Fünfter Teil
Datenschutz/Compliance

Kapitel 70 Compliance und Datenschutz

Literatur: *Eßer/Kramer/von Lewinski (Hrsg.)*, DSGVO/BDSG, Kommentar, 8. Aufl. 2023; *Auer-Reinsdorff/Conrad*, IT- und Datenschutzrecht, 3. Aufl. 2019; BeckOK Datenschutzrecht, 48. Edition, Stand 1.11.2021; *Badura/Brychcy*, Die Rolle des Betriebsrats im Hinweisgeberschutzgesetz, DB 2024, 799; *Bayreuther*, Whistleblowing und das neue Hinweisgeberschutzgesetz, NZA-Beilage 2022, 20; *Böhm/Brams*, Aktuelle Entscheidungen zum Beschäftigtendatenschutz, NZA-RR 2023, 625; *Breinlinger*, Die Kontrolle des Datenschutzbeauftragten aus Sicht der Aufsichtsbehörde, RDV 1995, 7; *Bruns*, Das neue Hinweisgeberschutzgesetz, NJW 2023, 1609; *Dann/Schmidt*, Im Würgegriff der SEC? – Mitarbeiterbefragungen und die Selbstbelastungsfreiheit, NJW 2009, 1851; *Conzelmann* (Hrsg.), HR-Compliance, 2020; *Däubler/Wedde/Weichert/Sommer*, EU-DSGVO und BDSG, 3. Aufl. 2024; *Diller*, Der Arbeitnehmer als Informant, Handlanger und Zeuge im Prozess des Arbeitgebers gegen Dritte, DB 2004, 313; *Diller*, „Konten-Ausspäh-Skandal" bei der Deutschen Bahn: Wo ist das Problem?, BB 2009, 438; *Düwell/Brink*, Beschäftigtendatenschutz nach der Umsetzung der Datenschutz-Grundverordnung: Viele Änderungen und wenig Neues, NZA 2017, 1081; *Dzida/Kröpelin*, Sonderkündigungsschutz des Datenschutzbeauftragten bei Umstrukturierung und Personalabbau, BB 2010, 1026; *Dzida/Seibt*, Neues Hinweisgeberschutzgesetz: Analyse und Antworten auf Praxisfragen, NZA 2023, 657; *Ege*, Online-Bewerbermanagement und AGG, AuA 2008, 154; *Erfurth*, Der „neue" Arbeitnehmerdatenschutz im BDSG, NJW 2009, 2723; *Fecker/Kinzl*, Ausgestaltung der arbeitsrechtlichen Stellung des Compliance-Officers – Schlussfolgerungen aus der BSR-Entscheidung des BGH, CCZ 2010, 13; *Fischer*, Datenschutzrechtliche Stolperfallen im Arbeitsverhältnis und nach dessen Beendigung, NZA 2018, 8; *Fuhlrott*, Arbeitnehmerdatenschutz – Aktuelle Entwicklungen, ArbRAktuell 2020, 103; *Fuhlrott/Oltmanns*, Arbeitnehmerüberwachung und interne Ermittlungen im Lichte der Datenschutz-Grundverordnung, NZA 2019, 1105; *Gerdemann*, Revolution des Whistleblowing-Rechts oder Pfeifen im Walde?, RdA 2019, 16; *Gola*, Die Digitalisierung der Personalakte und der Datenschutz, RDV 2008, 135; *Gola*, Das Internet als Quelle von Bewerberdaten, NZA 2019, 654; *Gola/Heckmann*, DS-GVO/BDSG, 3. Aufl. 2022; *Greiner/Senk*, Der Datenschutzbeauftragte und sein Schutz vor Benachteiligung, Abberufung und Kündigung – Ein Wegweiser durch DS-GVO und BDSG, NZA 2020, 201; *Groß/Platzer*, Whistleblowing: Keine Klarheit beim Umgang mit Informationen und Daten, NZA 2017, 1097; *Haußmann/Thieme*, Reformbedarf und Handlungsoptionen in der IT-Mitbestimmung, NZA 2019, 1612; *Kainer/Feinauer*, Interne Ermittlungen im Referentenentwurf zum Verbandssanktionengesetz, NZA 2020, 363; *Kaufmann/Wegmann/Wieg*, Beschäftigtendatenschutz – Spielräume und Herausforderungen mitgliedstaatlicher Regelungen, NZA 2023, 740; *Keilich/von Lieres und Wilkau*, Whistleblowerschutz – Ausblick auf das Hinweisgeberschutzgesetz und dessen praktische Umsetzung,

SPA 2023, 65; *Kock/Francke*, Mitarbeiterkontrolle durch systematischen Datenabgleich zur Korruptionsbekämpfung, NZA 2009, 646; *Körner*, Beschäftigtendatenschutz in Betriebsvereinbarungen unter der Geltung der DS-GVO, NZA 2019, 1389; *Korinth*, Beweisverwertungsprobleme beim illegalen Speichern von Dateien, ArbRB 2005, 178; *Kramer*, IT-Arbeitsrecht, 3. Aufl. 2023; *von Lewinski*, Persönlichkeitsprofile und Datenschutz bei CRM, RDV 2003, 122; *Löwisch*, Fernmeldegeheimnis und Datenschutz bei der Mitarbeiterkontrolle, DB 2009, 2782; *Menzel*, Datenschutzrechtliche Einwilligungen – Ein Plädoyer für eine Rückkehr zur Selbstbestimmung, DuD 2008, 400; *Mojsilov/Reuther*, Hinweisgeberschutzgesetz – ein Überblick, GuP 2023, 125; *Moos/Bandehzadeh/Bodenstedt*, Datenschutzrechtliche Zulässigkeit der Aufbewahrung von Bewerberdaten unter Berücksichtigung des AGG, DB 2007, 1194; *Naber/Ahrens*, Befragung von Mitarbeitern im Rahmen von Internal Investigations – Vorgehensweise und aktuelle Herausforderungen, CCZ 2020, 36; *Niklas/Faas*, Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung, NZA 2017, 1091; *Oberwetter*, Bewerberprofilerstellung durch das Internet – Verstoß gegen das Datenschutzrecht?, BB 2008, 1562; *Ohly*, Das neue Geschäftsgeheimnisgesetz im Überblick, GRUR 2019, 441 ff.; *Ohmann-Sauer*, Compliance-Audit im Arbeitsrecht, AuA 2007, 520; *Plath*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023; *Reufels/Soltysiak*, Das neue Whistleblowing-Recht, 1. Aufl. 2023; *Salvenmoser/Hauschka*, Korruption, Datenschutz und Compliance, NJW 2010, 331; *Schlegel*, Einsatz von sog. „Data Loss Prevention"-Software im Unternehmen, MMR 2020, 3; *Schmolke*, Die neue Whistleblower-Richtlinie ist da! Und nun?, NZG 2020, 5; *Schulte/Welge*, Der datenschutzrechtliche Kopieanspruch im Arbeitsrecht, NZA 2019, 1110; *Schuster/Darsow*, Einführung von Ethikrichtlinien, NZA 2005, 273; *Steffen/Stöhr*, Die Umsetzung von Compliance-Maßnahmen im Arbeitsrecht, RdA 2017, 43; *Steinhauser/Trouvain*, Das deutsche Hinweisgeberschutzgesetz – Was lange währt, wird endlich gut?, ESG 2023, 9; *Stück*, Datenschutz = Tatenschutz? Ausgewählte datenschutz- und arbeitsrechtliche Aspekte nach DSGVO und BDSG 2018 bei präventiver und repressiver Compliance, CCZ 2020, 77 ff.; *Thüsing*, Hinweisgeberschutzgesetz, 1. Aufl. 2024; *Thum*, Background Checks im Einstellungsverfahren: Zulässigkeit und Risiken für Arbeitgeber, BB 2007, 2405; *Tinnefeld/Viethen*, Arbeitnehmerdatenschutz und Internet-Ökonomie, NZA 2000, 977; *Vogel/Glas*, Datenschutzrechtliche Probleme unternehmensinterner Ermittlungen, DB 2009, 1747; *Wastl/Pusch*, Haftungsrechtliche Konsequenzen einer so genannten Mitarbeiter-Amnestie – dargestellt am Beispiel „Siemens", RdA 2009, 376; *Weichert*, Datenschutz und Mitbestimmung in Matrixorganisationen, NZA 2023, 13; *Weidmann*, Datenschutzrechtliche Anforderungen an die Einrichtung interner Hinweisgebersysteme unter Berücksichtigung der EU-Whistleblowing-Richtlinie, DB 2019, 2393; *Wisskirchen/Bissels*, Das Fragerecht des Arbeitgebers bei Einstellung unter Berücksichtigung des AGG, NZA 2007, 169; *Wisskirchen/Jordan/Bissels*, Arbeitsrechtliche Probleme bei der Einführung internationaler Verhaltens- und Ethikrichtlinien (Codes of Conduct/Codes of Ethics), DB 2005, 2190; *Wisskirchen/Körber/Bissels*, „Whistleblowing" und „Ethikhotlines", BB 2006, 1567; *Wybitul*, Das neue Bundesdatenschutzgesetz: Verschärfte Regeln für Compliance und interne Ermittlungen, BB 2009, 1582; *Wybitul/Brams*, Welche Reichweite hat das Recht auf Auskunft und eine Kopie nach Art. 15 I DS-GVO?, NZA 2019, 672; *Wybitul/Brink/Albrecht*, Interview: Beschäftigtendatenschutz nach der DS-GVO, NZA 2019, 285; *Zilkens/Klett*, Datenschutz im Personalwesen, DuD 2008, 41; *Zimmer/Millfahrt*, Die Rolle des Betriebsrats beim Hinweisgeberschutz, BB 2023, 1269; *Zimmer/Stetter*, Korruption und Arbeitsrecht, BB 2006, 1445.

I. Einführung

1. Compliance

70.1 Mit „Compliance" ist die **Einhaltung von Geboten und Gesetzen gemeint**. Die von Behörden und Gerichten verhängten Geldbußen und -strafen haben eine Höhe erreicht, die häufig erheblich über den mit dem Gesetzesverstoß erzielten Vorteilen liegt. Überdies hat sich das Risiko einer persönlichen zivil- und strafrechtlichen Haftung des Managements erheblich erhöht. Eine Politik des Wegsehens und Ignorierens können sich moderne Unternehmen deshalb nicht mehr leisten. Ganz im Gegenteil werden inzwischen bei den meisten Unternehmen große Anstrengungen unternommen – auch unter dem Gesichtspunkt des Risikomanagements (§ 91 Abs. 2 AktG) – durch den Aufbau von Compliance-Abteilungen die bessere Beachtung der im In- und Ausland geltenden Gesetze durch die Mitarbeiter zu gewährleisten. Dabei hat Compliance viele unterschiedliche Facetten:

- **Schulung und Information** der Mitarbeiter, beispielsweise darüber, was kartellrechtlich erlaubt oder verboten ist.

- **Klare interne Regelwerke** (Verhaltensrichtlinien, Ethikrichtlinien, Codes of Conduct, s. **M 70.2**) sollen Zweifel darüber beseitigen, welches Verhalten akzeptabel ist und welches nicht.
- Es wird ein **effektives** System aufgebaut, mit dem eigene Mitarbeiter oder Geschäftskunden Verstöße von Mitarbeitern gegen geltendes Recht oder verbindliche Verhaltensrichtlinien **melden** können (ggf. anonym) und welches sicherstellt, dass solchen Meldungen auch nachgegangen wird (dazu gehört zB die Gestaltung des Meldeverfahrens nach dem HinSchG, s. **M 70.1**).
- Unabhängig von Zufallsmeldungen (s.o.) werden **Überwachungssysteme** installiert, die so weit wie möglich sicherstellen, dass Unregelmäßigkeiten rechtzeitig bemerkt werden (wobei sich schwierige datenschutzrechtliche Probleme stellen, dazu Rz. 70.4 ff.).
- Es werden Systeme etabliert, die nach Bekanntwerden konkreter Verdachtsmomente eine **zügige und effektive interne Aufklärung** des Sachverhalts gewährleisteten. Ziel ist regelmäßig, mit der internen Untersuchung der externen Untersuchung durch Behörden oder schlimmstenfalls Gerichte zuvorzukommen. In diesem Zusammenhang spielen vor allem **Amnestiezusagen** (s. **M 70.4** und **M 70.5**) eine große Rolle.

Wesentliches Ziel von Compliance-Bemühungen ist aber nicht nur die Vermeidung, Meldung und Aufklärung von Gesetzesverstößen, die Mitarbeiter zum (vermeintlichen) Wohl des Unternehmens gegenüber Dritten begehen. Mindestens ebenso wichtig ist die Vermeidung, Bekämpfung und Aufklärung von Gesetzesverstößen, die Mitarbeiter **zu Lasten des Unternehmens** begehen, sei es durch die Annahme von Schmiergeldern, durch Industriespionage, durch Unterschlagung oder simplen Warendiebstahl. Gerade hierbei sind Konflikte mit datenschutzrechtlichen Vorgaben vorprogrammiert. 70.2

Compliance wirft stets auch die Frage auf, inwieweit der Arbeitgeber **einseitig bestimmte Verhaltenspflichten** aufstellen darf. Einseitig aufgestellte Verhaltenspflichten können mit der Menschenwürde oder dem Recht auf freie Entfaltung der Persönlichkeit kollidieren (zB bei sog. „Flirtverboten"). Unabhängig davon stellt sich die Frage, wo das Direktionsrecht des Arbeitgebers endet und die weisungsfreie Privatsphäre des Arbeitnehmers beginnt (zB wenn Verhaltensregeln privaten Aktienbesitz oder private Meinungsäußerungen über den Arbeitgeber und dessen Branche erfassen). Überdies stellen sich häufig Fragen der Mitbestimmung des Betriebsrats, sei es bei der Einführung technischer Überwachungssysteme (§ 87 Abs. 1 Nr. 6 BetrVG; dazu Kap. 37) oder allgemein bei Verhaltensrichtlinien, die der Ordnung des Betriebs dienen (§ 87 Abs. 1 Nr. 1 BetrVG). 70.3

2. Datenschutzrecht

a) Gerade die verstärkten Compliance-Bemühungen führen zu Konflikten mit dem Arbeitnehmerdatenschutz. Das Spannungsverhältnis liegt auf der Hand. Je engmaschiger der Arbeitgeber versucht, die Einhaltung von Gesetzen durch die Mitarbeiter sicherzustellen, desto mehr personenbezogene Daten wird er verarbeiten. Dabei entfalten sich gerade Compliance-Bemühungen regelmäßig auf drei verschiedenen Ebenen, nämlich einer **präventiven** („prevent"), einer **aufklärenden** („detect") und einer **reaktiven** („respond"). Hat ein **Verstoß stattgefunden**, den es aufzuklären gilt (sei es hinsichtlich des Täters, sei es hinsichtlich der Tatumstände), ist eine Erhebung personenbezogener Daten regelmäßig unausweichlich: Der Arbeitgeber muss Unterlagen einsehen, gespeicherte Dateien und E-Mails screenen sowie durch Mitarbeiterbefragung den Sachverhalt aufklären. Seit jeher unterhalten Unternehmen aber auch eigene Abteilungen („**Innenrevision**"), die stichprobenartige Prüfungen vornehmen. Bei solchen Stichproben gibt es häufig keinen konkreten Anlass, es wird lediglich bezüglich einzelner Bereiche oder Geschäftsvorfälle geprüft, ob alles mit rechten Dingen zugegangen ist. Auch das setzt regelmäßig die Erhebung und Nutzung personenbezogener Daten voraus, mindestens in einem zweiten Schritt. Die stichprobenartige nachträgliche Prüfung hat zugleich ein wichtiges präventives Element: Weil jeder weiß, dass im Nachhinein stichprobenartig Geschäftsvorfälle geprüft werden, werden viele Mitarbeiter vor Gesetzesverstößen zurückschrecken. Zusätzlich unterhalten viele Arbeitgeber aber auch rein **präventive Überwachungssysteme**, die Gesetzesverstöße entweder von vornherein ausschließen oder aber sofort aufdecken sollen (zB videoüberwachte 70.4

Lager oder Kassen zur Vermeidung von Diebstählen/Unterschlagungen). Die Grenzen sind oft fließend. Compliance ist ohne Verarbeitung personenbezogener Arbeitnehmerdaten nicht machbar. Je höher die Anforderungen an den Arbeitnehmer-Datenschutz sind, desto schwieriger wird es für Unternehmen, effektiv sicherzustellen, dass die Mitarbeiter geltende Gesetze einhalten. Was Not tut, ist ein besonnener Ausgleich zwischen den Zielen des Arbeitnehmerdatenschutzes und den Zielen von Compliance. Dies gilt insb. auch im Hinblick auf Datensicherungsvorgaben zum Schutz Dritter, zB den aufsichtsrechtlichen Vorgaben an Banken und Versicherungen, die die Unternehmen verpflichten, Daten vor Cyberattacken zu schützen, aus denen sich als Kehrseite die Notwendigkeit der Mitarbeiterkontrolle ergibt.

70.5 **b)** Die Sensibilität für den Datenschutz steigt. Besondere Aufmerksamkeit hat der Arbeitnehmerdatenschutz, aber auch der Umgang des Unternehmens mit den Daten seiner Kunden und Lieferanten. Ein „Datenskandal" kann ein Unternehmen dazu zwingen, seine Geschäftspraktiken zu ändern. Zugleich schädigt er das Ansehen des Unternehmens in der Öffentlichkeit. Dies droht selbst dann, wenn die beanstandete Auswertung von Daten einem anerkannten Zweck, zB der Korruptionsbekämpfung, diente. Die Aufgabe der Unternehmensleitung besteht darin, den Datenschutz zu wahren, zugleich aber unter Umständen auch darin, Pflichtverletzungen aufzuspüren und darauf so zu reagieren, dass sie sich nicht wiederholen. Fehlerquellen ergeben sich anlässlich von Unternehmenskäufen zum Beispiel beim Übergang von (Kunden-)Datenbeständen – durch die damit verbundenen Informationspflichten und verbundenen Zustimmungserfordernisse. Gestaltungsbedarf zur Einhaltung des Datenschutzes besteht insb. bei Haftungsregelungen und Closing Conditions im Kaufvertrag, Zwischenlösungen bis zum Vollzug des Kaufes in sog. Transitional Services Agreement und nach dem Closing in Vereinbarungen zur sog. Post Merger Integration – Datenübermittlung im (internationalen) Konzern.

70.6 Die **Europäische Datenschutz-Grundverordnung**[1] **(DS-GVO)** ist seit **Mai 2018** europaeinheitlich in Kraft und setzt, nicht zuletzt durch ihre immens hohen Bußgeldandrohungen für Datenschutzverstöße von bis zu 20 Mio. Euro oder 4 % des globalen Jahresumsatzes[2], neue Maßstäbe.

70.7 Inhaltlich sind von zentraler Bedeutung das generelle Verbot der Datenverarbeitung unter dem Vorbehalt der Erlaubnis durch Rechtsvorschrift oder Einwilligung, das Gebot der Zweckbindung der Datenverarbeitung, das Transparenzgebot und der technische und organisatorische Datenschutz.

70.8 **c)** Das Datenschutzrecht definiert seinen Schutzgegenstand extrem weit. „**Personenbezogene Daten**" sind alle Informationen, die sich auf ein bestimmtes oder bestimmbares Individuum beziehen. Geschützt sind damit nicht nur Namen, Adressen, Telefonnummern etc., sondern alle nur denkbaren Angaben (Kontonummern, Arbeitsplatzbeschreibungen, digitale Bilder, E-Mails oä.), die sich mit einer identifizierbaren Person in Verbindung bringen lassen. Dies sind auch sog. Log-Daten, die dokumentieren, welcher Nutzer wann was im System gemacht hat.

70.9 Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage. Dies gilt auch für gesellschaftsübergreifende Verarbeitungen von Beschäftigtendaten in der Matrix. Die DS-GVO kennt nach herrschender Meinung kein Konzernprivileg.[3] Auch die Aufsichtsbehörden schließen sich dieser Einschätzung an: „*Ein sogenanntes ‚Konzernprivileg' […] ist sowohl der DS-GVO als auch dem BDSG […] fremd. Jedes eigenständige Unternehmen, das Teil dieser Unternehmensgruppe oder des Konzerns ist, stellt grundsätzlich also jeweils eine eigene verantwortliche Stelle dar. Jeder Austausch von Daten bedarf einer Rechtsgrundlage.*".[4]

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. Nr. L 119, S. 1.

2 S. Art. 83 DS-GVO; zur Behördenpraxis *Roßnagel/Rost*, ZD 2023, 502.

3 *Schulz* in Gola/Heckmann, Art. 6 DS-GVO Rz. 131; *Kort*, DB 2016, 711, 714.

4 LfDI Baden-Württemberg, Ratgeber Beschäftigtendatenschutz, 4 Aufl. 2020, S. 39 f.

70.10 Art. 6 Abs. 1 DS-GVO zählt „Bedingungen" (Rechtsgrundlagen) auf, von denen mindestens eine für eine rechtmäßige Datenverarbeitung erfüllt sein muss. Als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten kommen grds. in Betracht[5]

- die Einwilligung der betroffenen Person (Art. 6 Abs. 1 lit. a DS-GVO),
- der Dienstvertrag mit dem Beschäftigten (Art. 6 Abs. 1 Satz 1 lit. b DS-GVO),[6]
- die berechtigten Interessen des (Vertrags-)Arbeitgebers oder eines Dritten (Art. 6 Abs. 1 Satz 1 lit. f DS-GVO),
- für (Vertrags-)Arbeitgeber in Deutschland: Regelungen in Betriebsvereinbarungen (§ 26 Abs. 4 BDSG), soweit sie den Anforderungen einer Öffnungsklausel, insbesondere des Art. 88 DS-GVO genügen.[7]

70.11 Besondere zusätzliche Anforderungen sind schließlich bei der Übermittlung von personenbezogenen Daten der Beschäftigten von EU-Unternehmen an Konzerngesellschaften in Drittstaaten zu beachten.

70.12 Es ist weder praktikabel noch sinnvoll, die vielfältigen Datenverarbeitungsvorgänge im Arbeitsverhältnis auf die Einwilligung der betroffenen Beschäftigten zu stützen (Art. 6 Abs. 1 Satz 1 lit. a DS-GVO). Die Einwilligung ist nur wirksam, wenn sie **freiwillig** für den bestimmten Fall, in informierter Weise und unmissverständlich abgegeben wird (Art. 4 Nr. 11 DS-GVO). Insb. die Freiwilligkeit der Einwilligung ist im Beschäftigungskontext wegen des strukturellen Machtungleichgewichts zwischen Arbeitgeber und Arbeitnehmer problematisch. Zwar schließt das die Anwendung der Einwilligung im Beschäftigungsverhältnis nicht generell aus. Freiwilligkeit der Einwilligung kann insb. anzunehmen sein, wenn die Datenverarbeitung einen wirtschaftlichen Vorteil für die beschäftigte Person bringt oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen (§ 26 Abs. 2 Satz 2 BDSG). Voraussetzung ist aber stets, dass die beschäftigte Person eine echte Wahl hat und die Einwilligung verweigern kann, ohne Nachteile für das Beschäftigungsverhältnis befürchten zu müssen, zB. im Zusammenhang mit der privaten Nutzung des dienstlichen Internet-Anschlusses (s. **M 70.7**) oder bei der Hinterlegung von Bewerber-Daten für eventuell künftig freiwerdende Stellen (s. **M 70.6**). Das ist nicht der Fall, wenn es um Datenverarbeitungen geht, die für die Durchführung des Beschäftigungsverhältnisses essentiell sind. Die Datenverarbeitungen, die für die Mitarbeit eines Beschäftigten erforderlich sind, weil diese die Grundlage für die Ausübung des fachlichen Weisungsrechts bilden, können daher nicht zur Disposition des Betroffenen gestellt werden.[8]

70.13 Darüber hinaus sind Einwilligungen jederzeit **frei widerruflich**, sodass es auch nach Abgabe der Einwilligung dauerhaft vom Willen des Arbeitnehmers abhinge, die Datenverarbeitungen weiterhin zuzulassen.

70.14 Datenverarbeitungen, die im Arbeitsverhältnis notwendig sind, müssen deshalb auf gesetzliche Grundlagen gestützt werden.

---

5 Zum Verhältnis der Rechtsgrundlagen zueinander beachte VG Hamburg v. 16.1.2020 – 17 K 3920/19, DSB 2020, 104 ff.

6 Verarbeitungen personenbezogener Daten für die Zwecke des Beschäftigungsverhältnisses sind bislang vorrangig auf § 26 Abs. 1 Satz 1 BDSG gestützt worden. Nach der Entscheidung des EuGH v. 30.3.2023 – C-34/21 (Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium), DB 2023, 2501, ist wegen Verstoßes gegen das Normwiederholungsverbot von der Unanwendbarkeit der Vorschrift auszugehen; vgl. *Kaufmann/Wegmann/Wieg*, NZA 2023, 740, 741.

7 Als „spezifischere Vorschrift" iSd. Art. 88 Abs. 2 DS-GVO müsste eine Betriebsvereinbarung besondere und geeignete Garantien zum Schutz der Rechte und Freiheiten von Beschäftigten regeln, *Kaufmann/Wegmann/Wieg*, NZA 2023, 740, 745. Ob Betriebsvereinbarungen darüber hinaus die sonstigen Vorgaben der DS-GVO einzuhalten haben, hat das BAG dem EuGH zur Vorabentscheidung vorgelegt, BAG v. 22.9.2022 – 8 AZR 209/21 (A), NZA 2023, 363, und BAG v. 25.4.2024 – 8 AZR 209/21 (B), BeckRS 2024, 9543 (Rücknahme der weiteren Vorlagefragen zu den Voraussetzungen und den Berechnungskriterien für einen Schaden i.S.d. Art. 82 Abs. 1 DS-GVO nach Klärung durch den EuGH).

8 U.a. *Selk* in Ehmann/Selmayr, DS-GVO, 3. Aufl. 2024, Art. 88 DS-GVO Rz. 200.

70.15 **Erleichterungen** gelten für die Weitergabe von Daten an sog. Auftragsverarbeiter, die als Dienstleister in die Datenverarbeitung eingebunden sind. Auftragsverarbeiter verwenden die ihnen überlassenen Daten für Zwecke des Auftraggebers und nach dessen Weisungen. Sie gelten im Verhältnis zum Auftraggeber nicht als „Dritte" und dürfen die Daten deshalb ohne besondere Voraussetzungen erhalten. Gegenüber Betroffenen und Aufsichtsbehörden ist allein der Auftraggeber für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Das Gesetz fordert für die Auftragsverarbeitung den Abschluss eines schriftlichen Vertrages, dessen Inhalte im Einzelnen gesetzlich vorgegeben sind.

70.16 Besondere Anforderungen sind einzuhalten, wenn personenbezogene Daten an Geschäftspartner oder Auftragsverarbeiter in Ländern außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums (EWR) weitergegeben werden sollen (dazu Rz. 70.19).

70.17 **e)** Im Konzern ist die Weitergabe von Mitarbeiter- und Kundendaten an andere konzernangehörige Gesellschaften tägliche Praxis. Die enge wirtschaftliche und organisatorische Verflechtung rechtlich selbstständiger Konzernunternehmen, insb. „Matrix-Strukturen" begründen das Konzerninteresse an einem ungehinderten Austausch von Personal- und Kundendaten zwischen den Konzernunternehmen. In Vertriebsdatenbanken werden Kundendaten erfasst und verarbeitet, konzernweite Personalentwicklungsprogramme bauen auf konzernweiten Informationen über die aktuelle Tätigkeit und die Kenntnisse und Fähigkeiten der Mitarbeiter auf. In arbeitsteiligen Produktionsprozessen werden Informationen der Auftraggeber weitergegeben. Die konzernweite Erhebung, Verarbeitung und Speicherung von Daten ist auch nach Inkrafttreten der DS-GVO im Datenschutzrecht nur unzureichend geregelt. Es gibt kein allgemeines Konzernprivileg, das die Weitergabe innerhalb eines Konzerns so gestattet, als wäre der Konzern ein einziges Unternehmen. Für den Datenaustausch ist eine gesetzliche Erlaubnis erforderlich. Die Einwilligung ist schon wegen ihrer Widerruflichkeit impraktikabel (Rz. 70.12). Der Austausch von Beschäftigtendaten ist zwischen Konzernunternehmen zulässig, wenn das entweder für die Zwecke des Beschäftigungsverhältnisses (zB bei Führungskräften oder Mitarbeit in einem gemeinsamen Projekt mehrerer Konzernunternehmen) oder zur Wahrung berechtigter Interessen der beteiligten Konzerngesellschaften (zB zur Ermöglichung eines konzernweiten HR-Informationssystems) erforderlich ist. Im letzten Fall muss sichergestellt sein, dass überwiegende schutzwürdige Interessen der Betroffenen nicht verletzt werden. Dazu kann insb. eine Konzernrichtlinie zum Datenschutz beitragen, die festlegt, wie in den konzernangehörigen Unternehmen mit den personenbezogenen Daten von Mitarbeitern und anderen Betroffenen rechtmäßig umzugehen ist.

70.18 Schließlich können Konzernunternehmen im Verhältnis zueinander auch als Auftragsverarbeiter tätig werden, wenn zB eine zentrale IT-Servicegesellschaft IT-Dienstleistungen für andere Konzernunternehmen erbringt und dabei auf personenbezogene Daten von Kunden und Mitarbeitern dieser Unternehmen Zugriff erhält. Genau wie mit externen Dienstleistern müssen auch mit einem konzernangehörigen Auftragsverarbeiter die gesetzlich geforderten schriftlichen Verträge mit dem vorgegebenen Inhalt abgeschlossen werden.

70.19 Umfassen die Konzernmatrixstrukturen auch Konzernunternehmen in Drittstaaten außerhalb der EU bzw. des EWR, sind für Übermittlungen von Beschäftigtendaten an diese Unternehmen die Art. 44 ff. DS-GVO maßgeblich. Zusätzlich zu der allgemeinen Rechtsgrundlage für die Verarbeitung muss in diesem Fall eine der folgenden Voraussetzungen erfüllt sein:

In Bezug auf den Drittstaat liegt ein **Angemessenheitsbeschluss** der Europäischen Kommission vor, Art. 45 DS-GVO. Dieser Angemessenheitsbeschluss kann sich auf das in dem jeweiligen Drittstaat herrschende Datenschutzniveau im Allgemeinen beziehen (so zB für die Schweiz, Kanada oder Japan). Alternativ kann sich der Angemessenheitsbeschluss auch auf bestimmte Sektoren, Gebiete oder sogar einzelne Adressaten beziehen.[9]

9 Dazu EuGH v. 16.7.2020 – C 311/18 – „Schrems II" zur Unwirksamkeit des Angemessenheitsbeschlusses für USA.

Für die Datenübermittlung liegen geeignete **Garantien** vor, die die Interessen der betroffenen Personen sowie ihre Rechte wirksam schützen. Gem. Art. 46 Abs. 2 DS-GVO zählen dazu u.a. verbindliche interne Datenschutzvorschriften nach Art. 47 DS-GVO sowie Standarddatenschutzklauseln, die von der Kommission erlassen worden sind.

- **Binding Corporate Rules** nach Art. 47 DS-GVO haben den Vorteil, dass sie inhaltlich flexibel und umfassend den Datenaustausch in der Matrixstruktur regeln können und auf die Unternehmenslage individuell zugeschnitten sind. Sie gewährleisten dadurch einen hohen Datenschutzstandard und ausgesprochene Homogenität. Sie sind für die Beschäftigten transparenter und bieten auch Compliance-Vorteile, ihre Erstellung ist aber außerordentlich aufwändig und langwierig, weil sie aufsichtsbehördlich genehmigt werden müssen.
- Demgegenüber können die von der Europäischen Kommission erlassenen **Standarddatenschutzklauseln** schnell, unkompliziert, kostengünstig, rechtssicher und genehmigungsfrei eingesetzt werden. Je komplexer die Datenverarbeitungen in der Matrix und je mehr Konzernunternehmen in die Datenverarbeitungen eingebunden sind, desto höher wird ihre Anzahl und desto aufwändiger wird auch die Pflege und der Erhalt.[10]

Schließlich können Datenübermittlungen an Drittstaaten auch im Einzelfall nach Art. 49 DS-GVO gerechtfertigt sein.

- Hier ist insb. in Abs. 1 lit. b vorgesehen, dass Übermittlungen, die für die Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen erforderlich sind, zulässig sind. Dieser Tatbestand korrespondiert mit Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO.
- Darüber hinaus ist unter Art. 49 DS-GVO eine dauerhafte Datenverarbeitung in der Matrix aufgrund einer Interessenabwägung nicht zulässig. Dies wäre nach Abs. 1 UAbs. 2 nur im absoluten Einzelfall und nicht wiederholt möglich und müsste auch gegenüber der Aufsichtsbehörde gemeldet werden.

f) Zentrale Voraussetzung für die Verarbeitung von Arbeitnehmerdaten ist die „**Erforderlichkeit**". 70.20
„Erforderlich" ist nach richtiger Auffassung nicht nur das, was zur Durchführung des Arbeitsverhältnisses unabdingbarer Mindeststandard ist. Vielmehr darf der Arbeitgeber Daten auch verarbeiten, soweit dies der Optimierung des Arbeitsverhältnisses dient (zB wenn er Daten erhebt und speichert, um über eine spätere Beförderung des Mitarbeiters sachgerecht entscheiden zu können). Im Übrigen ist die Erforderlichkeit richtigerweise nicht objektiv zu bestimmen, sondern sie richtet sich nach dem jeweils aufgrund unternehmerischer Entscheidung des Arbeitgebers festgelegten betrieblichen Konzept. Wenn beispielsweise der Arbeitgeber entscheidet, dass das Tragen von Namensschildern durch Servicemitarbeiter zu seinem unternehmerischen Konzept gehört und er dabei die Mitbestimmungsrechte des Betriebsrats achtet, können nicht das Arbeitsgericht oder die Datenschutzbehörde zu der Entscheidung kommen, man könne ein Serviceunternehmen auch ohne Namensschilder betreiben, so dass diese nicht erforderlich seien.

Praxistipp: Zur Vorbereitung einer datenschutzrechtlichen Bewertung ist möglichst genau aufzubereiten, welche Daten zu welchen betrieblichen Zwecken benötigt werden.

Besonders umstritten ist die Reichweite des § 26 Abs. 1 Satz 2 BDSG bezogen auf die Aufdeckung 70.21
von Pflichtverletzungen. § 26 Abs. 1 Satz 2 BDSG regelt, dass die Datenerhebung, -speicherung und -nutzung zur Aufdeckung begangener Straftaten zulässig ist, wenn konkrete, zu dokumentierende Anhaltspunkte bestehen und Art und Ausmaß der Datennutzung in angemessenem Verhältnis zur Schwere der Tat stehen. Nach richtiger Auffassung[11] sperrt diese Regelung nicht die Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO zur Aufklärung zivilrechtlicher Vertragsverletzungen oder zur vorbeugenden Vermeidung von Straftaten.

10 *Wieczorek* in Specht/Mantz, Handbuch europäisches und deutsches Datenschutzrecht, 2019, § 7 Rz. 95.
11 *Gola/Pötters* in Gola/Heckmann, § 26 BDSG Rz. 65.

70.22 Der durch das Betriebsrätemodernisierungsgesetz eingeführte § 79a BetrVG stellt die in der Vergangenheit umstrittene Frage[12] klar, dass der Arbeitgeber und nicht der Betriebsrat der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften ist. Nach § 79a Satz 3 BetrVG unterstützen sich Arbeitgeber und Betriebsrat gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften. Eine praktische Lösung dafür ist es, den Betriebsrat, Gesamt- oder Konzernbetriebsrat auf seine Verantwortung für den Datenschutz im Betriebsratsbüro hinzuweisen (s. **M 70.8**). So wird der Arbeitgeber seiner Organisationsverantwortung gerecht und zugleich werden betriebsverfassungsrechtliche Geheimhaltungsbedürfnisse respektiert.

12 Vgl. BAG v. 14.1.2014 – 1 ABR 54/12, aA *Kleinebrink*, DB 2018, 2566.

II. Muster

70.23 M 70.1 Betriebsvereinbarung zur Gestaltung des Meldeverfahrens nach dem HinSchG

Präambel[1]

Das Unternehmen hat die Abteilung […] unternehmensübergreifend mit den Aufgaben einer internen Meldestelle im Sinne des HinSchG betraut.[2] Zur Ausgestaltung des Meldeverfahrens[3] schließen die Betriebsparteien die folgende Gesamtbetriebsvereinbarung[4]:

1 Das Gesetz für einen besseren Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz – HinSchG), BGBl. 2023 I Nr. 140 v. 2.6.2023, ist am 2.7.2023 in Kraft getreten und setzt die 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. EU L 305 v. 26.11.2019, S. 17 („**Whistleblower-Richtlinie**"), um. § 12 HinSchG verpflichtet Unternehmen mit jeweils idR mind. 50 Beschäftigten sowie bestimmte Unternehmen unabhängig von ihrer Beschäftigtenzahl (ua. Wertpapierdienstleistungsunternehmen, Börsenträger, Kapitalverwaltungsgesellschaften), mind. eine interne Meldestelle einzurichten und zu betreiben. Nach § 14 Abs. 1 HinSchG kann das Unternehmen die interne Meldestelle mit eigenem Personal besetzen oder einen Dritten mit den Aufgaben betrauen. Im Falle der internen Besetzung kommt in Betracht, einer Person oder einer Arbeitseinheit die Aufgaben zu übertragen. Dabei muss sichergestellt sein, dass sie bei der Ausübung ihrer Tätigkeit unabhängig sind (§ 15 Abs. 1 Satz 1 HinSchG). Doppelfunktionen (zB als Leiter der Compliance-Abteilung) sind zulässig (§ 15 Abs. 1 Satz 2 HinSchG); dazu *Fischbach* in Thüsing, HinSchG, 1. Aufl. 2024, § 14 Rz. 4). Sachlich erfasst der Hinweisgeberschutz Meldungen und Offenlegungen von Verstößen gegen das Unionsrecht, die durch Art. 2 der Whistleblower-Richtlinie vorgegeben sind, insb. betreffend das öffentliche Auftragswesen, Verhinderung von Geldwäsche und Terrorismusfinanzierung, Produktsicherheit und -konformität, Verkehrssicherheit, Umweltschutz, Lebensmittel- und Futtermittelsicherheit, öffentliche Gesundheit, Verbraucherschutz, Datenschutz, Informationssicherheit, die finanziellen Interessen der Union und Binnenmarktvorschriften (§ 2 Abs. 1 Nr. 3–9 HinSchG). Ergänzend erstreckt sich der sachliche Anwendungsbereich auf Verstöße gegen das nationale Recht, ua. strafbewehrte Verstöße sowie bußgeldbewerte Verstöße gegen Vorschriften, die Leben, Leib oder Gesundheit oder Rechte von Beschäftigten oder ihrer Vertretungsorgane schützen (§ Abs. 1 Nr. 1, 2 und 10 HinSchG); dazu *Dzida*/*Seibt*, NZA 2023, 657, 659 f.

2 Soweit eine gesetzliche Pflicht zur Errichtung einer internen Meldestelle nach § 12 HinSchG besteht, ist ein Mitbestimmungsrecht des Betriebsrats hinsichtlich des „Ob" nach § 87 Abs. 1 BetrVG ausgeschlossen; vgl. Rz. 35.1. Trotz des Spielraums des Unternehmens nach § 14 f. HinSchG, besteht kein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG hinsichtlich der organisatorischen Verortung und der Besetzung der internen Meldestelle. Für eine AGG-Beschwerdestelle hatte das BAG herausgearbeitet, zur mitbestimmungsfreien Organisation des Betriebs zählten die Bestimmung, welche Personen oder Stellen für den Arbeitgeber im Verhältnis zu den Arbeitnehmern Rechte wahrzunehmen und Pflichten zu erfüllen hätten, und die personelle Besetzung (BAG v. 21.7.2009 – 1 ABR 42/08, NZA 2009, 1049 Rz. 20 ff.). Diese Entscheidung ist auf die interne Meldestelle nach dem HinSchG übertragbar; so auch *Zimmer*/*Millfahrt*, BB 2023, 1269, 1270 f.; aA wohl *Bayreuther*, NZA-Beilage 2022, 20, 21; *Badura*/*Brychcy*, DB 2024, 799, 801.

1. Kreis der Hinweisgeber

Meldeberechtigt sind Arbeitnehmer des Unternehmens sowie an das Unternehmen überlassene Leiharbeitskräfte.[5]

2. Meldekanal

Über das digitale Hinweisgebersystem […][6] *können Hinweisgeber online oder telefonisch Informationen über Verstöße im Sinne des § 2 HinSchG melden.*

Verlangt der Hinweisgeber bei Abgabe seiner Meldung eine persönliche Zusammenkunft mit einer zuständigen Person der internen Meldestelle, soll binnen […] Wochen[7] *ein Termin mit dem Hinweisgeber vereinbart werden. Soweit der Hinweisgeber mit einer Zusammenkunft im Wege der Bild- und Tonübertragung nicht einverstanden ist, hat die persönliche Zusammenkunft in Präsenz an einem geeigneten neutralen Ort in Wohnortnähe des Hinweisgebers stattzufinden.*

3. Vertraulichkeit und anonyme Meldungen[8]

Hinweisgeber werden ermutigt, ihre Identität bei der Meldung offenzulegen.[9]

Gibt ein Hinweisgeber eine anonyme Meldung ab, sind die dem Hinweisgeber nach § 17 HinSchG gegenüber abzugebenden Erklärungen sowie die mit ihm erforderliche Kommunikation über das ihm zugewiesene sichere Postfach abzuwickeln.[10]

---

3 Zum Meldeverfahren trifft das HinSchG keine abschließende Regelung, sondern sieht lediglich vor, dass für die internen Meldestellen Meldekanäle einzurichten sind, über die Beschäftigte und an das Unternehmen überlassene Leiharbeitnehmer Informationen über Verstöße melden können (§ 16 Abs. 1 Satz 1 HinSchG). Interne Meldekanäle müssen mündliche Meldungen (telefonisch oder mittels einer anderen Art der Sprachübermittlung) oder Meldungen in Textform ermöglichen (§ 16 Abs. 3 Satz 1 und 2 HinSchG). Nach der Rechtsprechung des BAG betrifft die Einführung und Ausgestaltung eines jedenfalls in gewissen Umfang standardisierten Meldeverfahrens wegen seiner Steuerungswirkung das Ordnungsverhalten der Arbeitnehmer im Betrieb und unterliegt somit der Mitbestimmung nach § 87 Abs. 1 Nr. 1 BetrVG, selbst wenn keine Meldepflicht etabliert ist (BAG v. 21.7.2009 – 1 ABR 42/08, NZA 2009, 1049 Rz. 29 ff.); so zum HinSchG auch *Badura/Brychcy*, DB 2024, 799, 800.

4 Im Falle einer unternehmensweiten internen Meldestelle steht das Mitbestimmungsrecht zur Ausgestaltung des Meldeverfahrens dem Gesamtbetriebsrat zu (BAG v. 21.7.2009 – 1 ABR 42/08, NZA 2009, 1049 Rz. 33).

5 Vgl. § 16 Abs. 1 Satz 1 HinSchG. Über die Öffnung interner Meldekanäle für natürliche Personen, die im Rahmen ihrer beruflichen Tätigkeit mit dem Unternehmen in Kontakt stehen (§ 16 Abs. 1 Satz 3 HinSchG), kann das Unternehmen mangels Zuständigkeit des Arbeitnehmervertretungsgremiums mitbestimmungsfrei entscheiden, sodass diese nicht Gegenstand der Gesamtbetriebsvereinbarung wäre.

6 Hinsichtlich der Einführung und Anwendung der technischen Einrichtung besteht ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG; vgl. Kap. 37. In Anlehnung an die Betriebsvereinbarungen zu technischen Einrichtungen ist hier eine Systembeschreibung sinnvoll.

7 Das HinSchG verlangt die Ermöglichung einer persönlichen Zusammenkunft in angemessener Zeit (§ 16 Abs. 3 Satz 2 und 3). Den äußeren Rahmen dieses Zeitraums bestimmen die Pflichten der internen Meldestelle nach § 17 Abs. 1 Nr. 1 HinSchG, dem Hinweisgeber den Eingang der Meldung spätestens nach sieben Tagen zu bestätigen, und nach § 17 Abs. 2 Satz 1 HinSchG, innerhalb von drei Monaten nach der Bestätigung des Eingangs der Meldung oder im Falle des Fehlens einer Eingangsbestätigung spätestens drei Monate und sieben Tage nach Eingang der Meldung eine Rückmeldung zu geben; dazu *Fischbach* in Thüsing, HinSchG, § 16 HinSchG Rz. 16.

8 Die interne Meldestelle soll auch anonym eingehende Meldungen bearbeiten, wobei keine Verpflichtung besteht, die Abgabe anonymer Meldungen zu ermöglichen (§ 16 Abs. 1 Satz 4 und 5 HinSchG). Das Hinweisgebersystem kann daher die Abgabe anonymer Meldungen technisch ausschließen; *Dzida/Seibt*, NZA 2023, 657, 662.

9 Die Pflicht zur Vertraulichkeit und der Umfang des Vertraulichkeitsgebots sind abschließend in §§ 8 f. HinSchG geregelt.

10 Soweit das Hinweisgebersystem eine anonyme Kommunikation nicht ermöglicht, müsste ggf. die Einschaltung einer Ombudsperson geregelt werden; vgl. dazu *Fischbach* in Thüsing, HinSchG, § 16 HinSchG Rz. 9.

4. Folgemaßnahmen

[…][11]

11 Soweit das Verfahren im HinSchG gesetzlich abschließend geregelt ist, besteht kein Mitbestimmungsrecht des zuständigen Arbeitnehmervertretungsgremiums. Denkbar wären – ggf. freiwillige – Regelungen zur Durchführung interner Untersuchungen (vgl. § 18 Nr. 1 und Nr. 4 lit. a) HinSchG; dazu BAG v. 27.9.2005 – 1 ABR 32/04, NJOZ 2006, 1776).

70.24

M 70.2 Betriebsvereinbarung Ethikrichtlinie

1. Regelungsziel[1]

Die Betriebsparteien[2] stimmen darin überein, dass es dem Direktionsrecht des Arbeitgebers vorbehalten ist, die Leistungspflichten der Arbeitnehmer hinsichtlich Inhalt, Art und Weise, Ort und Zeit der Arbeitsleistung auszufüllen. Zweck dieser Betriebsvereinbarung sind darüber hinausgehende Verhaltenspflichten, die die Zusammenarbeit im Unternehmen und deren Gesetzmäßigkeit sichern sollen und damit nicht zuletzt auch Rufschädigungen des Unternehmens wegen möglichen Fehlverhaltens von Mitarbeitern vermeiden sollen.

2. Mitteilung von Vertrags- oder Gesetzesverstößen

Mitarbeiter, die feststellen, dass es während der Arbeit zu unrechtmäßigem Verhalten gekommen ist oder einen entsprechenden Verdacht haben, müssen[3] ihren Vorgesetzten unverzüglich darüber in Kenntnis setzen. Fürchten sie dadurch Nachteile, steht ihnen das Hinweisgebersystem zur Verfügung.[4]

3. Politik der offenen Tür

In unserem Haus stehen die Türen offen. Wer ein Anliegen hat, spricht seinen Vorgesetzten möglichst direkt an.

4. Geschenke und Zuwendungen

Es ist nicht erlaubt, von Lieferanten, potentiellen Lieferanten oder anderen Personen, die möglicherweise Einfluss auf Geschäftsentscheidungen nehmen möchten, Geschenke oder Zuwendungen anzunehmen, zu erbitten oder zu fördern. Mitarbeiter dürfen auch keine Geschenke oder Zuwendungen von Kunden annehmen, wenn damit eine Arbeit belohnt werden soll, die sie im Rahmen ihres Arbeitsverhältnisses verrichtet haben.[5] Dies gilt nicht für Geschenke oder Zuwendungen mit einem Wert von weniger als Euro 15,–.

5. Respektvoller Umgang untereinander

(1) Beleidigende oder beschimpfende Bemerkungen haben im Betrieb nichts zu suchen. Wer sich selbst über die Wortwahl anderer Personen im Betrieb ärgert, spricht ihn möglichst direkt an und erklärt, warum er Bemerkungen als beleidigend oder herabsetzend empfindet. Jede Art von Belästigung und unangemessenem Verhalten ist dem zuständigen Vorgesetzten zu berichten.

1 Vgl. BAG v. 22.7.2008 – 1 ABR 40/07, BB 2008, 2520 m. Anm. *Sittard*, BB 2008, 2524.
2 Zur Zuständigkeit des örtlichen Betriebsrates, wenn die Konzernspitze im Ausland ansässig ist, vgl. LAG München v. 4.9.2014 – 2 TaBV 50/13, BeckRS 2015, 68238.
3 Das Mitbestimmungsrecht des Betriebsrats greift ein, soweit Verhaltenspflichten begründet werden, die über eine Konkretisierung der Arbeitspflicht hinausgehen, BAG v. 22.7.2008 – 1 ABR 40/07; LAG München v. 4.9.2014 – 2 TaBV 50/13, BeckRS 2015, 68238; uU. auch bei der Pflicht zur Mitwirkung an internen Untersuchungen; BAG v. 27.9.2005 – 1 ABR 32/04, NJOZ 2006, 1776.
4 S. dazu **M 70.1**. Der Gegenstand des Hinweisgebersystems müsste entsprechend erweitert werden.
5 Diese Verpflichtung ergibt sich aus Gesetzen und ist insoweit mitbestimmungsfrei.