chatard*, NZG 2020, 893, 895.

881 LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, 242; *Thüsing/Pötters,* in: Compliance, § 18 Rn.37.

Dazu ist das berechtigte Geheimhaltungsinteresse des datenschutzrechtlich Verantwortlichen (Art. 12 Abs. 1 GG, Art. 14 Abs. 1 GG sowie Art. 16, 17 GR-CH) mit dem Auskunftsinteresse des von der Datenverarbeitung betroffenen Arbeitnehmers (Art. 8 Abs. 2 S. 2 GR-CH) nach Maßgabe des Verhältnismäßigkeitsgrundsatzes in einen angemessenen Ausgleich zu bringen, wobei das Regel-Ausnahme-Verhältnis des Art. 15 DS-GVO dafür streitet, dass in Zweifelsfragen das Recht auf Datenauskunft überwiegt.[882] Ein pauschaler Hinweis auf den Geschäftsgeheimnisschutz genügt mithin nicht.[883] Vielmehr bedarf es eines Nachweises durch den datenschutzrechtlich Verantwortlichen, dass das berechtigte Geheimhaltungsinteresse das informationelle Selbstbestimmungsrecht der von der Datenverarbeitung betroffenen Person überwiegt. Maßgeblich sind die Umstände des jeweiligen Einzelfalls.[884]

Ist das Geschäftsgeheimnis dem Auskunftsersuchenden bereits bekannt, scheidet eine Beschränkung der Datenauskunft von vornherein aus. Gleiches gilt, sollte die Erlangung des Geschäftsgeheimnisses nach Maßgabe des § 3 GeschGehG erlaubt sein.[885] Dabei ist zu beachten, dass das Auskunftsrecht nach Art. 15 DS-GVO kein Informationsrecht im Sinne des § 3 Abs. 1 Nr. 3 GeschGehG ist. Nach § 3 Abs. 1 Nr. 3 GeschGehG darf ein Geschäftsgeheimnis durch die Ausübung „*von Informations- und Anhörungsrechten der Arbeitnehmer*“ erlangt werden. Schon dem Wortlaut nach verlangt § 3 Abs. 1 Nr. 3 GeschGehG ein spezifisches Arbeitnehmerrecht, das

882 *Brobeil*, Die Auswirkungen der Richtlinie (EU) 2019/1937 auf Arbeitnehmer-Hinweisgeber, S. 285.

883 BGH, Urteil v. 22.02.2022 - VI ZR 14/21, BeckRS 2022, 5496, Rn.26.

884 BGH, Urteil v. 22.02.2022 - VI ZR 14/21, BeckRS 2022, 5496, Rn.26; LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, 242.

885 *Alexander*, in: Köhler/Bornkamm/Feddersen, UWG, § 3 GeschGehG, Rn.7a; *Reinfeld*, Das neue Gesetz zum Schutz von Geschäftsgeheimnissen, § 2 Rn.19.

seine Begründung im Arbeitsverhältnis findet.[886] Art. 15 DS-GVO gilt jedoch unabhängig vom Bestehen eines Arbeitsverhältnisses für jede von einer Datenverarbeitung betroffenen Person. Art. 15 DS-GVO ist daher kein Informationsrecht im Sinne des § 3 Abs. 1 Nr. 3 GeschGehG. Die Datenauskunft ist nicht generell erlaubt, § 3 Abs. 1 Nr. 3 GeschGehG.[887]

Berücksichtigungsfähige Umstände zu Gunsten des Geheimnisschutzes im Rahmen des Art. 15 Abs. 4 DS-GVO können insbesondere die mit der Offenlegung verbundenen Risiken für den Geheimnisinhaber sein. Dabei ist zu bedenken, dass mit jeder Offenlegung der Kreis der Mitwissenden steigt und infolgedessen das Risiko einer unberechtigten Offenlegung oder Weitergabe wächst. Dem Unternehmen drohen erhebliche Wettbewerbsnachteile. Insofern stellt die Beauskunftung eines Geschäftsgeheimnisses in aller Regel eine tatsächliche Beeinträchtigung der unternehmerischen Geheimhaltungsinteressen dar.[888] Im Ergebnis wird daher das betriebliche Geheimhaltungsinteresse das informationelle Selbstbestimmungsrecht regelmäßig überwiegen.[889] Dafür spricht, dass die Datenauskunft nicht dazu dienen darf, den datenschutzrechtlich Verantwortlichen über sensible Informationen auszuspionieren. Beschäftigte sollen sich über die

---

886 Dafür spricht, dass das GeschGehG die Rechte und Pflichten aus dem Arbeitsverhältnis nicht berührt, § 1 Abs. 3 Nr. 4 GeschGehG bzw. Art. 3 Abs. 2 GeschGeh-RL, vgl. BT-Drs. 19/4724, S. 26.

887 Vgl. *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 440, 441.

888 Vgl. *Schmidt-Wudy*, in: BeckOK-DatenschutzR, Art. 15 Rn.96.

889 So auch: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 440; *Schulte*/*Welge*, NZA 2019, 1110, 1112. Gleiches gilt für die Offenlegung der Korrespondenz des Arbeitgebers mit seinem Rechtsanwalt. Auch in diesem Fall überwiegt das Geheimhaltungsinteresse des Arbeitgebers in aller Regel das Auskunftsinteresse des Arbeitnehmers, vgl. *Raji,* ZD 2020, 279, 284. Laut Gericht der Europäischen Union sei die Vertraulichkeit der Kommunikation zwischen Rechtsanwalt und Mandant im hohen Maße schützenswert, Art. 47 Abs. 2 S. 2 der Grundrechte-Charta; EuG, Urteile v. 17.09.2007 - T-125/03 u. T-253/03.

Datenauskunft keinen generellen Zugang zu Geschäftsgeheimnissen verschaffen.[890]

Der Grundsatz der Verhältnismäßigkeit gebietet es jedoch, dass die gegenläufigen Geheimhaltungsinteressen zu keinem Ausschluss der Datenauskunft führen, sondern diese lediglich in Bezug auf die geheimen Informationen und solche Informationen, die Rückschlüsse ermöglichen, beschränken (sog. „*partielle Auskunftsverweigerung*“[891]), vgl. Erwägungsgrund 63 S. 6 der DS-GVO.[892] Arbeitgeber haben in diesen Fällen die entsprechenden Passagen zu schwärzen bzw. anderweitig unkenntlich zu machen, ehe sie dem Auskunftsverlangen nachkommen.[893] In Betracht kommt auch eine strafbewehrte Verschwiegenheitsvereinbarungen.[894] Der datenschutzrechtlich Verantwortliche ist hier in der Wahl seiner Mittel frei. Nach Art. 12 Abs. 4 DS-GVO ist der Auskunftsersuchende auf die Beschränkung hinzuweisen.

Herausfordernd im Zusammenhang mit der Beschränkung der Datenauskunft aus Gründen des Geschäftsgeheimnisschutzes ist jedoch, dass die arbeitsgerichtliche Praxis hohe Anforderungen an den darlegungs- und beweispflichtigen datenschutzrechtlich Verantwortlichen in Bezug auf den Nachweis seines berechtigten Geheimhaltungs-

---

890 *Ziegelmayer*, CR 2018; 693, 697; *Brink*/*Joos*, ZD 2019, 483, 487.

891 So bezeichnet bei: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 440.

892 VG Schwerin, Urteil v. 19.04.2021 - 1 A 1343/19, BeckRS 2021, 14406 Rn.57; LAG Hessen, Urteil v. 10.06.2021 - 9Sa 1431/19, BeckRS 2021, 32421 Rn.48; *Bienemann*, in: Sydow/Marsch, DS-GVO, Art. 15 Rn.64; vgl. *Franzen*, NZA 2020, 1593, 1596.

893 *Schmidt-Wudy*, in: BeckOK-DatenschutzR, Art. 15 DS-GVO Rn.99.2.

894 *Schmidt-Wudy*, in: BeckOK-DatenschutzR, Art. 15 DS-GVO Rn.99.2.

interesses stellt.[895] So seien insbesondere konkrete Angaben zu machen, worauf sich das Geheimhaltungsinteresse beziehe. Im Prozess läuft dies regelmäßig auf die Offenlegung des Geschäftsgeheimnisses hinaus. Zwar stellen die §§ 19 ff. GeschGehG sicher, dass der Personenkreis derjenigen, die Kenntnis von dem Geschäftsgeheimnis erhalten, klein gehalten wird. Dennoch erfolgt eine Offenlegung an wenigstens eine natürliche Person jeder Partei und ihre Prozessvertreter oder sonstige Vertreter, die für den Geheimnisinhaber stets risikobehaftet ist.[896] Zu Recht fordert *Peisker* daher die Aufwertung der §§ 19 ff. GeschGehG hin zu einem sog. in-camera-Verfahren wie es in § 99 Abs. 2 VWGO verankert ist.[897]

3. Verhältnis der Datenauskunft zum Akteneinsichtsrecht

Eine weitere Kontroverse, die in Teilen des Schrifttums geführt wird, betrifft die Frage, ob und inwieweit das personalaktenrechtliche Einsichtsrecht in § 83 Abs. 1 S. 1 BetrVG das Recht auf Datenauskunft verdrängt. Entscheidet sich der Arbeitgeber dazu, Personalakten anzulegen und zu führen, handelt es sich regelmäßig um eine Datenverarbeitung im Sinne der DS-GVO.[898] Nicht abschließend geklärt ist in diesem Zusammenhang, ob und inwieweit das Auskunftsrecht nach Art. 15 Abs. 1 und 3 DS-GVO neben dem betriebsverfassungsrechtlichen Einsichtsrecht des Arbeitnehmers aus § 83 Abs. 1 S. 1 BetrVG bestehen bleibt.

---

[895] Etwa: LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, 242 Rn.183; LAG, Baden-Württemberg, Urteil v. 21.03.2021 - 21 Sa 43/20, NZA-RR 2021, 410 Rn.39; LAG Niedersachsen, Urteil v. 22.10.2021 - 16 Sa 761/20, BeckRS 2021, 32008 Rn.176; zustimmend: *Lembke*, NJW 2020, 1841, 1846; *Lembke*/*Fischels*, NZA 2022, 513, 517; kritisch: *Dzida*/*Granetzky*, NZA 2020, 1201, 1206. Siehe auch: *Bäcker*, in: Kühling/Buchner, DS-GVO, Art. 15 Rn.42a.

[896] BT-Drs. 19/4724, S. 36.

[897] *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 430.

[898] *Thüsing*, in: Richardi, § 83 BetrVG Rn.4. Sollten Beschäftigtendaten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen, eröffnet § 26 Abs. 7 BDSG den Anwendungsbereich des BDSG, vgl. *Boemke/Lakies*, in: Düwell, § 83 BetrVG Rn.55.

Grundsätzlich gilt die DS-GVO aufgrund ihres Verordnungscharakters unmittelbar und zwingend, vgl. Art. 288 AEUV. Eine verdrängende Wirkung des § 83 Abs. 1 S. 1 BetrVG setzt daher voraus, dass die Vorschrift auf eine Öffnungsklausel der DS-GVO rückführbar ist. In Betracht kommen Art. 88 Abs. 1 DS-GVO und Art. 23 Abs. 1 lit. i) DS-GVO. Da beide Öffnungsklauseln im Falle einer Beschränkung der Datenauskunft Maßnahmen erfordern, die die Risiken für die von der Datenverarbeitung betroffene Person adressieren, soll für ein besseres Verständnis der nachfolgenden Analyse zunächst der Regelungsgehalt des personalaktenrechtlichen Einsichtsrechts dargestellt werden. Daran anschließend wird der Frage nachgegangen, ob und inwieweit § 83 Abs. 1 S. 1 BetrVG eine Verdrängungswirkung gegenüber Art. 15 DS-GVO zuteilwird und was dies für den Geschäftsgeheimnisschutz bedeutet, sollte § 83 Abs. 1 S. 1 BetrVG der Datenauskunft vorgehen oder neben dieser bestehen bleiben.

a) Regelungsinhalt des Einsichtsrechts

Nach § 83 Abs. 1 S. 1 BetrVG hat der Arbeitnehmer im bestehenden Arbeitsverhältnis das Recht, in die über ihn geführte Personalakte Einsicht zu nehmen.[899] Das Einsichtsrecht besteht für jeden Arbeitnehmer im Sinne des § 5 BetrVG und stellt eine Konkretisierung der arbeitsvertraglichen Rücksichtnahmepflicht dar.[900] Auf die Existenz eines Betriebsrats oder eines betriebsratsfähigen Betriebs kommt es nicht an.[901] Die Personalakte als Gegenstand der Einsicht ist begrifflich weit

---

899 Nach Beendigung des Arbeitsverhältnisses besteht das Einsichtsrecht gegenüber dem ehemaligen Arbeitgeber fort. Abgeleitet wird dies aus der nachwirkenden Rücksichtnahmepflicht des Arbeitgebers, vgl. BAG, Urteil v. 16.11.2010 - 9 AZR 573/09, NZA-RR 2021, 410.

900 *Kania*, in: ErfK-ArbR, § 83 BetrVG Rn.1; *Franzen,* NZA 2020, 1593, 1596 m. w. N. Für Beamte gilt § 110 BBG, für Angestellte des öffentlichen Dienstes § 13 BAT. § 26 Abs. 2 SprAuG enthält eine Sonderregelung für leitende Angestellte.

901 *Kania*, in: ErfK-ArbR, § 83 BetrVG Rn.1; *Franzen*, NZA 2020, 1593, 1596; *Engels*, in: Fitting, BetrVG, § 83 Rn.1; *Thüsing*, in: Richardi, § 83 BetrVG Rn.2.

zu verstehen.[902] Laut BAG gehören sämtliche Sammlungen von Urkunden und Vorgängen zum Begriff der Personalakte, die die persönlichen und dienstlichen Verhältnisse des Arbeitnehmers betreffen und die in einem inneren Zusammenhang mit dem Arbeitsverhältnis stehen, unabhängig von Form, Material, Stelle und Ort, an dem die Urkunde bzw. der Vorgang geführt werde („*materieller Begriff der Personalakte*").[903] Teil der Personalakte dürfen jedoch nur solche sein, an denen der Arbeitgeber ein berechtigtes Interesse an der Aufnahme hat.[904]

Nach dem Telos des § 83 Abs. 1 S. 1 BetrVG soll der Arbeitnehmer in der Lage sein, sich über alle personenbezogenen Daten, die der Arbeitgeber über ihn im Hinblick auf die Bewertung oder Leitung seiner Person sammelt, Kenntnis zu verschaffen.[905] Der Arbeitgeber hat dem Arbeitnehmer die in der Personalakte enthaltenen Informationen so zugänglich zu machen, dass der Arbeitnehmer den gesamten Inhalt der Personalakte visuell zur Kenntnis nehmen kann.[906] Soweit nötig, sind die Informationen vorab zu entschlüsseln und lesbar zu

---

902 *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 142.

903 Vgl. LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, 242; BAG, Urteil v. 19.07.2012 - 2 AZR 782/11, NZA 2013, 91; BAG, Urteil v. 16.11.2010 - 9 AZR 573/09, FD-ArbR 2011, 316116; BAG, Urteil v. 13.04.1988 - 5 AZR 537/86, NZA 1988, 654; BAG, Urteil v. 07.05.1980 - 4 AZR 214/78, BeckRS 1980, 30706869; *Engels*, in: Fitting/*Engels*, § 83 BetrVG Rn.5, 10; *Boemke/Lakies,* in: Düwell, § 83 BetrVG Rn.4.

904 *Engels*, in: Fitting, § 83 BetrVG Rn.5; *Franzen*, in: GK-BetrVG, § 83 BetrVG Rn.16; *Thüsing*, in: Richardi, § 83 BetrVG Rn.4.

905 *Thüsing*, in: Richardi, § 83 BetrVG Rn.4, 28, 29, mit dem zutreffenden Hinweis, dass Prozessakten eines Rechtsstreits zwischen Arbeitgeber und Arbeitnehmer nicht zu den Personalakten zählen. Es widerspräche den allgemeinen Regeln des Prozessrechts, wäre der Arbeitgeber dazu verpflichtet, dem Arbeitnehmer als gegnerische Partei Einblick in die Proessakten zu gewähren, vgl. *Engels*, in: Fitting, § 83 Rn.6; *Franzen*, in: Däubler/Hjort/Schubert, § 83 BetrVG Rn.8.

906 *Thüsing*, in: Richardi, § 83 BetrVG Rn.18; *Engels*, in: Fitting, § 83 BetrVG Rn.11; *Franzen*, in: GK-BetrVG, § 83 BetrVG Rn.23.

machen.[907] Die Akten selbst muss der Arbeitgeber dem Arbeitnehmer hingegen nicht überlassen.[908] Der Arbeitgeber hat nur dort Einsicht zu gewähren, wo sich die Personalakten befinden. Dies ergibt sich aus dem Umstand, dass es sich bei § 83 Abs. 1 S. 1 BetrVG lediglich um ein „*Einsichtsrecht*" handelt.[909] Dies schließt nicht aus, dass sich der Arbeitnehmer auf eigene Kosten Fotokopien oder Abschriften anfertigen darf.[910] Während der Einsichtnahme ist eine Anwesenheit solcher Personen, die den Arbeitnehmer überwachen sollen, nicht zulässig.[911] Die Einsichtnahme erfolgt während der Arbeitszeit, wobei Rücksicht auf die betrieblichen Belange zu nehmen ist.[912] Einen Grund muss der Arbeitnehmer nicht darlegen, die Einsicht in seine Personalakte kann er ohne besonderen Anlass begehren.

b) Verdrängungswirkung des § 83 Abs. 1 S. 1 BetrVG?

Ob und inwieweit § 83 Abs. 1 S. 1 BetrVG eine Verdrängungswirkung gegenüber Art. 15 DS-GVO entfaltet, wird im Schrifttum unterschiedlich beurteilt. Dazu sogleich. Eine verdrängende Wirkung des § 83 Abs. 1 S. 1 BetrVG setzt voraus, dass die Vorschrift auf eine Öffnungsklausel der DS-GVO rückführbar ist. Dafür gilt es zunächst zu klären, ob das personalaktenrechtliche Einsichtsrecht einen von der Datenauskunft abweichenden Regelungsgehalt aufweist.

---

907 *Boemke/Lakies,* in: Düwell, § 83 BetrVG Rn.17; *Thüsing*, in: Richardi, § 83 BetrVG Rn.18.

908 *Engels*, in: Fitting, § 83 BetrVG Rn.11; *Franzen*, in: GK-BetrVG, § 83 BetrVG Rn.23; *Thüsing*, in: Richardi, § 83 BetrVG Rn.17.

909 *Thüsing,* in: Richardi*,* § 83 BetrVG Rn.27.

910 LAG Niedersachsen, Urteil v. 31.03.1981 - 2 Sa 79/80, BeckRS 1981, 30464938; in diese Richtung auch: BAG, Urteil v. 12.07.2016 - 9 AZR 791/14, NZA 2016, 1344 Rn.10, 14; *Thüsing*, in: Richardi, § 83 BetrVG Rn.17.

911 *Thüsing*, in: Richardi, § 83 BetrVG Rn.23.

912 *Engels*, in: Fitting, § 83 BetrVG Rn.12; *Franzen*, in: GK-BetrVG, § 83 BetrVG Rn.22; *Thüsing*, in: Richardi, § 83 BetrVG Rn.22.

Ein Vergleich der Regelungsgehalte der beiden Vorschriften zeigt, dass beide dazu dienen, dem Arbeitnehmer Kenntnis von seinen in der Personalakte gespeicherten Daten zu verschaffen, um diese auf Rechtmäßigkeit überprüfen zu können.[913] Unterschiede bestehen insoweit, dass sich das personalaktenrechtliche Einsichtsrecht auf eine Einsichtnahme des Arbeitnehmers in die Personalakte während der Arbeitszeit am Arbeitsort beschränkt.[914] Währenddessen ist der Arbeitnehmer berechtigt, auf eigene Kosten Kopien anzufertigen.[915] Die Datenauskunft besteht hingegen personell uneingeschränkt und umfasst jede Datenverarbeitung, solange diese andauert.[916] Nach Art. 15 Abs. 1 und Abs. 3 DS-GVO hat der Arbeitgeber dem Arbeitnehmer dazu eine Kopie der personenbezogenen Daten in leicht verständlicher und transparenter Form auszuhändigen.[917] Das könne laut EuGH dazu führen, dass dem Arbeitnehmer Kopien vollständiger Originaldokumente zu übergeben sind, sofern diese für die Verständlichkeit der jeweiligen Datenverarbeitung unerlässlich seien.[918] Festzuhalten ist in diesem Kontext auch, dass Verstöße gegen § 83 Abs. 1 S. 1 BetrVG nicht sanktionierbar sind,[919] während Verstöße gegen die Datenauskunft empfindliche Bußgelder nach sich ziehen können, vgl. Art. 83 Abs. 5 lit. b) DS-GVO. Folgerichtig ergibt sich daraus, dass das personalaktenrechtliche Einsichtsrecht eine Beschränkung der

---

913 Vgl. BGH. Urteil v. 16.11.2010 - 9 AZR 573/09, NZA 2011, 453, Rn.42 ff.; *Franzen*, NZA 2020, 1593, 1594.

914 *Thüsing,* in: Richardi*,* § 83 BetrVG Rn.27.

915 LAG Niedersachsen, Urteil v. 31.03.1981 - 2 Sa 79/80, BeckRS 1981, 30464938; in die Richtung auch: BAG, Urteil v. 12.07.2016 - 9 AZR 791/14, NZA 2016, 1344 Rn.10, 14; *Thüsing*, in: Richardi, § 83 BetrVG Rn.17.

916 *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 145; vgl. auch LAG Hessen, Urteil v. 10.06.2021 - 9 Sa 1431/19, BeckRS 2021, 32421 Rn.32.

917 Art. 12 Abs. 1 und Art. 15 Abs. 3 DS-GVO.

918 EuGH, Urteil v. 04.05.2023 - C-487/21, Rn.45.

919 § 121 BetrVG enthält keinen Bußgeldtatbestand für Verstöße gegen § 83 Abs. 1 S. 1 BetrVG, vgl. *Schulte*/*Welge*, NZA 2019, 1110, 1111.

Datenauskunft darstellt.[920] Um zu der Annahme einer verdrängenden Wirkung des § 83 Abs. 1 S. 1 BetrVG zu gelangen, bedarf es daher einer Öffnungsklausel, auf die das personalaktenrechtliche Einsichtsrecht gestützt werden kann. In Betracht kommen Art. 88 Abs. 1 DS-GVO und Art. 23 Abs. 1 lit. i) DS-GVO.

Der Blick auf das Meinungsspektrum zeigt sodann, dass die Frage nach der Verdrängungswirkung des § 83 Abs. 1 S. 1 BetrVG nicht einheitlich diskutiert wird. Einerseits wird vertreten, dass § 83 Abs. 1 S.1 BetrVG und Art. 15 Abs. 4 DS-GVO nebeneinander bestehen.[921] Davon scheint auch das LAG Baden-Württemberg auszugehen, indem es beide Vorschriften nacheinander prüft.[922] Andererseits wird vertreten, dass § 83 Abs. 1 S. 1 BetrVG in seinem Regelungsbereich gegenüber Art. 15 Abs. 4 DS-GVO vorrangig sei, soweit Tatbestandskongruenz bestehe.[923] Gestützt wird diese Sichtweise auf § 1 Abs. 2 S. 1

---

920 So im Ergebnis auch: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 146.

921 Für ein Nebeneinander exemplarisch: *Bienemann*, in: Sydow/Marsch, Art. 15 DS-GVO Rn.90, *Franck*, in: Gola/Heckmann, Art. 15 DS-GVO Rn.4; *König*, Beschäftigtendatenschutz, § 5 Rn.15; *Fuhlrott*, NZA-RR 2019, 242, 252; *Grau/Seidensticker*, EWiR 2019, 443, 444; *Lentz*, ArbRB 2019, 150, 151; vgl. LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, 242, 252 - m. Anm. *Fuhlrott*.

922 LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18 NZA-RR 2019, 242, 252.

923 *Kania,* in: ErfK-ArbR, § 83 BetrVG Rn.13; differenziert: *Däubler*, in: Däubler/Hjort/Schubert/Wolmerath, § 26 BDSG Rn.176; *Boemke/Lakies,* in: Düwell, § 83 BetrVG Rn.56 ff.; *Franzen*, ZfA 2023, 100, 105; *Franzen*, NZA 2020, 1593, 1596; *Brink/Joos*, ZD 2019, 483, 485, 486, wobei innerhalb des Schrifttums Uneinigkeit über die Rechtsdogmatik des Art. 15 Abs. 3 DS-GVO herrscht. Außerdem unterscheiden sich diese Stimmen in der Reichweite der Tatbestandskongruenz nach Maßgabe des § 1 Abs. 2 BDSG in Bezug auf Art. 15 Abs. 3 DS-GVO. Für eine weitgehende tatbestandliche Kongruenz: *Franzen*, in: EUArbK, Art. 15 Rn.8; *Franzen*, in: GK-BetrVG, § 83 BetrVG Rn.13; *Franzen*, NZA 2020, 1593, 1596, 1597; a. A.: *Gola*, Handbuch Beschäftigtendatenschutz, Rn.2410. Die Beauskunftung der Metainformationen sei dagegen übereinstimmend nach Maßgabe des Art. 15 Abs. 1 Hs. 2 DS-GVO mangels Tatbestandskongruenz möglich.

und 2 BDSG, wonach andere Rechtsvorschriften des Bundes über den Datenschutz den Vorschriften BDSG vorgehen, soweit sie einen Sachverhalt abschließend regeln, für den auch das BDSG gilt.[924] Diese Lesart übersieht jedoch, dass § 1 Abs. 2 S. 1 und 2 BDSG nicht das Verhältnis zwischen der DS-GVO zu anderen Bundesgesetzen regelt, sondern das Verhältnis des BDSG zu anderen Bundesgesetzen in den Blick nimmt.[925] Insofern mag es noch nachvollziehbar sein, § 29 Abs. 1 S. 2 BDSG ins Feld zu führen. In diesem Fall könnte überlegt werden, ob § 83 Abs. 1 S. 1 BetrVG gegenüber § 29 Abs. 1 S. 2 BDSG vorrangig ist. Allerdings haben die vorherigen Ausführungen belegt, dass § 29 Abs. 1 S. 2 BDSG unionsrechtswidrig ist und infolgedessen unangewendet bleiben muss.[926] Selbst bei unterstellter Unionsrechtsmäßigkeit wäre zu beachten, dass § 29 Abs. 1 S. 2 BDSG auf die Öffnungsklausel des Art. 23 Abs. 1 lit. i) DS-GVO zu stützen ist. Dasselbe muss auch für § 83 Abs. 1 S. 1 BetrVG gelten. Der nationale Gesetzgeber ist nicht befugt, eine einfachgesetzliche Beschränkung von der DS-GVO herbeizuführen, um sodann im Wege einer ebenfalls einfachgesetzlichen Kollisionsregelung (§ 1 Abs. 2 S. 1 und 2 BDSG) - dafür Sorge zu tragen, dass am Ende eine dritte Norm Vorrang genießt, ohne dass es darauf ankommt, ob diese ihrerseits auf eine der Öffnungsklausel der DS-GVO gestützt werden kann. Ein solches Konstrukt übersieht den Anwendungsvorrang der DS-GVO.[927] Der Verweis auf § 1 Abs. 2 S. 1, S. 2 BDSG ist daher nicht zielführend.[928] Die DS-GVO beansprucht unmittelbare und zwingende Geltung, Art. 288 AEUV. Von ihr kann nur

---

924 BT-Drs. 18/11325, S. 79; *Reif*, in: Gola/Heckmann, § 1 BDSG Rn.10; *Franzen*, in: EuArbRK, Art. 15 DS-GVO Rn.8; *Gola*, Handbuch Beschäftigtendatenschutz, Rn.2410; *Franzen*, NZA 2020, 1593, 1596.

925 In diese Richtung auch: *Klar*, in: *Kühling*/*Buchner*, § 1 BDSG Rn.15; *Böken*, in: Sydow/Marsch, § 1 BDSG Rn.22; *Gusy*/*Eichenhofer*, in: BeckOK-DatenschutzR, § 1 BDSG Rn.79.

926 Siehe: Kapitel C) I. 3. c) bb) (2).

927 Vgl. EuGH, Urteil v. 14.10.2004 - C-113/02, NvWZ 2005, 432 Rn.6; EuGH, Urteil v. 21.12.2011 - C-136/10, BeckRS 2012, 80086 Rn.41; EuGH, Urteil v. 25.10.2012 - C-592/11, BeckRS 2012, 82208 Rn.36.

928 Ebenso: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 148.

abgewichen werden, soweit sich diese Abweichung auf eine Öffnungsklausel stützen lässt. Dementsprechend muss die Frage des Verhältnisses zwischen § 83 Abs. 1 S. 1 BetrVG und Art. 15 DS-GVO anhand einer Öffnungsklausel der DS-GVO analysiert werden. In Betracht kommen Art. 88 Abs. 1 DS-GVO und Art. 23 Abs. 1 lit. i) DS-GVO.

Fraglich ist, ob § 83 Abs. 1 S. 1 BetrVG auf die Öffnungsklausel des Art. 88 Abs. 1 DS-GVO gestützt werden kann. Das Einsichtsrecht stellt zunächst eine Vorschrift im Beschäftigungskontext dar.[929] Des Weiteren ist festzustellen, dass Art. 88 Abs. 1 DS-GVO nicht auf spezifische Vorschriften begrenzt ist, deren Regelungsgegenstand eine Rechtsgrundlage für eine Datenverarbeitung ist.[930] Wie bereits zuvor herausgearbeitet, umfassen spezifischere Vorschriften die einer jeden Datenverarbeitung immanenten Grundsätze der Datenverarbeitung (Art. 5 DS-GVO). Der Grundsatz der Datentransparenz wohnt demgemäß jeder Datenverarbeitung inne, vgl. Art. 5 Abs. 1 lit. a) DS-GVO. Dementsprechend können spezifischere Vorschriften im Sinne des Art. 88 Abs. 1 DS-GVO auch Transparenzvorgaben hinsichtlich der Betroffenenrechte sein. Allerdings können spezifischere Vorschriften im Sinne des Art. 88 Abs. 1 DS-GVO nur solche sein, die die Vorgaben des Art. 88 Abs. 2 DS-GVO wahren. Art. 88 Abs. 1 DS-GVO ist daher in Zusammenhang mit Art. 88 Abs. 2 DS-GVO zu verstehen. Dies hat der EuGH jüngst bestätigt.[931] Laut EuGH sei Art. 88 Abs. 1 DS-GVO dahingehend auszulegen, dass eine nationale Rechtsvorschrift keine „*spezifischere Vorschrift*“ sei, wenn sie nicht die Vorgaben von Art. 88 Abs. 2 DS-GVO erfülle.[932] Nötig sei, dass die spezifischere Vorschrift geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf

---

929 *Tiedemann*, in: Sydow/Marsch, Art. 88 DS-GVO Rn.6.

930 A. A.: *Lembke*, in: HWK, Art. 88 DS-GVO Rn.6; *Lembke*, NJW 2020, 1841, 1845 f.; *Schulte*/*Welge*, NZA 2019, 1110, 1115.

931 EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.85.

932 EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.85.

die Transparenz der Verarbeitung enthält.[933] Gemeint sind damit Vorgaben, die die Rechte der von der Datenverarbeitung betroffenen Person achtet und sicherstellt, dass der Grundsatz der Datentransparenz (Art. 5 Abs. 1 lit. a) DS-GVO) hinreichend besteht.[934]

Demzufolge darf eine spezifischere Vorschrift nach Art. 88 Abs. 1 DS-GVO nicht die allgemeinen Grundsätze einer Datenverarbeitung unterlaufen (Art. 5 DS-GVO). Die Grundsätze bilden folgerichtig einen Mindestschutz für die Verarbeitung personenbezogener Daten im Beschäftigungskontext, wobei der nationale Gesetzgeber in ihrer konkreten Ausgestaltung frei bleibt.[935] Dieses Verständnis überzeugt, weil auf die Art ein einheitliches Datenschutzniveau innerhalb der Europäischen Union gewährleistet ist, ohne dass den Mitgliedstaaten der gebotene Handlungsspielraum genommen wird, den es insbesondere im Beschäftigungskontext braucht. Vor diesem Hintergrund sind eigenständige Vorschriften in Bezug auf die Datenauskunft möglich, soweit sie die Grundsätze der Datenverarbeitung in Art. 5 DS-GVO nicht unterlaufen.[936] Erwägungsgrund 11 der DS-GVO formuliert in diesem Zusammenhang, dass ein unionsweiter wirksamer Schutz eine präzise Festlegung der Rechte der betroffenen Person erfordert. Dem

---

933 *Thüsing*/*Peisker,* fragen in diesem Zusammenhang zu Recht in Bezug auf Betriebsvereinbarungen, ob immer explizite Vorgaben nötig seien, vgl. *Thüsing*/*Peisker*, NZA 2023, 213, 214. Nach hiesiger Auffassung sind explizite Vorgaben zumindest bzgl. der Datentransparenz nötig, soweit die spezifischere Vorschrift eine Beschränkung der Betroffenenrechte, respektive des Transparenzgrundsatzes darstellt, vgl. Art. 5 Abs. 1 lit. a) DS-GVO, Art. 12 ff. DS-GVO. Im Übrigen stellen die ohnehin zu beachtenden Betroffenenrechte in Art. 12 ff. DS-GVO den Grundsatz der Datentransparenz sicher. Diese repetitiv zu wiederholen, erscheint nicht sachgerecht. Sinnvoll scheint dagegen eine Bezugnahme in Form eines Hinweises, z. B. im Rahmen der Gesetzesbegründung respektive einer Betriebsvereinbarung.

934 EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.50, 96.

935 Zu der im Schrifttum bislang breit diskutierten Frage, inwieweit Abweichungen vom Schutzniveau der DS-GVO über Art. 88 Abs. 1 und Abs. 2 DS-GVO möglich sind, siehe: Kapitel C) I. 3. c) bb) (1) (c), dort: Fn.716.

936 Vgl. EuGH, Urteil v. 30.03.2023, NJW 2023, 1639 Rn.85.

Telos der Datentransparenz entsprechend kommt es dafür darauf an, ob die Vorschrift Maßnahmen vorsieht, die sicherstellen, dass die von der Datenverarbeitung betroffene Person über die Datenverarbeitung hinreichend Kenntnis erlangt, um die Rechtmäßigkeit der Datenverarbeitung zu überprüfen und ggf. durchzusetzen.[937]

Demgemäß ist zu fragen, ob § 83 Abs. 1 S. 1 BetrVG sicherstellt, dass die von der Datenverarbeitung betroffene Person im Rahmen des personalaktenrechtlichen Einsichtsrechts hinreichend Kenntnis von den über sie gespeicherten Daten in der Personalakte erhält, um deren Rechtmäßigkeit zu prüfen und ggf. durchzusetzen.

Die Gegenüberstellung von § 83 Abs. 1 S. 1 BetrVG und Art. 15 DS-GVO hat gezeigt, dass das personalaktenrechtliche Einsichtsrecht im Vergleich zu der Datenauskunft zeitlich und örtlich begrenzt ist.[938] Darüber hinaus erhält der Arbeitnehmer nach § 83 Abs. 1S. 1 BetrVG seine Daten lediglich zur Einsicht, verbunden mit der Möglichkeit auf eigene Kosten Kopien anzufertigen. Sollten ihm dabei Fehler unterlaufen, gingen diese zu seinen Lasten.[939] Insbesondere mit Blick auf die in der Personalakte typischerweise enthaltenen Daten, die sich für den Arbeitnehmer arbeitsrechtlich fundamental auswirken können (z. B. Abmahnung), ist es für diesen von besonderer Wichtigkeit, deren rechtmäßige Verarbeitung sicherzustellen. Dafür ist der Arbeitnehmer darauf angewiesen, seine Daten dauerhaft in einer verständlichen und transparenten Weise zur Verfügung gestellt zu bekommen, ohne dabei das Risiko für etwaige Fehler tragen zu müssen, die im Rahmen der Kenntniserlangung unterlaufen können.[940] Beschränkt sich das Einsichtsrecht daher auf selbst angefertigte Kopien, die während der Arbeitszeit am Betriebsort durch den Arbeitnehmer selbst

---

[937] Erwägungsgrund 63 S. 1 der DS-GVO; vgl. LAG Baden-Württemberg, Urteil v. 17.03.2021, 21 Sa 43/20, NZA-RR 2021, 410.
Siehe auch: Kapitel C) I. 1. a).

[938] Vgl. *Wünschelbaum*, BB 2019, 2102, 2106.

[939] *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 157.

[940] So auch: *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, S. 157.

angefertigt worden sind, ist die Überprüfung der Rechtmäßigkeit der Datenverarbeitung nicht hinreichend gewährleistet.[941] Erschwerend kommt hinzu, dass nach § 83 Abs. 1 S. 1 BetrVG kein Anspruch auf Überlassung der Personalakte besteht, selbst dann nicht, wenn es im Betrieb keine Möglichkeit gibt, Fotokopien zu fertigen.[942] Folgerichtig erfüllt das personalaktenrechtliche Einsichtsrecht in § 83 Abs. 1 S. 1 BetrVG die obligatorischen Transparenzanforderungen des Art. 88 Abs. 2 DS-GVO nicht und kann deshalb nicht als spezifischere Vorschrift im Beschäftigungskontext auf die Öffnungsklausel des Art. 88 Abs. 1 DS-GVO gestützt werden.

Aus denselben Gründen lässt sich § 83 Abs. 1 S. 1 BetrVG auch nicht auf die Öffnungsklausel des Art. 23 Abs. 1 lit. i) DS-GVO zurückführen. Die hinreichende Gewährleistung des Transparenzgrundsatzes ist auch nach Art. 23 Abs. 2 lit. g) DS-GVO zwingende Voraussetzung für eine Beschränkung der Datenauskunft im Sinne des Art. 23 Abs. 1 lit. i) DS-GVO. Mangels Öffnungsklausel verdrängt das personalaktenrechtliche Einsichtsrecht die Datenauskunft daher nicht. Da § 83 Abs. 1 S. 1 BetrVG jedoch nicht im Widerspruch zur Datenauskunft steht,[943] bleibt das personalaktenrechtliche Einsichtsrecht neben der Datenauskunft bestehen.[944] Zu Recht hat das LAG Baden-Württemberg daher beide Vorschriften nebeneinander geprüft.[945]

---

941 *Buschmann*, in: DKW, § 83 BetrVG Rn.4; *Engels*, in: Fitting, § 83 BetrVG Rn.4; *Franzen*, in: GK-BetrVG, § 83 BetrVG Rn.16.

942 *Thüsing,* in: Richardi*,* § 83 BetrVG Rn.17; *Engels*, in: Fitting, § 83 BetrVG Rn.11; *Franzen*, in: Däubler/Hjort/Schubert, § 83 BetrVG Rn.82.

943 Vgl. EuGH, Urteil v. 09.03.1978 - 106/77, ECLI:EU:C:1978:49 Rn.17, NJW 1978, 1741; EuGH, Urteil v. 19.06.1990 - C-213/89, ECLI:EU:C:1990:257 Rn.18, NJW 1991, 2271; EuGH, Urteil v. 04.02.2016 - C-336/14, ECLI:EU:C:2016:72 Rn.52, NVwZ 2016, 369.

944 So auch die überwiegende Literaturmeinung. Exemplarisch: *Bienemann*, in: Sydow/Marsch, Art. 15 DS-GVO Rn.90, *Franck*, in: Gola/Heckmann, Art. 15 DS-GVO Rn.4; *König*, Beschäftigtendatenschutz, § 5 Rn.15; *Fuhlrott*, NZA-RR 2019, 242, 252; *Grau*/*Seidensticker*, EWiR 2019, 443, 444; *Lentz*, ArbRB 2019, 150, 151.

945 LAG Baden-Württemberg, Urteil v. 20.12.2018 – 17 Sa 11/18, NZA-RR 2019, 242 Rn.155.

c) Berücksichtigungsfähigkeit der Geheimhaltungsinteressen

Inwieweit betriebliche Geheimhaltungsinteressen im Rahmen des § 83 Abs. 1 S. 1 BetrVG berücksichtigungsfähig sind, ist ebenfalls nicht abschließend geklärt. Richtig ist, dass die bloße Kennzeichnung als „*vertraulich*" das Einsichtsrecht nicht einschränkt.[946] Hintergrund ist, dass das Führen von Geheimakten unzulässig ist.[947] Das Einsichtsrecht nach § 83 Abs. 1 S. 1 BetrVG bezieht sich daher in der Regel auch auf solche Unterlagen, die der Arbeitgeber als „*vertraulich*" gekennzeichnet hat.[948] Die Kennzeichnung stellt sodann die Erkennbarkeit der arbeitgeberseitigen Geheimhaltungsinteressen sicher, sodass der Arbeitnehmer aufgrund seiner arbeitsvertraglichen Treuepflicht zur Verschwiegenheit verpflichtet ist.

Nach hiesiger Auffassung scheint eine Berücksichtigung betrieblicher Geheimhaltungsinteressen im Sinne der Regelung des Art. 15 Abs. 4 DS-GVO geboten. Dafür spricht einerseits ein praktisches Bedürfnis. Aus Arbeitgebersicht wird es sich nicht immer vermeiden lassen, Personalakten frei von Geschäftsgeheimnissen zu führen.[949] Darüber hinaus ist § 83 Abs. 1 S. 1 BetrVG Ausdruck der arbeitsvertraglichen Rücksichtnahmepflicht, § 241 Abs. 2 BGB. Das Wesen dieser Rücksichtnahmepflicht ist jedoch, dass diese auf Gegenseitigkeit beruht. So hat der Arbeitgeber einerseits die Interessen des Arbeitnehmers zu berücksichtigen und ihm zur Überprüfung der Daten in seiner Personalakte Einsicht nach § 83 Abs. 1 S. 1 BetrVG zu gewähren. Auf der

---

946 *Thüsing,* in: Richardi*,* § 83 BetrVG Rn.9, 16; *Engels*, in: Fitting, § 83 BetrVG Rn.5; *Franzen*, in: GK-BetrVG, § 83 BetrVG Rn.7; *Kania*, in: ErK-ArbR*,* § 83 BetrVG Rn.2. Anders wohl das LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, 242, das eine Beschränkung des Einsichtsrechts aufgrund der Geheimhaltungsinteressen des Arbeitgebers geprüft hat.

947 *Thüsing,* in: Richardi*,* § 83 BetrVG Rn.9; *Engels*, in: Fitting, § 83 BetrVG Rn.5; *Franzen*, in: Däubler/Hjort/Schubert, § 83 BetrVG Rn.7; *Kania*, in: ErK-ArbR, § 83 BetrVG Rn.2.

948 *Thüsing*, in: Richardi, § 83 BetrVG Rn.9, 16.

949 *Thüsing*, in: Richardi*,* § 83 BetrVG Rn.16.

anderen Seite hat aber auch der Arbeitnehmer Rücksicht auf die Geheimhaltungsinteressen des Arbeitgebers zu nehmen, § 241 Abs. 2 BGB. Das Akteneinsichtsrecht ist daher keineswegs absolut zu verstehen. Der Arbeitgeber ist nach hiesiger Auffassung berechtigt, geheime Informationen zu schwärzen, soweit es seine berechtigten Geheimhaltungsinteressen erfordern, ehe er dem Arbeitnehmer Akteneinsicht gewährt.[950] Aus Gründen der Einheit der Rechtsordnung sind dazu dieselben Maßstäbe anzusetzen, die sich aus Art. 15 Abs. 4 DS-GVO ergeben.

4. Zusammenfassender Überblick

Das Spannungsverhältnis zwischen Geschäftsgeheimnisschutz und datenschutzrechtlichem Auskunftsrecht bildet einen Konflikt widerstreitender Rechtspositionen, die jeweils grundrechtliche, unionsrechtliche und völkerrechtliche Verankerung erfahren haben und notwendigerweise in einen angemessenen Ausgleich zu bringen sind. Das Recht auf Datenauskunft ist charta-rechtlich in Form eines subjektiven Rechts in Art. 8 Abs. 2 GR-CH verankert. Es handelt sich folgerichtig um ein normgeprägtes Grundrecht mit einem eigenen Schutzgehalt, dessen Beschränkungsmöglichkeiten sich aus Art. 52 Abs. 1 GR-CH ergeben. Telos der Datenauskunft ist, die von der Datenverarbeitung betroffene Person in die Lage zu versetzen, die Rechtmäßigkeit der Verarbeitung ihrer personenbezogenen Daten zu prüfen, um diese ggf. durchsetzen zu können. Auf die Art stellt die Datenauskunft zugleich sicher, dass die Eingriffsintensität der Datenverarbeitung in die informationelle Selbstbestimmungsfreiheit der von der Datenverarbeitung betroffenen Person abgesenkt wird. Das Grundgesetz enthält ebenfalls ein verfassungsunmittelbares Auskunftsrecht mit vergleichbarem Telos. Dies ist nach der Rechtsprechung des BVerfG mittlerweile anerkannt und Teil des informationellen Selbstbestimmungsrechts.[951]

---

[950] Vgl. auch: LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, 242.

[951] Siehe: Kapitel C) I. 1. a). und Kapitel C) II. 1.

Nach Art. 15 Abs. 1 Hs. 1 DS-GVO hat die von der Datenverarbeitung betroffene Person das Recht, von der für die Datenverarbeitung verantwortlichen Stelle eine Bestätigung darüber zu verlangen, ob diese sie betreffende personenbezogene Daten verarbeitet (sog. „*Ob*“ der Datenverarbeitung). Ist dies der Fall, hat die von der Datenverarbeitung betroffene Person ein Recht auf Auskunft über diese personenbezogenen Daten (Art 15 Abs. 1 Hs. 2 Var. 1 DS-GVO) sowie die in Art. 15 Abs. 1 Hs. 2 Var. 2 DS-GVO gelisteten Metainformationen der Datenverarbeitung. Das „*Ob*“ der Datenverarbeitung geht der weiteren Auskunft demgemäß zeitlich vor. Die Kopie-Verpflichtung in Art. 15 Abs. 3 DS-GVO bildet die Erfüllungsmodalität der Auskunft, wenn es auf Rechtsfolgenseite darum geht, auf welche Art und Weise die Datenauskunft nach Art. 15 Abs. 1 DS-GVO zu erfüllen ist. Der EuGH hat klargestellt, dass das Recht auf Kopie kein eigenständiges Recht neben dem Auskunftsrecht gewähre, sondern lediglich dessen Modalitäten festlege.[952] Art. 15 Abs. 3 DS-GVO ist deshalb als eine Erweiterung des Art. 12 DS-GVO zu verstehen, der ebenfalls die Modalitäten in Bezug auf die Datenauskunft regelt. Zu beachten ist allerdings, dass sich die Erfüllungsmodalität der Kopie in Art. 15 Abs. 3 S. 1 DS-GVO ihrem Wortlaut nach ausschließlich auf die Beauskunftung der „*personenbezogenen Daten*“, nicht jedoch auf die Beauskunftung der „*Informationen*“ in Art. 15 Abs. 1 Hs. 2 Var. 2 DS-GVO bezieht. Dies ist vor dem Hintergrund der Kopie in ihrer Eigenschaft als Erfüllungsmodalität zu verstehen. Die Kopie bezieht sich auf die personenbezogenen Daten in Art. 15 Abs. 1 Hs. 2 Var. 1 DS-GVO, weil über diese ohne Weiteres in Form einer Kopie Auskunft erteilt werden kann. Dagegen erweist sich eine Kopie-Erteilung in Bezug auf die Metainformationen in aller Regel schwierig. Zu Recht bleibt der Verantwortliche daher in Bezug auf die Beauskunftung der Metainformationen in der Art und Weise seiner Auskunftserteilung nach Maßgabe des Art. 12 DS-GVO frei.[953]

---

[952] Vgl. EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.31, 32, EuZW 2023, 575.
[953] Siehe: Kapitel C) II. 1. a).

Gleichwohl ist zu bedenken, dass sich die Beschränkungsmöglichkeit in Art. 15 Abs. 4 DS-GVO - trotz des Verweises auf die Kopie in Art. 15 Abs. 3 S. 1 DS-GVO - auf das Auskunftsrecht mitsamt der Metainformationen erstreckt, vgl. Art. 15 Abs. 1 Hs. 2 Var. 2 DS-GVO.[954] Die Frage der Beschränkung des Auskunftsrechts ist losgelöst vom Bezugspunkt der Erfüllungsmodalität zu beantworten. Aus Art. 52 GR-CH folgt, dass das Recht auf Datenauskunft nicht absolut gilt. Die gebotene charta-rechtliche Auslegung des Art. 15 DS-GVO führt daher zwingend zu der Annahme, dass kollidierende grundrechtlich geschützte Positionen die Beauskunftung der Metainformationen beschränken können müssen. Vor diesem Hintergrund wäre es sinnvoll, Art. 15 Abs. 4 DS-GVO an den Wortlaut seines dazugehörigen Erwägungsgrundes 63 der DS-GVO sprachlich anzupassen. Anders als Art. 15 Abs. 4 DS-GVO unterscheidet Erwägungsgrund 63 der DS-GVO nicht zwischen „*personenbezogenen Daten*“ und „*Informationen*“, sondern formuliert allgemein „*Auskunftsrecht*“ bzw. „*Recht*“.

Hinsichtlich der inhaltlichen Reichweite des Auskunftsrechts verlangt das Recht auf Kopie zwar nicht zwingend die Reproduktion von Auszügen aus Dokumenten oder gar von vollständigen Dokumenten. Einzelfallbezogen ist dies aber möglich. Maßgeblich ist, ob sich die verarbeiteten Daten nur in ihrem jeweiligen Kontext erschließen lassen.[955] Entscheidend ist, ob die nach Art. 12 Abs. 1 DS-GVO obligatorische Verständlichkeit und Transparenz der Datenauskunft eine Kontextualisierung der verarbeiteten Daten erfordert. Die Frage, wann eine Kontextualisierung erforderlich oder unerlässlich ist, lässt der EuGH unbeantwortet. Maßgeblich sind die Umstände des jeweiligen Einzelfalls. Richtschnur ist das Telos der Datenauskunft, das der von der Datenverarbeitung betroffenen Person ermöglichen will, Kenntnis von der Datenverarbeitung zu erlangen, um sodann deren Rechtmäßigkeit prüfen und ggf. durchsetzen zu können. Eine bloße Auflistung oder Beschreibung der verarbeiteten personenbezogenen Daten wird

[954] Siehe: Kapitel C) II. 1. a).
[955] Siehe: Kapitel C) II. 1. b).

dem nicht gerecht.[956] Dies hat zur Folge, dass die Datenauskunft im Einzelfall sehr weit gehen kann. Inwieweit hier eine einschränkende Lesart gelingen kann, bleibt abzuwarten. Es spricht Vieles dafür, dass der EuGH auch im Falle eines Auskunftsersuchens zu datenschutzfremden Zwecken zu der grundsätzlichen Annahme eines Auskunftsrechts gelangen wird.[957]

Beschränkungen erfährt die Datenauskunft verordnungsunmittelbar durch die Rechte und Freiheiten anderer, vgl. Art. 15 Abs. 4 DS-GVO. In Betracht kommt auch der Abschluss einer Betriebsvereinbarung, Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 4 BDSG. Im Rahmen des Art. 15 Abs. 4 DS-GVO entscheidet eine umfassende Interessenabwägung zwischen dem informationellen Selbstbestimmungsrecht der von der Datenverarbeitung betroffenen Person und den berechtigten Geheimhaltungsinteressen des datenschutzrechtlich Verantwortlichen.

Im Bereich des Geschäftsgeheimnisschutzes ist davon auszugehen, dass ein berechtigtes Geheimhaltungsinteresse besteht, soweit es sich um ein Geschäftsgeheimnis im Sinne des GeschGehG handelt. Inwieweit der Geschäftsgeheimnisschutz überwiegt, ist sodann einzelfallbezogen zu entscheiden. Aus dem Vorliegen eines berechtigten Geheimhaltungsinteresses folgt noch keine Beschränkung der Datenauskunft. Vielmehr erfordert Art. 15 Abs. 4 DS-GVO eine eigenständige Interessenabwägung. Dazu ist das berechtigte Geheimhaltungsinteresse des datenschutzrechtlich Verantwortlichen (Art. 12 Abs. 1 GG, Art. 14 Abs. 1 GG sowie Art. 16 und Art. 17 GR-CH) mit dem Auskunftsinteresse des Arbeitnehmers (Art. 8 Abs. 2 S. 2 Grundrechte-Charta) nach Maßgabe des Verhältnismäßigkeitsgrundsatzes in einen angemessenen Ausgleich zu bringen. Ein pauschaler Hinweis

---

956 EuGH, Urteil v. 04.05.2023 - C-487/21 Rn.21.

957 Vgl. GA *Emiliou*, Schlussantrag v. 20.04.2023 - C-307/22, BeckRS 2023, 7659 Rn.84; ebenso der dazu vorausgegangene BGH, Beschluss v. 29.03.2022 - VI ZR 1352/20, ZD 2022, 497 Rn.19 sowie das OLG Köln, Urteil v. 13.05.2022 - 20 U 295/21, ZD 2022, 619 Rn.54.

auf den Geschäftsgeheimnisschutz genügt jedenfalls nicht. Vielmehr bedarf es eines Nachweises durch den datenschutzrechtlichen Verantwortlichen, dass ein berechtigtes Geheimhaltungsinteresse besteht und dieses das informationelle Selbstbestimmungsrecht der von der Datenverarbeitung betroffenen Person überwiegt. Maßgeblich sind die Umstände des jeweiligen Einzelfalls.

Ist das Geschäftsgeheimnis dem Auskunftsersuchenden bereits bekannt, scheidet eine Beschränkung der Datenauskunft von Vornherein aus. Gleiches gilt, sollte die Erlangung des Geschäftsgeheimnisses nach Maßgabe des § 3 GeschGehG erlaubt sein. Dabei ist zu beachten, dass das Auskunftsrecht nach Art. 15 DS-GVO kein Informationsrecht im Sinne des § 3 Abs. 1 Nr. 3 GeschGehG ist. Art. 15 DS-GVO gilt unabhängig vom Bestehen eines Arbeitsverhältnisses für jede von einer Datenverarbeitung betroffene Person. Art. 15 DS-GVO ist daher kein Informationsrecht im Sinne des § 3 Abs. 1 Nr. 3 GeschGehG. Die Datenauskunft ist also nicht generell nach § 3 Abs. 1 Nr. 3 GeschGehG erlaubt.[958] Berücksichtigungsfähige Umstände zu Gunsten des Geheimnisschutzes im Rahmen des Art. 15 Abs. 4 DS-GVO können insbesondere die mit der Offenlegung verbundenen Risiken für den Geheimnisinhaber sein. Dem Unternehmen drohen erhebliche Wettbewerbsnachteile. Im Ergebnis wird daher das betriebliche Geheimhaltungsinteresse das informationelle Selbstbestimmungsrecht regelmäßig überwiegen. Dafür spricht, dass die Datenauskunft nicht dazu dienen darf, den datenschutzrechtlich Verantwortlichen über sensible Informationen auszuspionieren. Auch sollen sich Beschäftigte über die Datenauskunft keinen generellen Zugang zu Geschäftsgeheimnissen verschaffen können.

Der Grundsatz der Verhältnismäßigkeit gebietet es, dass die gegenläufigen Geheimhaltungsinteressen zu keinem Ausschluss der Datenauskunft führen. Arbeitgeber haben daher die entsprechenden Passagen zu schwärzen bzw. anderweitig unkenntlich zu machen, ehe sie dem

[958] Siehe: Kapitel C) II. 2.

Auskunftsverlangen nachkommen. In Betracht kommt auch eine strafbewehrte Verschwiegenheitsvereinbarungen. Herausfordernd ist allerdings, dass die arbeitsgerichtliche Praxis hohe Anforderungen an den darlegungs- und beweispflichtigen datenschutzrechtlichen Verantwortlichen in Bezug auf den Nachweis seines berechtigten Geheimhaltungsinteresses stellt.[959] Im Prozess läuft dies regelmäßig auf die Offenlegung des Geschäftsgeheimnisses hinaus. Zwar stellen die §§ 19 ff. GeschGehG sicher, dass der Personenkreis derjenigen, die Kenntnis von dem Geschäftsgeheimnis erhalten, klein gehalten wird. Dennoch erfolgt eine Offenlegung an wenigstens eine natürliche Person jeder Partei und ihre Prozessvertreter oder sonstige Vertreter, die für den Geheimnisinhaber stets risikobehaftet ist.

Darüber hinaus ist zu beachten, dass § 83 Abs. 1 S. 1 BetrVG das Recht auf Datenauskunft nicht verdrängt. Wäre das personalaktenrechtliche Einsichtsrecht vorrangig, ginge dies mit einer Beschränkung der Datenauskunft einher. Eine verdrängende Wirkung des § 83 Abs. 1 S. 1 BetrVG setzt daher voraus, dass die Vorschrift auf eine Öffnungsklausel der DS-GVO rückführbar ist. § 1 Abs. 2 BDSG ist insofern ohne Bedeutung.[960] Mit Blick auf die Öffnungsklausel des Art. 88 Abs. 1 DS-GVO erfüllt das personalaktenrechtliche Einsichtsrecht die obligatorischen Transparenzanforderungen des Art. 88 Abs. 2 DS-GVO nicht. Es kann deshalb nicht als spezifischere Vorschrift im Beschäftigungskontext auf die Öffnungsklausel des Art. 88 Abs. 1 DS-GVO gestützt werden. Indem sich das Einsichtsrecht auf selbst angefertigte Kopien während der Arbeitszeit am Betriebsort durch den Arbeitnehmer beschränkt, ist die Überprüfung der Rechtmäßigkeit der Datenverarbeitung nicht hinreichend

---

[959] Etwa: LAG Baden-Württemberg, Urteil v. 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, 242 Rn.183; LAG, Baden-Württemberg, Urteil v. 21.03.2021 - 21 Sa 43/20, NZA-RR 2021, 410 Rn.39; LAG Niedersachsen, Urteil v. 22.10.2021 – 16 Sa 761/20, BeckRS 2021, 32008 Rn.176; zustimmend: *Lembke*, NJW 2020, 1841, 1846; *Lembke*/*Fischels*, NZA 2022, 513, 517; kritisch: *Dzida*/*Granetzky*, NZA 2020, 1201, 1206. Siehe auch: *Bäcker*, in: Kühling/Buchner, DS-GVO, Art. 15 Rn.42a.

[960] Siehe: Kapitel C) II. 2. b).

gewährleistet. Der Arbeitnehmer ist jedoch darauf angewiesen, seine Daten dauerhaft in einer verständlichen und transparenten Weise zur Verfügung gestellt zu bekommen, ohne dabei das Risiko für etwaige Fehler tragen zu müssen, die im Rahmen der Kenntniserlangung unterlaufen können. Aus denselben Gründen lässt sich § 83 Abs. 1 S. 1 BetrVG auch nicht auf die Öffnungsklausel Art. 23 Abs. 1 lit. i) DS-GVO zurückführen. Die hinreichende Gewährleistung des Transparenzgrundsatzes ist ebenfalls zwingende Voraussetzung für eine Beschränkung der Datenauskunft im Sinne des Art. 23 Abs. 2 lit. g) DS-GVO. Folgerichtig ist Art. 15 DS-GVO im Beschäftigungskontext uneingeschränkt anwendbar. Die Kopie-Erteilung kann nicht durch eine Einsichtnahme ersetzt werden. Mangels Öffnungsklausel verdrängt das personalaktenrechtliche Einsichtsrecht die Datenauskunft daher nicht.[961]

Da § 83 Abs. 1 S. 1 BetrVG nicht im Widerspruch zur Datenauskunft steht, bleibt das personalaktenrechtliche Einsichtsrecht neben der Datenauskunft bestehen. Aus Gründen der Einheit der Rechtsordnung sind sodann dieselben Maßstäbe im Rahmen des § 83 Abs. 1 S. 1 BetrVG anzusetzen, die sich aus Art. 15 Abs. 4 DS-GVO ergeben. Der Arbeitgeber ist berechtigt, geheime Informationen zu schwärzen, soweit es seine berechtigten Geheimhaltungsinteressen erfordern, ehe er Akteneinsicht gewährt.[962]

III. Geschäftsgeheimnisschutz im Rahmen der Betriebsratsarbeit

Ein weiteres Spannungsfeld bildet der Geschäftsgeheimnisschutz im Hinblick auf die Beteiligungsrechte des Betriebsrats. In den nächsten Abschnitten wird die Darstellung die Grundlagen des Geheimnisschutzes im Bereich der Betriebsratsarbeit herausstellen. Dazu stellt die vorliegende Arbeit zunächst die Verschwiegenheitspflicht der Betriebsratsmitglieder nach § 79 Abs. 1 S. 1 BetrVG dar. Anschlie-

961 Siehe: Kapitel C) II. 2. b).
962 Siehe: Kapitel C) II. 2. c).

ßend geht die Untersuchung der Frage nach, unter welchen Voraussetzungen ein Betriebsratsmitglied ein Geschäftsgeheimnis erlangen darf und welche Besonderheiten mit Blick auf eine etwaige Weitergabe bestehen, sollte ein Betriebsratsmitglied eine Informationsweitergabe zu Zwecken des Whistleblowings beabsichtigen. Zu beachten ist, dass sich ein Betriebsratsmitglied in diesen Fällen nicht mehr nur im Spannungsfeld zwischen eigener Meinungsfreiheit und unternehmerischen Geheimhaltungsinteressen bewegt, sondern auch dem betriebsverfassungsrechtlichen Gebot der vertrauensvollen Zusammenarbeit unterliegt (§ 2 Abs. 1 BetrVG).

1. Verschwiegenheitspflicht, § 79 Abs. 1 S. 1 BetrVG

Nach § 79 Abs. 1 S. 1 BetrVG sind die (Ersatz-) Mitglieder des Betriebsrats verpflichtet, Betriebs- oder Geschäftsgeheimnisse, die ihnen wegen ihrer Zugehörigkeit zum Betriebsrat bekannt geworden und vom Arbeitgeber ausdrücklich als geheimhaltungsbedürftig bezeichnet worden sind, nicht zu offenbaren und nicht zu verwerten.[963] Nach § 79 Abs. 1 S. 2 BetrVG gilt die Verschwiegenheitspflicht nicht gegenüber Mitgliedern des Betriebsrats und weiteren Stellen, da diese ihrerseits zur Verschwiegenheit verpflichtet sind. Die Verschwiegenheitspflicht endet, soweit es sich bei der jeweiligen Tatsache um kein Betriebs- oder Geschäftsgeheimnis mehr handelt bzw. der Arbeitgeber seine Vertraulichkeitserklärung aufgibt.[964] Ein Ausscheiden aus dem Betriebsrat oder die Beendigung des Arbeitsverhältnisses hebt die Verschwiegenheitspflicht nicht auf, vgl. § 79 Abs. 1 S. 2 BetrVG.[965]

Im Vergleich zu der Definition eines Geschäftsgeheimnisses i. S. d. § 2 GeschGehG, hat sich in der Rechtsprechung zu § 79 Abs. 1 S. 1 BetrVG eine eigenständige Definition des Betriebs- oder

963 *Naber/Peukert/Seeger,* NZA 2019, 583, 588; *Trebeck/Schulte-Wissermann*, NZA 2018, 1175, 1180; *Karthaus*, NZA 2018, 1190, 1192.
964 *Niklas*, ArbRB 2020, S. 122, 123.
965 *Thüsing*, in: Richardi, § 79 BetrVG Rn.17.

Geschäftsgeheimnisses entwickelt.[966] Diese ist auch nach Einführung des GeschGehG weiter maßgeblich.[967] Dafür spricht, dass die Definition des Geschäftsgeheimnisses im Sinne des § 2 Nr. 1 GeschGehG ausschließlich für das GeschGehG gilt und nicht auf andere Regelwerke übertragen werden kann. Für diese Lesart streitet bereits der Wortlaut des § 2 GeschGehG, der die Begriffe „*im Sinne dieses Gesetzes*", also dem GeschGehG bestimmt.[968] Für dieses Verständnis spricht ferner, dass der Gesetzgeber mit der Einführung des GeschGehG das Verhältnis von Arbeitgeber, Arbeitnehmern und Arbeitnehmervertretungen nicht berühren wollte, §§ 1 Abs. 3 Nr. 4, 3 und Abs. 1 Nr. 3, Abs. 2, 5 Nr. 3 GeschGehG.[969]

Darüber hinaus ist zu beachten, dass das Erfordernis der angemessenen Geheimhaltungsmaßnahmen (§ 2 Nr. 1 lit. b) GeschGehG) im Rahmen des § 79 Abs. 1 S. 1 BetrVG zur Folge hätte, dass die betriebsverfassungsrechtliche Verschwiegenheitspflicht im Falle fehlender Geheimhaltungsmaßnahmen sinnwidrig leerliefe und der innerbetriebliche Informationsfluss keinerlei Einschränkungen erfahren würde. § 79 Abs. 1 S. 1 BetrVG könnte den Konflikt zwischen Informationsinteresse des Betriebsrats bzw. der Belegschaft und dem Geheimhaltungsinteresse des Arbeitgebers unter diesen Umständen nur noch einseitig zu Lasten des Arbeitgebers auflösen. Im Ergebnis sind Betriebs- und Geschäftsgeheimnisse i. S. d. § 79 Abs. 1 S. 1 BetrVG daher weiterhin als Tatsachen zu verstehen, die im Zusammenhang mit dem Geschäftsbetrieb stehen, nicht offenkundig sind und nach dem erkennbaren Willen des Betriebsinhabers geheim gehalten werden sollen, weil dieser an deren Geheimhaltung ein objektiv berechtigtes wirtschaftliches Interesse hat.[970]

---

966 BAG, Urteil v. 16.03.1982, AP BGB § 611 Nr. 1; BAG, Urteil v. 26.02.1987, AP BetrVG 1972 § 79 Nr. 2.

967 *Kania*, in: ErfK-ArbR, § 79 BetrVG Rn.2; a. A.: *Preis/Seiwerth*, RdA 2019, 351, 353.

968 BT-Drs. 19/4724, S. 24.

969 BT-Drs. 19/4724, S. 24.

970 BAG, Beschluss v. 10.03.2009 - 1 ABR 87/07, FD-ArbR 2009, 287049; LAG Schleswig-Holstein v. 20.05.2015 - 3 TaBV 35/14.

Der Arbeitgeber hat dementsprechend darauf zu achten, die Informationen vor der Weitergabe an den Betriebsrat ausdrücklich als geheimhaltungsbedürftig zu bezeichnen. Die Erklärung des Arbeitgebers ist konstitutiv und unterliegt keinem bestimmten Formerfordernis.[971] Zum Nachweis etwaiger Verschwiegenheitsverstöße empfiehlt es sich für Arbeitgeber zumindest die Textform zu wahren, vgl. § 126b BGB. Die Geheimhaltungspflicht des § 79 Abs. 1 BetrVG gilt nicht, soweit eine Offenbarungspflicht des Betriebsratsmitglieds besteht.[972]

2. Geheimnisschutz bei der Erlangung eines Geschäftsgeheimnisses

§ 1 Abs. 3 Nr. 4 Var. 2 GeschGehG und § 3 Abs. 1 Nr. 3 Var. 2 GeschGehG regeln die Erlangung eines Geschäftsgeheimnisses des Betriebsrats durch den Arbeitgeber.[973] Danach ist die Erlangung eines Geschäftsgeheimnisses durch ein Ausüben der Mitwirkungs- und Mitbestimmungsrechte der Arbeitnehmervertretung erlaubt. Nach dem Willen des Gesetzgebers sollen die Beteiligungsrechte des Betriebsrats nicht mit dem Hinweis auf das Vorliegen von Geschäftsgeheimnissen eingeschränkt werden können.[974] Erfolgt eine Weitergabe an den Betriebsrat, wird das Geheimhaltungsinteresse des Arbeitgebers insbesondere über die Verschwiegenheitspflicht nach § 79 Abs. 1 S. 1 BetrVG sichergestellt.[975] § 79 Abs. 1 BetrVG schafft damit den Interessenausgleich zwischen dem Informationsinteresse des Betriebsrats bzw. der Belegschaft und dem Geheimhaltungsinteresse des Arbeitge-

---

971 Vgl. *Fuhlrott*, in: BeckOK-GeschGehG, § 3 GeschGehG Rn.22.

972 *Kania*, in: ErfK-ArbR, § 79 BetrVG Rn.13; *Thüsing*, in: Richardi, § 79 BetrVG Rn.16, unter Hinweis auf Zeugenaussagen vor Gericht, die Anzeige strafbarer Handlungen nach § 138 StGB und die Auskunftserteilung im Rahmen des Arbeitsschutzes sowie die Mitwirkung des Betriebsrats bei der Bekämpfung von Unfall- und Gesundheitsgefahren.

973 Aus §§ 1 Abs. 3 Nr. 4 Var. 2, 3 Abs. 1 Nr. 3 Var. 2 GeschGehG i. V. m. § 80 Abs. 2 BetrVG geht hervor, dass der Arbeitgeber zur Weitergabe von Geschäftsgeheimnissen an den Betriebsrat verpflichtet ist, sofern dies zur Gewährleistung der Betriebsratstätigkeit erforderlich ist, vgl. § 80 Abs. 1 und 2 BetrVG.

974 BT-Drs. 19/4724, S. 26.

975 Vgl. § 1 Abs. 3 Nr. 4 Var. 1 GeschGehG.

bers. Hintergrund ist, dass dem Betriebsrat unter Umständen zur Gewährleistung einer effektiven Betriebsratsarbeit vertrauliche Daten zugänglich gemacht werden müssen. Im Gegenzug soll der Arbeitgeber darauf vertrauen dürfen, dass der Betriebsrat diese nicht unberechtigt nutzt oder offenlegt. Vor diesem Hintergrund ist § 79 Abs. 1 BetrVG auch als Ausprägung des Gebots der vertrauensvollen Zusammenarbeit zwischen Arbeitgeber und Betriebsrat zu verstehen, § 2 Abs. 1 BetrVG.[976]

Darüber hinaus regelt die Tatbestandsausnahme des § 5 Nr. 3 GeschGehG die zulässige Erlangung eines Geschäftsgeheimnisses des Betriebsrats durch den Arbeitnehmer.[977] Nach § 5 Nr. 3 GeschGehG ist die Erlangung, Nutzung oder Offenlegung eines Geschäftsgeheimnisses nicht verboten, wenn dies im Rahmen der Offenlegung durch den Arbeitnehmer gegenüber dem Betriebsrat erforderlich ist, damit dieser seine Aufgaben erfüllen kann. Ob die Offenlegung erforderlich war, entscheiden die Umstände des jeweiligen Einzelfalls. Die Betriebsparteien sind insofern berechtigt, den Ausnahmetatbestand des § 5 Nr. 3 GeschGehG z. B. mittels Betriebsvereinbarung zu konkretisieren (§ 3 Abs. 2 GeschGehG), sofern damit keine Beschränkung des Ausnahmetatbestands einhergeht.[978]

Nicht abschließend geklärt ist, wie das Kriterium der Erforderlichkeit im Sinne des § 5 Nr. 3 GeschGehG zu bestimmen ist. In Teilen der Literatur wird z. B. ein rein objektiver Bewertungsmaßstab in Erwägung gezogen.[979] Der Gesetzgeber geht demgegenüber davon aus, dass auch subjektive Erwägungen berücksichtigungsfähig sind.[980] In der Gesetzesbegründung zum GeschGehG heißt es: „*Arbeitnehmer*

---

976 Vgl. *Thüsing*, in: Richardi, § 83 BetrVG, Vorb. § 79 BetrVG Rn.1.
977 Vgl. BT-Drs. 19/8300, S. 14.
978 Eine Beschränkung des § 5 Nr. 3 GeschGehG ist nicht möglich, vgl. Art. 1 Abs. 2 lit. d) GeschGeh-RL i. V. m. Erwägungsgrund 12 der GeschGeh-RL; *Naber/Peukert/Seeger*, NZA 2019, 583, 588.
979 Vgl. *Fuhlrott*, in: BeckOK-GeschGehG, § 5 Rn.53.
980 BT-Drs. 19/4724, S. 29.

haben das Recht, ihre Arbeitnehmervertretung zu kontaktieren. Es ist möglich, dass sie in diesem Zusammenhang Geschäftsgeheimnisse offenlegen bzw. nutzen. Gleichzeitig kann die Arbeitnehmervertretung durch diesen Vorgang ein Geschäftsgeheimnis erlangen. Daher privilegiert § 5 Nr. 3 GeschGehG die Erlangung, die Nutzung oder die Offenlegung eines Geschäftsgeheimnisses im Rahmen der Offenlegung gegenüber der Arbeitnehmervertretung, soweit die Offenlegung aus Sicht des Arbeitnehmers erforderlich ist, damit die Arbeitnehmervertretung ihre Aufgaben erfüllen kann. Die Regelung dient dem Schutz von Arbeitnehmern, die sich mit einem Geschäftsgeheimnis an die Arbeitnehmervertretung wenden. Gleichzeitig dient sie dem Schutz der Arbeitnehmervertretung, die auf diesem Weg ein Geschäftsgeheimnis erlangt."[981]

Für eine weite Auslegung des Kriteriums der Erforderlichkeit spricht, dass die Geheimhaltungsinteressen des Arbeitgebers gewahrt bleiben. Eine direkte Anwendung des § 79 Abs. 1 BetrVG ist zwar nicht möglich. Dafür fehlt es an der konstitutiven, ausdrücklichen Vertraulichkeitserklärung des Arbeitgebers. Der Betriebsrat ist aber aus dem Gebot der vertrauensvollen Zusammenarbeit mit dem Arbeitgeber zur Verschwiegenheit verpflichtet, § 2 Abs. 1 BetrVG. Erlangt ein Betriebsratsmitglied nach Maßgabe des § 5 Nr. 3 GeschGehG ein Geschäftsgeheimnis durch den Arbeitnehmer, ist der Arbeitnehmer aufgrund seiner arbeitsvertraglichen Rücksichtnahmepflicht gegenüber den Interessen des Arbeitgebers verpflichtet, den Betriebsrat darauf hinzuweisen, inwieweit ein arbeitgeberseitiges Geheimhaltungsinteresse an den offenbarten Informationen besteht, §§ 241 Abs. 2, 242, 611a BGB.[982] Der Betriebsrat ist sodann aus dem Gebot der vertrauensvollen Zusammenarbeit mit dem Arbeitgeber zur Ver-

---

[981] BT-Drs. 19/4724, S. 29.

[982] Die Erklärung des Arbeitnehmers tritt an die Stelle der Vertraulichkeitserklärung des Arbeitgebers im Sinne des § 79 Abs. 1 BetrVG. Es könnte auch eine analoge Anwendung des § 79 Abs. 1 BetrVG in Fällen des § 5 Nr. 3 GeschGehG erwogen werden, vgl. *Fuhlrott*, in: BeckOK-GeschGehG, § 5 Rn.53.

schwiegenheit verpflichtet, § 2 Abs. 1 BetrVG. Auf die Art ist ein angemessener Interessenausgleich zwischen dem Informationsinteresse des Betriebsrats und dem Geheimhaltungsinteresse des Arbeitgebers geschaffen. Der Arbeitgeber kann darauf vertrauen, dass der Betriebsrat Geschäftsgeheimnisse, die ihm im Rahmen seiner Tätigkeit offenbart werden, nicht unberechtigt nutzt oder offenlegt.

Erfolgt die Offenlegung des Geschäftsgeheimnisses allerdings ohne Bezug zur Aufgabenerfüllung des Betriebsrats und war dies zum Zeitpunkt der Offenlegung für den Arbeitnehmer offensichtlich erkennbar, ist dieser nicht schutzwürdig im Sinne des § 5 Nr. 3 GeschGehG. Wer nicht in gutem Glauben handelt, verdient den Schutz der Rechtsordnung nicht. An den Arbeitnehmer sind in diesem Zusammenhang jedoch keine zu hohen Anforderungen zu stellen. Andernfalls bestünde die Gefahr, dass ein Arbeitnehmer aus Sorge einer Geschäftsgeheimnisverletzung den Betriebsrat nicht informiert. Dies liefe dem Telos des § 5 Nr. 3 GeschGehG zuwider, der Arbeitnehmer dazu ermutigen will, ihre Arbeitnehmervertretungen wie gewohnt in erforderlichem Maße zu kontaktieren. Sollte es dabei zur Offenlegung von Geschäftsgeheimnissen kommen, soll dieser Umstand den Arbeitnehmer nicht davon abhalten, die jeweiligen Informationen offenzulegen. Das Kriterium der Erforderlichkeit ist insofern weit auszulegen. Im Ergebnis müssen nach hiesiger Auffassung daher auch subjektive Erwägungen des Arbeitnehmers berücksichtigungsfähig sein.

3. Whistleblower: Betriebsratsmitglied

Entscheidet sich ein Betriebsratsmitglied zur Meldung eines Geschäftsgeheimnisses zu Zwecken des Whistleblowings, befindet es sich in einem Spannungsfeld zwischen Meinungsfreiheit und unternehmerischen Geheimhaltungsinteressen. Zugleich unterliegt das Betriebsratsmitglied der Verschwiegenheitspflicht nach § 79 Abs. 1 BetrVG sowie dem Gebot der vertrauensvollen Zusammenarbeit gemäß § 2 Abs. 1 BetrVG. Dieses Spannungsfeld gilt es im Folgenden aufzulösen. Aufgrund des Untersuchungsgegenstands beschränkt sich

die folgende Darstellung jedoch auf die Frage der Meldung eines Geschäftsgeheimnisses durch das Betriebsratsmitglied.

Zunächst ist festzustellen, dass die Vorgaben des HinSchG auch für Betriebsratsmitglieder gelten.[983] Dementsprechend finden die § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG auch auf Betriebsratsmitglieder Anwendung. Die vorstehenden Ausführungen haben gezeigt, dass im Rahmen des § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG eine (Prüf-) Obliegenheit des Whistleblowers besteht.[984] Beabsichtigt ein Betriebsratsmitglied einen Verstoß zu melden und hat es hinreichenden Grund zu der Annahme, der interne Meldeweg sei zur Beseitigung des Missstands geeignet, resultiert daraus nach hiesiger Auffassung ein Vorrang des internen Meldekanals.

Fraglich ist, ob diese Grundsätze vor dem Hintergrund der betriebsverfassungsrechtlichen Spezifika einer Fortentwicklung bedürfen. Dafür spricht, dass ein Betriebsratsmitglied unter Umständen nur deshalb Kenntnis von dem Geschäftsgeheimnis hat, weil der Arbeitgeber betriebsverfassungsrechtlich zur Offenlegung verpflichtet ist.[985] Kehrseite dieser Offenlegungspflicht ist das betriebsverfassungsrechtlich abgesicherte Vertrauen des Arbeitgebers, dass das Betriebsratsmitglied die Information geheim hält.[986] Die Verschwiegenheitspflicht des § 79 Abs. 1 S. 1 BetrVG ist folgerichtig als Ausprägung des Gebots der vertrauensvollen Zusammenarbeit zwischen Arbeitgeber und Betriebsrat zu verstehen, vgl. § 2 Abs. 1 BetrVG. Eine Zusammenarbeit kann jedoch nur dann vertrauensvoll sein, wenn jeder dem

---

983 BT-Drs. 20/3442, S. 56.

984 Siehe: Kapitel C) I. 2. b) ee) und Kapitel C) I. 2. c).

985 Aus § 1 Abs. 3 Nr. 4 Var. 2 und § 3 Abs. 1 Nr. 3 Var. 2 GeschGehG i. V. m. § 80 Abs. 2 BetrVG geht hervor, dass der Arbeitgeber zur Weitergabe von Geschäftsgeheimnissen an den Betriebsrat verpflichtet ist, sofern dies zur Gewährleistung der Betriebsratstätigkeit erforderlich ist, vgl. § 80 Abs. 1 und Abs. 2 BetrVG.

986 *Werner*, in: BeckOK-ArbR, Einl. § 79 BetrVG.

anderen trauen kann.[987] Dies erfordert ein gewisses Maß an Rücksichtnahme auf die Interessen des jeweils anderen und bedarf einer betriebsverfassungsrechtlichen Lösung.

Geben beispielsweise die Umstände des jeweiligen Einzelfalls zu erkennen, dass die Funktionsfähigkeit eines internen Meldesystems nicht gewährleistet ist, ist das Betriebsratsmitglied aus dem Gebot der vertrauensvollen Zusammenarbeit heraus dazu verpflichtet, den Arbeitgeber auf diesen Umstand hinzuweisen, § 2 Abs. 1 BetrVG. Das Gebot der vertrauensvollen Zusammenarbeit verpflichtet das Betriebsratsmitglied, gemeinsam mit dem Arbeitgeber darauf hinzuwirken, dass aus der (Prüf-) Obliegenheit im Rahmen des § 6 Abs. 1 HinSchG ein Vorrang des internen Meldekanals resultiert. Maßstab bildet der Grundsatz von Treu und Glauben.[988] Für dieses Verständnis spricht, dass das Betriebsratsmitglied unabhängig von einer beabsichtigten Meldung verpflichtet ist, dem Arbeitgeber ihm bekannte bzw. bekannt gewordene Anhaltspunkte, die gegen die Funktionsfähigkeit des Hinweisgeberschutzsystems sprechen, mitzuteilen.[989] Solange der Betriebsrat den Arbeitgeber nicht auf Anhaltspunkte aufmerksam macht, die gegen die Wirksamkeit des internen Meldekanals sprechen, darf dieser konsequenterweise darauf vertrauen, dass der Vorrang des internen Meldekanals im Rahmen des § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG zumindest für die Betriebsratsmitglieder besteht.

---

987 BAG, Beschluss v. 21.04.1983 - 6 ABR 70/8221, NJW 1984, 2309; BAG, Beschluss v. 22.05.1959 - 1 ABR 2/59 22, AP BetrVG § 23 Nr. 3.

988 *Koch*, in: ErfK-ArbR, § 2 BetrVG Rn.1; *Maschmann*, in: Richardi, § 2 BetrVG Rn.7. Zur Herleitung der (Prüf-) Obliegenheit: Kapitel B) I. 2. b).

989 Gründe, die gegen ein wirksames Hinweisgeberschutzsystem sprechen sind z. B. die häufige Nichterreichbarkeit der internen Meldestelle oder Äußerungen von Vorgesetzten bzw. Führungskräften, die Ankündigungen oder Andeutungen enthalten, internen Meldungen werde nicht hinreichend nachgegangen.

4. Zusammenfassender Überblick

Geht es um die Erlangung eines Geschäftsgeheimnisses des Betriebsrats durch den Arbeitgeber, sind die Vorschriften § 1 Abs. 3 Nr. 4 Var. 2 GeschGehG und § 3 Abs. 1 Nr. 3 Var. 2 GeschGehG maßgeblich. Erfolgt eine Weitergabe an den Betriebsrat, wird das Geheimhaltungsinteresse des Arbeitgebers insbesondere über die Verschwiegenheitspflicht nach § 79 Abs. 1 S. 1 BetrVG sichergestellt. Hintergrund ist, dass dem Betriebsrat unter Umständen zur Gewährleistung einer effektiven Betriebsratsarbeit vertrauliche Daten zugänglich gemacht werden müssen. Im Gegenzug soll der Arbeitgeber darauf vertrauen dürfen, dass der Betriebsrat diese nicht unberechtigt nutzt oder offenlegt.

Im Vergleich zu der Definition eines Geschäftsgeheimnisses im Sinne des § 2 GeschGehG, hat sich in der Rechtsprechung zu § 79 Abs. 1 S. 1 BetrVG eine eigenständige Definition des Betriebs- oder Geschäftsgeheimnisses entwickelt.[990] Diese ist nach hiesiger Auffassung auch nach Einführung des GeschGehG weiter maßgeblich.[991] Demzufolge sind Betriebs- und Geschäftsgeheimnisse im Sinne des § 79 Abs. 1 S. 1 BetrVG weiterhin als Tatsachen zu verstehen, die im Zusammenhang mit dem Geschäftsbetrieb stehen, nicht offenkundig sind und nach dem erkennbaren Willen des Betriebsinhabers geheim gehalten werden sollen, weil dieser an deren Geheimhaltung ein objektiv berechtigtes wirtschaftliches Interesse hat. Die Erklärung des Arbeitgebers ist konstitutiv und unterliegt keinem bestimmten Formerfordernis.

Die Tatbestandsausnahme des § 5 Nr. 3 GeschGehG regelt die zulässige Erlangung eines Geschäftsgeheimnisses des Betriebsrats durch den Arbeitnehmer. Nach § 5 Nr. 3 GeschGehG ist die Erlangung,

---

990 BAG, Beschluss v. 10.03.2009 - 1 ABR 87/07, FD-ArbR 2009, 287049; LAG Schleswig-Holstein v. 20.05.2015 - 3 TaBV 35/14.

991 *Kania*, in: ErfK, § 79 BetrVG Rn.2; a. A.: *Preis/Seiwerth*, RdA 2019, 351, 353. Siehe: Kapitel C) III. 1.

Nutzung oder Offenlegung eines Geschäftsgeheimnisses nicht verboten, wenn dies im Rahmen der Offenlegung durch den Arbeitnehmer gegenüber dem Betriebsrat erforderlich ist, damit dieser seine Aufgaben erfüllen kann. Ob die Offenlegung erforderlich ist, entscheiden die Umstände des jeweiligen Einzelfalls. Hinsichtlich der Erforderlichkeit sind nach hiesiger Auffassung auch subjektive Erwägungen des Arbeitnehmers berücksichtigungsfähig.[992] Für dieses weite Verständnis spricht, dass die Geheimhaltungsinteressen des Arbeitgebers gewahrt bleiben. Für eine direkte Anwendung des § 79 Abs. 1 BetrVG fehlt es zwar an der konstitutiven Vertraulichkeitserklärung des Arbeitgebers. Der Betriebsrat ist aber aus dem Gebot der vertrauensvollen Zusammenarbeit zur Verschwiegenheit verpflichtet, § 2 Abs. 1 BetrVG. An den Arbeitnehmer sind dennoch keine zu hohen Anforderungen zu stellen. § 5 Nr. 3 GeschGehG bezweckt, Arbeitnehmer zu ermutigen, ihre Arbeitnehmervertretungen wie gewohnt in erforderlichem Maße zu kontaktieren.

Erfolgt die Offenlegung des Geschäftsgeheimnisses allerdings ohne Bezug zur Aufgabenerfüllung des Betriebsrats und war dies zum Zeitpunkt der Offenlegung für den Arbeitnehmer offensichtlich erkennbar, ist dieser nicht schutzwürdig im Sinne des § 5 Nr. 3 GeschGehG.

Entscheidet sich ein Betriebsratsmitglied zur Meldung eines Geschäftsgeheimnisses zu Zwecken des Whistleblowings, befindet es sich in einem Spannungsfeld zwischen eigener Meinungsfreiheit und unternehmerischen Geheimhaltungsinteressen. Zugleich unterliegt das Betriebsratsmitglied der Verschwiegenheitspflicht nach § 79 Abs. 1 S. 1 BetrVG sowie dem Gebot der vertrauensvollen Zusammenarbeit aus § 2 Abs. 1 BetrVG. Festzuhalten ist zunächst, dass die Regelungen des § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG auch auf Betriebsratsmitglieder Anwendung finden. Beabsichtigt also ein Betriebsratsmitglied einen Verstoß zu melden und hat es hinreichenden Grund zu der Annahme, der

[992] Siehe: Kapitel C) III. 2.

interne Meldeweg sei zur Beseitigung des Missstands geeignet, resultiert daraus nach hiesiger Auffassung ein Vorrang des internen Meldekanals.[993]

Entscheidet sich ein Betriebsratsmitglied allerdings zur Meldung einer geschützten Information, die ihm ausschließlich wegen seiner Zugehörigkeit zum Betriebsrat in Wahrnehmung seiner Betriebsratstätigkeit durch den Arbeitgeber unter Hinweis auf die Vertraulichkeit bekannt geworden ist, bedarf dies einer betriebsverfassungsrechtlichen Lösung.[994]

Das Gebot der vertrauensvollen Zusammenarbeit verpflichtet das Betriebsratsmitglied, gemeinsam mit dem Arbeitgeber darauf hinzuwirken, dass aus der (Prüf-) Obliegenheit im Rahmen des § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG ein Vorrang des internen Meldekanals resultiert. Maßstab bildet der Grundsatz von Treu und Glauben. Solange der Betriebsrat den Arbeitgeber nicht auf Anhaltspunkte aufmerksam macht, die gegen die Wirksamkeit des internen Meldekanals sprechen, darf dieser konsequenterweise darauf vertrauen, dass der Vorrang des internen Meldekanals im Rahmen des § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG zumindest für die Betriebsratsmitglieder besteht.

---

[993] Siehe: Kapitel C) I. 2. b) ee).
[994] Siehe: Siehe: Kapitel C) III. 3.

IV. Eine zweite Sammlung der Erkenntnisse

Die Reichweite des Geschäftsgeheimnisses ist ein komplexes Feld, das sich nur unter Zuhilfenahme weiterer Regelungskomplexe erschließt. Der Geschäftsgeheimnisschutz befindet sich inmitten eines Spannungsfelds zwischen Whistleblowing, datenschutzrechtlichen Betroffenenrechte und dem Informationsinteresse des Betriebsrats. Weder der Geschäftsgeheimnisschutz noch kollidierende Rechte gelten absolut. Anhand der vorstehenden Ausführungen lassen sich folgende Erkenntnisse zu den eingangs aufgezeigten Leitfragen festhalten:

Wie können die Friktionen zwischen GeschGehG und HinSchG überwunden werden?

1. Eine erste Friktion bezieht sich auf den sachlichen Anwendungsbereich.[995] Der Whistleblower ist im Anwendungsbereich des § 2 HinSchG berechtigt, Verstöße und treuwidriges Verhalten, das auf Gesetzeslücken hindeutet, zu melden bzw. offenzulegen. Daneben erfasst § 5 Nr. 2 GeschGehG die Offenlegung rechtswidriger Handlungen, wobei eine rechtswidrige Handlung von einigem Gewicht sein muss. Anzumerken ist, dass das Kriterium der „*rechtswidrigen Handlung*“ die beiden weiteren Kriterien des „*beruflichen oder sonstigen Fehlverhaltens“* erfasst, vgl. § 5 Nr. 2 GeschGehG.[996] Der nationale Gesetzgeber geht von einem Nebeneinander von § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG und § 5 Nr. 2 GeschGehG aus. Die Vorgaben des HinSchG entfalten demnach keine Sperrwirkung gegenüber § 5 Nr. 2 GeschGehG.[997] Ist der Anwendungsbereich des § 2 HinSchG nicht eröffnet, kann Hinweisgeberschutz nach § 5 Nr. 2 GeschGehG bestehen.

---

995 Siehe: Kapitel C) I. 1. c) aa).
996 Siehe: Kapitel C) I. 1. c) aa).
997 Siehe: Kapitel C) I. 1. c) ee).

2. Eine weitere Friktion bezieht sich auf die verschiedenen Auslegungsmaßstäbe, die im Rahmen der obligatorischen Verhältnismäßigkeitserwägungen anzustrengen sind.[998] Während § 6 Abs. 1 HinSchG in Zweifelsfällen von einem grundsätzlichen Vorrang des Hinweisgeberschutzes ausgeht, besteht im Rahmen des § 5 Nr. 2 GeschGehG in ebendiesen Zweifelsfällen ein Vorrang des Geschäftsgeheimnisschutzes. Den Verhältnismäßigkeitserwägungen liegen insofern verschiedene Wertungen zugrunde. Anzumerken ist, dass beide Vorschriften keine eigenständige Interessenabwägung vorsehen, die über die obligatorischen Verhältnismäßigkeitserwägungen anhand der Zweckbestimmung der Meldung hinausgeht. Die Einheit der Rechtsordnung gebietet es aus Gründen der Rechtssicherheit, ein identisches Verständnis der Maßstäbe anzuwenden. Der Maßstab des § 6 Abs. 1 HinSchG ist vorzugwürdig, weil der Gesetzgeber mit der Vorgabe des § 5 Nr. 2 GeschGehG das Verhältnis zwischen Hinweisgeberschutz und Geschäftsgeheimnisschutz nicht verschieben wollte.[999] Soweit die Regelung des § 5 Nr. 2 GeschGehG enger ist, bedarf es daher einer harmonisierenden Auslegung, die den Anforderungen des HinSchG entspricht. Ist § 5 Nr. 2 GeschGehG weiter, so verbleibt § 5 Nr. 2 GeschGehG ein eigenständiger Anwendungsbereich.

3. Der einheitliche Auslegungsmaßstab belegt, dass keine Friktion in Bezug auf die Relevanz der subjektiven Motivlage besteht. Weder § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG noch § 5 Nr. 2 GeschGehG lassen sich losgelöst von subjektiven Wertungen des Hinweisgebers beurteilen.[1000] Die Meldung ist als Ausdruck der Meinungsfreiheit im Sinne eines Mehrwerts für die öffentliche Meinungsbildung zu verstehen und hat im allgemeinen öffentlichen Interesse zu erfolgen. Die Zweckbestimmung ist zwar objektiv zu bestimmen, enthält aber zugleich ein subjektives Element.

---

998 Siehe: Kapitel C) I. 1. c) cc).
999 Siehe: Kapitel C) I. 1. c) ee).
1000 Siehe: Kapitel C) I. 1. c) bb).

Dies gilt für § 5 Nr. 2 GeschGehG und § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG gleichermaßen.

4. Eine weitere Friktion bezieht sich auf den Umfang des Haftungsausschlusses im Falle einer Meldung bzw. Offenlegung in Bezug auf die vorherige Erlangung bzw. Informationsbeschaffung.[1001] Erfolgt eine Meldung nach Maßgabe des § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG, bleibt nach § 35 Abs. 1 HinSchG die Strafbarkeit in Bezug auf die vorherige Informationsbeschaffung bestehen. Dagegen nimmt § 5 Nr. 2 GeschGehG den Whistleblower hinsichtlich der Informationserlangung von der straffrechtlichen Verantwortung nach § 23 GeschGehG aus. Dort, wo § 35 Abs. 1 HinSchG keinen Hinweisgeberschutz gewährt, greift der Hinweisgeberschutz des § 5 Nr. 2 GeschGehG ergänzend.[1002]

Wem darf ein Whistleblower Geschäftsgeheimnisse melden?

1. Nach § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG ist die Weitergabe eines Geschäftsgeheimnisses an eine interne oder externe Meldestelle oder dessen Offenlegung erlaubt, sofern der Whistleblower hinreichenden Grund zu der Annahme hat, dass die Weitergabe oder Offenlegung notwendig ist, um einen Verstoß aufzudecken und die Voraussetzungen des § 33 Abs. 1 Nr. 2 und 3 HinSchG erfüllt sind. In Bezug auf den Inhalt und die Form der Weitergabe eines Geschäftsgeheimnisses unterliegt der Whistleblower einer Prüfpflicht im Sinne einer Bemühenspflicht, deren Anforderungen denjenigen bzgl. des Wahrheitsgehaltes entsprechen, vgl. § 33 Abs. 1 Nr. 2 HinSchG.[1003] Der Whistleblower darf nicht mehr als das unbedingt notwendige Maß an geheimen Informationen weitergeben. In der Regel wird der Whistleblower vor der Weitergabe eines Geschäftsgeheimnisses einen Anwalt zu

[1001] Siehe: Kapitel C) I. 1. c) dd).
[1002] Siehe: Kapitel C) I. 1. c) ee).
[1003] Siehe: Kapitel C) I. 2. a).

konsultieren haben, um dem Erfordernis der Notwendigkeit in § 6 Abs. 1 HinSchG gerecht zu werden. Etwas anderes gilt, soweit eine begründete und erhebliche Gefahr für das Leben oder die Gesundheit anderer besteht, sodass eine anwaltliche Konsultation nicht abgewartet werden kann.

2. In Bezug auf die Form hat der Whistleblower eine Unkenntlichmachung der geheimen Informationen in Erwägung zu ziehen. Dazu gehört auch eine Prüfung alternativer Mittel, die in gleicher Weise geeignet sind, Rechtskonformität herzustellen. Daraus kann sich ein Vorrang eines internen Meldekanals ergeben.[1004] Hat der Whistleblower zum Zeitpunkt der beabsichtigten Meldung hinreichenden Grund zu der Annahme, der interne Meldeweg sei zur Beseitigung des möglichen Missstands geeignet, resultiert daraus ein Vorrang des internen Meldekanals. Maßgeblich ist, ob Anhaltspunkte vorliegen, die gegen die Funktionsfähigkeit und Wirksamkeit des internen Hinweisgeberschutzsystems sprechen. Unzumutbar ist eine interne Meldung, wenn dem Whistleblower infolge der internen Meldung Repressalien drohen.

3. Setzt sich der Whistleblower über den Vorrang der internen Meldung im Rahmen des § 6 Abs. 1 HinSchG hinweg, greift das Haftungssystem des GeschGehG. Gleiches gilt mit Blick auf arbeitsrechtliche Konsequenzen in Folge der Verletzung einer arbeitsvertraglichen Verschwiegenheitspflicht, § 6 Abs. 2 HinSchG. Die Anforderungen des § 6 Abs. 2 HinSchG entsprechen denen in § 6 Abs. 1 HinSchG, soweit es um die Weitergabe von Geschäftsgeheimnissen geht. Für die Meldestellen gilt dennoch das Vertraulichkeitsgebot der §§ 8, 9 HinSchG. Der Whistleblower ist auch weiterhin nach Maßgabe des § 33 Abs. 1 HinSchG vor einer weitergehenden Haftung über § 35 Abs. 2 GeschGehG insbesondere vor Schäden Dritter geschützt und es besteht das Verbot von Repressalien nach § 36 HinSchG fort. Im Ergebnis handelt es sich

[1004] Siehe: Kapitel C) I. 2. b) ee).

daher um eine Prüfobliegenheit des Whistleblowers, aus der ein Vorrang des internen Meldewegs im Rahmen des § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG resultieren kann.

4. § 7 Abs. 1 S. 1 HinSchG steht der Annahme einer (Prüf-) Obliegenheit, aus der ein Vorrang des internen Meldewegs resultieren kann, nicht entgegen. Systematik und Telos streiten für eine eigenständige Auslegungsweise des Notwendigkeitsvorbehalts in § 6 Abs. 1 HinSchG, losgelöst von der Vorgabe des § 7 Abs. 1 S. 1 HinSchG. Aus der Systematik folgt, dass die Weitergabe von Geschäftsgeheimnissen eine hervorgehobene Stellung einnimmt. Das Wahlrecht wurde dagegen bei den Grundsätzen zur Arbeitsweise der Meldestelle verortet, weshalb aus systematischer Sicht davon auszugehen ist, dass die Regelung keine Wirkkraft im Hinblick auf die allgemeine Vorschrift des § 6 Abs. 1 HinSchG entfaltet. § 6 Abs. 1 HinSchG bezweckt einen angemessenen Ausgleich zwischen dem Hinweisgeberschutz und dem Geschäftsgeheimnisschutz. Andere Vorgaben lassen gegenläufige Geschäftsgeheimnisinteressen des Beschäftigungsgebers außen vor. § 6 Abs. 1 HinSchG ist daher eigenständig auszulegen. Das Wahlrecht in § 7 Abs 1 S. 1 HinSchG bezieht sich ausschließlich auf Informationen, die keine Geschäftsgeheimnisse sind.[1005]

5. Aus Gründen der Einheit der Rechtsordnung sind die Voraussetzungen des § 6 Abs. 1 HinSchG in § 5 Nr. 2 GeschGehG hineinzulesen.[1006] Diese Lesart wird dem Anliegen des nationalen Gesetzgebers gerecht, den Hinweisgeberschutz zu stärken und schafft Rechtssicherheit. Folgerichtig sind die gefundenen Maßstäbe des Notwendigkeitskriteriums auch im Rahmen des § 5 Nr. 2 GeschGehG zu beachten, insbesondere mit Blick auf die herausgearbeitete Prüfobliegenheit, aus der ein Vorrang eines internen Meldewegs resultieren kann.

[1005] Siehe: Kapitel C) I. 2. b) ee).
[1006] Siehe: Kapitel C) I. 2. c).

Was folgt daraus für die unternehmerischen Compliance-Systeme?

1. Die Geschäftsleitung ist gesellschaftsrechtlich verpflichtet, sicherzustellen, dass aus der Prüfobliegenheit im Rahmen des § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG ein Vorrang des internen Meldewegs resultiert. Dies gelingt durch die Implementierung eines wirksamen Hinweisgebersystems, von dem der Whistleblower hinreichenden Grund zu der Annahme hat, dass dieses zur Beseitigung des Missstands geeignet ist, ohne dass ihm durch die Meldung Repressalien drohen. In diesem Kontext stellt die Implementierung eines wirksamen Hinweisgeberschutzsystems gleichzeitig einen Bestandteil des Geheimnisschutzkonzepts dar, § 2 Nr. 1 lit. b) GeschGehG.[1007]

2. Um das Unternehmen vor einem Reputationsverlust und weiteren Schäden in Folge des Bekanntwerdens von sensiblen Informationen, die noch keine Geschäftsgeheimnisse sind, hinreichend zu schützen, ist die Geschäftsleitung verpflichtet, darauf hinzuwirken, dass ein Whistleblower sich für einen internen Meldeweg entscheidet. Die Unternehmensleitung hat daher Anreize dafür zu schaffen, dass Whistleblower einen internen Meldekanal bevorzugen. Diese Anreize bilden einen notwendigen Zwischenschritt, um die sensiblen Informationen anschließend in den Schutzbereich des GeschGehG zu überführen.

3. Die Geschäftsleitung darf den Whistleblower nicht zur vorrangigen Nutzung eines internen Meldewegs verpflichten.[1008] Vereinbarungen, die den Zugang zu den externen Meldestellen einschränken, sind unwirksam, §§ 7, 39 HinSchG i. V. m. § 134 BGB. Ein Vorrang einer internen Meldung ergibt sich auch nicht aus § 17 Abs. 2 S. 1 ArbSchG. Nach § 17 Abs. 2 S. 3 ArbSchG hat der Arbeitnehmer die Wahl, ob er sich für ein Vorgehen im Sinne des

[1007] Siehe: Kapitel C) I. 3.
[1008] Siehe: Kapitel C) I. 3. a).

§ 17 Abs. 2 S. 1 ArbSchG entscheidet oder als Whistleblower im Sinne des HinSchG agiert. Ihm bleibt der Weg zu einer externen Meldestelle nicht verwehrt.

4. Eine interne Meldepflicht ist möglich, sofern dem Whistleblower der Zugang zum externen Meldeweg erhalten bleibt.[1009] Die Klausel muss hinreichend bestimmt sein und darf den Whistleblower nicht unangemessen benachteiligen, § 307 Abs. 1 BGB. Voraussetzung ist die Implementierung eines wirksamen Hinweisgeberschutzsystems. Zu beachten ist, dass eine interne Meldepflicht den Whistleblower in seinem Recht, keine Meldung zu tätigen, tangiert. Nötig sind deshalb insbesondere Konkretisierungen hinsichtlich des objektiven Verdachtsgrads und des Schweregrads eines Missstands, die es vermögen, den Eingriff in das Recht auf negative Meinungsfreiheit zu rechtfertigen. Je schwerer und gewichtiger der Missstand, desto eher überwiegen die Interessen des Unternehmens an der Beseitigung des Missstands. Auch mögliche Gewissenskonflikte sind im Rahmen der Interessenabwägung mitzudenken.

5. Da Unternehmen auch in Fällen einer internen Meldepflicht nicht abgesichert sind, dass Informationen über Missstände intern bleiben, müssen sie Anreize dafür schaffen, dass ein Whistleblower so viel Vertrauen in die Funktionsfähigkeit und Wirksamkeit des internen Meldekanals hegt, dass er freiwillig von einer externen Meldung absieht. Dazu zählt der Identitätsschutz. §§ 8, 9 HinSchG normieren zwar einen weitreichenden Identitätsschutz.[1010] Die Ausnahme des § 9 Abs. 1 HinSchG greift nur im Ausnahmefall und bedarf zudem einer einschränkenden Auslegung, dass nur solche Falschinformationen zum Ausschluss des Vertraulichkeitsgebots führen können, soweit diese geeignet sind, Schadensersatzansprüche der von der Meldung betroffenen Person auszulösen oder

[1009] Siehe: Kapitel C) I. 3. b).
[1010] Siehe: Kapitel C) I. 3. c) aa).

die gemeldeten Falschinformationen von strafrechtlicher Relevanz für diese sind. Der Identitätsschutz kollidiert allerdings mit den datenschutzrechtlichen Betroffenenrechten.[1011]

6. Die Informationspflicht nach Art. 14 Abs. 5 lit. b) DS-GVO besteht nicht, soweit die Kenntnis über die Identität des Whistleblowers den Zweck interner Untersuchungen gefährden würde, weil Beweismittel drohen verlustig zu gehen oder die begründete Annahme besteht, die Erhebung weiterer Beweismittel werde gefährdet. Im Übrigen besteht die Informationspflicht fort.[1012] §§ 8, 9 HinSchG sind keine Rechtsvorschriften im Sinne des Art. 14 Abs. 5 lit. c) DS-GVO. Sie können auch nicht auf die Öffnungsklauseln in Art. 23 Abs. 1 DS-GVO oder Art. 88 Abs. 1 DS-GVO gestützt werden. Ein Ausschluss der Informationspflicht folgt auch nicht aus § 29 Abs. 1 S. 1 BDSG, da diese Vorschrift ebenfalls auf keine Öffnungsklausel zurückgeführt werden kann und infolge des Anwendungsvorrangs der DS-GVO unangewendet bleiben muss.

7. Die Datenauskunft erfährt keine Beschränkung durch § 29 Abs. 1 S. 2 BDSG.[1013] Auch diese Vorschrift kann nach hiesiger Auffassung auf keine Öffnungsklausel der DS-GVO zurückgeführt werden. In Bezug auf die Datenauskunft verbleibt es bei der allgemeinen Beschränkungsmöglichkeit über Art. 15 Abs. 4 DS-GVO.[1014] Die Beschränkung bezieht sich auf das Auskunftsrecht mitsamt der Metainformationen in Art. 15 Abs. 1 Hs. 2 Var. 2 DS-GVO. Die Frage der Beschränkung des Auskunftsrechts ist losgelöst vom Bezugspunkt der Erfüllungsmodalität in Art. 15 Abs. 3 DS-GVO zu beantworten und im Wege einer charta-rechtlichen Auslegung des Art. 15 DS-GVO zwingend geboten, vgl. Art. 52 GR-CH.

[1011] Siehe: Kapitel C) I. 3. c) bb).
[1012] Siehe: Kapitel C) I. 3. c) bb) (1).
[1013] Siehe: Kapitel C) I. 3. c) bb) (2).
[1014] Siehe: Kapitel C) I. 3. c) bb) (2).

8. Im Rahmen des Art. 15 Abs. 4 DS-GVO entscheidet eine Interessenabwägung zwischen dem Identitätsschutz des Whistleblowers und dem Recht auf informationelle Selbstbestimmung der von der Meldung betroffenen Person.[1015] Die Interessenabwägung ist eigenständig durchzuführen. Der Identitätsschutz nach §§ 8, 9 HinSchG führt nicht automatisch zu einer Beschränkung der Datenauskunft. Aus dem Regel-Ausnahme-Verhältnis in Art. 15 DS-GVO folgt, dass in Zweifelsfragen das Recht auf Datenauskunft überwiegt. Darüber können sich die Vorgaben des HinSchG nicht hinwegsetzen. Überwiegt der Identitätsschutz, ist die Datenauskunft zu beschränken, indem geheime Informationen z. B. unkenntlich gemacht werden.

9. Aufgrund der großen Rechtsunsicherheit im Spannungsverhältnis zwischen Identitätsschutz und Betroffenenrechte, können Arbeitgeber Maßnahmen ergreifen, um den Identitätsschutz zu erhöhen. Eine Verzichtserklärung in Bezug auf die Betroffenenrechte scheidet im Beschäftigungskontext allerdings aus.[1016] Demgegenüber eignet sich die Einschaltung einer externen, anwaltlichen Ombudsperson zur Erhöhung des Identitätsschutzes.[1017] Aufgrund des anwaltlichen Berufsgeheimnisses (§ 43a Abs. 2 BRAO sowie § 203 StGB) wird die Ausnahmeregelung des Art. 14 Abs. 5 lit. d) DS-GVO aktiviert. Dies gilt allerdings nur, bis die externe Ombudsstelle die Daten an den Beschäftigungsgeber für etwaige Folgemaßnahmen weiterleitet. Maßgeblich ist auch, dass die externe Ombudsstelle nach den Vorgaben der DS-GVO selbst datenschutzrechtlich verantwortliche Stelle ist. Daneben kommt der Abschluss einer Betriebsvereinbarung zur Erhöhung des Identitätsschutzes in Betracht.[1018] Die Grundsätze der Datenverarbeitung (Art. 5 und Art. 6 DS-GVO) bilden einen Mindestschutz, den die Betriebsparteien nicht unterlaufen dürfen, Art. 88 Abs. 2

[1015] Siehe: Kapitel C) I. 3. c) bb) (2).
[1016] Siehe: Kapitel C) I. 3. c) cc) (1).
[1017] Siehe: Kapitel C) I. 3. c) cc) (2).
[1018] Siehe: Kapitel C) I. 3. c) cc) (3).

DS-GVO. Im Übrigen bleiben die Betriebsparteien in der konkreten Ausgestaltung frei, diesen Mindestschutz im Rahmen einer Betriebsvereinbarung zu verankern.

Wann muss der datenschutzrechtlich Verantwortliche Geschäftsgeheimnisse beauskunften?

1. Die Beschränkungsmöglichkeit in Art. 15 Abs. 4 DS-GVO erstreckt sich trotz des Verweises auf die Kopie, auf das Auskunftsrecht mitsamt der Metainformationen (siehe davor: Erkenntnis 7). Maßgeblich ist eine umfassende Interessenabwägung zwischen dem informationellen Selbstbestimmungsrecht der von der Datenverarbeitung betroffenen Person und den berechtigten Geheimhaltungsinteressen des datenschutzrechtlich Verantwortlichen. Im Bereich des Geschäftsgeheimnisschutzes ist davon auszugehen, dass ein berechtigtes Geheimhaltungsinteresse besteht, soweit es sich um ein Geschäftsgeheimnis im Sinne des GeschGehG handelt.[1019] Art. 15 Abs. 4 DS-GVO erfordert eine eigenständige Interessenabwägung. Inwieweit der Geschäftsgeheimnisschutz überwiegt, ist einzelfallbezogen zu entscheiden. Aus dem Vorliegen eines berechtigten Geheimhaltungsinteresses folgt noch keine Beschränkung der Datenauskunft. Aufgrund der hohen Risiken, die mit der Offenlegung eines Geschäftsgeheimnisses für das Unternehmen einhergehen, ist jedoch regelmäßig von einem Überwiegen der Geheimhaltungsinteressen auszugehen. Die geheimen Informationen sind unkenntlich zu machen.

2. § 83 Abs. 1 S. 1 BetrVG tritt neben die Datenauskunft und verdrängt diese nicht.[1020] Mit Blick auf die Öffnungsklausel des Art. 88 Abs. 1 DS-GVO erfüllt das personalaktenrechtliche Einsichtsrecht die obligatorischen Transparenzanforderungen des Art. 88 Abs. 2 DS-GVO nicht. Der Arbeitnehmer ist darauf

[1019] Siehe: Kapitel C) II. 2.
[1020] Siehe: Kapitel C) II. 3. b).

angewiesen, seine Daten dauerhaft in einer verständlichen und transparenten Weise zur Verfügung gestellt zu bekommen, ohne dabei das Risiko für etwaige Fehler tragen zu müssen, die im Rahmen der Kenntniserlangung unterlaufen können. Die Kopie-Erteilung kann nicht durch eine Einsichtnahme ersetzt werden. Aus denselben Gründen lässt sich § 83 Abs. 1 S. 1 BetrVG auch nicht auf die Öffnungsklausel des Art. 23 Abs. 1 lit. i) DS-GVO zurückführen. Aus Gründen der Einheit der Rechtsordnung sind jedoch dieselben Maßstäbe im Rahmen des § 83 Abs. 1 S. 1 BetrVG anzusetzen, die sich aus Art. 15 Abs. 4 DS-GVO ergeben. Der Arbeitgeber ist daher berechtigt, soweit es seine berechtigten Geheimhaltungsinteressen erfordern, geheime Informationen zu schwärzen, ehe er dem Arbeitnehmer Akteneinsicht gewährt.[1021]

Wie wird der Geschäftsgeheimnisschutz im Rahmen der Betriebsratsarbeit gewährleistet?

1. Die Erlangung eines Geschäftsgeheimnisses des Betriebsrats durch den Arbeitgeber erfolgt im Sinne einer effektiven Betriebsratsarbeit. Das Geheimhaltungsinteresse des Arbeitgebers wird insbesondere über die Verschwiegenheitspflicht gemäß § 79 Abs. 1 S. 1 BetrVG sichergestellt.[1022] In der Rechtsprechung zu § 79 Abs. 1 S. 1 BetrVG hat sich eine eigenständige Definition des Betriebs- oder Geschäftsgeheimnisses entwickelt. Diese ist auch nach Einführung des GeschGehG weiter maßgeblich. Betriebs- und Geschäftsgeheimnisse im Sinne des § 79 Abs. 1 S. 1 BetrVG sind Tatsachen, die im Zusammenhang mit dem Geschäftsbetrieb stehen, nicht offenkundig sind und nach dem erkennbaren Willen des Betriebsinhabers geheim gehalten werden sollen, weil dieser an deren Geheimhaltung ein objektiv berechtigtes wirtschaftliches Interesse hat. Die Erklärung des Arbeitgebers über die Geheimhaltungsbedürftigkeit eines Geschäftsgeheim-

[1021] Siehe: Kapitel C) II. 3. c).
[1022] Siehe: Kapitel C) III. 1.

nisses ist konstitutiv und unterliegt keinem bestimmten Formerfordernis.

2. Die Tatbestandsausnahme des § 5 Nr. 3 GeschGehG regelt die zulässige Erlangung eines Geschäftsgeheimnisses des Betriebsrats durch den Arbeitnehmer. Nach § 5 Nr. 3 GeschGehG ist die Erlangung, Nutzung oder Offenlegung eines Geschäftsgeheimnisses nicht verboten, wenn dies im Rahmen der Offenlegung durch den Arbeitnehmer gegenüber dem Betriebsrat erforderlich ist, damit dieser seine Aufgaben erfüllen kann. Mangels konstitutiver Vertraulichkeitserklärung des Arbeitgebers ist der Betriebsrat aus dem Gebot der vertrauensvollen Zusammenarbeit mit dem Arbeitgeber zur Verschwiegenheit verpflichtet, § 2 Abs. 1 BetrVG. Hinsichtlich der Erforderlichkeit sind nach hiesiger Auffassung auch subjektive Erwägungen des Arbeitnehmers berücksichtigungsfähig.[1023] Dies gilt nicht, wenn die Offenlegung des Geschäftsgeheimnisses ohne Bezug zur Aufgabenerfüllung des Betriebsrats steht und dies zum Zeitpunkt der Offenlegung für den Arbeitnehmer offensichtlich erkennbar war.

3. Entscheidet sich ein Betriebsratsmitglied zur Meldung eines Geschäftsgeheimnisses zu Zwecken des Whistleblowings, gelten die allgemeinen Regelungen des HinSchG.[1024] Beabsichtigt ein Betriebsratsmitglied die Meldung eines Verstoßes und hat es hinreichenden Grund zu der Annahme, der interne Meldeweg sei zur Beseitigung des Missstands geeignet, resultiert daraus nach hiesiger Auffassung ein Vorrang des internen Meldekanals, vgl. § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG.[1025]

[1023] Siehe: Kapitel C) III. 2.
[1024] Siehe: Kapitel C) III. 3.
[1025] Siehe: Kapitel C) I. 2. b) ee).

4. Entscheidet sich ein Betriebsratsmitglied zur Meldung einer geschützten Information, die ihm ausschließlich wegen seiner Zugehörigkeit zum Betriebsrat in Wahrnehmung seiner Betriebsratstätigkeit durch den Arbeitgeber unter Hinweis auf die Vertraulichkeit bekannt geworden ist, erweitert sich das Spannungsfeld zwischen eigener Meinungsfreiheit und unternehmerischen Geheimhaltungsinteressen um das Gebot der vertrauensvollen Zusammenarbeit (§§ 2 Abs. 1, 79 Abs. 1 S. 1 BetrVG). Hierfür bedarf es einer betriebsverfassungsrechtlichen Lösung.[1026] Das Gebot der vertrauensvollen Zusammenarbeit verpflichtet das Betriebsratsmitglied, gemeinsam mit dem Arbeitgeber darauf hinzuwirken, dass aus der (Prüf-) Obliegenheit im Rahmen des § 6 Abs. 1 HinSchG ein Vorrang des internen Meldekanals resultiert. Maßstab bildet der Grundsatz von Treu und Glauben. Das Betriebsratsmitglied ist unabhängig von einer beabsichtigten Meldung verpflichtet, dem Arbeitgeber ihm bekannte bzw. bekannt gewordene Anhaltspunkte, die gegen die Funktionsfähigkeit des Hinweisgeberschutzsystems sprechen, mitzuteilen. Solange der Betriebsrat den Arbeitgeber nicht auf Anhaltspunkte aufmerksam macht, die gegen die Funktionsfähigkeit oder Wirksamkeit des internen Meldekanals sprechen, darf der Arbeitgeber konsequenterweise darauf vertrauen, dass der Vorrang des internen Meldekanals für die Betriebsratsmitglieder im Rahmen des § 6 Abs. 1 HinSchG besteht.

[1026] Siehe: Kapitel C) III. 3.

D) Die Gewinnung neuen exklusiven Wissens: Eine Balance zwischen Innovation und Rechtskonformität

Die Erforschung neuen Wissens ist notwendige Voraussetzung, um an Informationen zu gelangen, die sodann durch die Implementierung angemessener Geheimhaltungsmaßnahmen zu neuen Geschäftsgeheimnissen werden können. Überwiegend geht es dabei um Fragen der Produktverbesserung. Aufgrund ihres fehlenden Bezugs zum Arbeitsrecht sind diese jedoch nicht Untersuchungsgegenstand der vorliegenden Arbeit. Stattdessen geht die vorliegende Darstellung der Erlangung neuen Wissens im Beschäftigungskontext nach. Dies betrifft Fragen der betrieblichen Arbeitsprozess-Optimierung, wenn beispielsweise Laufwege der Beschäftigten analysiert und effizienter gestaltet werden sollen. Die Erkenntnisse solcher Analysen können schützenswerte Informationen darstellen. In diesem Zusammenhang stellt sich auch die Frage, inwieweit der Einsatz algorithmusbasierter KI-Systeme zu Zwecken der Prozessoptimierung möglich ist.[1027] Grenzen setzen in erster Linie die datenschutzrechtlichen Vorgaben zum Schutz des informationellen Selbstbestimmungsrechts der Beschäftigten. Die Herausforderung besteht darin, ein Gleichgewicht zwischen Persönlichkeitsschutz und berechtigtem Informationsbedürfnis zu schaffen. In Anbetracht der nahezu unüberschaubaren Menge an Möglichkeiten, die bei der Gewinnung neuen exklusiven Wissens in Betracht kommen, lässt es die vorliegende Darstellung in Teilen bei allgemeinen Ausführungen und Grundsätzen bewenden. Die vorliegende Arbeit kann hier nur als allgemeine Orientierungshilfe aufzeigen, was bei der Implementierung relevanter Maßnahmen zu beachten sein kann.

Der Einsatz neuer (Überwachungs-) Technologien verspricht innovative Lösungen und Wettbewerbsvorteile. Welche betrieblichen Überwachungsmaßnahmen im Einzelnen zu implementieren sind, ist

[1027] Denkbar ist auch, z. B. mittels einer Softskill-Analyse effektivere Teams für Projektgruppen zu bilden.

unternehmensbezogen zu entscheiden. Begrenzende Wirkung haben insbesondere die datenschutzrechtlichen Vorgaben. Personenbezogene Daten dürfen nur insoweit verarbeitet werden, als dies auf eine datenschutzrechtliche Legitimationsgrundlage gestützt werden kann. Die Legitimationsgrundlagen im Bereich des Beschäftigungskontexts enthält Art. 88 Abs. 1 DS-GVO i. V. m. § 26 BDSG. Dazu zählen beispielsweise eine Betriebsvereinbarung, Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 4 BDSG oder eine Einwilligung, vgl. § 26 Abs. 2 BDSG.[1028] Im Hinblick auf die Legitimationsgrundlage des Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 1 S. 1 BDSG muss nach der Entscheidung des EuGH allerdings von der Unionsrechtswidrigkeit des § 26 Abs. 1 S. 1 BDSG ausgegangen werden, weil es sich um keine „*spezifischere Vorschrift*" im Sinne des Art. 88 Abs. 1 DS-GVO handelt.[1029] Für die Praxis ändert sich dadurch nicht viel.[1030] Datenverarbeitungen sind auch weiterhin in dem von § 26 Abs. 1 S. 1

[1028] Vgl. Art. 4 Nr. 11, Art. 7 Abs. 4, Art. 9 Abs. 2 lit. a) DS-GVO i. V. m. § 26 Abs. 2 und 3 S. 2 BDSG. Nach § 26 Abs. 2 S. 2 BDSG ist eine Einwilligung nur dann freiwillig, wenn für den Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder wenn Arbeitgeber und Arbeitnehmer mit der Datenverarbeitung gleichgelagerte Interessen verfolgen. Eine Einwilligung bietet aufgrund ihrer Widerruflichkeit unter Umständen keine dauerhafte Legitimationsgrundlage, Art. 7 Abs. 3 DS-GVO, § 26 Abs. 2 S. 4 BDSG, Art. 22 Abs. 1 lit. c) DS-GVO.

[1029] Infolge der Entscheidung des EuGH zu § 23 HDSIG ist davon auszugehen, dass Datenverarbeitungen im Beschäftigungskontext nicht mehr auf § 26 Abs. 1 S. 1 BDSG, sondern jedenfalls auf Art. 6 Abs. 1 S. 1 lit. f) DS-GVO gestützt werden müssen, vgl. EuGH, Urteil v. 30.03.2023 - C-34/2. Auch dort findet eine Interessenabwägung statt, sodass die unter § 32 BDSG a.F. entwickelten Grundsätze nunmehr im Rahmen des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO Beachtung finden. Zu derselben Einschätzung gelangt das Land Hessen in Bezug auf § 23 HDSIG im Rahmen seiner Handreichung zur Verarbeitung personenbezogener Daten von Beschäftigten in Reaktion auf die Entscheidung des EuGH, Urteil v. 30.03.2023 - C-34/21.

[1030] Siehe: Kapitel B) I. 4. b).

BDSG vorgezeichneten Umfang über Art. 6 Abs. 1 S. 1 lit. f) DS-GVO möglich.[1031]

Nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO (bzw. § 26 Abs. 1 S. 1 BDSG) dürfen personenbezogene Daten für Zwecke des Beschäftigungsverhältnisses unter anderem verarbeitet werden, wenn dies für dessen Durchführung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes erforderlich ist. Die Frage der datenschutzrechtlichen Zulässigkeit betrieblicher Maßnahmen zu Zwecken der Prozessoptimierung läuft daher auch weiterhin auf eine umfassende Interessenabwägung zwischen dem Interesse des Arbeitgebers an effizient gestalteten Arbeitsabläufen zur Gewährleistung der eigenen Wettbewerbsfähigkeit (Art. 12 Abs. 1 und Art. 14 Abs. 1 GG) und dem Recht des von der Datenverarbeitung betroffenen Arbeitnehmers auf informationelle Selbstbestimmung (Art. 2 Abs. 1, Art. 1 Abs. 1 GG) nach Maßgabe des Verhältnismäßigkeitsgrundsatzes hinaus.[1032] Sammeln digitale Programme Mitarbeiterdaten, die ohne Bezug zur Arbeitsleistung stehen, sind die Anforderungen an die datenschutzrechtliche Zulässigkeit hoch. Gleiches gilt für die Fälle, in denen die Überwachung eine Drucksituation bewirkt, die bei objektiver Betrachtung zu einem psychischen Anpassungsdruck führt. Beispiele betrieblicher Maßnahmen, die einen psychischen Anpassungsdruck bewirken können, sind

[1031] Bestätigt wird diese Sichtweise auch dadurch, dass Art. 6 Abs. 1 S. 1 lit. f) DS-GVO im Beschäftigungskontext anwendbar ist und inhaltlich nicht von § 26 Abs. 1 S. 1 BDSG abweicht, vgl. allgemein zum Verhältnis der spezifischeren Vorschriften nach Art. 88 Abs. 1 DS-GVO zu Art. 6 Abs. 1 S. 1 lit. f) DS-GVO: *Franzen*, in: ErfK-ArbR, § 26 BDSG Rn.4, der zu der Zeit noch wie viele andere von der Unionsrechtsmäßigkeit des § 26 Abs. 1 S. 1 BDSG ausging und der Frage einer eigenständigen Anwendbarkeit des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO neben § 26 Abs. 1 S. 1 BDSG im Unternehmenskontext nachging.

[1032] Vgl. BAG, Urteil v. 07.05.2019 - 1 ABR 53/17, BAGE 166, 309 Rn.42, NZA 2019, 1218 zu § 32 BDSG a. F.

insbesondere Videoüberwachungssysteme, GPS-Tracker sowie Maßnahmen zur Überwachung der elektronischen Kommunikation.[1033]

Daneben ist zu beachten, dass eine Prozessoptimierung auch im Eigeninteresse des Arbeitnehmers liegt. Das VG Hannover formuliert zutreffend: „*Die Verarbeitung der Beschäftigtenleistungsdaten ist zum Zwecke der Steuerung der Logistikprozesse, der Qualifizierung von Mitarbeiterinnen und Mitarbeitern, zur Erteilung objektiven Feedbacks und als Grundlage für Personalentscheidungen erforderlich und angemessen. Entsprechend durchgeführte Feedbackschleifen liegen im Eigeninteresse der Mitarbeiterinnen und Mitarbeiter, da permanentes Feedback den Mitarbeiterinnen und Mitarbeitern ermöglicht, sich und ihr Leistungsvermögen anhand der Rückmeldungen kontinuierlich weiterzuentwickeln.*“[1034] Zulässig ist beispielsweise eine Datenverarbeitung, wenn das digitale System der Verbesserung der betrieblichen Infrastruktur dient und im Rahmen der Datenverarbeitung keine Bewertung über das Verhalten des Arbeitnehmers vorgenommen wird. Das VG Hannover hat zu Recht entschieden, dass die Überwachung der Arbeitsgeschwindigkeit zur verbesserten Steuerung logistischer Abläufe datenschutzrechtlich nach Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 1 S. 1 BDSG zulässig sei,[1035] soweit keine persönlichen Eigenschaften, sondern lediglich das Leistungsverhalten überwacht werde.[1036] In Betracht kommen z. B. GPS- oder Handy-Ortungsdienste oder Smart-ID-Batches sowie Videoüberwachungen. Häufig sind GPS-Tracker in den Fahrzeugen verbaut. Eine Datenverarbeitung im Sinne des § 26 Abs. 1 S. 1 BDSG liegt vor, sofern die

[1033] *Däubler*, Gläserne Belegschaften, § 6 Rn.318 ff. Die Daten sind mittelbar einem bestimmten Arbeitnehmer zuordbar, vgl. *Thüsing*/*Forst*, in: Compliance, § 12 Rn.16 ff.

[1034] VG Hannover, Urteil v. 09.02.2023 - 10 A 6199/20, Rn.1, 78; *Höpfner/Daum,* ZfA 2021, 467, 480, 486.

[1035] Diese Wertung gilt auch für Art. 6 Abs. 1 S. 1 lit. f) DS-GVO.

[1036] VG Hannover, Urteil v. 09.02.2023 - 10 A 6199/20.

Ortungsdaten einem bestimmten Mitarbeiter - ggf. unter Hinzuziehung weiterer Informationen - zuordbar sind.[1037]

Nicht abschließend geklärt ist, inwieweit Mitarbeiterdaten im Rahmen betrieblicher Leistungskontrollen zu Zwecken automatisierter Weisungen verarbeitet werden dürfen. Derartige Kontrollmaßnahmen dienen - in einem ersten Schritt - der Informationsgewinnung, auf deren Grundlage das Algorithmus basierte System eigenständig Entscheidungen trifft, aus denen das Unternehmen - in einem zweiten Schritt - schützenswerte Informationen ableiten kann.[1038] Im Bereich des Personen- und Gütertransports legen technische Programme z. B. konkrete Routen fest und geben vor, wo getankt werden soll oder wann und wo eine Pausenzeit einzulegen ist. Vorfrage ist jedoch, ob eine automatisierte Entscheidung überhaupt Weisungsqualität im Sinne der §§ 315, 611a Abs. 1 S. 2 BGB haben kann.

Eine Weisung ist eine empfangsbedürftige Willenserklärung, die der Konkretisierung des Arbeitsvertrags dient und einer Erklärung gegenüber dem Arbeitnehmer bedarf.[1039] Werden digitale Systeme zur Weisungserteilung eingesetzt, kann zwischen automatisierten Willenserklärungen und autonomen Willenserklärungen unterschieden werden. Eine automatisierte Willenserklärung folgt einer sog. „*wenn-dann*" Programmierung.[1040] Der Verwender definiert bestimmte Bedingungen, bei deren Eintritt das Programm ein zuvor festgelegtes Ergebnis erzeugt. Der Verwender setzt das Programm bewusst zur Abgabe einer vordefinierten rechtserheblichen Erklärung ein. Damit erfüllt eine automatisierte Willenserklärung sämtliche Voraussetzungen einer Willenserklärung.[1041] In Fällen einer autonomen Willenserklärung

---

[1037] BGH, Urteil v. 04.06.2013 - 1 StR 32/13, BGHSt 58, 268, NJW 2013, 2530 Rn.35 ff.; VG Lüneburg, Teilurteil v. 19.03.2019 - 4 A 12/19, LSK 2019, 3816.

[1038] *Waas*, RdA 2022, 125, 127.

[1039] BAG, Urteil v. 16.04.2015 - 6 AZR 242/14, NZA-RR 2015, 534 Rn.24.

[1040] *Höpfner/Daum,* ZfA 2021, 467, 473.

[1041] Zu den Voraussetzungen einer Willenserklärung: *Armbrüster*, in: MüKo-BGB, vor § 116 Rn.3-19.

definiert der Anwender ebenfalls bestimmte Bedingungen. Treten diese Bedingungen ein, erzeugt das Programm allerdings ein eigenes, nicht zuvor festgelegtes Ergebnis.[1042] Dies hat zur Folge, dass es einer autonomen Willenserklärung am Geschäftswillen ihres Anwenders fehlt.[1043] Dies ist jedoch unschädlich: Ein fehlender Geschäftswille steht der Annahme einer Willenserklärung nicht entgegen, vgl. §§ 119 ff. BGB.[1044] Demzufolge kann eine automatisierte Entscheidung, unabhängig davon, ob sie als automatisierte oder autonome Willenserklärung einzuordnen ist, Weisungsqualität im Sinne der §§ 315, 611a Abs. 1 S. 2 BGB aufweisen.

Für die Wirksamkeit einer automatisierten Weisung kommt es dann darauf an, ob sie der Billigkeit im Sinne des § 315 Abs. 1 und Abs. 3 BGB, § 106 S. 1 GewO entspricht.[1045] Der Begriff der „*Billigkeit*" stellt einen unbestimmten Rechtsbegriff dar, der dem informationellen Selbstbestimmungsrecht des Weisungsunterworfenen als Einfallstor dient (sog. mittelbare Drittwirkung), Art. 2 Abs. 1 und Art. 1 Abs. 1 GG.[1046] Die Richtschnur geben insofern die datenschutzrechtlichen Bestimmungen vor. Hintergrund ist, dass die datenschutzrechtlichen Vorgaben den Schutz des informationellen Selbstbestimmungsrechts sicherstellen.[1047] Darüber hinaus ist ggf. das zwingende Mitbestim-

---

[1042] *Höpfner/Daum*, ZfA 2021, 467, 475.

[1043] *Paulus,* JuS 2019, 960, 965; *Höpfner/Daum*, ZFA 2021, 467, 476.

[1044] Handlungs- und Erklärungswille liegen vor, da die Entscheidung des Programms zumindest mittelbar auf den Willen des Anwenders rückführbar ist. Dafür spricht, dass der Anwender die Entscheidung bewusst auf die KI auslagert, vgl. *Höpfner/Daum,* ZfA 2021, 467, 476, 477, der zu Recht den Verweis auf eine Blankett-Erklärung zieht. A. A.: *Grützmacher/Heckmann*, CR 2019, 553, 558.

[1045] Maßgeblich ist allein das Ergebnis der Weisung, nicht inwieweit ein umfassender Abwägungsprozess stattgefunden hat, vgl. BAG, Urteil v. 24.10.2018 - 10 AZR 19/18, NZA 2019, 619 Rn.26; BAG, Urteil v. 18.10.2017 - 10 AZR 47/17, NZA 2018, 162 Rn.19; BAG, Urteil v. 18.10.2017 - 10 AZR 330/16, NZA 2017, 1452 Rn.45.

[1046] BVerfG, Beschluss v. 11.04.2018 - 1 BvR 3080/09, BVerfGE 148, 267, NJW 2018, 1667, Rn.32; *Sprau*, in: Grüneberg, § 823 Rn.84 ff.

[1047] Siehe: Kapitel C) I. 1. a).

mungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG zu beachten. Nach der vom BAG entwickelten „*Theorie der Wirksamkeitsvoraussetzung*“ kann ein Verstoß gegen § 87 Abs. 1 Nr. 6 BetrVG zur Unwirksamkeit einer Weisung führen, sofern diese auf einer Maßnahme beruht, die in mitbestimmungswidriger Weise ergangen ist.[1048] Das Mitbestimmungsrecht sichert den Persönlichkeitsschutz demgemäß doppelt ab.[1049]

Fraglich ist, ob die Regelung des Art. 22 Abs. 1 DS-GVO der datenschutzrechtlichen Zulässigkeit einer automatisierten Weisung grundsätzlich entgegensteht. Nach Art. 22 Abs. 1 DS-GVO darf die von der Datenverarbeitung betroffene Person nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Stimmen in der Literatur sprechen sich für eine Anwendung des Art. 22 Abs. 1 DS-GVO aus, sobald eine automatisierte Entscheidung bzw. Weisung keiner weiteren Überprüfung durch den Menschen unterzogen wird.[1050] Diese Sichtweise greift allerdings zu kurz und übersieht, dass eine teleologische Reduktion des Art. 22 Abs. 1 DS-GVO geboten ist.[1051] Zweck des Art. 22 Abs. 1 DS-GVO ist, dass kein Mensch der Entscheidung einer Maschine unterworfen werden soll, um den

---

[1048] BAG, Beschluss v. 03.12.1991 - GS 2/90, NZA 1992, 749, 759; *Thüsing/Granetzny*, in: Compliance § 20 Rn.42; *Wiese*, in: GK-BetrVG § 87 Rn.100 ff.; a. A.: *Richardi*, in: Richardi, BetrVG, § 87 Rn.104 ff.

[1049] Der Betriebsrat überwacht die Einhaltung der datenschutzrechtlichen Vorgaben durch den Arbeitgeber, vgl. § 80 Abs. 1 Nr. 1 BetrVG. Der Betriebsrat gilt daher auch als „*Wächter des Beschäftigtendatenschutzes*“, vgl. *Gola*, in: Gola/Pötters, § 26 BDSG Rn.17.

[1050] Art. 22 Abs. 1 DS-GVO erfasst nicht den Fall, dass sich der Arbeitgeber lediglich zur Vorbereitung seiner Entscheidungen eines KI-Systems bedient, vgl. *Höpfner/Daum,* ZfA 2021, 467, 480, 482 m. w. N.

[1051] *Höpfner/Daum*, ZfA 2021, 467, 480, 481; *Von Lewinski*, in: BeckOK-DatenschutzR, Art. 22 DS-GVO Rn.33; *Kumkar/Roth-Isigkeit,* JZ 2020, 277, 279.

Einzelnen vor Verobjektivierung zu schützen.[1052] Demzufolge kann Art. 22 Abs. 1 DS-GVO nur einschlägig sein, wenn die automatisierte Entscheidung zugleich die Gefahr einer Verobjektivierung birgt. Von einer Verobjektivierung des Arbeitnehmers kann jedoch nur gesprochen werden, soweit die automatisierte Entscheidung eine für den von der Datenverarbeitung Betroffenen nachteilige Rechtswirkung entfaltet. Art. 22 Abs. 1 DS-GVO ist demnach dahingehend teleologisch zu reduzieren, dass nur solche automatisierten Entscheidungen verboten sind, die sich für den Betroffenen nachteilig im Sinne einer Beschränkung seiner Rechtspositionen auswirken. Für diese Lesart spricht auch die Formulierung in Art. 22 Abs. 1 DS-GVO („*oder in ähnlicher Weise erheblich beeinträchtigt*"), die darauf hindeutet, dass die „*rechtliche Wirkung*" einer automatisierten Entscheidung ebenfalls eine gewissen Erheblichkeit erfordert.[1053]

Für die Frage der datenschutzrechtlichen Zulässigkeit einer automatisierten Weisung kommt es darauf an, ob diese eine rechtlich nachteilige Wirkung gegenüber dem Arbeitnehmer entfaltet, Art. 22 Abs. 1 DS-GVO. Eine Weisung entfaltet zunächst insoweit Rechtswirkung, als sie die arbeitsvertraglich geschuldete Leistung des Arbeitnehmers in Bezug auf den Inhalt, die Durchführung, die Zeit und den Ort (§ 611a Abs. 1 S. 2 BGB) konkretisiert.[1054] Allerdings ist diese Konkretisierung für den Arbeitnehmer nicht nachteilig. Dafür spricht, dass eine Weisung ausschließlich der Durchführung des Arbeitsvertrages dient, die demzufolge auch im Eigeninteresse des Arbeitnehmers erfolgt, § 611a Abs. 1 S. 2 BGB.[1055] Soweit eine Weisung im Einzelfall als unangenehm empfunden wird, weil eine Zusammenarbeit mit

---

[1052] Dieser Gedanke ist auf die Würde des Menschen (Art. 1 Abs. 1 GG) zurückzuführen, vgl. *Höpfner/Daum*, ZfA 2021, 467, 480 m. w. N.

[1053] *Höpfner/Daum*, ZfA 2021, 467, 486, mit dem zutreffenden Hinweis, dass andernfalls die Formulierung „*in ähnlicher Weise erheblich beeinträchtigt*" obsolet wäre.

[1054] BAG, Urteil v. 16.04.2015 - 6 AZR 242/14, NZA-RR 2015, 534 Rn.24.

[1055] *Höpfner/Daum,* ZfA 2021*,* 467, 480, 486, unter Hinweis auf BAG, Urteil v. 21.02.2017 - 1 AZR 367/15, NZA 2017, 740 Rn.19; BAG, Urteil v. 24.06.2015 - 5 AZR 462/14, NZA 2016, 108 Rn.34.

anderen Kollegen als angenehmer betrachtet wird, ist dieser Umstand dem Arbeitsvertrag immanent und beschränkt den Arbeitnehmer jedenfalls nicht in seinen Rechtspositionen. Eine darüberhinausgehende nachteilige Rechtswirkung entfaltet die Weisung nicht. Damit steht Art. 22 Abs. 1 DS-GVO der datenschutzrechtlichen Zulässigkeit einer automatisierten Weisung nicht entgegen.[1056] Geht es um die effizientere Gestaltung von Arbeitsprozessen, dürfen Mitarbeiterdaten im Rahmen betrieblicher Leistungskontrollen zu Zwecken automatisierter Weisungen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes folgerichtig verarbeitet werden.

Soll ein KI-System anhand von Mitarbeiterdaten erst noch trainiert werden, ist Art. 6 Abs. 1 S. 1 lit. f) DS-GVO maßgebliche Legitimationsgrundlage für eine Neuerhebung der Mitarbeiterdaten.[1057] Entscheidet sich der Arbeitgeber im Rahmen eines KI-Trainings auf Mitarbeiterdaten zurückzugreifen, die bereits zuvor im Beschäftigungskontext verarbeitet wurden, müssen die Anforderungen an eine Zweckänderung nach Art. 6 Abs. 4 DS-GVO erfüllt sein.[1058] Wurden KI-Systeme bereits vom Hersteller entsprechend trainiert, eignen sich Mitarbeiterdaten, um das KI-System vorab zu testen, ehe es z. B. im Bewerbungsverfahren zum Einsatz kommt. Bei der Einführung eines KI-Systems bzw. der Durchführung einer KI-basierten Maßnahme sind die Beteiligungsrechte des Betriebsrats zu beachten. Dazu gehören insbesondere das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG und die Unterrichtungsrechte in § 90 Abs. 1 Nr. 2 und Nr. 3 BetrVG. Flankiert werden die Beteiligungsrechte durch den allgemeinen Unterrichtungsanspruch des Betriebsrats nach § 80 Abs. 2 BetrVG. Muss der Betriebsrat zur Durchführung seiner Aufgaben die Einführung oder Anwendung von künstlicher Intelligenz beurteilen,

---

[1056] So im Ergebnis auch: *Höpfner/Daum*, ZfA 2021, 467, 480, 483 m. w. N.
[1057] *Malorny*, JuS 2022, 289, 293.
[1058] Hintergrund ist, dass personenbezogene Daten nach dem Grundsatz der Zweckbindung nur für vorher festgelegte Zwecke verarbeitet werden dürfen, vgl. Art. 5 Abs. 1 lit. b) DS-GVO, vgl. *Ziegenhorn/Schulz-Große*, ZD 2023, 581, 582.

gilt die Hinzuziehung eines Sachverständigen nach § 80 Abs. 3 S. 2 BetrVG insoweit als erforderlich. Eine Prüfung der Erforderlichkeit findet aufgrund der Fiktion nicht mehr statt.

E) Resümee: Eine Zusammenfassung in 25 Thesen

Unternehmen stehen vor der Herausforderung, angemessene Geheimhaltungsmaßnahmen zu implementieren, deren tatsächliches Vorliegen konstitutiv ist, um Schutz durch das GeschGehG zu erfahren. Erst die Konnexion gesetzlicher und arbeitsvertraglicher Verschwiegenheitspflichten, flankiert von technischen und organisatorischen Sicherungsmechanismen vermag es, einen adäquaten Geschäftsgeheimnisschutz im Beschäftigungskontext sicherzustellen. Kommt es im Bereich des Whistleblowings oder den datenschutzrechtlichen Betroffenenrechten zu Kollisionen mit dem Geschäftsgeheimnisschutz, birgt die Auflösung der mehrdimensionalen Interessenkonflikte fortwährende Risiken. Unbestimmt ist nahezu alles - umstritten Vieles. Für den Rechtsanwender ist es daher von besonderer Dringlichkeit, belastbare Orientierung zu finden. Die vorliegende Dissertation hat sich dem angenommen.

Richtschnur waren folgende Leitfragen:

Kapitel B): Rechtliche Grundlagen des Geschäftsgeheimnisschutzes

- Wann unterfällt eine Information dem GeschGehG-Schutzregime?
- Welche Besonderheiten gelten im Beschäftigungskontext?
- Was bedeutet das für das unternehmerische Compliance-System?

Kapitel C): Der Geschäftsgeheimnisschutz: Reichweite und Grenzen im Beschäftigungskontext

- Wie können die Friktionen zwischen GeschGehG und HinSchG überwunden werden?
- Wem darf ein Whistleblower Geschäftsgeheimnisse melden?
- Was folgt daraus für die unternehmerischen Compliance-Systeme?
- Wann muss der datenschutzrechtlich Verantwortliche Geschäftsgeheimnisse beauskunften?
- Wie wird der Geschäftsgeheimnisschutz im Rahmen der Betriebsratsarbeit gewährleistet?

Kapitel D): Die Gewinnung neuen exklusiven Wissens: Eine Balance zwischen Innovation und Rechtskonformität

- Was ist bei der Implementierung betrieblicher Maßnahmen zu Innovationszwecken im Beschäftigungskontext zu beachten?

Fasst man diese Leitfragen unter einer einzigen zusammen, müsste diese wie folgt lauten:

Was braucht es für einen adäquaten Geschäftsgeheimnisschutz im Beschäftigungskontext?

Nach den vorstehenden Ausführungen lassen sich folgende Erkenntnisse thesenartig festhalten:

1. Ausgangspunkt des Geschäftsgeheimnisschutzes ist ein umfassendes Begriffsverständnis. Nach § 2 Nr. 1 lit. a) GeschGehG bedarf es einer geheimen Information von wirtschaftlichem Wert mit Unternehmensbezug im Sinne einer Marktrelevanz.[1059] Dies können auch private Informationen sein. Besteht eine Information aus mehreren Bestandteilen, kann sie geheim sein, obgleich ihre Einzelteile öffentlich zugänglich sind. § 2 Nr. 1 lit. a) GeschGehG ist dahingehend auszulegen, dass die „*weder […] noch*“ Formulierung im Sinne eines alternativen *„entweder […] oder*“ Verständnisses zu begreifen ist. Der Begriff des „*wirtschaftlichen Werts*“ entspricht dem des „*kommerziellen Werts*“ in der GeschGehG-RL. Hinsichtlich der Kausalverbindung zwischen Geheimhaltung und Wertigkeit einer Information genügt es, dass eine Information durch die Geheimhaltung einen (potenziellen) Wertzuwachs erfährt.

[1059] Siehe: Kapitel B) II. 3. a).

2. Der Begriff des „*berechtigten Interesses*“ in § 2 Nr. 1 lit. c) GeschGehG entspricht dem des „*legitimen Interesses*“ in Erwägungsgrund 14 GeschGeh-RL.[1060] Das Kriterium geht vollständig in dem Erfordernis des „*wirtschaftlichen Werts*“ auf, § 2 Nr. 1 lit. a) GeschGehG. Auf Definitionsebene besteht die unwiderlegliche Vermutung, dass an einer Information, die wirtschaftlichen Wert aufweist, ein berechtigtes Interesse an der Geheimhaltung besteht.[1061]

3. Rechtswidrige Informationen sind schutzfähig im Sinne des GeschGehG. Da Unternehmen im Falle ihres Bekanntwerdens Wertverluste durch Reputationsschäden bzw. Schadensersatzforderungen drohen, sind rechtswidrige Informationen von „*wirtschaftlichem Wert*“.[1062] Das Kriterium des „*berechtigten Interesses*“ wird bei Vorliegen eines wirtschaftlichen Werts fingiert und führt folgerichtig ebenfalls nicht zum Ausschluss rechtswidriger Informationen.[1063] Interessengerechte Lösungen lassen sich über § 5 GeschGehG realisieren.

4. Ob den Umständen nach „*angemessene Geheimhaltungsmaßnahmen*“ getroffen wurden, ist unternehmensspezifisch im Rahmen einer umfassenden Abwägung zu beurteilen, § 2 Nr. 1 lit. b) GeschGehG. Dazu ist das Interesse des Unternehmens an der Geheimhaltung der Information mit dem für das Unternehmen möglichen und zumutbaren Aufwand, den das Unternehmen tatsächlich unternommen hat, um die Erkennbarkeit der Geheimhaltung zu erreichen und die Information vor unberechtigtem Zugriff zu schützen, ins Verhältnis zu setzen, wobei die Anforderungen an die angemessenen Geheimhaltungsmaßnahmen keine abschreckende Wirkung entfalten dürfen.[1064] Soweit die Geltendmachung

[1060] Siehe: Kapitel B) II. 3. b).
[1061] Siehe: Kapitel B) II. 3. b) ff).
[1062] Siehe: Kapitel B) II. 3. a) cc) und Kapitel B) II. 3. b).
[1063] Siehe: Kapitel B) II. 3. b) ff).
[1064] Siehe: Kapitel B) II. 3. c) aa) (6).

von Schutzansprüchen angesichts der getroffenen Geheimhaltungsmaßnahmen im Einzelfall unverhältnismäßig erscheint, findet dies sein Korrektiv in § 9 Nr. 2 GeschGehG. Im Beschäftigungskontext läuft es in der Regel auf eine Kombination organisatorischer, rechtlicher und technischer Maßnahmen hinaus. Ereignet sich ein Geheimnisverrat, entscheiden die Umstände des Einzelfalls, ob das Unternehmen zum Zeitpunkt des Geheimnisverrats berechtigterweise davon ausgehen durfte, dass die geheime Information hinreichend geschützt sei.

5. Um wirtschaftliche Nachteile vom Unternehmen fernzuhalten, ist die Geschäftsleitung gesellschaftsrechtlich verpflichtet, geheime Informationen mittels angemessener Geheimhaltungsmaßnahmen dem Schutzregime des GeschGehG zu unterstellen. Aus Nachweisgründen sind die implementierten Maßnahmen zu dokumentieren. Der Wandel der Zeit erfordert außerdem eine fortlaufende Überprüfung, respektive Weiterentwicklung der Geheimnisschutzkonzepte. Es kann sich anbieten, mögliche Synergien mit dem Datensicherheitskonzept zu heben.[1065] Kommt es in diesem Zusammenhang zur Offenlegung von Geschäftsgeheimnissen gegenüber dem Datenschutzbeauftragten, ist dieser zur Verschwiegenheit verpflichtet, vgl. Art. 38 Abs. 5 DS-GVO. Es bleibt ihm allerdings unbenommen, etwaige Missstände nach Maßgabe des § 6 HinSchG bzw. § 5 Nr. 2 GeschGehG zu melden.

6. Rechtswidrige Geheimhaltungsmaßnahmen sind bei der Beurteilung der „*angemessenen Geheimhaltungsmaßnahmen*“ berücksichtigungsfähig, soweit der Geheimnisinhaber im Zeitpunkt des Geheimnisverrats berechtigterweise von der Wirksamkeit bzw. Zulässigkeit der Geheimhaltungsmaßnahme ausgehen durfte, §§ 2 Nr. 1 lit. b), 9 Nr. 2 GeschGehG.[1066] Die Frage der Berücksichtigungsfähigkeit einer unwirksamen Maßnahme stellt sich,

[1065] Siehe: Kapitel B) III.
[1066] Siehe: Kapitel B) II. 3. c) bb) (1).

wenn keine anderweitigen Sicherungsvorkehrungen für die Annahme eines angemessenen Schutzniveaus vorhanden sind. Sollte eine unwirksame arbeitsvertragliche Verschwiegenheitsklausel nicht berücksichtigungsfähig sein, kann die arbeitsvertragliche Treuepflicht berücksichtigungsfähig sein, sofern die unwirksame Klausel bestimmt genug ist, die nötige Erkennbarkeit des arbeitgeberseitigen Geheimhaltungsinteresses sicherzustellen.

7. Enthält eine Verschwiegenheitsvereinbarung eine sog. „*Catch-All-Klausel*“, ist diese unwirksam, weil der Arbeitnehmer in unzumutbarer Weise an seinem beruflichen Fortkommen gehindert wird.[1067] Dies folgt aus einer Einzelfallabwägung zwischen dem Geheimhaltungsinteresse des Arbeitgebers mit dem von der Berufsfreiheit (Art. 12 Abs. 1 GG) geschützten Interesse des Arbeitnehmers, sein erworbenes Wissen für sein berufliches Fortkommen nutzbar zu machen. Sieht eine arbeitsvertragliche Verschwiegenheitsvereinbarung vor, dass die Informationen über die Beendigung des Arbeitsverhältnisses hinaus geheim zu halten sind, sorgt die Klausel dafür, dass das Geheimhaltungsinteresse des ehemaligen Arbeitgebers für den ausgeschiedenen Arbeitnehmer erkennbar fortbesteht.[1068] Die nachwirkende Treuepflicht erstreckt sich sodann auf Informationen, die nicht zu den redlich erworbenen Erfahrungen und Fähigkeiten eines Arbeitnehmers zählen, weil sie z. B. nicht ohne Zuhilfenahme angefertigter Unterlagen abrufbar sind.

8. Überwachungs- und Kontrollmaßnahmen im Bereich des Geheimnisschutzes wirken auf die Regeltreue der Beschäftigten hin und gewährleisten eine effektive Aufarbeitung im Falle eines Geheimnisverrats. Begrenzende Wirkung haben insbesondere die datenschutzrechtlichen Vorgaben, wobei von der Unionsrechtswidrigkeit des § 26 Abs. 1 S. 1 BDSG und des § 26 Abs. 1 S. 2 BDSG

[1067] Siehe: Kapitel B) II. 4. a).
[1068] Siehe: Kapitel B) II. 4. a).

auszugehen ist.[1069] Die unter § 26 Abs. 1 S. 1 und S. 2 BDSG entwickelten Maßstäbe beanspruchen auf der Grundlage des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO weiterhin Geltung. Abweichungen ergeben sich mit Blick auf verdeckt durchgeführte Überwachungsmaßnahmen. Zentrales Abwägungskriterium bleibt die Eingriffsintensität der jeweiligen Überwachungsmaßnahme. Die Beteiligungsrechte in § 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG geben Anlass für den Abschluss einer Betriebsvereinbarung, die zugleich als datenschutzrechtliche Legitimationsgrundlage fungiert. Bewerberprüfungen dienen der Integritätsprüfung und sind ebenfalls Teil des unternehmerischen Geschäftsgeheimnisschutzes.[1070] Fragen nach einschlägigen Vorstrafen sind ebenso erlaubt wie die Durchführung elektronischer Datenabgleiche. Kommen KI-Systeme zum Einsatz, ist das arbeitgeberseitige Interesse an einer effektiven und objektiven Auswahlentscheidung mit dem Persönlichkeitsschutz des Bewerbers in einen angemessenen Ausgleich zu bringen.

9. Der Geschäftsgeheimnisschutz gilt nicht uneingeschränkt. Die Weitergabe eines Geschäftsgeheimnisses durch einen Whistleblower bemisst sich nach § 3 Abs. 2 GeschGehG i. V. m. § 6 Abs. 1 HinSchG und § 5 Nr. 2 GeschGehG, wobei die Regelungen inkongruent sind.[1071] Friktionen bestehen in Bezug auf den sachlichen Anwendungsbereich, den Auslegungsmaßstab und den Umfang des Haftungsausschlusses. Die Einheit der Rechtsordnung gebietet es, aus Gründen der Rechtssicherheit ein einheitliches Verständnis herbeizuführen.[1072] Soweit die Regelung des § 5 Nr. 2 GeschGehG enger ist, bedarf es einer harmonisierenden Auslegung, die den vorzugswürdigen Anforderungen des HinSchG entspricht. Ist § 6 Abs. 1 HinSchG in seinem Anwendungsbereich enger, verbleibt § 5 Nr. 2 GeschGehG ein

[1069] Siehe: Kapitel B) II. 4. b).
[1070] Siehe: Kapitel B) II. 4. c).
[1071] Siehe: Kapitel C) I. 1. c).
[1072] Siehe: Kapitel C) I. 1. c) ee).

eigenständiger Anwendungsbereich. Das HinSchG entfaltet insofern keine Sperrwirkung. Anzumerken ist, dass beide Vorschriften keiner eigenständigen Interessenabwägung unterliegen, die über die obligatorischen Verhältnismäßigkeitserwägungen anhand der Zweckbestimmung der Meldung hinausgeht.

10. In Bezug auf den Inhalt und die Form der Weitergabe eines Geschäftsgeheimnisses unterliegt der Whistleblower nach § 6 Abs. 1 HinSchG einer Prüfobliegenheit, deren Anforderungen denjenigen bzgl. der Validierung des Wahrheitsgehalts entsprechen, vgl. § 33 Abs. 1 Nr. 2 HinSchG.[1073] Der Whistleblower darf nicht mehr als das unbedingt notwendige Maß an geheimen Informationen weitergeben. Um dem Erfordernis der „*Notwendigkeit*“ in § 6 Abs. 1 HinSchG in Bezug auf den Umfang einer Meldung gerecht zu werden, hat der Whistleblower vorab einen Rechtsanwalt zu konsultieren, es sei denn eine anwaltliche Konsultation kann nicht mehr abgewartet werden, weil z. B. der begründete Verdacht einer erheblichen Gefahr für das Leben oder die Gesundheit anderer besteht.

11. Der Whistleblower hat im Rahmen des § 6 Abs. 1 HinSchG alternative Mittel zu prüfen, die in gleicher Weise geeignet sind, Rechtskonformität herzustellen. Hat der Whistleblower zum Zeitpunkt der beabsichtigten Meldung hinreichenden Grund zu der Annahme, der interne Meldeweg sei zur Beseitigung des Missstands geeignet, resultiert daraus ein Vorrang des internen Meldekanals in Form einer Obliegenheit.[1074] Dies gilt nicht, sofern Anhaltspunkte dafür vorliegen, dass dem Whistleblower infolge der internen Meldung Repressalien drohen.

[1073] Siehe: Kapitel C) I. 2. a).
[1074] Siehe: Kapitel C) I. 2. b) ee).

12. Setzt sich der Whistleblower über den Vorrang der internen Meldung im Rahmen des § 6 Abs. 1 HinSchG hinweg, greift das Haftungssystem des GeschGehG. Daneben drohen arbeitsrechtliche Konsequenzen, vgl. § 6 Abs. 2 HinSchG. Im Übrigen bleibt der Hinweisgeberschutz insbesondere hinsichtlich des Identitätsschutzes und des Verbots vor Repressalien bestehen. Richtigerweise muss daher von einer Prüfobliegenheit des Whistleblowers im Rahmen des § 6 Abs. 1 HinSchG gesprochen werden, aus der ein Vorrang des internen Meldewegs resultieren kann.[1075] Soweit es um die Weitergabe bzw. Offenlegung eines Geschäftsgeheimnisses eines Dritten geht, bestimmt sich die Frage des Haftungsausschlusses bzgl. des Haftungssystems des GeschGehG abermals nach § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG.

13. Die Geschäftsleitung ist gesellschaftsrechtlich verpflichtet, sicherzustellen, dass aus der Prüfobliegenheit im Rahmen des § 6 Abs. 1 HinSchG ein Vorrang des internen Meldewegs resultiert.[1076] Die Implementierung eines wirksamen Hinweisgeberschutzsystems ist daher Teil des unternehmerischen Geheimnisschutzkonzepts. § 7 Abs. 1 S. 1 HinSchG steht der Annahme der (Prüf-) Obliegenheit im Rahmen des § 6 Abs. 1 HinSchG nicht entgegen. Das Wahlrecht in § 7 Abs 1 S. 1 HinSchG bezieht sich ausschließlich auf Informationen, die keine Geschäftsgeheimnisse sind. § 6 Abs. 1 HinSchG ist - seiner Sonderstellung entsprechend - eigenständig auszulegen.

14. Um das Unternehmen vor Schäden in Folge des Bekanntwerdens sensibler Informationen, die noch keine Geschäftsgeheimnisse sind, hinreichend zu schützen, ist die Geschäftsleitung verpflichtet, darauf hinzuwirken, dass sich ein Whistleblower (über § 6 Abs. 1 HinSchG hinaus) für einen internen Meldeweg entscheidet. Die Unternehmensleitung hat Anreize zu schaffen, dass

[1075] Siehe: Kapitel C) I. 2. b) ee).
[1076] Siehe: Kapitel C) I. 3.

ein Whistleblower einen internen Meldekanal bevorzugt. Die interne Meldung bildet in diesen Fällen einen notwendigen Zwischenschritt, um sensible Informationen in den Schutzbereich des GeschGehG zu überführen. Neben der Schaffung anonymer Meldekanäle und Maßnahmen zur Erhöhung des Identitätsschutzes kommen insbesondere berufliche und finanzielle Anreize in Betracht. Darüber hinaus sind interne Meldeverpflichtungen zu erwägen.

15. Die Vereinbarung einer internen Meldepflicht ist möglich, sofern dem Arbeitnehmer der Zugang zum externen Meldeweg erhalten bleibt.[1077] Die Klausel muss hinreichend bestimmt sein und darf den Whistleblower nicht unangemessen benachteiligen, § 307 Abs. 1 BGB. Voraussetzung ist die Implementierung eines wirksamen Hinweisgeberschutzsystems. Nötig sind außerdem Konkretisierungen hinsichtlich des objektiven Verdachtsgrads und des Schweregrads eines Missstands, die es vermögen, den Eingriff in das Recht auf negative Meinungsfreiheit zu rechtfertigen. Auch mögliche Gewissenskonflikte sind mitzudenken. Je schwerer und gewichtiger der Missstand, desto eher überwiegen die Interessen des Unternehmens an der Beseitigung des Missstands. Dagegen können Whistleblower in Bezug auf Informationen, die (noch) keine Geschäftsgeheimnisse sind, nicht zur vorrangigen Nutzung eines internen Meldewegs verpflichtet werden.[1078] Vereinbarungen, die den Zugang zu den externen Meldestellen einschränken, sind unwirksam, §§ 7, 39 HinSchG i. V. m. § 134 BGB. Ein Vorrang einer internen Meldung ergibt sich auch nicht aus § 17 Abs. 2 S. 1 ArbSchG.

16. Da Unternehmen nicht hinreichend davor gewahrt sind, dass Informationen über Missstände extern gemeldet werden, sind weitere Anreize nötig, damit ein Whistleblower freiwillig von einer

[1077] Siehe: Kapitel C) I. 3. b).
[1078] Siehe: Kapitel C) I. 3. a).

externen Meldung absieht. Dazu zählt die Gewährleistung eines umfassenden Identitätsschutzes. Zwar normieren die §§ 8, 9 HinSchG bereits einen weitreichenden Identitätsschutz: Die Ausnahme des § 9 Abs. 1 HinSchG greift nur im Ausnahmefall und erfasst im Wege einer einschränkenden Auslegung Falschinformationen, die geeignet sind, Schadensersatzansprüche der von der Meldung betroffenen Person auszulösen oder von strafrechtlicher Relevanz für diese sind.[1079] Der Identitätsschutz kollidiert jedoch mit den datenschutzrechtlichen Betroffenenrechten, über die sich das HinSchG nicht hinwegsetzen kann.[1080]

17. Die Informationspflicht des Arbeitgebers bzgl. der Identität des Whistleblowers entfällt nach Art. 14 Abs. 5 lit. b) DS-GVO, soweit die Kenntnis über dessen Identität den Zweck der internen Untersuchung gefährdet, weil Beweismittel drohen verlustig zu gehen oder die begründete Annahme besteht, die Erhebung weiterer Beweismittel werde gefährdet. Im Übrigen besteht die Informationspflicht uneingeschränkt fort. §§ 8, 9 HinSchG sind keine Rechtsvorschriften im Sinne des Art. 14 Abs. 5 lit. c) DS-GVO und können nicht auf die Öffnungsklauseln in Art. 23 Abs. 1 DS-GVO oder Art. 88 Abs. 1 DS-GVO gestützt werden.[1081] Ein Ausschluss der Informationspflicht folgt auch nicht aus § 29 Abs. 1 S. 1 BDSG, da diese Vorschrift ebenfalls auf keine Öffnungsklausel zurückgeführt werden kann und infolge des Anwendungsvorrangs der DS-GVO unangewendet bleiben muss.

18. Im Rahmen des datenschutzrechtlichen Auskunftsrechts ist die Identität des Whistleblowers nicht zu beauskunften, soweit der Identitätsschutz das informationelle Selbstbestimmungsrecht der von der Meldung betroffenen Person überwiegt, vgl. Art. 15 Abs. 4 DS-GVO.[1082] Die Interessenabwägung ist eigenständig durchzu-

[1079] Siehe: Kapitel C) I. 3. c) aa).
[1080] Siehe: Kapitel C) I. 3. c) bb).
[1081] Siehe: Kapitel C) I. 3. c) bb) (1) (a) bis (d).
[1082] Siehe: Kapitel C) I. 3. c) bb) (2).

führen. Das Bestehen des Identitätsschutzes nach §§ 8, 9 HinSchG führt nicht automatisch zu einer Beschränkung der Datenauskunft. Anzumerken ist, dass sich die Beschränkungsmöglichkeit des Art. 15 Abs. 4 DS-GVO auf die Datenauskunft mitsamt der Metainformationen in Art. 15 Abs. 1 Hs. 2 Var. 2 bezieht. Der Verweis ist losgelöst vom Bezugspunkt der Erfüllungsmodalität in Art. 15 Abs. 3 DS-GVO zu verstehen und stellt die charta-rechtlich gebotene Berücksichtigung kollidierender Grundrechtspositionen sicher. Darüber hinaus erfährt die Datenauskunft keine Beschränkung durch § 29 Abs. 1 S. 2 BDSG. Die Vorschrift kann auf keine Öffnungsklausel der DS-GVO zurückgeführt werden und muss infolge des Anwendungsvorrangs der DS-GVO unangewendet bleiben.

19. Die Einschaltung einer externen, anwaltlichen Ombudsperson trägt zur Erhöhung des Identitätsschutzes bei.[1083] Aufgrund des anwaltlichen Berufsgeheimnisses wird die Ausnahmeregelung des Art. 14 Abs. 5 lit. d) DS-GVO aktiviert, bis die Daten an den Beschäftigungsgeber für etwaige Folgemaßnahmen weitergeleitet werden. Maßgeblich ist, dass die externe Ombudsstelle selbst datenschutzrechtlich verantwortliche Stelle ist. Daneben kommt der Abschluss einer Betriebsvereinbarung zur Erhöhung des Identitätsschutzes in Betracht, wobei die Grundsätze der Datenverarbeitung (Art. 5, Art. 6 DS-GVO) im Sinne eines Mindestschutzes nicht unterlaufen werden dürfen und eigene Regelungen zur Gewährleistung der Datentransparenz getroffen werden müssen, vgl. Art. 88 Abs. 2 DS-GVO. Dagegen scheidet eine Verzichtserklärung in Bezug auf die Betroffenenrechte im Beschäftigungskontext aus.[1084]

[1083] Siehe: Kapitel C) I. 3. c) cc) (2).
[1084] Siehe: Kapitel C) I. 3. c) cc) (1).

20. Will der datenschutzrechtlich Verantwortliche einer Datenauskunft eigene Geheimhaltungsinteressen entgegenhalten, entscheidet eine umfassende Interessenabwägung zwischen dem informationellen Selbstbestimmungsrecht der von der Datenverarbeitung betroffenen Person und den berechtigten Geheimhaltungsinteressen des datenschutzrechtlich Verantwortlichen, Art. 15 Abs. 4 DS-GVO. Aus dem Vorliegen eines Geschäfts-geheimnisses folgt noch keine Beschränkung der Datenauskunft. Aufgrund der hohen Risiken, die mit der Offenlegung eines Geschäftsgeheimnisses einhergehen, ist allerdings regelmäßig von einem Überwiegen der Geheimhaltungsinteressen auszugehen.[1085]

21. Das personalaktenrechtliche Einsichtsrecht des § 83 Abs. 1 S. 1 BetrVG tritt neben das Recht auf Datenauskunft, Art. 15 DS-GVO.[1086] Für die Annahme einer Verdrängungswirkung fehlt es an der dafür notwendigen Öffnungsklausel in der DS-GVO. Die Kollisionsvorschrift des § 1 Abs. 2 BDSG findet keine Anwendung. Aus Gründen der Einheit der Rechtsordnung sind die Maßstäbe des Art. 15 Abs. 4 DS-GVO im Rahmen des § 83 Abs. 1 S. 1 BetrVG anzusetzen.[1087] In Erfüllung der Akteneinsicht ist der Arbeitgeber daher berechtigt, geheime Informationen zu schwärzen, soweit seine berechtigten Geheimhaltungsinteressen dies erfordern.

22. Kommt es im Rahmen der Betriebsratsarbeit zur Erlangung eines Geschäftsgeheimnisses durch den Arbeitgeber, wird das Geheimhaltungsinteresse des Arbeitgebers insbesondere über die Verschwiegenheitspflicht nach § 79 Abs. 1 S. 1 BetrVG sichergestellt.[1088] Im Falle einer zulässigen Erlangung eines Geschäftsgeheimnisses durch den Arbeitnehmer (§ 5 Nr. 3 GeschGehG) sind die Betriebsratsmitglieder in Ermangelung einer konstitutiven

[1085] Siehe: Kapitel C) II. 2.
[1086] Siehe: Kapitel C) II. 3. b).
[1087] Siehe: Kapitel C) II. 3. c).
[1088] Siehe: Kapitel C) III. 1.

Vertraulichkeitserklärung des Arbeitgebers aus dem Gebot der vertrauensvollen Zusammenarbeit zur Verschwiegenheit verpflichtet, § 2 Abs. 1 BetrVG.[1089] Anzumerken ist, dass im Rahmen der Erforderlichkeit des § 5 Nr. 3 GeschGehG grundsätzlich auch subjektive Erwägungen des Arbeitnehmers berücksichtigungsfähig sind.

23. Entscheidet sich ein Betriebsratsmitglied zur Meldung eines Geschäftsgeheimnisses zu Zwecken des Whistleblowings, gelten die allgemeinen Vorgaben des § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG.[1090] Ist dem Betriebsratsmitglied die geschützte Information bekannt, weil sie ihm wegen seiner Betriebsratszugehörigkeit durch den Arbeitgeber unter Hinweis auf die Vertraulichkeit bekannt geworden ist, erweitert sich das Spannungsfeld zwischen eigener Meinungsfreiheit und unternehmerischen Geheimhaltungsinteressen um das Gebot der vertrauensvollen Zusammenarbeit (§§ 2 Abs. 1, 79 Abs. 1 S. 1 BetrVG). Hierfür bedarf es einer betriebsverfassungsrechtlichen Lösung.

24. Das Gebot der vertrauensvollen Zusammenarbeit verpflichtet das Betriebsratsmitglied, gemeinsam mit dem Arbeitgeber darauf hinzuwirken, dass aus der (Prüf-) Obliegenheit im Rahmen des § 6 Abs. 1 HinSchG ein Vorrang des internen Meldekanals resultiert.[1091] Maßstab bildet der Grundsatz von Treu und Glauben. Danach ist das Betriebsratsmitglied unabhängig von einer beabsichtigten Meldung verpflichtet, dem Arbeitgeber ihm bekannte bzw. bekannt gewordene Anhaltspunkte, die gegen die Wirksamkeit des Hinweisgeberschutzsystems sprechen, mitzuteilen. Solange der Betriebsrat den Arbeitgeber nicht auf ebensolche Anhaltspunkte aufmerksam macht, darf dieser konsequenterweise darauf vertrauen, dass der Vorrang des internen Meldekanals im

[1089] Siehe: Kapitel C) III. 2.
[1090] Siehe: Kapitel C) III. 3.
[1091] Siehe: Kapitel C) III. 3.

Rahmen des § 6 Abs. 1 HinSchG bzw. § 5 Nr. 2 GeschGehG jedenfalls für die Betriebsratsmitglieder besteht.

25. Die Erforschung neuen, exklusiven Wissens erfolgt im Beschäftigungskontext zu Zwecken der Arbeitsprozessoptimierung. Die datenschutzrechtliche Zulässigkeit ist anhand einer Abwägung zwischen dem Interesse des Arbeitgebers an effizient gestalteten Arbeitsabläufen zur Gewährleistung der eigenen Wettbewerbsfähigkeit und dem Recht des Arbeitnehmers auf informationelle Selbstbestimmung zu beurteilen, wobei eine Prozessoptimierung grundsätzlich auch im Eigeninteresse des Arbeitnehmers liegt. Zulässig ist eine Leistungskontrolle zu Zwecken der Prozessoptimierung, wenn keine Bewertung über das Verhalten des Arbeitnehmers vorgenommen wird.[1092] Bewirkt eine Überwachungsmaßnahme allerdings eine Drucksituation, die bei objektiver Betrachtung zu einem psychischen Anpassungsdruck führt, sind die Anforderungen höhergesteckt. Beschäftigtendaten dürfen auch zu Zwecken automatisierter Weisungen verarbeitet werden.[1093] Art. 22 Abs. 1 DS-GVO steht der datenschutzrechtlichen Zulässigkeit einer automatisierten Weisung nicht entgegen. Eine Algorithmus basierte Entscheidung kann zwar Weisungsqualität haben, entfaltet jedoch keine rechtlich nachteilige Wirkung gegenüber dem Arbeitnehmer.

Abschließend ist noch einmal zu betonen: Die Bewahrung exklusiven Wissens ist Obligatorium und strategische Notwendigkeit zugleich, um als Unternehmen wirtschaftlich zu bestehen. Wie weit der Geschäftsgeheimnisschutz im Einzelnen reicht und unter welchen Voraussetzungen er zum Schutz gegenläufiger Interessen im Beschäftigungskontext weichen muss, entscheidet ein Balanceakt zwischen Wettbewerb, Innovation und Rechtskonformität.

[1092] Siehe: Kapitel D).
[1093] Siehe: Kapitel D).

Literaturverzeichnis

Aldoney Ramírez, Rodrigo, Der strafrechtliche Schutz von Geschäfts- und Betriebsgeheimnissen, Studien zum Wirtschaftsstrafrecht, zugleich Dissertation, 1. Auflage, Freiburg 2007 (zit.: *Aldony Ramírez*, Schutz von Geschäfts- und Betriebsgeheimnissen).

Alexander, Christian, „Gegenstand, Inhalt und Umfang des Schutzes von Geschäftsgeheimnissen nach der Richtlinie (EU) 2016/943", WRP 2017, S. 1034-1045.

Alexander, Christian, „Geheimnisschutz nach dem GeschGehG und investigativer Journalismus: Risikobereiche und Handlungsfreiräume", AfP 2019, S. 1-11.

Alexander, Christian, „Grundstrukturen des Schutzes von Geschäftsgeheimnissen durch das neue GeschGehG", WRP 2019, S. 673-679.

Alexander, Christian, „Zwingendes oder dispositives Recht: Welchen privatautonomen Gestaltungsspielraum belässt das GeschGehG?", WRP 2020, S. 1385-1391.

Altenbach, Thomas/*Dierkes, Kevin*, „EU-Whistleblowing-Richtlinie und DSGVO", CCZ 2020, S. 126-132.

Apel, Simon/*Boom, Annika*, „Zur (Un-) Abdingbarkeit des § 5 GeschGehG - Fallstricke für NDAs?", GRUR-Prax 2020, S. 225-227.

Apel, Simon/*Nickl, Afra*, „Drei Jahre GeschGehG - Eine Rechtsprechungsübersicht", K&R 2022, S. 385-394.

Apel, Simon/*Stolz, Alexander,* „Vertragliche Geheimhaltungsmaßnahmen nach „PU-Schaum" - Was bleibt hängen?", GRUR-Prax 2021, S. 1-3.

Apel, Simon/*Walling, Sebastian*, „Das neue Geschäftsgeheimnisgesetz: Überblick und erste Praxishinweise", DB 2019, S. 891-898.

Arens, Tobias, „Die Geltendmachung des datenschutzrechtlichen Auskunftsanspruchs durch Vertreter", NJW 2021, S. 3417-3421.

Auernhammer, Herbert, DS-GVO, BDSG, Kommentar, hrsg. v. *Eßer, Martin/Kramer, Philipp/ Lewinski, Kai von*, 7. Auflage, München 2020 (zit.: *Bearbeiter*, in: Auernhammer).

Azar, Rahimi, „Strafrechtliche Implikationen des Whistleblowings unter besonderer Berücksichtigung des § 17 UWG", JuS 2017, S. 930-935.

Baade, Isabelle/*Hößl, Theresa,* „Arbeits- und compliancerechtlicher Handlungsbedarf unter dem neuen Hinweisgeberschutzgesetz (Teil II)", DStR 2023, S. 1265-1270.

Bacon, Francis, Novum Organum Scientiarum, England 1620, übersetzt und hrsg. v. *Brück, Theobald Anton*, Neues Organ der Wissenschaften, Leipzig 1830.

Baranowski, Carolin/Pant, Benjamin, „Die janusköpfigen Verschwiegenheitsrechte und -pflichten des Rechtsanwalts in der Funktion einer Ombudsperson", CCZ 2018, S. 250-256.

Bayreuther, Frank, „Videoüberwachung am Arbeitsplatz", NZA 2005, S. 1038-1043.

Bayreuther, Frank, „Whistleblowing und das neue Hinweisgeberschutzgesetz", NZA-Beilage 2022, S. 20-29.

Beck´scher Online-Kommentar Arbeitsrecht, hrsg. v. *Rolfs, Christian/Giesen, Richard/Meßling, Miriam/Udsching, Peter,* 71. Edition, Stand 01.03.2024, München 2024 (zit.: *Bearbeiter*, in: BeckOK-ArbR).

Beck´scher Online-Kommentar BGB, hrsg. v. *Hau, Wolfgang/Poseck, Roman*, 70. Edition, Stand 01.05.2024, München 2024 (zit.: *Bearbeiter*, in: BeckOK-BGB).

Beck´scher Online-Kommentar Datenschutzrecht, hrsg. v. *Wolff, Amadeus/Brink, Stefan/Ungern-Sternberg, Antje von*, 47. Edition, Stand 01.02.2024, München 2022 (zit.: *Bearbeiter*, in: BeckOK-DatenschutzR).

Beck´scher Online-Kommentar GeschGehG, hrsg. v. *Fuhlrott, Michael/Hiéramente, Mayeul*, 19. Edition, Stand 15.03.2024, München 2024 (zit.: *Bearbeiter*, in: BeckOK-GeschGehG).

Beck´scher Online-Kommentar Grundgesetz, hrsg. v. *Epping, Volker/Hillgruber, Christian*, 57. Edition, Stand 15.01.2024, München 2024 (zit.: *Bearbeiter*, in: BeckOK-GG).

Beck´scher Online-Kommentar HinSchG, hrsg. v. *Colneric, Ninon/ Gerdemann, Simon*, 3. Edition, Stand 15.04.2024, München 2024 (zit.: *Bearbeiter*, in: BeckOK-HinSchG).

Beck´scher Online-Kommentar IT-Recht, hrsg. v. *Borges, Georg/ Hilber, Marc*, 14. Edition, Stand 01.04.2024, München 2024 (zit.: *Bearbeiter*, in: BeckOK-IT-Recht).

Beck´scher Online-Kommentar StGB, hrsg. v. *Kudlich, Hans/Heintschel-Heinegg, Bernd*, 60. Edition, Stand: 01.02.2024, München 2024 (zit.: *Bearbeiter*, in: BeckOK StGB).

Beck´scher Online-Kommentar, Großkommentar für das Zivilrecht, hrsg. v. *Gsell, Beate/Krüger, Wolfgang/Lorenz, Stephan/Reymann, Christoph*, Stand 01.05.2024, München 2024 (zit.: *Bearbeiter*, in: BeckOK-GK).

Becker, Ulrich/*Kussnik, Kathrin*, „Angemessene Geheimhaltungsmaßnahmen nach dem Gesetz zum Schutz von Geschäftsgeheimnissen: Auswirkungen auf die Unternehmens- und Vertragspraxis“, RAW 2018, S. 119-128.

Benkert, Daniel, „Beschäftigtendatenschutz in der DS-GVO-Welt“, NJW-Spezial 2018, S. 562.

Berger, Christian/*Tunze, Carlo*, „Geistiges Eigentum im Insolvenzverfahren“, ZIP 2020, S. 52-56.

Beukelmann, Stephan, „Schutz von Hinweisgebern“, NJW-Spezial 2019, S. 312.

Beyerbach, Hannes, Die geheime Unternehmensinformation, Studien und Beiträge zum Öffentlichen Recht, zugleich Dissertation, 1. Auflage, Tübingen 2012 (zit.: *Beyerbach*, Unternehmensinformation).

Böhm, Wolf-Tassilo/Brams, Isabelle, „Aktuelle Entscheidungen zum Beschäftigtendatenschutz", NZA-RR 2023, S. 625-632.

Böning, Marta/Heidfeld, Birgit, „Gesetzentwurf zum Schutz von Geschäftsgeheimnissen (GeschGehG) - Maulkorb zu Lasten der Beschäftigten und ihrer Interessenvertretungen", AuR 2018, S. 555-557.

Brammsen, Joerg, „Reformbedürftig! - Der Regierungsentwurf des neuen Geschäftsgeheimnisschutzgesetzes", BB 2018, S. 2446-2450.

Brammsen, Joerg, Lauterkeitsstrafrecht, Sonderband zum Münchener Kommentar Lauterkeitsrecht, 1. Auflage, München 2020 (zit.: *Brammsen*, Lauterkeitsstrafrecht).

Brammsen, Joerg/Apel, Simon, Geschäftsgeheimnisgesetz, 1. Auflage, Frankfurt a. M. 2022 (zit.: *Brammsen/Apel*, GeschGehG).

Brink, Stefan/Joos, Daniel, „Reichweite und Grenzen des Auskunftsanspruchs und des Rechts auf Kopie", ZD 2019, S. 483-488.

Brobeil, Anne, Die Auswirkungen der Richtlinie (EU) 2019/1937 auf Arbeitnehmer-Hinweisgeber, Studien zum deutschen und europäischen Arbeitsrecht, Band 101, zugleich Dissertation, Baden-Baden 2022 (zit.: *Brobeil*, Die Auswirkungen der Richtlinie (EU) 2019/1937 auf Arbeitnehmer-Hinweisgeber).

Brockhaus, Robert, „Das Geschäftsgeheimnisgesetz - Zur Frage der Strafbarkeit von Hinweisgebern unter Berücksichtigung der Whistleblowing-Richtlinie", ZIS 2020, S. 102-119.

Brockhaus, Robert, Geheimnisschutz und Transparenz, Studien und Beiträge zum Strafrecht, zugleich Dissertation, 1. Auflage, Tübingen 2022 (zit.: *Brockhaus*, Geheimnisschutz und Transparenz).

Brors, Christiane, „Mitbestimmung des Betriebsrats bei der Dokumentation der Arbeitszeit vor und nach der CCOO-Entscheidung des EuGH“, NZA 2019, S. 1176-1180.

Brost, Lucas/*Wolsing, Daniel*, „Presserechtlicher Schutz vor der Veröffentlichung von Geschäftsgeheimnissen“, ZUM 2019, S. 898-904.

Bruns, Patrick, „Das neue Hinweisgeberschutzgesetz“, NJW 2023, S. 1609-1617.

Buchert, Christoph/Buchert, Rainer, „Das Gesetz zum Schutz von Geschäftsgeheimnissen - auch ein Schutz für Whistleblower?“, ZWH 2019, S. 309-316.

Buchert, Christoph/*Buchert, Rainer,* „DSGVO-Auskunftsansprüche contra Hinweisgeberschutz, zugleich Besprechung von LAG-BW, Urteil v. 20.12.2018, 17 Sa 11/18“, ZWH 2019, S. 212-216.

Burger, Simon, „Das Recht auf Datenauskunft und Datenkopie im Arbeitsverhältnis“, öAT 2021, S. 221-224.

Burghardt-Richter, Ingrid/Bode, Johannes, „Geschäftsgeheimnisschutzgesetz: Überblick und Leitfaden für Unternehmen zur Wahrung ihrer Geschäftsgeheimnisse“, BB 2019, S. 2697-2702.

Byers, Philipp, „Die Zulässigkeit heimlicher Mitarbeiterkontrollen nach dem neuen Datenschutzrecht,“ NZA 2017, S. 1086-1091.

Byers, Philipp/*Fetsch, Kathrin*, „Vorsicht, Terrorist im Betrieb - Was nun?“, NZA 2015, S. 1364-1369.

Calliess, Christian/Ruffert, Matthias, EUV, AEUV mit Europäischer Grundrechtecharta, 6. Auflage, München 2022 (zit.: *Calliess/Ruffert,* GR-CH).

Cha, Wonil, Der verfassungsrechtliche Schutz der Betriebs- und Geschäftsgeheimnisse, Europäische Hochschulschriften, zugleich Dissertation, 1. Auflage, Lausanne 2016 (zit.: *Cha*, Betriebs- und Geschäftsgeheimnisse).

Claßen, Jörn/*Hassel, Dominik*, „Shitstorms und Skandalberichterstattung - Unternehmen am Pranger“, IPRB 2020, S. 65-69.

Colneric, Ninon/*Gerdemann, Simon*, Die Umsetzung der Whistleblowing-Richtlinie in deutsches Recht, HSI-Schriftenreihe, Band 34, Frankfurt a. M. 2020 (zit.: *Colneric*/*Gerdemann*, Umsetzung der Whistleblowing-RL).

Comenius, *Johann Amos,* Didactica Magna oder Große Didaktik: Die vollständige Kunst, alle Menschen alles zu lehren, hrsg. v. *Andreas Flitner*, 10. Auflage, Stuttgart 2008, erstmals veröffentlicht 1657.

Comenius, Johann Amos, Didactica Magna, im Jahr 1638 in lateinischer Sprache verfasst und 1657 erstmals veröffentlicht.

Dann, Matthias/Markgraf, Jochen, „Das neue Gesetz zum Schutz von Geschäftsgeheimnissen“, NJW 2019, S. 1774-1779.

Däubler, Wolfgang/Hjort, Jens Peter/Schubert, Michael/Wolmerath, Martin (Hrsg.), Nomos-Kommentar Arbeitsrecht, 5. Auflage, Baden-Baden 2022 (zit.: *Bearbeiter*, in: Däubler/Hjort/Schubert).

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter (Hrsg.), BetrVG Kommentar für die Praxis, 19. Auflage, Frankfurt a. M. 2024 (zit.: *Bearbeiter*, in: DKW).

Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/Sommer, Imke (Hrsg.), EU-DSGVO und BDSG, Kompaktkommentar, 3. Auflage, Frankfurt a. M. 2024 (zit.: *Bearbeiter*, in: DWWS).

Dausend, Tjorven, „Der Auskunftsanspruch in der Unternehmenspraxis“, ZD 2019, S. 103-107.

Dobler, *Carsten*, Geschäftsgeheimnisschutz und investigativer Journalismus, Schriften zum Medien- und Informationsrecht, zugleich Dissertation, 1. Auflage, Baden-Baden 2023 (zit.: *Dobler*, Geschäftsgeheimnisschutz und investigativer Journalismus).

Dreier, Horst, Grundgesetz Kommentar, Band I, hrsg. v. *Brosius-Gersdorf, Frauke*, 4. Auflage, Tübingen 2023 (zit.: *Dreier*, GG).

Druschel, Johannes/Jauch, Andreas, „Der Schutz von Know-how im deutschen Zivilprozess: Der Status quo und die zu erwartenden Änderungen“, BB 2018, S. 1218-1223.

Dumont, Nicolas M., „Happy End für ein Stiefkind? - Regierungsentwurf zur Umsetzung der Know-how-Richtlinie“, BB 2018, S. 2441-2446.

Dürig, Günter/Herzog, Roman/Scholz, Rupert/Herdegen, Matthias/Klein, Hans H. (Hrsg.), Kommentar zum Grundgesetz, Loseblattsammlung, 103. Auflage, München 2024 (zit.: *Bearbeiter*, in: Dürig/Herzog/Scholz, GG).

Düwell, Franz-Josef (Hrsg.), Betriebsverfassungsgesetz, Nomos-Kommentar, Handkommentar, 6. Auflage, Baden-Baden 2022 (zit.: *Bearbeiter*, in: Düwell).

Düwell, Franz-Josef/Brink, Stefan, „Die EU-Datenschutz-Grundverordnung und der Beschäftigtendatenschutz“, NZA 2016, S. 665-668.

Dzida, Boris, „Bundesrat stoppt das Hinweisgeberschutzgesetz“, NZA-Editorial, Heft 5/2023.

Dzida, Boris/Granetzky, Thomas, „Die neue EU-Whistleblowing-Richtlinie und ihre Auswirkungen auf Unternehmen“, NZA 2020, S. 1201-1207.

Dzida, Boris/Grau, Timon, „Beschäftigtendatenschutz nach der Datenschutzgrundverordnung und dem neuen BDSG“, DB 2018, S. 189-193.

Dzida, Boris/Seibt, Christoph, „Neues Hinweisgeberschutzgesetz: Analyse und Antworten auf Praxisfragen“, NZA 2023, S. 657-666.

Eckhoff, Frank/Reufels, Martin (Hrsg.), Münchener Anwalts Handbuch, Arbeitsrecht, 6. Auflage, München 2024 (zit.: *Bearbeiter*, in: Hdb-ArbR).

Ehmann, Eugen/Selmayr, Martin (Hrsg.), Datenschutz-Grundverordnung, Beck´sche Kurz-Kommentare, 3. Auflage, München 2024 (zit.: *Bearbeiter*, in: Ehmann/Selmayr).

Engelhardt, Jens, „Anspruch auf Benennung des Hinweisgebers im Rahmen der Erfüllung des Auskunftsanspruchs nach Art. 15 DS-GVO“, RDi 2022, S. 298-304.

Engländer, Armin/Zimmermann, Till, „Whistleblowing als strafbarer Verrat von Geschäfts- und Betriebsgeheimnissen? Zur Bedeutung des juristisch-ökonomischen Vermögensbegriffs für den Schutz illegaler Geheimnisse bei § 17 UWG“, NZWiST 2012, S. 328-333.

Erlebach, Kimberly/Veljovic, Miguel, „Das Stigma der Denunziation bei anonymen Hinweismeldungen am Beispiel des HinSchG-E - ein Trugschluss!“, KriPoZ 2021, S. 165-171.

Erlebach, Kimberly/Veljovic, Miguel, „Strafrechtliche Einordnung des § 5 GeschGehG“, wistra 2020, S. 190-195.

Fehr, Stefanie, „Datenschutzrechtliche Anforderungen an die Implementierung eines Hinweisgebersystems im Lichte des HinSchG und der DSGVO“, DB 2023, S. 180-185.

Fehr, Stefanie, „Whistleblowing und Datenschutz - ein unlösbares Spannungsfeld? Praktischer Diskurs der EU-Whistleblower-RL und der DS-GVO im Kontext des Hinweisgebermanagements“, ZD 2022, S. 256-260.

Festschrift für *Helmut Köhler*, zum 70. Geburtstag, hrsg. v. *Alexander, Christian/Bornkamm, Joahim/Buchner, Benedikt/Fritzsche, Jörg/Lettl, Tobias,* München 2014 (zit.: *Bearbeiter*, in: FS-Köhler).

Fezer, Karl-Heinz/Büscher, Wolfgang/Obergfell, Eva Inés (Hrsg.), Lauterkeitsrecht, Kommentar zum Gesetz gegen den unlauteren Wettbewerb (UWG), Band 2, 3. Auflage, München 2016 (zit.: *Bearbeiter*, in: Fezer/Büscher/Obergfell UWG).

Fleischer, Holger (Hrsg.), Handbuch des Vorstandsrechts, 1. Auflage, München 2006 (zit.: Bearbeiter, in: VorstandsR-HdB).

Fleischer, Holger/Goette, Wulf (Hrsg.), Münchener Kommentar zum GmbHG, Band 2, 4. Auflage, München 2023 (zit.: *Bearbeiter*, in: GmbHG-Kommentar).

Forgó, Nikolaus/Helfrich, Marcus/Schneider, Jochen (Hrsg.), Betrieblicher Datenschutz, Rechtshandbuch, 3. Auflage, München 2019 (zit.: *Bearbeiter*, in: Forgó/Helfrich/Schneider).

Forst, Gerrit, „Strafanzeige gegen den Arbeitgeber - Grund zur Kündigung des Arbeitsvertrags?“, NJW 2011, S. 3477-3482.

Franck, Lorenz, „Altverhältnisse unter DS-GVO und neuem BDSG - Anwendung des neuen Datenschutzrechts auf bereits laufende Datenverarbeitungen?“, ZD 2017, S. 509-513.

Franzen, Martin, „Das Verhältnis des Auskunftsanspruchs nach DS-GVO zu personalaktenrechtlichen Einsichtsrechten nach dem BetrVG“, NZA 2020, S. 1593-1597.

Franzen, Martin, „Datenschutzrechtlicher Auskunftsanspruch und Hinweisgeberschutz“, ZfA 2023, S. 100-111.

Franzen, Martin, „Persönlichkeitsrecht und Datenschutz im Arbeitsverhältnis“, ZfA 2019, S. 18-36.

Franzen, Martin/Gallner, Inken/Oetker, Hartmut (Hrsg.), Kommentar zum europäischen Arbeitsrecht, Beck´sche Kurz-Kommentare, 5. Auflage, München 2024 (zit.: *Bearbeiter*, in: EuArbRK).

Frenz, Walter, Handbuch Europarecht, Band 4/I, 2. Auflage, Heidelberg 2024 (zit.: *Frenz*, Handbuch Europarecht).

Freyler, Carmen, „Robot-Recruiting, Künstliche Intelligenz und das Antidiskriminierungsrecht“, NZA 2020, S. 284-290.

Fuhlrott, Michael, „LAG Baden-Württemberg: Recht auf Erteilung einer Kopie nach Art. 15 DS-GVO“, NZA-RR 2019, S. 242-252.

Fuhlrott, Michael/Fischer, Katharina, „Verschwiegenheitsklauseln im Lichte des Geschäftsgeheimnisschutzes“, NZA 2022, S. 809-815.

Fuhlrott, Michael/*Henckel, Christoph,* „Hinweisgeberschutzgesetz: Handlungsbedarf für Unternehmen und Personalabteilungen“, ArbRAktuell 2022, S. 441-445.

Fuhlrott, Michael/Hiéramente, Mayeul, „Arbeitsrechtlicher Handlungsbedarf durch das Geschäftsgeheimnisgesetz“, DB 2019, S. 967-972.

Gajeck, Niclas Alexander, Das Wirtschaftsgeheimnis in der Verfassung, Studien zur Informationsfreiheit, zugleich Dissertation, 1. Auflage, Baden-Baden 2018 (zit.: *Gajeck*, Wirtschaftsgeheimnis).

Garden, Florian/*Hiéramente, Mayeul*, „Die neue Whistleblowing-Richtlinie der EU - Handlungsbedarf für Unternehmen und Gesetzgeber“, BB 2019, S. 963-969.

Gärtner, Anette/*Oppermann, Antonie*, „Viel Licht und etwas Schatten - wann besteht ein berechtigtes Geheimhaltungsinteresse?“, BB 2019, Heft 35, Umschlagteil I (Die Erste Seite).

Gerdemann, Simon, „Referentenentwurf für ein deutsches Hinweisgeberschutzgesetz“, ZRP 2021, S. 37-40.

Gerdemann, Simon/*Spindler, Gerald*, „Die Europäische Whistleblower-Richtlinie und ihre Folgen für das deutsche Gesellschaftsrecht“, ZIP 2020, S. 1896-1904.

Goette, Wulf/Habersack, Mathias/Kalss, Susanne (Hrsg.), Münchener Kommentar zum Aktiengesetz, Band 1, 6. Auflage, München 2024 (zit.: *Bearbeiter*, in: MüKo-AktG).

Gola, Peter (Hrsg.), DS-GVO, Kommentar, 2. Auflage, München 2018 (zit.: *Bearbeiter*, in: Gola).

Gola, Peter, „Der „neue” Beschäftigtendatenschutz nach § 26 BDSG n. F.“, BB 2017, S. 1462-1472.

Gola, Peter, Handbuch Beschäftigtendatenschutz, 8. Auflage, Frechen 2019 (zit.: *Gola*, Handbuch Beschäftigtendatenschutz).

Gola, Peter/Heckmann, Dirk (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO/BDSG, Kommentar, 3. Auflage, München 2022 (zit.: *Bearbeiter*, in: Gola/Heckmann).

Goldhammer, Michael, „Geschäftsgeheimnis-Richtlinie und Informationsfreiheit - Zur Neudefinition des Geschäftsgeheimnisses als Chance für das öffentliche Recht", NVwZ 2017, S. 1809-1814.

Gramlich, Ludwig/Lütke, Hans-Josef, „Die Strafvorschrift des § 23 GeschGehG - kein gesetzgeberisches Meisterstück", wistra 2022, S. 97-105.

Granetzny, Thomas/*Krause, Melena*, „Was kostet ein gutes Gewissen? - Förderung von Whistleblowing durch Prämien nach US-Vorbild?", CCZ 2020, S. 29-36.

Grau, Timon/*Seidensticker, Thomas*, „Zum DSGVO-Auskunftsanspruch des Arbeitnehmers gegen Arbeitgeber bei Geheimhaltungsinteressen Dritter", EWiR 2019, S. 443-444.

Grüneberg, Christian (Hrsg.), Bürgerliches Gesetzbuch, Beck´sche Kurz-Kommentare, 83. Auflage, München 2024
(zit.: *Bearbeiter*, in: Grüneberg).

Grützmacher, Malte/Heckmann, Jörn, „Autonome Systeme und KI - vom vollautomatisierten zum autonomen Vertragsschluss?", CR 2019, S. 553-554.

Haak, Marius/*Spittka, Jan*, „Datenschutzkonforme Ausgestaltung von Hinweisgebersystemen in Konzernkonstellationen", CB 2023, S. 356-360.

Harte-Bavendamm, Henning/Ohly, Ansgar/Kalbfus, Björn, GeschGehG, Gesetz zum Schutz von Geschäftsgeheimnissen, 2. Auflage, München 2024 (zit.: *Bearbeiter*, in: Harte-Bavendamm/Ohly/Kalbfus, GeschGehG).

Härting, Niko, „Was ist eigentlich eine "Kopie"?“, CR 2019, S. 219-221.

Hauck, Ronny, „Geheimnisschutz im Zivilprozess - was bringt die neue EU-Richtlinie für das deutsche Recht?“, NJW 2016, S. 2218-2223.

Hauck, Ronny, „Grenzen des Geheimnisschutzes“, WRP 2018, S. 1032-1034.

Hauck, Ronny, „Schutz von Geschäftsgeheimnissen und Handlungsfreiräume für Medien“, AfP 2021, S. 193-203.

Hauck, Ronny, „Was lange währt … - Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) ist in Kraft“, GRUR-Prax 2019, S. 223-225.

Henssler, Martin/Prütting, Hanns (Hrsg.), Bundesrechtsanwaltsordnung: BRAO (zit.: *Bearbeiter*, in: Henssler/Prütting, BRAO).

Henssler, Martin/Willemsen, Heinz Josef/Kalb, Heinz-Jürgen (Hrsg.), Arbeitsrecht Kommentar, 11. Auflage, Köln 2024
(zit.: *Bearbeiter*, in: HWK).

Hoeren, Thomas/Münker, Reiner (Hrsg.), GeschGehG - Gesetz zum Schutz von Geschäftsgeheimnissen, Kommentar (zit.: *Bearbeiter*, in: Hoeren/Münker, GeschGehG).

Hoffmann von Fallersleben, August Heinrich, in Zitatensammlung v. *Zoozmann, Richard*, Zitaten- und Sentenzenschatz der Weltliteratur alter und neuer Zeit, Leipzig 1910.

Hoffmann, Michel, „Möglichkeit und Zulässigkeit von Künstlicher Intelligenz und Algorithmen im Recruiting“, NZA 2022, S. 19-24.

Hofmann, Andreas, „Abgabe einer Sperrerklärung gem. § 99 I 2 VwGO“, NVwZ 2020, S. 715-719.

Holthausen, Joachim, „Die arbeitsvertragliche Verschwiegenheit - Vertragsgestaltung nach Inkrafttreten des GeschGehG“, NZA 2019, S. 1377-1383.

Höpfner, Clemens/Daum, Alexander, „Der „Robo-Boss“ - Künstliche Intelligenz im Arbeitsverhältnis“, ZfA 2021, S. 467-501.

Hoppe, Daniel/Oldekop, Axel (Hrsg.), Geschäftsgeheimnisse, Schutz von Know-how und Geschäftsinformationen, 2. Auflage, Hürth 2022 (zit.: *Hoppe/Oldekop*, Geschäftsgeheimnisse).

Jacksch, Christian/*Hoffmann, Raphael*, „Datenschutzrechtliche Informationspflichten bei Verarbeitungen ohne aktive Beteiligung der betroffenen Person - Grenzen der Anwendbarkeit von Art. 13 DS-GVO“, ZD 2022, S. 605-611.

Jarass, Hans D., „Der grundrechtliche Eigentumsschutz im EU-Recht“, NVwZ 2006, S. 1089-1095.

Jarass, Hans D., Charta der Grundrechte der Europäischen Union unter Einbeziehung der sonstigen Grundrechtsregelungen des Primärrechts und der EMRK, Kommentar, 4. Auflage, München 2021 (zit.: *Jarass*, GR-CH).

Jerchel, Kerstin/*Schubert, Jens M.*, „Neustart im Datenschutz für Beschäftigte - Möglichkeit von Kollektivvereinbarungen zur Regelung des Datenschutzes nach der DS-GVO“, DuD 2016, S. 782-786.

Kalbfus, Björn, „Angemessene Geheimhaltungsmaßnahmen nach der Geschäftsgeheimnis-Richtlinie“, GRUR-Prax 2017, S. 391-393.

*Kalbfus, Björn, „*Die EU-Geschäftsgeheimnis-Richtlinie“, GRUR 2016, S. 1009-1017.

Kalbus, Björn, Know-how-Schutz in Deutschland zwischen Strafrecht und Zivilrecht - welcher Reformbedarf besteht?, GEW Band 25, zugleich Dissertation, Köln 2011 (zit.: *Kalbfus,* Know-how-Schutz).

Keller, Erhard/Schönknecht, Marcus/Glinke, Anna, Geschäftsgeheimnisschutz, Beck´sche Kurzkommentare, 1. Auflage, München 2021 (zit.: Keller/Schönknecht/Glinke, GeschGehG).

Kiefer, Jonas, „Das Geschäftsgeheimnis nach dem Referentenentwurf zum Geschäftsgeheimnisgesetz: Ein Immaterialgüterrecht“, WRP 2018, S. 910-917.

Klinkert, Friedrich, „Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) ist in Kraft getreten“, WRP 2019, Heft 06, Umschlagteil, I, (Editorial).

Klösel, Daniel/*Mahnhold, Thilo*, „Die Zukunft der datenschutzrechtlichen Betriebsvereinbarung - Mindestanforderungen und betriebliche Ermessensspielräume nach DS-GVO und BDSG n. F.“, NZA 2017, S. 1428-1433.

Köhler, Helmut/Bornkamm, Joachim/Feddersen, Jörn (Hrsg.), Gesetz gegen den unlauteren Wettbewerb, 42. Auflage, München 2024 (zit.: *Bearbeiter*, in: Köhler/Bornkamm/Feddersen).

König, Tassilo-Rouven, „Das Recht auf eine Datenkopie im Arbeitsverhältnis“, CR 2019, S. 295-301.

König, Tassilo-Rouven, Beschäftigtendatenschutz, 1. Auflage, Baden-Baden 2020 (zit.: *König*, Beschäftigtendatenschutz).

Korch, Stefan/*Chatard, Yannick*, „Der datenschutzrechtliche Auskunftsanspruch in Geschäftsleiterhaftungsfällen - Unverhoffte Hilfe für Organe in Beweisnot?“, NZG 2020, S. 893-898.

Koreng, Ansgar, „Das „Unternehmenspersönlichkeitsrecht” als Element des gewerblichen Reputationsschutzes“, GRUR 2010, S. 1065-1070.

Koreng, Ansgar, „Reichweite des datenschutzrechtlichen Auskunftsanspruchs“, NJW 2021, S. 2692-2694.

Körner, Marita, „Die Datenschutz-Grundverordnung und nationale Regelungsmöglichkeiten für Beschäftigtendatenschutz“, NZA 2016, S. 1383-1386.

Kort, Michael, „Die Zukunft des deutschen Beschäftigtendatenschutzes - Erfüllung der Vorgaben der DS-GVO“, ZD 2016, S. 555-560.

Kort, Michael, „Neuer Beschäftigtendatenschutz und Industrie 4.0“, RdA 2018, S. 24-33.

Kramer, Stefan Frank (Hrsg.), IT-Arbeitsrecht, Handbuch, 3. Auflage, München 2023 (zit.: *Bearbeiter*, in: Kramer, IT-ArbRecht).

Krause, Rüdiger, „Zwischen Treuepflichtverletzung und Rechtsdurchsetzungsinstrument - Externes Whistleblowing im Wandel der Zeiten“, SR 2019, S. 138-152.

Kreis, Simona, Whistleblowing als Beitrag zur Rechtsdurchsetzung - Das öffentliche Informationsinteresse im Arbeitsrecht, Beiträge zum Arbeitsrecht, zugleich Dissertation, Tübingen 2017
(zit.: *Kreis*, Whistleblowing).

Kremer, Sascha, „Das Auskunftsrecht der betroffenen Person in der DSGVO“, CR 2018, S. 560-569.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung/BDSG, Kommentar, 4. Auflage, München 2024
(zit.: *Bearbeiter*, in: Kühling/Buchner).

Kumkar, Lea Katharina/*Roth-Isigkeit, David,* „Erklärungspflichten bei automatisierten Datenverarbeitungen nach der DSGVO“, JZ 2020, S. 277-286.

Lang, Flavia/*Reinbach, Hubertus*, „Künstliche Intelligenz im Arbeitsrecht“, NZA 2023, S. 1273-1281.

Lang, Markus, „Datenschutzrechtliche Implikationen des Hinweisgeberschutzgesetzes - Einrichtung und Betrieb eines Hinweisgebersystems unter Beachtung der datenschutzrechtlichen Vorgaben“, ZD 2024, S. 17-22.

Leibold, Kevin, „Reichweite, Umfang und Bedeutung des Auskunftsrechts nach Art. 15 DS-GVO - Entscheidungsübersicht“, ZD-Aktuell 2021, 05313.

Leistner, Matthias, „Angemessene Geheimhaltungsmaßnahmen i. S. d. § 2 Nr. 1 b) GeschGehG“, WRP 2021, S. 835-844.

Lembke, Mark, „Der datenschutzrechtliche Auskunftsanspruch im Anstellungsverhältnis“, NJW 2020, S. 1841-1846.

Lembke, Mark/*Fischels, André,* „Datenschutzrechtlicher Auskunfts- und Kopieanspruch im Fokus von Rechtsprechung und Praxis“, NZA 2022, S. 513-521.

Lentz, Alexander, „Der Auskunftsanspruch nach Art. 15 DSGVO“, ArbRB 2019, S. 150-154.

Libor, Christine, „Investigativer Journalismus: Schutz von Geschäftsgeheimnissen und Verwendung rechtswidrig erlangter Informationen“, AfP 2019, S. 25-30.

Lühning, Torsten, „Auskunftsersuchen des Beschuldigten bei internen Ermittlungen - Kriterien zur Interessenabwägung zwischen Daten- und Hinweisgeberschutz“, ZD 2023, S. 136-140.

Maaßen, Stefan, „Angemessene Geheimhaltungsmaßnahmen für Geschäftsgeheimnisse“, GRUR 2019, S. 352-360.

Malorny, Friederike, „Auswahlentscheidungen durch künstlich intelligente Systeme“, JuS 2022, S. 289-296.

Marsch, Nikolaus, Das europäische Datenschutzgrundrecht: Grundlagen - Dimensionen - Verflechtungen, Schriftenreihe Jus Publicum, Beiträge zum öffentlichen Recht, zugleich Habilitationsschrift, Tübingen 2018 (zit.: *Marsch*, Das europäische Datenschutzgrundrecht).

Maschmann, Frank, „Der Anspruch auf Datenkopie: ein neues Geschäftsmodell?“, NZA-Beilage 2022, S. 50-56.

McGuire, Mary-Rose, „Geheimnisschutz: In vier Schritten zur angemessenen Maßnahme“, IPRB 2018, S. 202-206.

Miege, Christian/Ahrens, Tim, „Referentenentwurf der Koalition zum Hinweisgeberschutzgesetz - Stellungnahme des Deutschen Instituts für Compliance (DICO e. V.)“, CCZ 2022, S. 171-177.

Mohn, Mathias, „Das Recht auf Auskunft nach Art. 15 DS-GVO und der Schutz des Hinweisgebers“, NZA 2022, S. 1159-1167.

Möllenkamp, Olaf, „Zustimmungsersetzungsverfahren unter Einsatz eines Bewerbungsmanagementsystems“, NZA-RR 2021, S. 76-81.

Müller, Michael, „Whistleblowing - Ein Kündigungsgrund?“, NZA 2002, S. 424-437.

Müller-Glöge, Rudi/Preis, Ulrich/Gallner, Inken/Schmidt, Ingrid (Hrsg.), Erfurter Kommentar zum Arbeitsrecht, Beck´sche Kurzkommentare, begr. v. *Dieterich, Thomas/Hanau, Peter/Schaub, Günter*, 24. Auflage, München 2024 (zit.: *Bearbeiter*, in: ErfK-ArbR).

Müllmann, Dirk, „Mehr als nur Whistleblowing: Gesetz zum Schutz von Geschäftsgeheimnissen“, ZRP 2019, S. 25, 26.

Musiol, Philip, Hinweisgeberschutz und Datenschutz - Datenschutzrechtliche Implikationen bei Einrichtung und Betrieb einer internen Meldestelle nach dem HinSchG, Schriften zur Compliance, zugleich Dissertation, 1. Auflage, Baden-Baden 2023 (zit.: *Musiol*, Hinweisgeberschutz und Datenschutz).

Naber, Sebastian/Peukert, Matthias/Seeger, Börge, „Arbeitsrechtliche Aspekte des Geschäftsgeheimnisgesetzes“, NZA 2019, S. 583-588.

Niklas, Thomas, „Die Verschwiegenheitspflicht des Betriebsrates“, ArbRB 2020, S. 122-125.

Nikol, Dominik, „Zum Spannungsfeld von Hinweisgeberschutz und Datenschutzrecht“, CB 2023, S.351-355.

Nöbel, Eileen/Veljovic, Miguel, „Strafbarkeitsrisiken des Whistleblowers in Deutschland“, CB 2020, S. 34-38.

Nomos-Kommentar, Charta der Grundrechte der Europäischen Union, hrsg. v. *Meyer, Jürgen/Hölscheidt, Sven*, 5. Auflage, Baden-Baden 2019, (zit.: *Bearbeiter*, in: NK-GR-CH).

Ohly, Ansgar, „Das neue Geschäftsgeheimnisgesetz im Überblick“, GRUR 2019, S. 441-451.

Ohly, Ansgar, „Der Geheimnisschutz im deutschen Recht: heutiger Stand und Perspektiven“, GRUR 2014, S. 1-11.

Ohly, Ansgar/Sosnitza, Olaf, begr. v. *Köhler, Helmut/Piper, Henning,* Gesetz gegen den unlauteren Wettbewerb mit Geschäftsgeheimnisgesetz (Auszug), Kommentar, 8. Auflage, München 2023
(zit.: *Bearbeiter*, in: Ohly/Sosnitza UWG).

Paal, Boris P./Nikol, Dominik, „Zur Identifizierung von Hinweisgebern im Spannungsfeld von Hinweisgeberschutzgesetz, Whistleblowing-Richtlinie und Datenschutz-Grundverordnung“, CB 2022, 466-471.

Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Beck´sche Kompakt-Kommentare, 3. Auflage, München 2021 (zit.: *Bearbeiter*, in: Paal/Pauly).

Paulus, David, „Die automatisierte Willenserklärung“, JuS 2019, S. 960-965.

Pauly, Danie A./Mende, Luisa, „Der Bundesgerichtshof zur Reichweite des Auskunftsanspruchs nach Art. 15 DS-GVO“, CCZ 2022, S. 28-31.

Payandeh, Mehrdad, „Der Schutz der Meinungsfreiheit nach der EMRK“, JuS 2016, S. 690-695.

Peisker, Yannick, Der datenschutzrechtliche Auskunftsanspruch: Grundlagen, Reichweite und praktische Probleme des Art. 15 DSGVO im Beschäftigungskontext, zugleich Dissertation, 1. Auflage, Baden-Baden 2023 (zit.: *Peisker*, Datenschutzrechtlicher Auskunftsanspruch).

Pfeifer, Karl-Nikolaus, UWG - Großkommentar zum Gesetz gegen den unlauteren Wettbewerb mit Nebengesetzen, Band 3, 3. Auflage, Berlin 2021 (zit.: GK-UWG).

Pielow, Tobias/*Volk*, Eva, „Der Referentenentwurf zum Hinweisgeberschutzgesetz - Quo vadis?“, CB 2021, S. 232-237.

Plath, Kai-Uwe (Hrsg.), Kommentar zu DSGVO, BDSG und TTDSG, 4. Auflage, Köln 2023 (zit.: *Bearbeiter*, in: Plath, DS-GVO).

Preis, Ulrich/Seiwerth, Stephan, „Geheimnisschutz im Arbeitsrecht nach dem Geschäftsgeheimnisgesetz“, RdA 2019, S. 351-360.

Raji, Behrang, „Auskunftsanspruch in der Praxis“, ZD 2020, S. 279-284.

Redder, Jan-Philipp, Der verfassungsrechtliche Schutz von Whistleblowern, Schriften zum Öffentlichen Recht, Band 1418, zugleich Dissertation, Berlin 2020 (zit.: *Redder*, Schutz von Whistleblowern).

Reinbacher, Tobias, „Die Strafbarkeit des Whistleblowings nach § 17 UWG im Lichte der Geheimnisschutzrichtlinie“, KriPoZ 2018, S. 115-121.

Reinfeld, Roland, Das neue Gesetz zum Schutz von Geschäftsgeheimnissen, 1. Auflage, München 2019 (zit.: *Reinfeld,* GeschGehG).

Reufels, Martin/*Osmakova, Maria,* „Der neue Entwurf des Hinweisgeberschutzgesetzes - Gelungene Umsetzung der EU-Whistleblower-Richtlinie?“, ArbRB 2022, S. 147-150.

Richardi, Reinhard (Hrsg.), Betriebsverfassungsgesetz mit Wahlordnung, 17. Auflage, München 2022 (zit.: *Bearbeiter*, in: Richardi).

Riemer, Martin, „Der Datenauskunftsanspruch als „discovery“ im deutschen Zivilprozess“, ZD 2019, S. 413-415.

Riemer, Martin, „Der Datenauskunftsanspruch gem. Art. 15 DSGVO als pre-trial-discovery und prima lex des Auskunftsrechts“, DSB 2019, S. 223-225.

Rody, Yasamin, Der Begriff und die Rechtsnatur von Geschäfts- und Betriebsgeheimnissen unter Berücksichtigung der Geheimnisschutz-Richtlinie, Nomos Universitätsschriften - Recht, Band 952, zugleich Dissertation, 1. Auflage, Baden-Baden 2019 (zit.: *Rody*, Geschäfts- und Betriebsgeheimnisse).

Röller, Jürgen (Hrsg.), begr. v. *Küttner, Jürgen*, Personalhandbuch 2024, Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, Handbuch, 31. Auflage, München 2024 (zit.: *Bearbeiter*, in: Küttner).

Roloff, Sebastian, „Erst die Auskunft, dann das gleiche Entgelt?“, RdA 2019, S. 28-41.

Rosenberg, Leo, Die Beweislast, 5. Auflage, München 1966 (zit.: *Rosenberg*, Die Beweislast).

Rossi, Matthias, „Zugang zu Unterlagen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)“, NVwZ 2019, S. 1847-1849.

Rüdiger, Andreas/Adelberg, Philipp, „Datenschutzrechtliche Herausforderungen des neuen Hinweisgeberschutzgesetzes“, K&R 2023, S. 172-178.

Rützel, Stefan, „Illegale Unternehmensgeheimnisse?“, GRUR 1995, S. 557-561.

Sachs, Michael (Hrsg.), Grundgesetz, Kommentar, 9. Auflage, München 2021 (zit.: *Bearbeiter*, in: Sachs, GG).

Sachs, Michael/Schmitz, Heribert/Stelkens, Ulrich (Hrsg.), begr. v. *Stelkens, Paul/Bonk, Heinz-Joachim/Leonhardt, Klaus*, Verwaltungsverfahrensgesetz, Beck´sche Kurz-Kommentare, 10. Auflage, München 2023 (zit.: *Bearbeiter*, in: Sachs/Schmitz/Stelkens, VwVfG).

Säcker, Franz Jürgen/Rixecker, Roland/Oetker, Hartmut/Limperg, Bettina (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 1, 9. Auflage, München 2021
(zit.: *Bearbeiter*, in: MüKo-BGB).

Schantz, Peter, „Die Datenschutz-Grundverordnung - Beginn einer neuen Zeitrechnung im Datenschutzrecht", NJW 2016, S. 1841-1847.

Schantz, Peter/Wolff, Heinrich Amadeus, Das neue Datenschutzrecht: Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, 1. Auflage, München 2017 (zit.: *Schantz/Wolff*, Das neue Datenschutzrecht).

Schlack, Ulrich, „Das neue Geschäftsgeheimnisgesetz, Schutz für Private vor Privaten - und Behörden?", ZWeR 2019, S. 192-199.

Schmidt, Bettina/Plote, Maximilian, „Die Zulässigkeit der Datenverarbeitung im betrieblichen Eingliederungsmanagement", NZA 2022, S. 1297-1305.

Schmitt, Laura, „Geheimnisschutz und Whistleblowing - Aktuelle Rechtslage und Überlegungen zur Umsetzung in Deutschland", NZW-Beilage 2020, S. 50-57.

Schmitt, Laura, „Whistleblowing revisited - Anpassungs- und Regelungsbedarf im deutschen Recht: Zugleich ein Beitrag zu den arbeitsrechtlichen Auswirkungen der Geheimnisschutzrichtlinie", RdA 2017, S. 365-373.

Schnabel, Christoph, „Rechtswidrige Praktiken als Betriebs- und Geschäftsgeheimnisse?", CR 2016, S. 342-348.

Scholtyssek, Swen/Judis, Christian, Michael/Krause, Sven, „Das neue Geschäftsgeheimnisgesetz - Risiken, Chancen und konkreter Handlungsbedarf für Unternehmen", CCZ 2020, S. 23-29.

Schreiber, Kristina/Brinke, Pauline, „Der Auskunftsanspruch als discovery-Ersatz? Überlegungen zu den Auswirkungen des Datenschutzrechts auf das Zivilprozessrecht, den Beibringungsgrundsatz und den Ausforschungsbeweis", RDi 2023, S. 232-239.

Schreiber, Markus, „Das neue Gesetz zum Schutz von Geschäftsgeheimnissen - ein „Freifahrtschein" für Whistleblower", NZWiSt 2019, S. 332-338.

Schröder, Thomas, „Integration des Whistleblowings in die nationale Rechtsordnung", ZRP 2020, S. 212-215.

*Schulte, Wienhold, „*Mehr Schutz für Geschäftsgeheimnisse", ArbRB 2019, S. 143-147.

Schulte, Willem/*Welge, Jonas*, „Der datenschutzrechtliche Kopieanspruch im Arbeitsrecht", NZA 2019, S. 1110-1116.

Schuth, Hendrike, Die Neuregelung zum Schutz der Geschäftsgeheimnisse und ihre Auswirkungen für das Arbeitsrecht, Zivilrechtliche Schriften, Band 77, zugleich Dissertation, 1. Auflage, Lausanne 2021 (zit.: *Schuth*, Neuregelung zum Schutz der Geschäftsgeheimnisse).

Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter (Hrsg.), DS-GVO/BDSG, Kommentar, 2. Auflage, Heidelberg 2020 (zit.: *Bearbeiter*, in: SJTK).

Siebert, Melanie, Geheimnisschutz und Auskunftsansprüche im Recht des Geistigen Eigentums: Der Konflikt mit dem Schutz von personenbezogenen Daten und Geschäftsgeheimnissen - Eine Analyse des europäischen und deutschen Rechts, Schriftenreihe Geistiges Eigentum und Wettbewerbsrecht, zugleich Dissertation, 1. Auflage, Tübingen 2011 (zit.: *Siebert*, Geheimnisschutz).

Siemes, Christiane, „Die hinreichend begründete Annahme des Whistleblowers nach Art. 6 Abs. 1 lit. a Richtlinie (EU) 2019/1937 - Auslegung und Umsetzung", CCZ 2022, S. 293-303.

Simitis, Spiros/*Fuckner, Gerhard*, „Informationelle Selbstbestimmung und staatliches Geheimhaltungsinteresse", NJW 1990, S. 2713-2717.

Simitis, Spiros/Hornung, Gerrit/Spiecker, Indra gen. Döhmann (Hrsg.), Datenschutzrecht: DS-GVO mit BDSG, Großkommentar, 1. Auflage, Baden-Baden 2019 (zit.: *Bearbeiter*, in: NK-DatenschutzR).

Simon, Johannes/*Vogel, Jan-Patrick*, „AG Aachen: „Catch-all-Klausel“ ist keine angemessene Geheimhaltungsmaßnahme“, CB 2022, S. 172-180.

Simon, Oliver/*Schilling, Jan Moritz*, „Kündigung wegen Whistleblowing?“, BB 2011, S. 2421-2428.

Sixt, Manuela, Whistleblowing im Spannungsfeld von Macht, Geheimnis und Information, DuD-Fachbeiträge, zugleich Dissertation, 1. Auflage, Heidelberg 2020 (zit.: *Sixt*, Whistleblowing im Spannungsfeld).

Sorber, Dominik, „Auskunftsanspruch nach der Datenschutz-Grundverordnung (DS-GVO) - Was sollten Unternehmen nach der BAG-Entscheidung vom 27.04.2021 beachten?“, BC 2021, S. 342-346.

Sörup, Thorsten, „Gestaltungsvorschläge zur Umsetzung der Informationspflichten der DS-GVO im Beschäftigungskontext“, ArbRAktuell 2016, S. 207-213.

Staat, Verwaltung und Rechtsschutz: Festschrift für *Wolf-Rüdiger Schenke* zum 70. Geburtstag, hrsg. v. *Baumeister, Peter/Roth, Wolfgang*, Schriften zum Öffentlichen Recht, Berlin 2011
(zit.: *Bearbeiter*, in: FS-Schenke).

Steinmann, Sabrina, „Die Geschäftsgeheimnis-Richtlinie: Vorwirkung und unmittelbare Anwendbarkeit“, WRP 2019, S. 703-709.

Stück, Volker, „Datenschutz = Tatenschutz? Ausgewählte datenschutz- und arbeitsrechtliche Aspekte nach DSGVO sowie BDSG 2018 bei präventiver und repressiver Compliance“, CCZ 2020, S. 77-83.

Suchan, Florian B., „Der „qualitative Exzess“ nach Art. 15 DS-GVO: Vorschlag zur Begrenzung ausforschender Auskunftsanträge“, ZD 2021, S. 198-202.

Sydow, Gernot/Marsch, Nikolaus (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Handkommentar, 3. Auflage, Baden-Baden 2022 (zit.: *Bearbeiter*, in: Sydow/Marsch).

Szesny, André-M., „Die Whistleblower-Richtlinie kommt - Abstandnahme vom Drei-Stufen-Modell“, BB 2019, Heft 16-17, Umschlagteil, I (Die Erste Seite).

Taeger, Jürgen/Gabel, Detlev (Hrsg.), DSGVO, BDSG, TTDSG, Kommentar, 4. Auflage, Frankfurt a. M. 2022 (zit.: *Bearbeiter*, in: Taeger/Gabel).

Taeger, Jürgen/*Rose, Edgar,* „Zum Stand des deutschen und europäischen Beschäftigtendatenschutzes“, BB 2016, S. 819-831.

Thiel, Linda, „Das neue Geschäftsgeheimnisgesetz (GeschGehG) - Risiken und Chancen für Geschäftsgeheimnisinhaber“, WRP 2019, S. 700-703.

Thüsing, Gregor (Hrsg.), Hinweisgeberschutzgesetz, Kommentar, 1. Auflage, München 2024 (zit.: *Bearbeiter*, in: Thüsing, HinSchG).

Thüsing, Gregor, „Effektiver Hinweisgeberschutz mit Augenmaß - Erste Gedanken zum neuen RefE eines Hinweisgeberschutzgesetzes (HinSchG)“, DB 2022, S. 1066-1069.

Thüsing, Gregor, Beschäftigtendatenschutz und Compliance, 3. Auflage, München 2021 (zit.: *Bearbeiter*, in: Compliance).

Thüsing, Gregor/*Fütterer, Johannes*/*Jänsch, Melanie*, „Petzen ist doof - Zu den datenschutzrechtlichen Grenzen des Whistleblowings“, RDV 2018, S. 133-144.

Thüsing, Gregor/Musiol, Philip, „Hinweise zum Hinweisgeberschutzgesetz“, BB 2022, S. 2420-2423.

Thüsing, Gregor/*Peisker, Yannick,* „Datenschutzrechtliches Glasperlenspiel? Zum Antrag des Generalanwalts Sánchez-Bordona im Verfahren Rs. C-34/21, BeckRS 2022, 24515”, NZA 2023, S. 213-215.

*Thüsing, Gregor/Rombey, Sebastian, „*Der verdeckte Einsatz von Privatdetektiven zur Kontrolle von Beschäftigten nach dem neuen Datenschutzrecht“, NZA 2018, S. 1105-1111.

Thüsing, Gregor/Rombey, Sebastian, „Verschränkungen von Daten- und Geheimnisschutz Happy Birthday: Geschäftsgeheimnisgesetz“, ZD 2020, S.221-222.

Trebeck, Joachim/Schulte-Wissermann, Lisa, „Die Geheimnisschutzrichtlinie und deren Anwendbarkeit“, NZA 2018, S. 1175-1180.

Trebinger, Yvonne/Linsenmaier, Wolfgang/ Schelz, Hanna/Schmidt, Ingrid (Hrsg.) Betriebsverfassungsgesetz mit Wahlordnung, Handkommentar, begr. v. *Fitting, Karl,* 32. Auflage, München 2024 (zit.: *Bearbeiter,* in: Fitting).

Ullrich, Ines, „Der Schutz von Whistleblowern aus strafrechtlicher Perspektive - Rechtslage de lege lata und de lege ferenda“, NZWiSt 2019, S. 65-71.

Ullrich, Ines, „Die EU-Whistleblower-Richtlinie oder Richtlinien-Potpourri zum Schutz von Whistleblowern“, WiJ 2019, S. 52-62.

Vitt, Tillmann, „Nachforschungs- und Sorgfaltspflichten des Whistleblowers? (Teil II)”, BB 2022, S. 1844-1848.

Vogel, Jan-Patrick/Poth, Christina, „Steine statt Brot für den Whistleblower”, CB 2019, S. 45-49.

Völkerrecht und deutsches Recht: Festschrift für *Walter Rudolf* zum 70. Geburtstag, hrsg. v. *Arndt, Hans-Wolfgang/ Knemeyer, Franz-Ludwig/Kugelmann, Dieter/Meng, Werner/Schweitzer, Michael*, München 2001 (zit.: *Bearbeiter*, in: FS-Rudolf).

Waas, Bern, „KI und Arbeitsrecht“, RdA 2022, S. 125-131.

Wegener, Bernhard W., Der geheime Staat: Arkantradition und Informationsfreiheitsrecht, zugleich Habilitationsschrift, 1. Auflage, Berlin 2006 (zit.: *Wegener*, Der geheime Staat).

Weidmann, Golo, „Datenschutzrechtliche Anforderungen an die Einrichtung interner Hinweisgebersysteme unter Berücksichtigung der EU-Whistleblowing-Richtlinie“, DB 2019, S. 2393-2398.

*Weigert, Daniel, „*Angemessene Geheimhaltungsmaßnahmen im Sinne des Geheimnisschutzgesetzes - Geheimnisschutz ad absurdum“, NZA 2020, S. 209-214.

Westermann, Ingo, Handbuch Know-how-Schutz, 1. Auflage, München 2007 (zit.: *Westermann*, Hdb. Know-How-Schutz).

Wiedmann, Michael/*Hoppmann, Vincent*, „Whistleblowing im DAX - Auswirkungen von HinSchG, LkSG, CSRD und CS3D-E“, CCZ 2023, S. 11-23.

Wiedmann, Michael/*Seyfert, Stefan*, „Richtlinienentwurf der EU-Kommission zum Whistleblowing“, CCZ 2019, S. 12-21.

Wiese, Günther/Kreutz, Peter/Oetker, Hartmut (Hrsg.), Gemeinschaftskommentar Betriebsverfassungsgesetz, Band 2, 12. Auflage, München 2021 (zit.: *Bearbeiter*, in: GK-BetrVG).

Winterhagen, Annabelle, „EDSA-Leitlinie zum Auskunftsrecht: Kurzanalyse der Anforderungen an den Umfang des Auskunftsrechts“, ZD-Aktuell 2022, 01066.

Wolf, Fabiana, Der Schutz des Betriebs- und Geschäftsgeheimnisses: Verfassungsrechtliche Grundlagen und Ausgestaltung in den modernen Informationszugangsgesetzen, Universitätsschriften Recht, Band 854, zugleich Dissertation, 1. Auflage, Baden-Baden 2015 (zit.: *Wolf*, Schutz des Betriebs- und Geschäftsgeheimnisses).

Wunner, Katharina, „Die zivilrechtliche Haftung für Geheimnisverwertungen durch Beschäftigte im Lichte der Geschäftsgeheimnis-RL“, WRP 2019, S. 710-716.

Wünschelbaum, Markus, „Neuer Datenschutz für betriebliche Kommunikationsdienste“, NJW 2022, S. 1561-1566.

Wünschelbaum, Markus, „Tabula rasa im Beschäftigtendatenschutz? - EuGH setzt neue Maßstäbe: Rechtsfolgen und Handlungsoptionen“, NZA 2023, S. 542-547.

Wünschelbaum, Markus, „Zur Einschränkung des DSGVO-Auskunftsanspruchs durch Betriebsvereinbarungen“, BB 2019, S. 2102-2106.

Wurzberger, Sebastian, „Anforderungen an Betriebsvereinbarungen nach der DS-GVO: Konsequenzen und Anpassungsbedarf für bestehende Regelungen“, ZD 2017, S. 258-263.

Wybitul, Tim, „Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte? Anpassungsbedarf bei Beschäftigtendatenschutz und Betriebsvereinbarungen“, ZD 2016, S. 203-208.

Wybitul, Tim/Brams, Isabelle, „Welche Reichweite hat das Recht auf Auskunft und auf eine Kopie nach Art. 15 I DS-GVO?“, NZA 2019, S. 672-677.

Wybitul, Tim/*Neu, Leonie*/*Strauch, Martin,* „Schadensersatzrisiken für Unternehmen bei Datenschutzverstößen: Verteidigung gegen Schadensersatzforderungen nach Art. 82 DS-GVO“, ZD 2018, S. 202-207.

Wybitul, Tim/*Sörup, Thorsten*/*Pötters, Stephan*, „Betriebsvereinbarungen und § 32 BDSG: Wie geht es nach der DS-GVO weiter? Handlungsempfehlungen für Unternehmen und Betriebsräte“, ZD 2015, S. 559-564.

Ziegelmayer, David, „Geheimnisschutz ist eine große Nische“, CR 2018, S. 693-699.

Zikesch, Philipp/*Sörup, Thorsten*, „Der Auskunftsanspruch nach Art. 15 DS-GVO - Reichweite und Begrenzung“, ZD 2019, S. 239-245.

Zimmer, Mark/*Millfahrt, Simon*, „Die Rolle des Betriebsrats beim Hinweisgeberschutzgesetz“, BB 2023, S. 1269-1273.

Zschieschack, Frank, „Der Informationsanspruch der Wohnungseigentümer“, ZWE 2023, S. 244-251.

Materialienverzeichnis

Algorithm Watch, Stellungnahme zu Zwischenbericht des UN-Beirats für Künstliche Intelligenz, 31. März 2024, https://algorithmwatch.org/de/wp-content/uploads/2024/04/AlgorithmWatch-Stance-UN-AI-Regulation.pdf (zuletzt abgerufen am: 01.04.2025).

BDA-Stellungnahme zum Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (Hinweisgeberschutzgesetz) August 2022, https://www.bundestag.de/resource/blob/916392/cd53b5e75d8f37667652d538b80c5a6b/Stellungnahme_BDA.pdf (zuletzt abgerufen am: 01.04.2025).

Bundesrechtsanwaltskammer-Stellungnahme zum Ref-E des Bundesjustizministeriums der Justiz zu einem Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (sog. HinSchG), Stellungnahme Nr. 22/2022, Mai 2022, https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Stellungnahmen/2022/0517_Stellungnahme_BRAK_HinSchG-E.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am: 01.04.2025).

DAV-Stellungnahme zum Referentenentwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, Nr. 23/2022, Mai 2022.

DGB-Stellungnahme zum Reg-E eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) vom 17. April 2018, abgedruckt im Wortprotokoll Nr. 19/30, S. 47 bis 65, https://www.bundestag.de/resource/blob/591320/b8599adbae3a13fd60d60c154ebcf598/wortprotokoll.pdf (zuletzt abgerufen am: 01.04.2025).

DSK-Kurzpapier Nr. 6, Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO, Stand: 17.12.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf
(zuletzt abgerufen am: 01.04.2025).

DSK-Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, Stand: 14.11.2018, https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf
(zuletzt abgerufen am: 01.04.2025).

Erster Bericht der Bundesregierung zur Wirksamkeit des Gesetzes zur Förderung der Entgelttransparenz zwischen Frauen und Männern, Juli 2019, https://www.bmfsfj.de/resource/blob/137224/79c7431772c3143670_59abc8a3242a55/bericht-der-br-foerderung-entgelttransparenz-data.pdf (zuletzt abgerufen am: 01.04.2025).

Handreichung zum Prinzip der Angemessenheit nach den Vorgaben des Lieferkettensorgfaltspflichtengesetzes, hrsg. v. Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA), 1. Auflage, Dezember 2022, file:///C:/Users/U783749/Downloads/handreichung_angemessenheit%20(1).pdf (zuletzt abgerufen am: 01.04.2025).

Hiéramente, Mayeul, Stellungnahme zum Regierungsentwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV), abgedruckt im Wortprotokoll Nr. 19/30, S. 73-101, https://www.bundestag.de/resource/blob/591320/b8599adbae3a13fd60d60c154ebcf598/wortprotokoll.pdf (zuletzt abgerufen am: 01.04.2025).

Koalitionsvertrag 2021-2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten (FDP), Mehr Fortschritt wagen: Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, 20. Legislatur, https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf (zuletzt abgerufen am: 01.04.2025).

Liebknecht, Wilhelm, Wissen ist Macht - Macht ist Wissen. Vortrag, gehalten zum Stiftungsfest des Dresdener Bildungsvereins am 5. Februar 1872 und zum Stiftungsfest des Leipziger Arbeiterbildungsvereins am 25. Februar 1872.

Max-Planck-Institut für Innovation und Wettbewerb, Stellungnahme zum Referentenentwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) vom 17. April 2018, https://www.bundesgerichtshof.de/SharedDocs/Downloads/DE/Bibliothek/Gesetzesmaterialien/19_wp/Geschaeftsgeheimnisse/stellung_refe_mpiiw.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am: 01.04.2025).

Obama, Michelle: ehem. First Lady der Vereinigten Staaten von Amerika in ihrer Rede „*The power of education*" vor der zweiten Klasse der Bell Multicultural High School in Washington, D.C. im Jahr 2013.

Orwat, Carsten, Studie zu Diskriminierungsrisiken durch Algorithmen, hrsg. v. der Antidiskriminierungsstelle des Bundes, 1. Auflage, Baden-Baden 2019, https://www.antidiskriminierungsstelle.de/SharedDocs/downloads/DE/publikationen/Expertisen/studie_diskriminierungsrisiken_durch_verwendung_von_algorithmen.pdf (zuletzt abgerufen am: 01.04.2025).

Study on the Legal Protection of Trade Secrets in the context of the data economy, Final Report, prepared by *Radauer Alfred/Bader, Martin/Aplin, Tanya/Konopka, Ute/ Searle, Nicola/Altenburger, Reinhard/Bachner, Christine*, for the European Commission, 2022, https://www.alexandria.unisg.ch/server/api/core/bitstreams/ec582dd7- ae8a-4ab5-9d30-2ff4d612ea8c/content (zuletzt abgerufen am: 01.04.2025).

Thüsing, Gregor, Stellungnahme zum Regierungsentwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, https://www.bundestag.de/resource/blob/916300/c9e376352f8d669db199efcb96e12c2e/Stellungnahme_Thuesing.pdf (zuletzt abgerufen am: 01.04.2025).

Wortprotokoll Nr. 19/30, Öffentliche Anhörung im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestags am 12.12.2018 zum Regierungsentwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) vom 17. April 2018, BT-Drs. 19/4724, https://www.bundestag.de/resource/blob/591320/b8599adbae3a13fd60d60c154ebcf598/wortprotokoll.pdf (zuletzt abgerufen am: 01.04.2025).

Zweiter Bericht der Bundesregierung zur Wirksamkeit des Gesetzes zur Förderung der Entgelttransparenz zwischen Frauen und Männern sowie zum Stand der Umsetzung des Entgeltgleichheitsgebots in Betrieben mit weniger als 200 Beschäftigten, August 2023, https://www.bmfsfj.de/resource/blob/229484/7c1deeee794163514c0221663af940d2/zweiter-bericht-entgelttransparenzgesetz-data.pdf (zuletzt abgerufen am: 01.04.2025).