Verzeichnis der Redakteure

Redakteur/Redakteurin	**Fach**
Dr. Stephan Beukelmann Rechtsanwalt, FA für Strafrecht, Lohberger & Leipold, München	10000 Wirtschaftsstrafrecht (zusammen mit Rosskopf)
Prof. Dr. Werner Beulke Rechtsanwalt, Passau	12000 Unternehmensinterne Ermittlungen (zusammen mit Ruhmannseder)
Dr. Corinna Boecker Wirtschaftsprüferin, Steuerberaterin, Dr. Kleeberg & Partner GmbH, München	11000 Rechnungslegung und Controlling (zusammen mit Zwirner)
Dr. Anne-Catherine Hahn, LL.M. Rechtsanwältin, IPrime Legal AG, Zürich	S 1000 Compliance in der Schweiz (zusammen mit Livschitz)
Mag. Christina Hartig Wirtschaftsprüferin -abgz. Sachverständige-, Zert. Compliance Officerin, Wien	O 1000 Compliance in Österreich (zusammen mit Ruhmannseder)
Dr. Simone Hartmann Regierungsdirektorin, Referentin, Bundesministerium der Finanzen (BMF), Berlin	7000 Öffentliche Unternehmen (zusammen mit Zwirner)
Dr. Hartmut Henninger Rechtsanwalt, GvW Graf von Westphalen, Hamburg	4000 Exportkontrolle und Außenwirtschaftsrecht
Dr. Thorsten Kuthe Rechtsanwalt, Heuking Kühn Lüer Wojtek, Köln	3000 Bank- und Kapitalmarktrecht (zusammen mit Zipperle)
Dr. Dieter Lehner Rechtsanwalt, FA für Steuerrecht, Zirngibl Rechtsanwälte Partnerschaft mbB, München	1000 Organhaftung und Compliance
Dr. Mark Livschitz Rechtsanwalt, Mark Livschitz AG, Zürich	S 1000 Compliance in der Schweiz (zusammen mit Hahn)

Redakteur/Redakteurin	**Fach**
Prof. Dr. Frank Maschmann Universität Regensburg	2000 Arbeitsrecht und Beschäftigtendatenschutz
Katharina Mitterer, LL.M. Rechtsanwältin, Zirngibl Rechtsanwälte Partnerschaft mbB, München	5000 Information Technology (IT) & Intellectual Property (IP)
Evelyn Niitväli Rechtsanwältin, RCAA Partnerschaft von Rechtsanwälten mbH, Frankfurt/Main	6000 Kartellrecht (zusammen mit Reysen)
Andreas Reuter Rechtsanwalt, Stuttgart	13000 Produkthaftung/ -sicherheit (zusammen mit Wuhrmann)
Dr. Marc Reysen Rechtsanwalt, RCAA Partnerschaft von Rechtsanwälten mbH, Frankfurt/Main	6000 Kartellrecht (zusammen mit Niitväli)
Dr. Christoph Ritzer Rechtsanwalt, Norton Rose Fulbright LLP, Frankfurt/Main	15000 Datenschutzrecht
Dr. Annette Rosskopf, LL.M. Rechtsanwältin, Attorney-at-Law (New York), MichalkeRosskopf Rechtsanwälte PartG mbB, München	10000 Wirtschaftsstrafrecht (zusammen mit Beukelmann)
Dr. Felix Ruhmannseder Rechtsanwalt (RAK Berlin, RAK Wien), wkk law Rechtsanwalts GmbH, Wien	8000 Steuer- und Steuerstrafrecht, 12000 Unternehmensinterne Ermittlungen (zusammen mit Beulke), O 1000 Compliance in Österreich (zusammen mit Hartig)
Michael Werner Syndikusrechtsanwalt, DEGES Deutsche Einheit Fernstraßenplanungs- und -bau GmbH, Berlin	9000 Vergaberecht
Daniel Wuhrmann Rechtsanwalt, Reusch Rechtsanwälte, Berlin	13000 Produkthaftung/ -sicherheit (zusammen mit Reuter)

Redakteur/Redakteurin	**Fach**
Madeleine Zipperle Rechtsanwältin, Heuking Kühn Lüer Wojtek, Köln	3000 Bank- und Kapitalmarktrecht (zusammen mit Kuthe)
Prof. Dr. Christian Zwirner Wirtschaftsprüfer, Steuerberater, Dr. Kleeberg & Partner GmbH, München	7000 Öffentliche Unternehmen (zusammen mit Hartmann), 11000 Rechnungslegung und Controlling (zusammen mit Boecker)

Zitiervorschlag

Compliance aktuell/*Maschmann* Fach 2010 Rn. 4

Inhaltsverzeichnis

Dr. Dieter Lehner[1]

Organhaftung und Compliance

1 Der Verfasser ist Rechtsanwalt und Fachanwalt für Steuerrecht bei Zirngibl, München.

I. Einführung

1 **„Compliance“** ist zum **festen Bestandteil** des **deutschen Rechts** geworden. Verstöße gegen Compliance-Anforderungen dienen nicht selten als Anknüpfungspunkte für **Haftungen von Unternehmen und ihren Managern** (vgl. z.B. *LG München I* Urteil v. 10.12.2018 - 5 HK O 1387/10 = NZG 2014, 345 ff. – Siemens/Neubürger). Auch Aufsichtsorgane können in den Fokus geraten. Die Aktualität des Themas wird durch spektakuläre Fälle wie Wirecard, den VW-Dieselskandal oder die sog. Cum/Ex-Geschäfte belegt.

In den letzten Jahren hat die Zahl der Haftungsfälle erheblich zugenommen. Diese Zunahme geht auf die wachsende **Komplexität der unternehmerischen Tätigkeit und der rechtlichen Rahmenbedingungen** in einem sich wandelnden Umfeld zurück. Daraus resultiert eine deutlich gesteigerte Verantwortung des Managements. Verstärkt wird die Entwicklung durch die **höchstrichterliche Rechtsprechung**. Danach ist der Aufsichtsrat einer Aktiengesellschaft bei Vorliegen von Anhaltspunkten verpflichtet, Ansprüche gegen Vorstandsmitglieder zu prüfen und ggf. zu verfolgen, wenn nicht ausnahmsweise gewichtige Interessen entgegenstehen (*BGHZ* 135, 244 ff. – ARAG/Garmenbeck). Motiviert ist die Inanspruchnahme nicht zuletzt durch das Bestehen von **D & O-Versicherungen** (Directors and Officers-Versicherungen), durch die die Organe von Gesellschaften gegen Vermögensschäden, die durch schuldhafte Pflichtverletzungen entstehen, abgesichert werden. Schließlich spielen die **Bußgeldtatbestände des § 30 OWiG und des § 130 OWiG** eine Rolle. Nach diesen Vorschriften können bei schuldhaften Aufsichtspflichtverletzungen **empfindliche Geldbußen** gegen Manager und auch gegen das Unternehmen festgesetzt werden.

2 Im Folgenden werden die Grundzüge der Compliance dargestellt und in das Haftungsregime der aktienrechtlichen und GmbH-rechtlichen Organhaftung eingefügt. Angesichts der zum Teil existenzvernichtenden Haftungsrisiken stellt sich die Frage nach dem **Umfang** und den **Grenzen** der **haftungsbegründenden Compliance-Verantwortung** der Geschäftsführung, also von Vorständen und Geschäftsführern, sowie des Aufsichtsrats. Die Darstellung gibt einen Überblick über die aktuelle Rechtslage.

II. Grundzüge der Compliance

1. Begriff der Compliance

3 Compliance bedeutet die **Einhaltung der gesetzlichen Bestimmungen, regulatorischen Standards** und der weiteren anwendbaren **Regeln und Richtlinien** (vgl. zum Begriff I/B/P/*Poppe* 1. Kap. Rn. 2). Compliance steht damit für **regelkonformes Verhalten**. Compliance im Unternehmen umfasst aber auch die Vorkehrungen zur Sicherstellung rechtmäßigen Verhaltens sowie zur Risikofrüherkennung und Risikominimierung (vgl. Hauschka*/Hauschka/Moosmayer/Lösler* Compliance

§ 1 Rn. 8). Damit steht Compliance auch für **Organisationspflichten** und **präventive Kontrolle** (Hüffer/*Koch* § 76 Rn. 16a).

2. Compliance-Verantwortung

Die **Verantwortung** dafür, dass sich eine Gesellschaft bei ihren unternehmerischen Aktivitäten an das geltende Recht hält, liegt bei dem **Geschäftsführungsorgan**. So definiert etwa **der Grundsatz 5 Deutscher Corporate Governance Kodex** (DCGK): „Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance)". Damit bestätigt der Kodex, wenngleich er unmittelbar nur auf börsennotierte Aktiengesellschaften Anwendung findet, die geltende Rechtslage (vgl. Spindler/Stilz/*Fleischer* § 91 Rn. 52). **4**

Wie die Compliance-Verantwortung allerdings umzusetzen ist, ist nicht allgemein verbindlich durch den Gesetzgeber festgelegt. Es gehört nämlich zu den Aufgaben der Geschäftsführung – nach einer entsprechenden Risikoanalyse – zu bestimmen, welche organisatorischen Maßnahmen getroffen werden, um regelkonformes Verhalten durch die Unternehmensangehörigen bestmöglich zu gewährleisten. Nicht jeder Regelverstoß im Unternehmen kann verhindert werden und führt zu einer Haftung der verantwortlichen Organe. Es geht vielmehr darum, **systematisches Fehlverhalten zu unterbinde**n, ggf. **Anzeichen zu erkennen** und **Gegenmaßnahmen zu ergreifen** (vgl. *Moosmayer* § 1 Rn. 6). **5**

3. Rechtsgrundlagen

Obwohl im Gesetz nicht ausdrücklich geregelt, ist **allgemein anerkannt**, dass es eine **Rechtspflicht der Unternehmensleitung** gibt, durch **organisatorische Vorkehrungen** für **regelkonformes Verhalten** der Unternehmensangehörigen zu sorgen (Spindler/Stilz/*Fleischer* § 91 Rn. 47 m.w.N., vgl. aber Rn. 59). Die rechtsdogmatische Begründung für diese Pflicht ist noch nicht abschließend geklärt. **6**

Die rechtliche Grundlage der Compliance wird zum Teil in den **Bestimmungen des Ordnungswidrigkeitenrechts** zur Haftung von im Unternehmen aufsichtspflichtigen Personen (§§ 130, 9 OWiG) und zur Haftung des Unternehmens selbst für zurechenbares Fehlverhalten seiner aufsichtspflichtigen Personen (§§ 30, 130, 9 OWiG) gesehen (*Moosmayer* § 2 Rn. 11). Zum Teil wird auch eine Analogie zu **spezialgesetzlichen Vorschriften** gezogen. Jedenfalls stellt die aus der **Leitungsverantwortung folgende Legalitätspflicht der Geschäftsführungsorgane** gem. §§ 76 Abs. 1, 93 Abs. 1 AktG bzw. § 43 GmbHG eine wesentliche Rechtsgrundlage dar (Spindler/Stilz/*Fleischer* § 91 Rn. 50; I/B/P/*Rieder* 2. Kap. Rn. 3; MK-GmbHG/*Fleischer* § 43 Rn. 21)). Schließlich kann das geplante Verbandssanktionengesetz künftig eine Rolle spielen (vgl. *Habersack* NZG 2021, 48 ff.) **7**

4. Compliance-Ziel

8 **Ziel von Compliance** ist es, die **Einhaltung der Gesetze**, der weiteren anwendbaren Bestimmungen und der internen Richtlinien **sicherzustellen**, um damit **Haftungen** oder andere Nachteile für die Gesellschaft, ihre Organe und ihre Mitarbeiter **zu vermeiden** (vgl. Hauschka*/Hauschka/Moosmayer/Löscher* Compliance § 13 Rn. 21). In Betracht kommen hier zivilrechtliche Ansprüche, strafrechtliche Konsequenzen, Bußgelder und öffentlich-rechtliche Sanktionen, aber auch sonstige wirtschaftlich negative Folgen, etwa durch Reputationsschäden oder im Rahmen der Vergabe von öffentlichen Aufträgen.

9 Um das Ziel von Compliance zu erreichen, sind die **unternehmensspezifischen Risiken zu erfassen und zu organisieren**. Die Implementierung eines adäquaten **Compliance Management Systems (CMS)** ist damit der Ausgangspunkt einer wirksamen Compliance-Struktur innerhalb eines Unternehmens (zu den Grundelementen eines Compliance Management Systems Ruhmannseder/Behr/Krakow/*Ruhmannseder/Behr* 2. Kap. Rn. 73 ff.). Compliance Management System bezeichnet die **Gesamtheit** der im Unternehmen eingerichteten **Maßnahmen und Prozesse zur Sicherstellung der Regelkonformität**. Um Schwächen des Systems aufzudecken und neuen Anforderungen zu genügen, sind Maßnahmen zur **kontinuierlichen Überprüfung und Verbesserung** notwendig.

5. Risikoanalyse

10 Die **Anforderungen** an Compliance in einem Unternehmen hängen von den Risiken, denen es ausgesetzt ist, ab. Die spezifischen Risiken sind dabei naturgemäß von Unternehmen zu Unternehmen unterschiedlich und hängen etwa von der ausgeübten Tätigkeit und der Unternehmensgröße ab. Daher ist zunächst eine individuelle, **unternehmensbezogene Risikoanalyse** notwendig. Die Geschäftsführung muss diejenigen Risikobereiche identifizieren, in denen wesentliche Gefahren für nicht regelgerechtes Verhalten bestehen (I/B/P*/Rieder* 2. Kap. Rn. 50). Risikobehaftete Bereiche können beispielsweise der Zahlungsverkehr, die Auftragsannahme und die Auftragsvergabe sein. Hier stellen sich Fragen nach Geldwäsche, Preisabsprachen oder Bestechung. Die Risikoanalyse beschränkt sich aber nicht auf diese allgemein bekannten Themen. Vielmehr können auch weniger herausgehobene Einheiten durch Fehlverhalten erhebliche Schäden verursachen. Dies beweisen etwa der Dieselskandal bei der Volkswagen AG und die Cum/Ex-Geschäfte, die eine Vielzahl von Banken getätigt haben.

11 Bei der Risikoanalyse sind auch die **Geschäftspraktiken der Geschäftspartner** eines Unternehmens nicht zu vernachlässigen. Fehlverhalten von Geschäftspartnern kann zu Haftungen führen, wenn die Gesellschaft die erforderlichen Prüfungshandlungen bei deren Auswahl und Bezahlung unterlassen hat (*Moosmayer* § 1 Rn. 3).

12 Compliance ist somit Teil des Risikomanagements. Eine allgemeine Pflicht, Risiken zu vermeiden, gibt es aber nicht.

6. Organisations- und Überwachungspflichten

Die **Organisation des Unternehmens** muss im **Einklang mit den identifizierten Risiken** stehen. Nach der Analyse der Risiken ist die bestehende Organisation daraufhin zu überprüfen, ob in den erkannten Risikobereichen Regelverstöße möglichst vermieden werden (I/B/P/*Rieder* 2. Kap. Rn. 51). Dabei sind die **Grundfunktionen der Compliance** abzudecken, nämlich **Prävention**, **Aufdeckung von Fehlverhalten** und die **Reaktion** hierauf (*Moosmayer* § 1 Rn. 4). 13

a) Compliance-Organisation

Die Compliance-Organisation kann unterschiedlich ausgestaltet werden. Dabei gibt es keine zwingenden Vorgaben. Allerdings lassen sich zwei Grundmodelle unterscheiden: Die Compliance-Aufgaben können den **einzelnen Fachabteilungen** innerhalb der Unternehmensorganisation zugeordnet und jeweils **Compliance-Verantwortliche** bestimmt werden. Möglich ist aber auch eine **eigenständige Compliance-Organisation**, die in die Unternehmensstrukturen eingebettet ist (I/B/P/*Hülsberg/Laue* 3. Kap. Rn. 8 ff.). Regelmäßig wird zumindest in größeren Unternehmen ein Compliance-Beauftragter benannt, vielfach als „Chief Compliance Officer" bezeichnet. 14

b) Delegation

Besteht das Geschäftsführungsorgan aus mehreren Personen, sind diese gemeinschaftlich zur Geschäftsführung verpflichtet. Selbstverständlich kann sich jedoch nicht jedes Mitglied der Geschäftsführung um sämtliche Aufgaben im Unternehmen selbst kümmern. 15

Zulässig ist es daher, Aufgabenbereiche an **einzelne Mitglieder der Geschäftsführung zu delegieren,** sog. **horizontale Delegation** (vgl. Bürgers/Körber/Lieder/*Bürgers* § 77 Rn. 15). Dies gilt **auch für die Compliance-Verantwortung**. Durch die horizontale Delegation reduziert sich das Haftungsrisiko der übrigen Mitglieder der Geschäftsführung, wenngleich es bei einer **Kontroll- und Aufsichtspflicht** des Gesamtorgans zwingend verbleibt (vgl. Hauschka/*Schmidt-Husson* Compliance § 6 Rn. 12). Die **Übertragung** von Verantwortung auf ein bestimmtes Mitglied der Geschäftsführung erfolgt im Rahmen der **Geschäftsverteilung,** etwa durch die Geschäftsordnung für die Geschäftsführung. 16

Soweit Aufgaben nicht ausnahmsweise explizit dem Geschäftsführungsorgan zwingend zugewiesen sind, können diese Aufgaben auf hierarchisch nachgeordnete Personen übertragen werden (Hauschka/*Schmidt-Husson* Compliance § 6 Rn. 8 m.w.N.). Bei der **vertikalen Delegation** von Aufgaben an nachgeordnete Mitarbeiter sind funktionsfähige **Kontrollstrukturen** einzurichten, um ein Fehlverhalten der Mitarbeiter im Vorfeld zu verhindern sowie ggf. aufzudecken und abzustellen, sogenannte **Überwachungspflicht** (Spindler/Stilz/*Fleischer* § 93 Rn. 100 ff. m.w.N.). Diese Überwachungspflicht umfasst die **ordnungsgemäße Auswahl, Einweisung** 17

und Kontrolle der Mitarbeiter. Weiterhin muss gewährleistet sein, dass die notwendigen **Informationen** an die Geschäftsführung gelangen.

18 Zulässig ist schließlich die **Delegation an externe Dritte** (Hauschka/*Schmidt-Husson* Compliance § 6 Rn. 9). Für die Organisations- und Überwachungspflichten gelten dabei die gleichen Grundsätze wie bei der vertikalen Delegation.

19 Die **Überwachungspflicht** trifft **jedes Mitglied des Geschäftsführungsorgans** ab **Beginn seiner Tätigkeit** für die Gesellschaft. Bei der Übertragung von bestimmten Aufgaben auf einzelne Mitglieder der Geschäftsführung trägt das **jeweilige Organmitglied** ab Inkrafttreten der **Geschäftsverteilung** die volle **Handlungsverantwortung** für das ihm zugewiesene Ressort (*Fleischer* § 8 Rn. 9 m.w.N.). Ab diesem Zeitpunkt ist das Organmitglied verpflichtet, in seinem Zuständigkeitsbereich für die Einrichtung funktionsfähiger Strukturen zu sorgen.

c) Aufbau- und Ablauforganisation

20 Die Geschäftsführung ist verpflichtet, für eine **geeignete Aufbau- und Ablauforganisation** zu sorgen (Spindler/Stilz/*Fleischer* § 93 Rn. 56). Die Einrichtung einer solchen Organisation setzt die **Bestimmung der Zuständigkeiten** der Mitarbeiter und die **Festlegung der Geschäfts- bzw. Prozessabläufe** einschließlich der notwendigen Kontrollen voraus. Die Geeignetheit der Aufbau- und Ablauforganisation ist zu überwachen und **regelmäßig neu zu bewerten**. An neue Gegebenheiten ist die Organisation anzupassen, etwaige Unzulänglichkeiten sind zu beseitigen (Spindler/Stilz/*Fleischer* § 93 Rn. 101 ff.).

21 Die Geschäftsführung hat durch geeignete organisatorische Maßnahmen dafür zu sorgen, dass die Mitarbeiter auf jeder Hierarchieebene in ihre **Verantwortlichkeit eingewiesen** und ihnen die **übertragenen Aufgaben erläutert** werden (Spindler/Stilz/*Fleischer* § 93 Rn. 103 m.w.N.). Die **Einweisung und Erläuterung** muss nicht durch die Geschäftsführung erfolgen, sondern **kann delegiert werden**.

d) Einrichtung von Kontrollstrukturen

22 **Art und Umfang der Kontrolle** der Mitarbeiter hängen von der Bedeutung der übertragenen **Aufgabe** und der **Person** ab, die die übertragene Aufgabe wahrnimmt (Spindler/Stilz/*Fleischer* § 93 Rn. 104 ff. m.w.N.). Die Angemessenheit und Funktionsfähigkeit der Kontrolle ist auf der Grundlage der identifizierten Risiken zu beurteilen.

23 Die Funktionsfähigkeit einer in den Prozess **integrierten Kontrolle** (prozessabhängige oder prozessimmanente Kontrolle) ist durch eine **prozessunabhängige Stelle**, z.B. die interne Revision, sicherzustellen (prozessunabhängige Kontrolle).

24 Nicht ausreichend ist die einmalige Einrichtung funktionsfähiger Kontrollstrukturen. Vielmehr besteht die Verpflichtung, die **Geeignetheit der Kontrollstrukturen** kontinuierlich zu **überwachen, anzupassen und fortzuentwickeln**.

Unabhängig von der Einrichtung eines Kontrollsystems besteht die Notwendigkeit für einen **reibungslosen Informationsfluss** zu sorgen und Informationsquellen zu schaffen, die es der Geschäftsführung erlauben, möglichst zuverlässig, früh und unmittelbar von Missständen zu erfahren (vgl. *OLG Düsseldorf* CCZ 2010, 117, 118 ff.). Aufgrund ihrer Prozesseinbindung erlangen oftmals die Mitarbeiter der unteren Hierarchieebenen als Erste Kenntnis von etwaigen Missständen oder Fehlverhalten. Ein Informationssystem ist daher erforderlich, um im Notfall erforderliche Maßnahmen zeitnah ergreifen zu können (vgl. Krieger/Schneider/*Vetter* § 18 Rn. 68 m.w.N.). **25**

e) Kontrolle der Tochtergesellschaften

Die Pflicht zur Leitung der Gesellschaft umfasst auch die **Steuerung und Überwachung** von in- und ausländischen **Beteiligungsgesellschaften**. Die Geschäftsführung hat die Geschäftstätigkeiten der Tochtergesellschaften zu steuern und die Tochtergesellschaften in die Organisation zur Vermeidung von Rechtsverstößen einzubeziehen (vgl. MK-AktG/*Spindler* § 76 Rn. 46 ff.). Die **Möglichkeiten zur Einflussnahme** und die sich fürdie Geschäftsführung ergebenden Pflichten sind hier nicht einheitlich. Sie hängen maßgeblich von dem **jeweiligen Rechtsregime**, das für die Tochtergesellschaft gilt, ab. **26**

f) Gesteigerte Überwachungspflicht

Bei **greifbaren Anhaltspunkten** für Regelverstöße ist die Geschäftsführung verpflichtet, umfassende **Prüfungen vorzunehmen**, erkennbare **Missstände abzustellen** und **Vorkehrungen gegen weitere Regelverstöße** zu treffen. Nicht jedes außergewöhnliche Geschäft führt allerdings zu einer Prüfungspflicht der Geschäftsführung. Vielmehr müssen sich die Anhaltspunkte gerade auf mögliche Regelverstöße beziehen. Anderenfalls führte dies zu einer Art Erfolgshaftung der Geschäftsführung, für rechtmäßiges Verhalten der Mitarbeiter zu sorgen. **27**

Eine Prüfungspflicht entsteht aber auch dann, wenn die **organisatorischen Abläufe** geändert werden. Dies gilt namentlich für diejenigen Bereiche, in denen unternehmensspezifische Risiken bestehen. Diese gesteigerte Pflicht folgt aus der Notwendigkeit, die Geeignetheit der Organisation kontinuierlich zu beobachten und weiter zu entwickeln. **28**

g) Strukturen in der Praxis

In der Compliance-Praxis haben sich gewisse Üblichkeiten zur Umsetzung der Compliance-Verantwortung etabliert. Bei der Implementierung ist in der Praxis darauf zu achten, dass die jeweils anwendbaren gesetzlichen Regelungen berücksichtigt, z.B. arbeitsrechtliche oder datenschutzrechtliche Anforderungen erfüllt werden. **29**

aa) „Tone from the top“

30 Die **Effektivität** und der **Erfolg** der Compliance hängen davon ab, dass die **Geschäftsleitung** sich klar und eindeutig **zu rechtskonformem Verhalten im Geschäftsverkehr bekennt**. Sie muss unmissverständlich deutlich machen, dass rechtswidriges Handeln im Unternehmen nicht geduldet und auf solche Geschäfte verzichtet wird, die nur durch Rechtsbruch zustande kommen. Erforderlich ist eine **dauerhafte und nachhaltige** Ansprache der Mitarbeiter, die von der Unternehmensführung glaubhaft vorgelebt wird (I/B/P/*Inderst/Steiner* 3. Kap. Rn. 2 ff.). Die Geschäftsleitung muss also mit gutem Beispiel vorangehen.

bb) Aufgabenzuweisung, Berichtswege

31 Die Zuständigkeiten und Verantwortlichkeiten müssen klar geregelt sein und sich eindeutig und nachvollziehbar aus der **Aufbau- und Ablauforganisation** ergeben. Wichtig sind **klare Zuständigkeiten, Berichtswege, Arbeitsabläufe und Zustimmungsanforderungen.** Die wesentlichen Bestandteile der Organisation sollten schriftlich niedergelegt werden (vgl. I/B/P/*Rieder* 2. Kap. Rn. 54).

cc) Verhaltenskodex (Code of Conduct)

32 In einem **Code of Conduct** werden möglichst übersichtlich und **allgemein verständlich Regelungen und Verhaltensanforderungen an Compliance** zusammengefasst. Der Code of Conduct hat unternehmensweite Gültigkeit und wird von der Geschäftsführung in Kraft gesetzt (*Moosmayer* § 4 Rn. 155). Die Anforderungen an den Inhalt hängen vom jeweiligen Unternehmen und seinem Risikoprofil ab. Üblicherweise enthält der Code of Conduct Aussagen zumindest zu folgenden Komplexen:

- Schutz vor Diskriminierung,
- Datenschutz,
- Wettbewerbs- und Kartellrecht,
- Beachtung der Menschenrechte,
- Bestechlichkeit,
- Verhalten gegenüber Amtsträgern,
- Ausschluss von Interessenskonflikten,
- Geschenke und Einladungen,
- Einhaltung von Umweltstandards.

33 Die vorstehende Aufzählung ist naturgemäß nicht abschließend (s. zum Inhalt des Code of Conduct etwa Bay/Hastenrath/*Borowa* Kap. 5 Rn. 84).

dd) Schulungen

34 Compliance-Themen betreffen teilweise **komplexe rechtliche Fragestellungen**. Die Effektivität der Compliance erfordert daher eine **professionelle Schulung** der Mitarbeiter, damit die im Unternehmen zu beachtenden Regeln von den Mit-

arbeitern nachvollzogen und korrekt angewendet werden können (I/B/P/*Inderst/Steiner* 3. Kap. Rn. 74 ff.). Dabei müssen selbstverständlich nicht alle Mitarbeiter in allen Bereichen, die im Unternehmen risikobehaftet sind, geschult werden. Wesentlich ist, dass die einzelnen Mitarbeiter spezifisch zu den von ihnen verantworteten Themen Schulungen erhalten. Dies kann durch Präsenzschulungen ebenso wie durch E-Learning Tools erfolgen. Der Lernerfolg sollte nachgehalten werden.

ee) Hinweisgebersystem („Whistleblower-System")

35 Durch geeignete **Hinweisgebersysteme** wird Mitarbeitern, aber auch Dritten, die Möglichkeit gegeben, **Compliance-Verstöße zu melden** (Ruhmannseder/Behr/Krakow/*Ruhmannseder/Behr* 1. Kap. Rn. 9). Damit ein derartiges System funktioniert, ist auf **Vertraulichkeit und Anonymität** zu achten. Ein derartiges „Whistleblower-System" kann beispielsweise ein interner oder externer Ombudsmann oder eine Telefonhotline sein. Das Hinweisgebersystem dient dazu, dass die Geschäftsleitung **Informationen über Compliance-Verstöße** tatsächlich erhält, ohne dass der Hinweisgeber Nachteile zu befürchten hat. Ende 2019 hat die EU eine Richtlinie zum Schutz von Whistleblowern verabschiedet (EU-Richtlinie 2019/1937), mit Frist zur Umsetzung in nationales Recht bis zum 16.12.2021.

ff) Kontrolle, Aufklärung und Ahndung

36 Die **Einhaltung der Compliance-Anforderungen** ist durch **geeignete Kontrollen** sicherzustellen. Dazu dienen neben den in der jeweiligen organisatorischen Einheit etablierten Kontrollmechanismen (prozessabhängige Kontrolle) auch von der jeweiligen Einheit unabhängige Kontrollen (prozessunabhängige Kontrolle), z.B. durch die interne Revision. Ein adäquates Mittel für Kontrollen sind **unangekündigte Stichproben** durch einen Compliance-Verantwortlichen. Darüber hinaus bedarf es regelmäßig formeller, **systematischer Prüfungen** der Risikobereiche im Unternehmen (**Compliance Audit**), in deren Mittelpunkt häufig die Befragung der Mitarbeiter steht. Soweit sich greifbare Anhaltspunkte für Rechtsverstöße ergeben, ist sicherzustellen, dass die Geschäftsleitung von diesen Anhaltspunkten Kenntnis erlangt. Den Anhaltspunkten für Rechtsverstöße ist durch die Geschäftsführung nachzugehen, aufgedeckte Missstände sind abzustellen.

gg) Richtlinien

36a Stehen die risikobehafteten Bereiche eines Unternehmens fest, empfehlen sich Richtlinien und Vorgaben zur Steuerung der identifizierten Risiken. Die Richtlinien enthalten abstrakte Regelungen für den Umgang mit Risikosituationen. Die Geschäftsleitung hat durch geeignete Maßnahmen sicherzustellen, dass der einzelne Mitarbeiter die Richtlinien in der konkreten Situation richtig versteht und umsetzen kann (Ruhmannseder/Behr/Krakow/*Ruhmannseder/Behr* 2. Kap. Rn. 34 ff.), etwa durch Schulungen.

h) IDW PS 980

37 Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) hat den Prüfungsstandard **„Grundsätze ordnungsgemäßer Prüfung von Compliance Management Systemen (IDW PS 980)"** verabschiedet. Zwar richtet sich dieser Standard an die Wirtschaftsprüfer und bestimmt den Inhalt der Prüfung von Compliance Management Systemen. Aus dem IDW PS 980 lassen sich aber Anforderungen an eine „Good Practice" für Compliance ableiten (vgl. I/B/P/*Inderst/Steiner* 3. Kap. Rn. 104 ff.).

38 Der IDW PS 980 stellt einen Standard für eine betriebswirtschaftlich konzipierte Systemprüfung zur Verfügung, kann aber auftretende Rechtsrisiken kaum sachkundig beurteilen und situationsbedingte Organpflichten nicht erfassen (*Fleischer* NZG 2014, 321, 325). **Ein positives Prüfungsurteil kann daher Haftungsrisiken für Organe reduzieren** (I/B/P/*Inderst/Steiner* 3. Kap. Rn. 134), **führt aber nicht generell zur Enthaftung** (*Fleischer* NZG 2014, 321, 325 m.w.N.).

i) ISO 19600, weitere Standards

39 Wie bereits ausgeführt, ist die Rechtskonformität im Unternehmen das zentrale Element von Compliance Management Systemen. Die internationale Organisation für Normung (ISO) hat die **ISO-Norm 19600 „Compliance Management Systems Guideline"** erarbeitet. Diese Norm beinhaltet internationale Maßstäbe für Compliance Management Systeme. Sie soll bei dem **Nachweis regelkonformen Verhaltens in behördlichen Ermittlungs- oder zivilrechtlichen Haftungsverfahren** helfen. Eine generelle Enthaftung kann aber aus den unter vorstehend Rn. 38 f. genannten Gründen nicht erreicht werden.

39a Daneben existieren weitere nationale und internationale Standards (vgl. z.B. Ruhmannseder/Behr/Krakow *Ruhmannseder/Behr* 2. Kap. Rn. 48 ff.).

39b Von wachsender Bedeutung für die Unternehmensführung sind Kriterien, die unter dem Begriff **„Enviromental Social Governance"** (ESG) zusammengefasst sind. Dabei handelt es sich um Standards für die Beachtung und Bewertung der unternehmerischen Verantwortung vor allem unter ökologischen und gesellschaftlichen Gesichtspunkten auf freiwilliger Basis. Für kapitalmarktorientierte Unternehmen sowie Kreditinstitute, Finanzdienstleistungsinstitute und Versicherungsunternehmen besteht die Verpflichtung, Erklärungen, mit dem Ziel, dem Markt Informationen über ökologische und soziale Aspekte der Unternehmenstätigkeit bereitzustellen, abzugeben. Die im Jahr 2014 verabschiedet der EU-CSR (**Corporate Social Responsibility**, EU-Richtlinie 2014/95/EU) wurde durch das CSR-Richtlinie-Umsetzungsgesetz in nationales Recht umgesetzt. Die EU-Kommission hat im April 2021 einen Vorschlag zur Änderung der aktuellen Richtlinie vorgelegt und will mit der Corporate Sustainability Reporting Directive die bestehende Pflicht zur Nachhaltigkeitsberichterstattung erweitern. Spezielle Anforderungen an die Compliance-Verantwortung der Geschäftsführung ergeben sich aus der Enviromental Social Governance nicht.

7. Dokumentation

Die Erfüllung der dargestellten Anforderungen an die Risikoanalyse und die Erfüllung der Organisations- und Überwachungspflichten sollte sorgfältig dokumentiert werden (*Freund* NZG 2015, 1419, 1424). Die Dokumentation ist erforderlich, um den **Beweis** des pflichtgemäßen Verhaltens führen zu können, sofern Compliance-Verstöße Gegenstand eines zivilrechtlichen **Haftungsprozesses** oder eines **behördlichen Ermittlungsverfahrens** sind. **40**

III. Haftung des Vorstands

1. Organhaftung

Für die Organhaftung von Vorständen einer Aktiengesellschaft und von GmbH-Geschäftsführern gelten ähnliche Grundsätze. **40a**

Vorstandsmitglieder, die schuldhaft ihre **Pflicht verletzen**, sind der Gesellschaft gem. § 93 Abs. 2 S. 1 AktG zum **Ersatz des der Gesellschaft daraus entstehenden Schadens** verpflichtet. Dies gilt auch für Verstöße gegen Compliance-Pflichten. Die Regelung ist **zwingendes Recht** und kann nicht durch die Satzung oder den Anstellungsvertrag abbedungen oder abgeschwächt werden (Hüffer/*Koch* AktG § 93 Rn. 2). **41**

Eine § 93 Abs. 2 S. 1 AktG entsprechende Regelung enthält § 43 Abs. 2 GmbHG für GmbH-Geschäftsführer. **41a**

a) Pflichtverletzung

Die Vorstandsmitglieder leiten gem. § 76 Abs. 1 AktG die Geschäfte der Gesellschaft in eigener Verantwortung. Dabei haben sie nach § 93 Abs. 1 S. 1 AktG die **Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters** anzuwenden. § 93 Abs. 1 S. 1 AktG ist nach herrschender Meinung sowohl **Verhaltenspflicht**, als auch **Verschuldensmaßstab**. Nach § 43 Abs. 1 treffen GmbH-Geschäftsführer die gleichen Sorgfaltspflichten. **42**

Zu den **wesentlichen Pflichten von Vorständen und Geschäftsführern** gehört es, **sich selbst** im Rahmen ihrer Amtsführung **gesetzestreu** zu verhalten (statt aller Bürgers/Körber/Lieder/*Bürgers/Israel* § 93 Rn. 7; *Freund* NZG 2021, 579, 579 m.w.N.). Daneben besteht die Pflicht, **regelkonformes Verhalten** von Organen, Mitarbeitern und Konzernunternehmen durch Organisation und Kontrolle sicherzustellen (vgl. I/B/P/*Rieder* 2. Kap. Rn. 4). Compliance ist also Teil der **Sorgfalts- und Legalitätspflicht der Geschäftsführungsorgane**. **43**

aa) Grundsatz der Gesamtverantwortung

Grundsätzlich sind sämtliche Mitglieder der Geschäftsführung für die sorgfaltsgerechte Führung der Geschäfte der Gesellschaft nach dem sogenannten **Grundsatz der Gesamtverantwortung** gemeinsam verantwortlich. Einzelnen Mitglie- **44**

dern können aber **bestimmte Aufgabenbereiche** zur eigenverantwortlichen Leitung **übertragen** werden. Besteht eine solche **Aufgabenverteilung**, führt dies zu einer **Zweiteilung der Aufgaben** der Geschäftsführung in eine **unmittelbar verwaltende** und in eine **beaufsichtigende** Tätigkeit (Spindler/Stilz/*Fleischer* § 77 Rn. 47 m.w.N.; MK-GmbHG/*Fleischer* § 43 Rn. 112).

45 Diese allgemeinen Grundsätze zur Gesamtverantwortung und die **Möglichkeit der Geschäftsverteilung** gelten auch für die Pflicht, durch geeignete organisatorische Maßnahmen Rechtsverstöße zu vermeiden, aufzudecken und zu ahnden. Dem **Gesamtvorstand** obliegt insoweit die **oberste Organisations- und Koordinationsverantwortung**, so dass es für die grundlegenden Ausgestaltungsfragen trotz Geschäftsverteilung bei der Gesamtverantwortung der Geschäftsführung verbleibt (KölnKomm-AktG/*Mertens/Cahn* § 91 Rn. 36). Im Übrigen kann die Organisations- und Überwachungspflicht sowohl Gegenstand der Geschäftsverteilung als auch der Delegation auf nachgeordnete Mitarbeiter sein.

bb) Ressortverantwortung

46 Jedes Mitglied des Geschäftsführungsorgans ist für die sorgfaltsgerechte Geschäftsführung in dem ihm zugewiesenen Zuständigkeitsbereich verantwortlich. Im Rahmen dieser **Ressortverantwortung** trifft das Mitglied auch die Pflicht, durch geeignete organisatorische Maßnahmen für rechtmäßiges Verhalten der Mitarbeiter in seinem Ressort zu sorgen.

47 Das Mitglied des Geschäftsführungsorgans muss daher die ihm berichtspflichtigen Mitarbeiter laufend überwachen. **Soweit es greifbare Anhaltspunkte für Gesetzesverletzungen** bzw. Unregelmäßigkeiten hat, ist es verpflichtet, Untersuchungen einzuleiten und ggf. geeignete Vorkehrungen gegen weitere Verstöße zu treffen (Spindler/Stilz/*Fleischer* § 93 Rn. 107 m.w.N.). Zudem ist die Geeignetheit der Organisation kontinuierlich zu beobachten und bei Veranlassung hierzu zu überprüfen und anzupassen. Das Vorstandsmitglied bzw. Mitglied der GmbH-Geschäftsführung hat in geeigneter Form sicherzustellen und zu überwachen, dass die Mitarbeiter in ihrem jeweiligen Zuständigkeitsbereich die von ihm getroffenen Anweisungen beachten. Die Überwachungsaufgabe kann auf unmittelbar **berichtspflichtige Führungskräfte delegiert** werden.

48 Über Maßnahmen von **besonderer Bedeutung** für die Gesellschaft darf das ressortverantwortliche Vorstandsmitglied bzw. Mitglied der GmbH-Geschäftsführung nicht alleine entscheiden. Wegen des Grundsatzes der Gesamtverantwortung ist für solche Entscheidungen der **Gesamtvorstand zuständig** (MK-AktG/*Spindler* § 77 Rn. 60 m.w.N.).

49 Das **ressortverantwortliche Mitglied des Geschäftsführungsorgans** ist verpflichtet, seine Geschäftsführung an etwaigen **Entscheidungen des Gesamtgremiums** auszurichten bzw. dessen Entscheidungen in seinem Zuständigkeitsbereich umzusetzen (MK-AktG/*Spindler* § 77 Rn. 33).

cc) Ressortübergreifende Überwachungspflicht

Die **Ressortverantwortung** des zuständigen Vorstandsmitglieds beseitigt die **Verantwortung der übrigen Vorstandsmitglieder** nicht. Soweit einem Vorstandsmitglied ein bestimmter Aufgabenbereich zugewiesen wurde, tragen die übrigen Vorstandsmitglieder zwar nicht mehr die volle Verantwortung für diesen Aufgabenbereich. Mit der Geschäftsverteilung soll nämlich die Verantwortlichkeit für ein bestimmtes Ressort gerade auf das jeweils ressortverantwortliche Vorstandsmitglied delegiert werden. Dies gilt auch und gerade für die Organisations- und Überwachungspflicht. Jedes Vorstandsmitglied ist aber verpflichtet, die ordnungsgemäße Leitung der übrigen Ressorts zu überwachen (Spindler/Stilz/*Fleischer* § 77 Rn. 49 ff.). Art und Umfang dieser Überwachungspflicht sind einzelfallabhängig. Dabei gilt der Grundsatz, dass jedes Vorstandsmitglied darauf vertrauen kann, dass die übrigen Vorstandsmitglieder sich in ihrem Pflichtenkreis ordnungsgemäß verhalten, **sog. Vertrauensgrundsatz** (vgl. MK-AktG/*Spindler* § 77 Rn. 58 m.w.N.). Anderenfalls hätte die regelmäßig auf fachlichen Gründen beruhende Ressortbildung und Geschäftsverteilung keinen Sinn. **50**

Das aufsichtspflichtige Vorstandsmitglied muss andere Ressorts daher **nicht generell beaufsichtigen**, es genügt eine kritische Begleitung der Geschäftsführung im Sinne einer Plausibilitätskontrolle. Soweit das Vorstandsmitglied **greifbare Anhaltspunkte** dafür hat, dass die Geschäfte in einem anderen Ressort nicht ordnungsgemäß geführt werden, sind die Missstände aufzuklären und ggf. dem Gesamtvorstand zur Kenntnis zu bringen (vgl. MK-AktG/*Spindler* § 77 Rn. 59). Die Überwachungspflicht ist umso intensiver, (1) je mehr Auffälligkeiten und Unregelmäßigkeiten in dem betroffenen Ressort in der Vergangenheit aufgetreten sind, (2) je kürzer das Vorstandsmitglied die ihm zugewiesene Aufgabe wahrnimmt oder (3) je bedeutender die Angelegenheit für das Unternehmen ist (Spindler/Stilz/*Fleischer* § 77 Rn. 51 ff.). **51**

Die vorstehenden Grundsätze gelten auch für GmbH-Geschäftsführer (vgl. MK-GmbHG/*Fleischer* § 43 Rn. 248). **51a**

dd) Unternehmerisches Ermessen („Business Judgement Rule")

Gem. § 93 Abs. 1 S. 2 AktG verstößt ein Vorstandsmitglied nicht gegen seine Sorgfaltspflicht, wenn es bei einer **unternehmerischen Entscheidung annehmen durfte**, auf der Grundlage **angemessener Information** zum **Wohl der Gesellschaft** zu handeln (**„Business Judgement Rule"**). Bei § 93 Abs. 1 S. 2 AktG handelt es sich um eine unwiderlegbare Vermutung objektiv pflichtgemäßen Verhaltens (Hüffer/*Koch* § 93 Rn. 14 m.w.N.). **52**

Dem Vorstand steht ein **weiter Beurteilungsspielraum** zu, der grundsätzlich nur sehr eingeschränkt der **richterlichen Prüfung zugänglich** ist (vgl. *Kocher* CCZ 2009, 215, 216). Die Prüfung beschränkt sich auf die Einhaltung der normativen Vorgaben sowie der Grundregeln ordnungsgemäßer Unternehmensführung. Die Frage der Zweckmäßigkeit einer Geschäftsführungsmaßnahme betrifft hingegen **53**

den nicht überprüfbaren Ermessensspielraum des Vorstands (*OLG Naumburg* NZG 2001, 136 [zur GmbH]). Ob ein objektiv evidentes Fehlverhalten der Organmitglieder vorlag oder sich eine Entscheidungsalternative offensichtlich aufdrängte, ist stets **ex ante** zu beurteilen. (Schmidt/Lutter/*Krieger/Sailer-Coceani* § 93 Rn. 10 ff.). Maßgeblich ist also allein der **Zeitpunkt, in dem das Vorstandsmitglied seine Entscheidung getroffen bzw. Handlung ausgeführt hat** (*BGH* NJW 2009, 850, 852). Selbst wenn es in der Folge wider Erwarten zu einem Schaden kommt, obwohl ein solcher aus der allein maßgeblichen ex ante-Perspektive nicht vorhersehbar war, ändert dies nichts an der fehlenden Pflichtverletzung (*BGH* NJW 2009, 850, 852). Der Schluss von einem Schaden auf eine Pflichtverletzung **ex post ist unzulässig**. In der Praxis ist allerdings zu beobachten, dass die Business Judgement Rule vor allem auf Grund der Schärfe der gesetzlichen Regelung und der höchstrichterlichen Rechtsprechung keinen ausreichenden Schutz für die Vorstände darstellt (*Freund* NZG, 2021, 579, 580 ff.).

54 Die Business Judgement Rule setzte voraus (vgl. zu den Voraussetzungen der Business Judgement Rule z.B. Hüffer/*Koch* § 93 Rn. 15 ff. m.w.N.), dass

- es sich um eine unternehmerische Entscheidung handelt,
- der Vorstand auf der Basis angemessener Information entscheidet,
- der Vorstand vernünftigerweise annehmen kann, zum Wohl der Gesellschaft zu handeln und
- der Vorstand frei von Interessenkonflikten und ohne Eingehung existenzgefährdender Risiken handelt.

55 Eine Sorgfaltspflichtverletzung ist nur dann gegeben, wenn – bei angemessener Informationsgrundlage – das mit einer unternehmerischen Entscheidung verbundene Risiko vom Vorstand in unverantwortlich falscher Weise beurteilt wurde (Hüffer/*Koch* § 93 Rn. 23). Es muss ein Leitungsfehler vorliegen, der auch für einen Außenstehenden derart evident ist, dass sich das Vorliegen eines Fehlers aufdrängt (MK-AktG/*Spindler* § 93 Rn. 65).

56 Die Business Judgement Rule findet allerdings auf **rechtlich gebundene Entscheidungen** keine Anwendung. Eine Einschränkung der Pflicht zu rechtskonformem Verhalten lässt sich aus der Business Judgement Rule daher nicht ableiten (vgl. Bürgers/Körber/Lieder/*Bürgers/Israel* § 93 Rn. 11). Daher sind auch Pflichtverletzungen, die für die Gesellschaft (vermeintlich) **nützlich** sind, Pflichtverletzungen (statt aller KölnKomm-AktG/*Mertens* § 93 Rn. 34). Der Vorstand darf daher die Entscheidung über rechtmäßiges Verhalten nicht von einer Kosten-Nutzen-Analyse abhängig machen (I/B/P/*Rieder* 2. Kap. Rn. 4 m.w.N.).

57 Während die Einhaltung der gesetzlichen Vorgaben eine Pflicht des Vorstands darstellt, ändert sich diese Einschätzung nach der herrschenden Literaturmeinung bei Vertragsverletzungen. Hier kann es der Vorstand nach sorgfältiger Abwägung der Risiken und Chancen für das Unternehmen auch auf einen Schadenersatz ankommen lassen (MK-AktG/*Spindler* § 93 Rn. 102 m.w.N.).

Gegenstand einer unternehmerischen Entscheidung kann sowohl ein **positives Tun** als auch ein **Unterlassen** sein. Besteht ausnahmsweise die Verpflichtung zu einem bestimmten Tun oder einem bestimmten Unterlassen, liegt keine unternehmerische Entscheidung vor. Das Vorstandsmitglied kann sich dann nicht auf unternehmerisches Ermessen berufen (*Fleischer* ZIP 2004, 685 ff. m.w.N.). **58**

Für die Verpflichtung des Vorstands, **Maßnahmen zur Vermeidung von Rechtsverstößen** im Unternehmen zu ergreifen, ist nach wohl überwiegender Meinung in der Literatur zu unterscheiden: Die Pflicht des Vorstands für eine ordnungsgemäße Unternehmensorganisation zu sorgen, d.h. **das „Ob" beinhaltet keine unternehmerische Entscheidung** (*LG München I* NZG 2014, 345, 348; a.A. Hauschka/*Hauschka/Moosmayer/Lösler* § 1 Rn. 30 f.). Die Art und Weise der Pflichterfüllung, d.h. **das „Wie" stellt eine unternehmerische Entscheidung dar**, auf die die Business Judgement Rule anwendbar ist, sogenanntes Organisationsermessen (Spindler/Stilz/*Fleischer* § 91 Rn. 53; *Meier-Grewe* BB 2009, 2555, 2556). **Unterlässt es die Geschäftsführung vollständig, grundlegende Organisationsstrukturen** einzurichten, liegt bereits darin nach der hier vertretenen Auffassung eine Pflichtverletzung. Bei der Frage, ob eine **funktionsfähige Struktur** einzurichten ist, handelt es sich um eine aus der Legalitätspflicht folgende, **gebundene Entscheidung**. Ein Organisationsermessen besteht insoweit nicht. **59**

Die Ordnungsmäßigkeit der Organisation hat jedenfalls für die von dem Vorstand zu treffenden einzelnen unternehmerischen Entscheidungen nicht zu unterschätzende Auswirkungen. Denn gerade **klare Berichtswege** und **funktionsfähige Kontrollstrukturen** im Rahmen der Organisation führen dazu, dass unternehmerische Entscheidungen des Vorstands auf **angemessener Informationsgrundlage** getroffen werden. § 93 Abs. 1 S. 2 AktG erfordert eine sorgfältige Ermittlung der Entscheidungsgrundlagen. Nach der höchstrichterlichen Rechtsprechung muss der Vorstand in der konkreten Entscheidungssituation **alle verfügbaren Informationsquellen** tatsächlicher und rechtlicher Art ausschöpfen und auf dieser Grundlage die Vor- und Nachteile der bestehenden Handlungsmöglichkeiten abwägen und den erkennbaren Risiken Rechnung tragen (*BGH* NJW 2008, 3361, 3362; zurückhaltender *BGH* NJW-RR 2009, 332). Eine vollständige Informationsgrundlage zu fordern, ist nach der wohl überwiegenden Ansicht im Schrifttum allerdings zu weitgehend (Schmidt/Lutter/*Krieger/Sailer-Coceani* § 93 Rn. 13 m.w.N.). Vielmehr geht es um eine angemessene Informationsgrundlage, die angesichts der konkreten Entscheidungssituation, insbesondere der Eilbedürftigkeit und der Tragweite der Entscheidung, angemessen erscheint. Damit ist dem Vorstand auch bei der Informationsgewinnung ein **Beurteilungsspielraum** zuzubilligen (Henssler/Strohn/*Dauner-Lieb §* 93 Rn. 22). Nach der neueren strafrechtlichen Rechtsprechung des BGH muss die Beurteilung im Zeitpunkt der Entscheidung aus der Sicht eines ordentlichen Geschäftsführers vertretbar erscheinen (*BGH* NZG, 2017, 116, 117 – HSH Nordbank). Fehlt allerdings ein funktionsfähiges Berichtswesen oder Kontrollsystem, trifft der Vorstand seine Entscheidungen oftmals nicht auf der Basis angemessener Information. Er kann sich bei seinen Entscheidungen dann nicht auf die Business Judgement Rule berufen (vgl. *Lorenz* ZRFG 2006, **60**

5, 9; I/B/P/*Poppe* 1. Kap. Rn. 28). Damit spielt die Organisation eine wesentliche Rolle auch bei der Beurteilung der Rechtmäßigkeit von getroffenen unternehmerischen Entscheidungen des Vorstands. Verfügt eine Gesellschaft über ein funktionierendes Compliance Management-System, können Sanktionen oder Nachteile aus Gesetzesverstößen vermieden oder reduziert werden (*Schulz/Block* CCZ 2020, 49, 49).

60a Die Grundsätze der Business Judgement Rule gelten für GmbH-Geschäftsführer entsprechend (MK-GmbHG/*Fleischer* § 43 Rn. 66).

b) Verschulden

61 Die Verpflichtung zum Schadensersatz setzt Verschulden voraus. Der **Verschuldensmaßstab** ergibt sich typisiert aus § 93 Abs. 1 S. 1 AktG bzw. § 43 Abs. 1 GmbHG (MK-GmbHG/*Fleischer* § 43 Rn. 255). Danach muss ein Mitglied des Geschäftsführungsorgans für diejenigen **Kenntnisse und Fähigkeiten** einstehen, welche die ihm anvertrauten **Aufgaben objektiv erfordern. Einfache Fahrlässigkeit** genügt. Allerdings dürften im Anwendungsbereich der Business Judgement Rule objektiv unvertretbare und daher pflichtwidrige Entscheidungen, die auf einfacher Fahrlässigkeit beruhen, allenfalls Ausnahmefälle sein.

62 Ein Mitglied des Geschäftsführungsorgans hat nur für **eigenes Verschulden** einzustehen. Es haftet nicht für das Verschulden seiner Kollegen oder von Mitarbeitern. Im Innenverhältnis kann das Vorstandsmitglied bzw. der GmbH-Geschäftsführer der Gesellschaft ein **Mitverschulden anderer Vorstandsmitglieder bzw. GmbH-Geschäftsführer nicht entgegenhalten** (zum Verschulden Spindler/Stilz/*Fleischer* § 93 Rn. 205 ff. m.w.N.).

c) Schaden

63 Die Haftung setzt weiter voraus, dass der Gesellschaft ein Schaden entstanden ist. Maßgebend ist der **Schadensbegriff der §§ 249 ff. BGB** (vgl. Hüffer/*Koch* § 93 Rn. 47). Schaden ist demnach jede Verminderung des Gesellschaftsvermögens. Verglichen wird das vorhandene Vermögen der Gesellschaft mit jenem, das die Gesellschaft ohne das schädigende Ereignis gehabt hätte (*BGH* WM 2013, 456, 458).

d) Kausalität

64 Die Haftung setzt schließlich voraus, dass der eingetretene Schaden auf die Pflichtverletzung des Geschäftsführungsorgans kausal zurückzuführen ist. Die Kausalität richtet sich nach den allgemeinen schadensrechtlichen Grundsätzen (MK-AktG/*Spindler* § 93 Rn. 196; s. zur Kausalität Palandt/*Grüneberg* Vorb. § 249 Rn. 24 ff.).

e) Darlegungs- und Beweislast

65 Nach § 93 Abs. 2 S. 2 AktG trägt der **Vorstand** die **Beweislast** dafür, dass er die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewendet hat. Daraus wird nach ganz herrschender Meinung gefolgert, dass ein **Vorstandsmitglied** in einem gegen ihn geführten **Schadensersatzprozess fehlendes Verschulden und fehlende Pflichtwidrigkeit** sowie **ggf. rechtmäßiges Alternativverhalten darlegen und beweisen** muss (*BGH* WM 2013, 456, 458; *LG München I* NZG 2014, 345, 347; *Hüffer/Koch* § 93 Rn. 53). Die **Gesellschaft** braucht daher **nur darzulegen und ggf. zu beweisen**, dass (1) das Verhalten des Vorstandsmitglieds sich als **möglicherweise pflichtwidrig** darstellt, (2) den Eintritt und die Höhe des entstandenen **Schadens** und (3) die **Kausalität** zwischen Vorstandshandeln und Schaden (Spindler/Stilz/*Fleischer* § 93 Rn. 215a m.w.N.; vgl. auch *LG München I* NZG 2014, 345, 347). Der Gesellschaft wird der Sachvortrag zum **Schaden gem. § 287 ZPO zudem erleichtert**. Danach genügt es, dass die Gesellschaft Tatsachen vorträgt und ggf. unter Beweis stellt, die für eine Schadensschätzung hinreichende Anhaltspunkte bieten (*Fleischer* NZG 2014, 321, 326 m.w.N.). Vergleichbare **Erleichterungen gelten auch für die Kausalität** (*Fleischer* NZG 2014, 321 327 f. m.w.N.).

66 In der Praxis beschränkt sich die klagende Gesellschaft unter Berufung auf die Rechtsprechung des Bundesgerichtshofs vielfach darauf, ein Handeln des Vorstands ohne konkrete Darlegung einer Pflichtverletzung sowie den eingetretenen Schaden vorzutragen und unter Beweis zu stellen. Dem beklagten Vorstand wird es dann häufig überlassen, zu interpretieren, welche Pflichtverletzung ihm vorgeworfen wird. Dies erscheint nicht sachgerecht. Damit der **Vorstand sich exkulpieren** kann, muss auch die sich aus einem **Vorstandshandeln oder -unterlassen ergebende Pflichtverletzung dargelegt** werden. Nur so kann der Vorstand sich exkulpieren. Nichts anderes ergibt sich aus § 93 Abs. 2 S. 2 AktG. Dort ist nämlich nur die Beweislast geregelt. Die Darlegungslast für pflichtwidriges Verhalten sollte nach den allgemeinen Grundsätzen die den Anspruch stellende Gesellschaft tragen.

67 Die dargestellten Regeln für die Verteilung der Darlegungs- und Beweislast gelten auch für **ausgeschiedene Vorstände** (Hüffer/*Koch* § 93 Rn. 56; kritisch *Foerster* ZHR 2012, 221, 225 ff.; s. Bürgers/Körber/Lieder/*Bürgers* § 93 Rn. 29). Da ausgeschiedene Vorstandsmitglieder allerdings keinen Zugriff mehr auf die Unterlagen der Gesellschaft haben, befinden sie sich in Beweisschwierigkeiten. Ihnen steht daher ein **Anspruch auf Einsicht in die Schriften und Unterlagen der Gesellschaft** zu, die sie zur Verteidigung benötigen (MK-AktG/*Spindler* § 93 Rn. 212 m.w.N.; zum Auskunftsanspruch des D & O-Versicherers Ruchatz, AG 2015, 1, 6 ff.). In der Praxis bereitet es häufig Schwierigkeiten, von der Gesellschaft die relevanten Unterlagen zu erhalten. Oft liegen die Vorgänge nämlich länger zurück, sodass der betroffene Vorstand die für seine Verteidigung notwendigen Unterlagen aus der Erinnerung nicht mehr genau bezeichnen kann.

67a Die dargestellten Grundsätze gelten im GmbH-Recht entsprechend (MK-GmbHG/*Fleischer* § 43 Rn. 270 ff. m.w.N.).

f) Verjährung

68 Nach § 93 Abs. 6 AktG verjähren Ansprüche der Gesellschaft gegen Vorstände aus § 93 AktG, soweit die Gesellschaft zum Zeitpunkt der Pflichtverletzung börsennotiert ist, in **zehn Jahren**, bei anderen Gesellschaften in **fünf Jahren**. Bei GmbH-Geschäftsführern beträgt die Verjährungsfrist nach § 43 Abs. 4 GmbHG fünf Jahre. Maßgeblich für den Beginn der Verjährung ist **§ 200 BGB**, somit die **Entstehung des Anspruchs** (MK-AktG/*Spindler* § 93 Rn. 325; s. zur Anspruchsentstehung Palandt/*Ellenberger* § 199 Rn. 3 ff., 14 ff.). Die Verjährung richtet sich also **nicht nach § 199 BGB**, so dass es insbesondere **nicht auf die Kenntnis oder die grob fahrlässige Unkenntnis** der anspruchsbegründenden Umstände ankommt. Außerdem ist die Verjährung **taggenau zu berechnen** und beginnt nicht wie bei § 199 BGB mit dem Schluss des betreffenden Jahres. Eine Sonderregelung enthält § 52a KWG. Danach gilt bei Kreditinstituten eine 10-jährige Verjährungsfrist.

69 Liegt die Pflichtverletzung eines Mitglieds der Geschäftsführung in einem Unterlassen, beginnt nach der im Vordringen befindlichen Meinung die Verjährung im Falle der Nachholbarkeit der unterlassenen Handlung erst dann, wenn die Nachholbarkeit endet (*LG München I* Urteil vom 10.12.2013 - 5 HK O 1387/10 m.w.N.). Danach beginnt die Verjährung im Falle des Unterlassens nicht bereits dann, wenn die pflichtgemäße Handlung hätte erfolgen müssen. Dies gilt namentlich für das Unterlassen der Implementierung eines effizienten Compliance-Systems (*LG München I* Urteil vom 10.12.2013 - 5 HK O 1387/10 m.w.N.).

70 Schadensersatzansprüche, die nach **anderen Vorschriften** begründet sind, **verjähren selbstständig** nach den für diese Vorschriften geltenden Regelungen (MK-AktG/*Spindler* § 93 Rn. 329 ff.).

g) Gesamtschuld

71 **Mehrere Vorstandsmitglieder**, die ihre Pflichten schuldhaft verletzen und dadurch einen Schaden verursachen, haften als **Gesamtschuldner** (Hüffer/*Koch* § 93 Rn. 57). Nach § 421 BGB können Schadensersatzansprüche daher gegen jedes einzelne Vorstandsmitglied in voller Höhe geltend gemacht werden. Der **Innenausgleich** zwischen den Vorstandsmitgliedern richtet sich nach § 426 BGB. Gem. § 426 Abs. 1 BGB steht jedem gesamtschuldnerisch haftenden Vorstandsmitglied gegen die übrigen gesamtschuldnerisch haftenden Vorstandsmitglieder ein **eigener, selbstständiger Ausgleichsanspruch** zu. Daneben besteht eine **cessio legis** (Legalzession) nach § 426 Abs. 2 BGB.

72 Zu **beachten** ist, dass der **eigene Ausgleichsanspruch nach § 426 Abs. 1 BGB** bereits mit der **Begründung der Gesamtschuld** entsteht und nicht erst mit Befriedigung des Gläubigers (Palandt/*Grüneberg* § 426 Rn. 4). Der Ausgleichsanspruch

unterliegt der regelmäßigen **Verjährung nach § 199 BGB**. In der Praxis ist daher darauf zu achten, dass der Innenausgleichsanspruch nicht verjährt. Die **cessio legis** nach § 426 Abs. 2 BGB kann nämlich dann **ins Leere laufen**, wenn die Gesellschaft ihrerseits den Anspruch gegen andere gesamtschuldnerisch haftende Vorstandsmitglieder verjähren lässt.

Die gesamtschuldnerische Haftung gilt gem. § 43 Abs. 2 GmbHG auch für GmbH-Geschäftsführer. **72a**

2. Weitere Anspruchsgrundlagen

Neben der Organhaftung gem. § 93 AktG kommen weitere Anspruchsgrundlagen für Ansprüche der Gesellschaft gegen die Geschäftsführungsorgane in Betracht. Außerdem können auch Ansprüche von Aktionären bzw. Gesellschaftern oder Dritten bestehen (s. zu den Anspruchsgrundlagen etwa Spindler/Stilz/*Fleischer* § 93 Rn. 309 ff.). Diese Ansprüche können grundsätzlich auch bei schuldhaften Verstößen von Vorstandsmitgliedern gegen Compliance-Pflichten geltend gemacht werden, soweit die weiteren Voraussetzungen der jeweiligen haftungsbegründenden Norm erfüllt sind. **73**

a) Ansprüche der Gesellschaft

§ 93 AktG regelt das Verhältnis zwischen der Gesellschaft und den Vorstandsmitgliedern nicht abschließend (vgl. Bürgers/Körber/Lieder/*Bürgers* § 93 Rn. 17). Gleiches gilt für § 43 GmbHG, sodass die nachfolgenden Ausführungen entsprechend für GmbH-Geschäftsführer gelten. Daneben sind auch vertragliche und gesetzliche Schadensersatzansprüche zu prüfen. **74**

aa) Dienstvertrag

Die Pflicht des Vorstands bzw. des GmbH-Geschäftsführers, die Gesellschaft in eigener Verantwortung zu leiten und dabei die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden, entsteht unmittelbar durch die Bestellung (Spindler/Stilz/*Fleischer* § 84 Rn. 75). Damit resultiert die Compliance-Verantwortung direkt aus der Organstellung. Die Haftung gem. § 280 BGB in Verbindung mit ihrem **Anstellungsvertrag** geht daher in der Haftung nach § 93 Abs. 2 S. 1 AktG bzw. § 43 Abs. 2 GmbHG auf und hat gegenüber dieser Vorschrift **keine gesonderte Bedeutung**. **75**

bb) Unerlaubte Handlung

Neben der Organhaftung nach § 93 Abs. 2 S. 1 AktG kommen auch Ansprüche aus § 823 ff. BGB in Betracht. Erfüllt das schuldhafte pflichtwidrige Verhalten eines Vorstandsmitglieds bzw. eines GmbH-Geschäftsführers zugleich den Tatbestand einer **unerlaubten Handlung**, steht dieser Anspruch neben der Organhaftung (KölnKomm-AktG/*Mertens/Cahn* § 93 Rn. 195). **76**

78 Bei schuldhaften Pflichtverletzungen können Ansprüche der Gesellschaft aus § 823 Abs. 1 BGB, § 823 Abs. 2 BGB und § 826 BGB bestehen, soweit der jeweilige Verstoß den Tatbestand der betreffenden Norm erfüllt.

79 Auch bei einem Verstoß gegen die Organisations- und Überwachungspflicht sind Ansprüche aus unerlaubter Handlung denkbar. Wird ein absolut geschütztes Recht oder Rechtsgut der Gesellschaft verletzt und handelt der Vorstand bzw. GmbH-Geschäftsführer außerhalb des ihm eingeräumten Organisationsermessens, ist er unter den weiteren Voraussetzungen des § 823 Abs. 1 BGB zum Ersatz des Schadens verpflichtet. Ein Anspruch aus § 823 Abs. 2 BGB scheidet hingegen aus, soweit sich nicht ausnahmsweise etwas Anderes aus Spezialgesetzen ergibt. Insbesondere stellt **§ 130 OWiG kein Schutzgesetz** i.S.d. § 823 Abs. 2 BGB dar (Palandt/*Sprau* § 823 Rn. 68 m.w.N.). Auch bei **§ 93 AktG und § 43 GmbHG** handelt es sich um **keine Schutzgesetze**. Reine **Vermögensschäden** der Gesellschaft werden daher allenfalls in den engen Grenzen des § 826 BGB bei vorsätzlicher sittenwidriger Schädigung oder soweit ein Spezialgesetz ausnahmsweise ein Schutzgesetz darstellt, erfasst.

80 Die Anwendbarkeit der §§ 823 ff. BGB neben § 93 Abs. 2 S. 1 AktG ist vor allem für die Frage der **Verjährung** von Ansprüchen von Bedeutung, weil auf unerlaubte Handlungen die Regelverjährung nach § 199 BGB Anwendung findet (Köln-Komm-AkG/*Mertens/Cahn* § 93 Rn. 195) und der Verjährungsbeginn – anders als bei der Organhaftung nach § 93 AktG – daher kenntnisabhängig ist.

b) Ansprüche der Gesellschafter oder Dritter

81 Die in § 93 Abs. 2 AktG und § 43 Abs. 2 GmbHG geregelte Innenhaftung führt zu einer Haftung der Geschäftsführung gegenüber der Gesellschaft und **schließt damit zumindest für den Regelfall die Organhaftung gegenüber Aktionären oder Dritten aus** (Hüffer/*Koch* § 93 Rn. 60). Die Mitglieder des Geschäftsführungsorgans trifft in erster Linie eine **interne Organisationspflicht**, deren schuldhafte Verletzung grundsätzlich nicht zu einer Haftung im Außenverhältnis führt (Hüffer/*Koch* § 93 Rn. 66 m.w.N.). Die Einzelheiten sind noch nicht abschließend geklärt. Von Bedeutung für die Außenhaftung sind bei Compliance-Verstößen jedenfalls Ansprüche aus unerlaubter Handlung.

83 Bei schuldhaften Pflichtverletzungen können Ansprüche aus §§ 823 ff. BGB bestehen (vgl. MK-AktG/*Spindler* § 93 Rn. 337). Dies hat zum Beispiel Bedeutung gegenüber Aktionären im Bereich des Kapitalmarktrechts. Haben etwa unrichtige ad-hoc-Mitteilungen den Anlass zum Aktienerwerb gegeben, kann dies zu einem Schadensersatzanspruch nach § 826 BGB führen (Hüffer/*Koch* § 93 Rn. 62).

84 Führt ein Verstoß gegen die **Organisations- und Überwachungspflichten** zu einer Verletzung eines **absolut geschützten Rechts oder Rechtsguts** eines Gesellschafters oder eines gesellschaftsfremden Dritten i.S.d. § 823 Abs. 1 BGB kommt nach der höchstrichterlichen Rechtsprechung ein Anspruch des Geschädigten auf

Schadensersatz in Betracht (*BGHZ* 109, 297, 203 ff.). Zu weitgehend ist es aber, allein aus der Stellung des Geschäftsführungsorgans, dass notwendigerweise die Pflichten der Gesellschaft nach außen wahrnimmt, abzuleiten, dass das Geschäftsführungsorgan eine generelle Verkehrssicherungspflicht gegenüber Gesellschaftern oder Dritten unmittelbar trifft (MK-AktG/*Spindler* § 93 Rn. 357). Zu weitgehend ist es erst recht, wenn die Verletzung allgemeiner vertraglicher Schutz- und Loyalitätspflichten der Gesellschaft gegenüber einem Vertragspartner als Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb und damit als deliktische Handlung angesehen wird (MK-AktG/*Spindler* § 93 Rn. 357; a.A. *BGHZ* 166 84, 114 ff. – Kirch/Deutsche Bank, Breuer). Bei der Organisations- und Überwachungspflicht handelt es sich um eine Pflicht gegenüber der Gesellschaft. Verstöße gegen diese Pflicht führen, wie dargestellt, zu Ansprüchen der Gesellschaft gegen das Vorstandsmitglied aus § 93 AktG bzw. gegen den GmbH-Geschäftsführer nach § 43 GmbHG und ausnahmsweise aus §§ 823 ff. BGB. Derartige Verstöße begründen jedoch keinen unmittelbaren Anspruch eines Aktionärs oder eines Dritten gegen das Organmitglied, weil eine aus der Compliance-Verantwortung resultierende Verkehrssicherungspflicht gegenüber Aktionären oder Dritten nicht besteht (MK-AktG/*Spindler* § 93 Rn. 357). Die Pflicht aus der Organstellung zur ordnungsgemäßen Geschäftsführung, zu der auch die Pflicht gehört, für die Rechtmäßigkeit des Handelns der Gesellschaft Sorge zu tragen, besteht grundsätzlich nur dieser gegenüber und lässt bei ihrer Verletzung Schadensersatzansprüche grundsätzlich nur der Gesellschaft entstehen (*BGH* NJW 2012, 3439). Etwas anderes kann auch bei Verletzung eines absolut geschützten Rechtsguts oder Rechts i.S.d. § 823 Abs. 1 BGB nicht gelten.

85 Grundsätzlich führt die Verletzung von Organisations- und Überwachungspflichten auch zu keinem Schadenersatzanspruch nach § 823 Abs. 2 BGB. Wie bereits ausgeführt (oben Rn. 79 ff.) stellen § 93 AktG und § 43 GmbHG kein Schutzgesetz dar. Gleiches gilt für § 130 OWiG (Hüffer/*Koch* § 93 Rn. 61, 65). Organisationspflichtverletzungen können jedoch dann zu Schadenersatzansprüchen nach § 823 Abs. 2 BGB führen, wenn die Pflicht nicht durch Delegation oder interne Aufgabenverteilung übertragbar ist (MK-AktG/*Spindler* § 93 Rn. 365). Dies gilt etwa für die Nichtabführung der Arbeitnehmeranteile zur Sozialversicherung. Hier ist § 266a StGB als Schutzgesetz anzusehen (*BGH* NJW 2005, 2546). Außerdem können Ansprüche aus § 823 Abs. 2 BGB i.V.m. Spezialgesetzen bestehen (s. zu den Spezialgesetzen etwa MK-AktG/*Spindler* § 93 Rn. 359 ff.).

86 Ein Anspruch aus § 826 BGB wegen vorsätzlicher sittenwidriger Schädigung aufgrund von schuldhaften Verstößen gegen Organisations- und Überwachungspflichten ohne Hinzutreten weiterer Umstände, die ein vorsätzliches, sittenwidriges Handeln begründen, scheidet aus den vorstehend zu § 823 Abs. 1 BGB genannten Gründen aus.

IV. Organhaftung des Aufsichtsrats einer Aktiengesellschaft

87 Wie unter vorstehend Rn. 42 f. dargelegt, trifft den Vorstand die Compliance-Verantwortung. Der **Aufsichtsrat** wiederum hat die **Wahrnehmung der Compliance-Verantwortung** durch den Vorstand zu **überwachen**. Durch die Vorgaben des Aktienrechts ist der Aufsichtsrat in seinen Einwirkungsmöglichkeiten eingeschränkt, so dass ihm auch in Bezug auf Compliance ein Initiativ- oder Weisungsrecht gegenüber dem Vorstand nicht zusteht (*Habersack* AG 2014, 1,3).

88 Nach der ständigen Rechtsprechung des Bundesgerichtshofs ist der Aufsichtsrat einer Aktiengesellschaft bei **Vorliegen von Anhaltspunkten** verpflichtet, **Ansprüche der Gesellschaft gegen Vorstandsmitglieder zu prüfen** und – soweit nicht gewichtige Interessen im Einzelfall entgegenstehen – diese Ansprüche **geltend zu machen und durchzusetzen** (*BGHZ* 135, 244 ff. – ARAG/Garmenbeck). Anderenfalls kann sich der Aufsichtsrat seinerseits schadensersatzpflichtig machen. Diese Grundsätze gelten auch, wenn der Gesellschaft ein Schaden entstanden ist, der auf einer schuldhaften Verletzung von Compliance-Pflichten des Vorstands beruht.

89 Die höchstrichterliche Rechtsprechung führt zu einer gestaffelten Prüfung der Vorstandshaftung:

Auf der ersten Prüfungsstufe hat der Aufsichtsrat zu klären, ob der Vorstand schuldhaft pflichtwidrig gehandelt hat und dadurch der Gesellschaft ein Schaden entstanden ist. Dazu hat der Aufsichtsrat den maßgeblichen Sachverhalt aufzuklären. Er muss also feststellen, welcher Schaden der Gesellschaft entstanden ist, ob Maßnahmen oder Versäumnisse des Vorstands für diesen Schaden ursächlich sind und ob eine schuldhafte Pflichtverletzung des Vorstands vorliegt (*Goette* S. 155, 156 f.).

90 Auf der zweiten Prüfungsstufe ist sodann zu klären, ob der Geltendmachung von Ansprüchen gewichtige Belange der Gesellschaft entgegenstehen (*Goette* S. 153, 160). Ausweislich der Gründe der „ARAG/Garmenbeck"-Entscheidung (*BGHZ* 135, 244 ff., 245 f.) kommt eine Nichtgeltendmachung nur dann in Betracht, wenn die Gesellschaftsinteressen, die für eine Nichtverfolgung von Schadensersatzansprüchen sprechen, überwiegen oder zumindest den Gesichtspunkten, die für eine Rechtsverfolgung sprechen, annähernd gleichwertig sind. Von Bedeutung sind dabei etwa negative Auswirkungen auf die Geschäftstätigkeit und das Ansehen der Gesellschaft in der Öffentlichkeit, die Behinderung der Vorstandsarbeit und die Beeinträchtigung des Betriebsklimas. Andere Gesichtspunkte wie die Schonung eines verdienten Vorstandsmitglieds sind nicht relevant. Nur in engen Grenzen wird dem Aufsichtsrat ein Beurteilungsspielraum eingeräumt, nachdem die gegeneinander abzuwägenden Interessen festgestellt worden sind (*BGHZ* 135, 244, 256).

91 Die Grundsätze der „ARAG/Garmenbeck"-Entscheidung haben in der Literatur von Anfang an ein geteiltes Echo gefunden. Zum Teil wird der höchstrichterlichen

Rechtsprechung grundsätzlich folgend ein der gerichtlichen Überprüfung entzogener Ermessens- oder Beurteilungsspielraum des Aufsichtsrats abgelehnt (Hüffer/*Koch* § 111 Rn. 15). Daneben wird vertreten, dass auf die Aufsichtsratsentscheidung die Grundsätze der Business Judgement Rule (s. oben Rn. 52 ff.) Anwendung finden (*Paefgen* AG 2014 554, 571 ff.). Nach vermittelnder Auffassung soll es zumindest einen begrenzten Ermessens- oder Beurteilungsspielraum des Aufsichtsrats geben (MK- AktG/*Habersack* § 111 Rn. 44).

92 Aus der höchstrichterlichen Rechtsprechung ergibt sich ein Regel-Ausnahmeverhältnis, wonach Ansprüche der Gesellschaft gegen den Vorstand grundsätzlich zu verfolgen sind. In der Praxis ist bei Compliance-Verstößen der Aufsichtsrat allerdings häufig damit konfrontiert, dass sich das Bestehen von Ansprüchen nicht zweifelsfrei aufklären lässt, zumal der Aufsichtsrat nicht über die Möglichkeiten eines staatlichen Richters oder der Staatsanwaltschaft zur Sachverhaltsermittlung verfügt. Außerdem ist das Unternehmenswohl in den Vordergrund zu stellen. Aufgabe des Aufsichtsrats ist es nämlich, die Interessen der Gesellschaft zu wahren. Im Ergebnis sollte dem Aufsichtsrat daher ein größerer Beurteilungsspielraum, der der gerichtlichen Kontrolle entzogen ist, eingeräumt werden. In diese Richtung geht auch die neuere Entwicklung in der Literatur. Soweit ein Vergleich oder ein Anspruchsverzicht mit Zustimmung der Hauptversammlung gem. § 93 Abs. 4 S. 3 AktG erfolgt, soll der Aufsichtsrat nicht an die „ARAG/Garmenbeck"-Grundsätze gebunden sein (*Bayer/Scholz* ZIP 2015, 149, 151 f.). Vielmehr soll ein weiter Beurteilungsspielraum des Aufsichtsrats bestehen. Zur Begründung dieser Auffassung wird nicht zuletzt die Entscheidung des BGH im Zusammenhang mit der Erstattung von Bußgeldern durch die Gesellschaft herangezogen. Danach steht das Vermögen der Gesellschaft wirtschaftlich nicht dem Aufsichtsrat, sondern den Aktionären zu. Die Aktionäre sind befugt, auch eine Selbstschädigung zu beschließen (*BGH* NZG 2014 1058 Rn. 20). Die „ARAG/Garmenbeck"-Entscheidung betraf eine Fallkonstellation, in der der Aufsichtsrat ohne Beteiligung der Hauptversammlung beschlossen hatte, Ansprüche nicht zu verfolgen.

Weiterführende Literatur: *Bayer/Scholz* Die Pflichten von Aufsichtsrat und Hauptversammlung beim Vergleich über Haftungsansprüche gegen Vorstandsmitglieder, ZIP 2015, 149; *Bürgers/Körber/Lieder* Aktiengesetz, 5. Aufl. 2020; *Fleischer* „Business Judgement Rule", Vom Richterrecht zur Kodifizierung, ZIP 2004, 685; *ders.* Handbuch des Vorstandsrechts, 2006; *ders.* Aktienrechtliche Compliance-Pflichten im Praxistest: Das Siemens/Neubürger-Urteil des LG München I, NZG 2014, 321; *Foerster* Beweislastverteilung und Einsichtsrecht bei Inanspruchnahme ausgeschiedener Organmitglieder, ZHR 2012, 221; *Freund* NZG 2021, 579; *Götte* „Zur ARAG/Garmenbeck-Doktrin", Gedächtnisschrift M. Winter, 2011; *Inderst/Bannenberg/Poppe* Compliance, 3. Aufl. 2017; *Habersack* Grund und Grenzen der Compliance-Verantwortung des Aufsichtsrats der AG, AG 2014, 1; *Henssler/Strohn* Gesellschaftsrecht, 3. Aufl. 20; Kölner Kommentar zum Aktiengesetz, Band 2 Teil 1, 3. Aufl. 2009; *Kocher* Zur Reichweite der Business Judgement Rule, CCZ 2009, 215; *Lorenz* Rechtliche Grundlagen des Risikomanagements, ZRFG 2006, 5; *Ruhmannseder/Behr/Krakow* Hinweisgebersysteme, 2. Aufl. 2021.

Prof. Dr. Frank Maschmann[1]

Arbeitsrecht und Beschäftigtendatenschutz

1 Der Verfasser ist Inhaber des Lehrstuhls für Bürgerliches Recht und Arbeitsrecht an der Universität Regensburg sowie Leiter des Masterstudiengangs Compliance der Universität Regensburg.

Arbeitshilfen: Betriebsvereinbarung Ethikrichtlinien **(2500 Nr. 1)**; Betriebsvereinbarung Torkontrolle **(2500 Nr. 2)**, Betriebsvereinbarung Videoüberwachung **(2500 Nr. 3)**, Betriebsvereinbarung Internetkontrolle **(2500 Nr. 4)**.

Texte: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, „Datenschutz-Grundverordnung" (ABlEU Nr. L 119/1 v. 4.5.2016); Datenschutz-Anpassungs- und Umsetzungsgesetz EU" (DSAnpUG-EU) v. 30.6.2017, BGBl I S. 2097.

I. Einleitung

1 Das Arbeitsrecht spielt für die Compliance in mehrfacher Hinsicht eine wichtige Rolle. Wenn es darum geht, Strafbarkeitsrisiken zu identifizieren, ist es zunächst Sache einer spezifisch arbeitsrechtlichen Compliance, die einschlägigen **Tatbestände des Arbeitsstrafrechts** zu sichten und an die Verantwortlichen zu kommunizieren. Dazu gehören z.B. die Straftaten um den Lohn, wie § 291 StGB (Bewucherung von Arbeitnehmern), § 266 StGB (Vorenthalten/Veruntreuen von Arbeitsentgelt), § 266a StGB (Nichtabführung von Sozialversicherungsbeiträgen), Verstöße gegen das Arbeitszeitgesetz (§ 23 ArbZG), das BundesdatenschutzG (§ 43 BDSG), das Arbeitsschutzgesetz (§ 26 ArbSchG) sowie Straftaten gegen Betriebsverfassungsorgane und ihre Mitglieder (§ 119 BetrVG). Hinzu kommen die zahllosen **Tatbestände von Ordnungswidrigkeiten** im Bereich des Arbeitsrechts, die mit teilweise erheblichen Bußgeldrahmen ausgestaltet wurden, z.B. bis zu 500 000 EUR für Verstöße gegen das G über den allgemeinen Mindestlohn (§ 21 Abs. 3 MiLoG) bzw. das ArbeitnehmerentsendeG (§ 23 Abs. 3 AEntG) und bis zu 30 000 EUR für Verstöße gegen das ArbeitnehmerüberlassungsG (§ 16 Abs. 2 AÜG).

2 Dabei kann man aber nicht stehenbleiben. Wenn gerade der Faktor „Mensch" eine wesentliche Risikoquelle im Unternehmen darstellt, muss die Compliance genau hier ansetzen und auf **das Mitarbeiterverhalten Einfluss nehmen** (Maschmann*/Rodewald* Corporate Compliance und Arbeitsrecht, S. 31, 34). Das Arbeitsrecht regelt, **welche verhaltenssteuernden Maßnahmen erlaubt** sind. Wichtigstes Mittel ist dabei das **Direktionsrecht** (§ 106 GewO), mit dem der Arbeitgeber sowohl im Einzelfall unmittelbar zu befolgende Anweisungen erteilen als auch abstrakt-generelle Verhaltensrichtlinien – zusammengefasst etwa in einem „Verhaltenskodex" (s. Rn. 5) – aufstellen kann.

Zum Dritten kommt das Arbeitsrecht ins Spiel, wenn es um die Grenzen der Verhaltenssteuerung geht. Diese werden vor allem bei der **Mitarbeiterkontrolle** aktuell, die zwar ein unverzichtbarer Baustein jeder Compliance-Organisation ist, aber Gefahr läuft, selbst Rechtsvorschriften zu verletzen (s. Rn. 1). Aufgabe des Arbeitsrechts ist es hier, zwischen den berechtigten Sicherheitsbelangen des Arbeitgebers und den nicht weniger berechtigten Persönlichkeitsrechten des Arbeitnehmers zu vermitteln. Dabei spielt das Recht des **Beschäftigtendatenschutzes** eine wichtige Rolle (s. Rn. 8), dessen Grundlage das vom BVerfG im Volkszählungsurteil (*BVerfGE* 65, 1) entwickelte **Recht auf informationelle Selbstbestimmung** bildet und das in Art. 8 EU-GRCh mittlerweile sogar auf der Ebene der EU Anerkennung erfahren hat (dazu und zum Wechselspiel mit den einschlägigen EU-Richtlinien und dem deutschen Verfassungsrecht instruktiv Maschmann/*Bäcker* Beschäftigtendatenschutz in der Reform, S. 15 ff.). Nicht weniger wichtig ist das **Recht der betrieblichen Mitbestimmung** in Betrieben bzw. Dienststellen mit Betriebs- bzw. Personalräten, weil die meisten Kontrollmaßnahmen der Mitbestimmung unterliegen, deren Durchführung deshalb durch Betriebs- bzw. Dienstvereinbarungen geregelt werden. **3**

Endlich entscheidet das Arbeitsrecht darüber, welche **Sanktionen** der Arbeitgeber gegen Arbeitnehmer verhängen darf, die die aus Sicht der Compliance notwendigen Regelungen missachten und damit ihre arbeitsvertraglichen Pflichten verletzen oder sogar strafbare Handlungen begehen (s. Rn. 93). In einem **Kündigungsschutzverfahren** wird dabei relevant, ob **Beweismittel,** die der Arbeitgeber im Zuge einer Mitarbeiterkontrolle erhoben hat, auch zur Verteidigung seiner Rechtsposition gegen den Mitarbeiter verwendet werden dürfen. Hier ist die Rechtsprechung im Fluss (s. Rn. 70). **4**

II. Verhaltenskodex

Ein Verhaltenskodex ist ein für den Arbeitnehmer verbindlicher **Katalog von Ge- und Verboten**, mit dem das regelkonforme Verhalten der Mitarbeiter sichergestellt werden soll. Als Baustein in einem **„Compliancesystem“** ist er ein wichtiges Element guter Unternehmensführung **(Corporate Governance).** Viele Unternehmen verfügen bereits über solche Bestimmungen. Sie tragen die unterschiedlichsten Bezeichnungen, wie etwa **„Ethik-Richtlinien“,** „Code of Conduct“ oder „Business Conduct Guidelines“ (*Wagner* Ethikrichtlinien, S. 17). Eine für alle Unternehmen geltende Pflicht zur Einführung eines betrieblichen Verhaltenskodex besteht derzeit zwar noch nicht (zu Verpflichtungen aus Spezialgesetzen *Wagner* Ethikrichtlinien, S. 20 ff.). Allerdings kann der Arbeitgeber mit dessen Erlass und tatsächlicher Durchsetzung einen Beitrag zur Erfüllung seiner Aufsichtspflichten leisten, die etwa nach 130 OWiG bestehen. Ob und inwieweit der Arbeitgeber einen Verhaltenskodex auch **rechtlich verbindlich** machen kann, **muss für jedes darin enthaltene Ge- oder Verbot jeweils einzeln beurteilt werden.** Entsprechendes gilt für die betrieblichen Mitbestimmungsrechte; auch sie hängen jeweils von der einzelnen Regelung ab (*BAG* NZA 2008, 1248, 1252). Die meisten Vorgaben kann der **5**

Arbeitgeber einseitig kraft Direktionsrechts aufstellen. Eines Einverständnisses oder einer Bestätigung seitens des Arbeitnehmers bedarf er hierzu nicht. Im Regelfall besteht deshalb auch keine Nebenpflicht, sich ausdrücklich zur Einhaltung des Kodex zu bekennen. Eine solche kommt nach § 241 Abs. 2 BGB allenfalls dann in Betracht, wenn der Arbeitgeber aus internationalen oder ausländischen Rechtsvorschriften oder aufgrund von AGB seiner Kunden gezwungen ist, entspr. Erklärungen einzuholen.

6 Regeln, die zur Einhaltung der im Zusammenhang mit der Tätigkeit zu beachtenden Gesetze auffordern oder Vorschriften nur erläutern, ohne sie unternehmens- oder betriebsspezifisch zu konkretisieren, beschreiben Pflichten, denen die Mitarbeiter ohnehin unterliegen. Einer Verbindlichmachung kraft Direktionsrechts bedarf es nicht (*Mahnhold* S. 173; *Schuster/Darsow* NZA 2005, 273, 275). Da es an einer eigenen, konstitutiven Regelung des Arbeitgebers fehlt, kommen auch keine Mitbestimmungsrechte in Betracht. Die meisten „Ethikrichtlinien" dienen der Korruptionsbekämpfung (Dölling/*Maschmann* Kap. 3 Rn. 1, 44 f.). Soweit Ethikregeln **allgemeine ethisch-moralische Programmsätze** enthalten, wie den Appell an ein faires, höfliches, vertrauensvolles und respektvolles Miteinander, können daraus keine hinreichend bestimmten Verhaltenspflichten abgeleitet werden. Mit diesen Regelungen ist daher auch keine Beeinträchtigung berechtigter Arbeitnehmerinteressen verbunden. Vielmehr wird auf Umgangsformen hingewiesen, die nicht justiziabel sind (*Wagner* Ethikrichtlinien, S. 115 f.).

7 Kraft Direktionsrechts kann der Arbeitgeber bestimmen, ob und inwieweit Arbeitnehmer **Geschenke** und andere Zuwendungen (Einladung zum Besuch eines Restaurants, Theater- und Konzertkarten, Reisen usw.) **annehmen** dürfen. Das ist unproblematisch, wenn Anlass und Umfang der Einladung angemessen sind und die Ablehnung der Einladung dem Gebot der Höflichkeit widersprechen würde. Einer eigenen Regelung bedarf es ohnehin nicht, soweit solche Zuwendungen den Tatbestand der Bestechlichkeit (§§ 299, 332 StGB) oder Vorteilsannahme (§ 331 StGB) erfüllen. Freilich kann der Arbeitgeber die Grenzen konkretisierend nachzeichnen und auch jegliche Annahme von Geschenken verbieten (so *BAG* DB 2006, 2068 ff. bezüglich dienstlich erworbener Bonusmeilen; vgl. ausführlicher *Wagner* Ethikrichtlinien, S. 94 f.) oder sie unter einen Genehmigungsvorbehalt stellen oder den Arbeitnehmer zur Anzeige erhaltener Vorteile verpflichten (vgl. Schaub/*Linck* § 53 Rn. 28). Auch das **Gewähren von Vorteilen** kann der Arbeitgeber untersagen, gleichviel ob diese aus dem Vermögen des Arbeitgebers oder des Arbeitnehmers stammen (*Wagner* Ethikrichtlinien, S. 98). Zulässig wäre überdies ein **Verbot, private Aufträge von Firmen ausführen zu lassen,** mit denen der Arbeitnehmer geschäftlich zu tun hat, wenn ihm dadurch Vorteile entstehen könnten. Hier kommen vor allem Mitarbeiter in Betracht, die Aufträge für den Arbeitgeber erteilen oder ihre Vergabe maßgeblich beeinflussen können. Kraft Direktionsrechts lassen sich ferner **Verschwiegenheitspflichten** hinsichtlich von Geschäfts- und Betriebsgeheimnissen (zum Begriff § 2 Nr. 1 GeschGehG) sowie von sonstigen vertraulichen Angaben regeln. Die geheimhaltungsbedürftigen Tatsachen müssen jedoch hinreichend bestimmt sein. Unzulässig sind daher sog.

All-Klauseln, wonach der Arbeitnehmer über sämtliche während der Tätigkeit bekannt gewordene Vorfälle zu schweigen hat (*Wagner* Ethikrichtlinien, S. 124). Umgekehrt kann der Arbeitgeber kraft Direktionsrechts auch eine **Pflicht zur Meldung von Verstößen gegen gesetzliche Vorschriften und den Verhaltenskodex** statuieren. Damit wird die arbeitsvertragliche Nebenpflicht konkretisiert, Schaden vom Arbeitgeber abzuwenden, soweit dies dem Arbeitnehmer möglich und zumutbar ist. Unzumutbar wäre eine Pflicht zur Selbstanzeige (*Schuster/Darsow* NZA 2005, 273, 276). Andererseits ist es dem Anzeigenden zuzumuten, seine Identität offen zu legen, sofern ihm zugesichert wird, hierdurch keine Nachteile befürchten zu müssen und die Identität vom Arbeitgeber vertraulich behandelt wird (*Wagner* Ethikrichtlinien, S. 128; a.A. *Bürkle* DB 2004, 2158, 2161). Umfassendere Anzeigepflichten können in formularvertraglichen Regelungen nur bedingt getroffen werden. Sog. All-Klauseln, die den Arbeitnehmer zu jedweder Anzeige unabhängig von der Schwere des Rechts- oder Richtlinienverstoßes verpflichten, sind auch insoweit nicht möglich. Dies gilt auch für die Verpflichtung zur Selbstanzeige. Der Verhaltenskodex kann einen allgemeinen Hinweis auf die **Sanktionen** enthalten oder diese im Einzelnen benennen. Fehlt ein Hinweis auf Sanktionen, heißt das nicht, dass keine Sanktionen verhängt werden dürfen. Ein Verstoß gegen den Verhaltenskodex bedeutet in aller Regel zugleich die Verletzung einer vertraglichen Nebenpflicht (§ 241 Abs. 2 BGB). Besonderer Vereinbarung bedürfen nur Vertragsstrafeversprechen.

III. Beschäftigtendatenschutz

1. Datenschutzrecht im Mehrebenensystem der EU

Die Zulässigkeit der Verarbeitung personenbezogener Daten richtet sich seit dem 25.5.2018 nach der Datenschutz-Grundverordnung (DS-GVO) 2016/679 der Europäischen Union. Mit ihren 99 Artikeln und 173 Erwägungsgründen (EG) aktualisiert sie das Grundrecht auf informationelle Selbstbestimmung. Dieses wird auf europäischer Ebene durch Art. 8 Abs. 1 EMRK sowie Art. 8 Abs. 1 GRCh gewährleistet. Personenbezogene Daten dürfen danach nur nach Treu und Glauben für festgelegte Zwecke auf einer gesetzlich geregelten legitimen Grundlage verarbeitet werden (Art. 8 Abs. 2 GRCh), die den **Wesensgehalt des Grundrechts** wahrt und den **Grundsatz der Verhältnismäßigkeit** beachtet (Art. 52 Abs. 1 GRCh). Dem dienen die Bestimmungen der DS-GVO. Sie gestalten die grundrechtliche Garantie aus und konkretisieren die Anforderungen an eine zulässige Datenverarbeitung. Ihr Ziel ist ein **unionsweit gleichmäßiges Datenschutzniveau.** Zugleich will sie die Unterschiede, die den freien Verkehr mit personenbezogenen Daten im Binnenmarkt behindern, beseitigen (EG 13 S. 1 DS-GVO). Um diese Ziele effektiv zu erreichen, hat sich die EU für die Handlungsform der Verordnung entschieden. Diese bedarf – anders als eine Richtlinie – keiner Umsetzungsgesetze der Mitgliedstaaten, sondern gilt in allen ihren Teilen unmittelbar (Art. 288 Abs. 2 AEUV). Nur eine einheitlich geltende Verordnung vermag es, „natürliche Personen in allen Mitgliedstaaten mit demselben Niveau an durchsetzbaren Rechten **8**

auszustatten, dieselben Pflichten und Zuständigkeiten für die Verantwortlichen vorzusehen und eine gleichmäßige Kontrolle der Datenverarbeitung und gleichwertige Sanktionen zu gewährleisten“ (so die ständige Rspr. zur Harmonisierungswirkung von arbeitsrechtlichen Rechtsvorschriften, vgl. nur *EuGH* NJW 2015, 2481 Rn. 32 f.). Allerdings trifft die DS-GVO in den Mitgliedstaaten auf ein ausdifferenziertes Datenschutzrecht, das sich von Land zu Land zum Teil erheblich voneinander unterscheidet. Um im Prozess der Konvergenz alle Mitgliedstaaten mitzunehmen, erlaubt ihnen die DS-GVO deshalb eigene datenschutzrechtliche Vorschriften, die aber den Vorgaben des Unionsrechts entsprechen müssen. Rechtstechnisch geschieht dies durch rund vier Dutzend mehr oder weniger weit gefasste Öffnungsklauseln (*Kühling/Martini* EuZW 2016, 448, 449; *dies.* Die DS-GVO und das nationale Recht, 2016, S. 1 f.).

9 Mit dem „Datenschutz-Anpassungs- und -Umsetzungsgesetz EU“ (DSAnpUG-EU v. 30.6.2017, BGBl I S. 2097) hat der deutsche Gesetzgeber diese Regelungsspielräume genutzt und ebenfalls zum 25.5.2018 das Bundesdatenschutzgesetz (BDSG) vollständig neu gefasst. Allerdings durfte er bei der Ausfüllung der Öffnungsklauseln den Wortlaut der DS-GVO weder ganz noch teilweise wiederholen. Mit diesem Wiederholungsverbot will die EU vermeiden, dass die unmittelbare Geltung einer Verordnung verschleiert wird und die Normadressaten über den wahren Urheber des Rechtsaktes getäuscht werden (*EuGH* Slg 1973, 981 Rn. 9 f.; *EuGH* Slg 1978, 99 Rn. 22/27). Beide Regelungsebenen sollen strikt voneinander getrennt bleiben. Zulässig sind allenfalls punktuelle Wiederholungen, soweit dies aus Gründen der Verständlichkeit und Kohärenz der nationalen Vorschrift notwendig ist (*EuGH* Slg 1985, 1057 Rn. 27). Die Nachteile liegen auf der Hand: Nationales Datenschutzrecht kann künftig nur noch im Zusammenspiel mit den Vorschriften der DS-GVO verstanden werden (dazu instruktiv *Kühling* NJW 2017, 1985, 1986 f.). Das kompliziert die Rechtsanwendung erheblich.

10 Hinzukommt, dass das BDSG in seiner Neufassung durch das DSAnpUG-EU selbst nur einen eingeschränkten Anwendungsbereich hat, den man zunächst sorgfältig anhand von § 1 BDSG ermitteln muss. Es gilt nur für Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes i.S.d. § 2 Abs. 1 BDSG sowie für nicht öffentliche Stellen, d.h. für natürliche Personen sowie für juristische Personen und Personenvereinigungen des privaten Rechts (§ 2 Abs. 4 BDSG), wenn sie Daten automatisiert i.S.d. § 1 Abs. 1 S. 2 BDSG verarbeiten. Außerdem hat das BDSG – wie bisher – den Charakter eines „Auffanggesetzes“ (*Kühling* NJW 2017, 1985,1987). Bereichsspezifisches Datenschutzrecht des Bundes genießt gegenüber den Vorschriften des BDSG grds. den Vorrang (§ 1 Abs. 2 S. 1 BDSG). Dazu gehören etwa die Regelungen des Telekommunikationsrechts nach dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) v. 23.6.2021 (BGBl. I S. 1982) und des Sozialdatenschutzrechts nach dem SGB X. Der Vorrang der spezielleren datenschutzrechtlichen Vorschrift gilt jedoch nur, soweit sie einen Sachverhalt, für den an sich das BDSG gilt, abschließend regelt. Ist das nicht der Fall, übernimmt das BDSG seine lückenfüllende Auffangfunktion. Auch eine nicht abschließende (teilweise) Regelung oder das Schweigen eines

bereichsspezifischen Gesetzes führt dazu, dass subsidiär auf die Vorschriften des BDSG zurückgegriffen werden kann. Die Vorschriften des BDSG finden keine Anwendung, soweit das Recht der Europäischen Union, im Besonderen die DS-GVO in der jeweils geltenden Fassung, unmittelbar gilt. Darauf weist § 1 Abs. 5 BDSG noch einmal ausdrücklich hin, obwohl sich diese Rechtsfolge bereits aus Art. 288 Abs. 2 AEUV ergibt.

11 Konkrete Regelungen zum Schutz von Beschäftigtendaten treffen weder die DS-GVO noch das BDSG. Art. 88 DS-GVO enthält nur eine Öffnungsklausel für mitgliedstaatliche Regelungen über die „Datenverarbeitung im Beschäftigungskontext", die der deutsche Gesetzgeber durch die neue Generalklausel des § 26 BDSG umgesetzt hat, allerdings weitgehend unzureichend (zur Kritik s. Kühling/Buchner/*Maschmann* DS-GVO Art. 88 Rn. 63, 65). Seitens des Bundesrats wurde deshalb erneut der Erlass eines Beschäftigtendatenschutzgesetzes angemahnt (BT-Drucks. 18/11655, 24). Der Koalitionsvertrag vom Februar 2018 hatte zwar ein solches für die 19. Legislaturperiode in Aussicht gestellt (Koalitionsvertrag S. 42). Zum Erlass kam es jedoch nicht.

12 Die inhaltlichen Vorgaben und Grenzen für den Datenschutz bestimmt künftig das Unionsrecht. Dabei kommt dem EuGH eine Schlüsselfunktion zu. Denn er entscheidet nicht nur über die Reichweite der Öffnungsklausel des Art. 88 Abs. 1 DS-GVO, sondern wacht zudem darüber, dass die Mitgliedstaaten beim Erlass ihres nationalen Datenschutzrechts die inhaltlichen Vorgaben des Art. 88 Abs. 2 DS-GVO einhalten. Erste wichtige Entscheidungen zur DS-GVO sind bereits ergangen, etwa zur Einwilligung hinsichtlich der Speicherung von „Cookies" (*EuGH* NJW 2019, 3433) zur Übermittlung personenbezogener Daten in die USA (*EuGH* NJW 2020, 2613 – „Schrems II") sowie zur anlasslosen Vorratsdatenspeicherung, die nur bei erheblicher Gefahrenlage zulässig ist (*EuGH* NJW 2021, 531). Liegt zu einer entscheidungserheblichen Frage des Unionsrechts noch keine einschlägige Rechtsprechung des EuGH vor oder hat er eine entscheidungserhebliche Frage möglicherweise noch nicht erschöpfend beantwortet oder erscheint eine Fortentwicklung der Rspr. des Gerichtshofs nicht nur als entfernte Möglichkeit, muss ein letztinstanzliches Fachgericht in Deutschland ein Vorabentscheidungsverfahren nach Art. 267 Abs. 3 AEUV einleiten. Das Recht auf den gesetzlichen Richter (Art. 101 Abs. 1 S. 2 GG) wird verletzt, wenn das Gericht den ihm in solchen Fällen notwendig zukommenden Beurteilungsrahmen in unvertretbarer Weise überschritten hat (*BVerfG* ZD 2021, 266); ein solches letztinstanzliches Urteil kann dann mit der Verfassungsbeschwerde angefochten werden. Eine Vorlagepflicht hatte das BVerfG jüngst für die Frage angenommen, unter welchen Voraussetzungen Art. 82 Abs. 1 DS-GVO einen Geldentschädigungsanspruch gewährt, da diese Frage in der Rechtsprechung des EuGH weder erschöpfend geklärt ist, noch unmittelbar aus der DS-GVO beantwortet werden kann (*BVerfG* ZD 2021, 266).

2. Anwendbarkeit des deutschen Beschäftigtendatenschutzrechts (§ 26 BDSG)

13 **Sachlich** gilt der in § 26 BDSG geregelte Schutz von Beschäftigtendaten für die Verarbeitung von **„personenbezogenen Daten für Zwecke des Beschäftigungsverhältnisses".** Der Begriff **„personenbezogene Daten"** ist in **Art. 4 Nr. 1 DS-GVO legaldefiniert.** Darunter sind alle Informationen zu verstehen, die sich auf eine „identifizierte oder identifizierbare natürliche Person beziehen". Identifizierbar ist eine natürliche Person, die direkt oder indirekt aufgrund gewisser Merkmale bestimmt werden kann, „die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind". Die Identifizierung kann insbesondere „mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten oder zu einer Online-Kennung" geschehen. Der Begriff **„Verarbeitung"** ist in **Art. 4 Nr. 2 DS-GVO** geregelt. Das Unionsrecht versteht darunter „jeden Vorgang im Zusammenhang mit personenbezogenen Daten", wie etwa „das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung" (*EuGH* 16.7.2020, NJW 2020, 2613 Rn. 82). Während die DS-GVO nur für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten (dazu zuletzt *EuGH* NZA 2018, 931) Anwendung findet (Art. 2 Abs. 1 DS-GVO), geht das **deutsche Beschäftigtendatenschutzrecht** des § 26 BDSG – schon wie bisher – darüber hinaus. Es gilt gem. § 26 Abs. 7 BDSG sogar dann, wenn **personenbezogene Daten nicht automatisiert verarbeitet werden (**ebenso *Kort* ZD 2017, 319, 323; *Wybitul* NZA 2017, 413, 418). Damit gilt § 26 BDSG für jede Art der Verarbeitung von Beschäftigtendaten (Gola/Heckmann/*Gola* BDSG § 26 Rn. 11; Taeger/Gabel/*Zöll* BDSG § 26 Rn. 101), wie z.B. bei Befragungen von Bewerbern und Beschäftigten, Tor-, Taschen- und Spindkontrollen oder bei rein tatsächlichen Beobachtungen von Arbeitnehmern durch Wach- und Sicherheitspersonal (Paal/Pauly/*Gräber/Nolden* DS-GVO BDSG, § 26 Rn. 5; *Gola* BB 2017, 1462, 1472). Mit dem den Anwendungsbereich der DS-GVO überschießenden Bereich wird § 26 Abs. 7 BDSG als nationale Sondervorschrift nicht von der DS-GVO verdrängt (*Kort* ZD 2017, 319, 323; *Wybitul* NZA 2017, 413, 418).

14 Was unter „Zwecke des Beschäftigungsverhältnisses" zu verstehen ist, ergibt sich aus § 26 Abs. 1 S. 1 BDSG, nämlich Datenverarbeitungen zur Entscheidung über die Begründung eines Beschäftigungsverhältnisses sowie für seine Durchführung und Beendigung. Sollen Beschäftigtendaten zur Aufdeckung von Straftaten verarbeitet werden, enthält § 26 Abs. 1 S. 2 BDSG eine Sondervorschrift. Sie gilt nur für die Aufdeckung, nicht für die Verhinderung von Straftaten und ist unanwendbar, wenn es (nur) um Verletzungen des Arbeitsvertrags geht (str.; vgl. *Kort* ZD 2017, 319, 321; *Wybitul* NZA 2017, 413, 416). Verarbeitungen zu anderen als den in § 26 Abs. 1 S. 1 BDSG bzw. Art. 88 Abs. 1 DS-GVO genannten Zwecken

schließt § 26 Abs. 1 BDSG nicht aus. Sie können nach Art. 6 Abs. 1 lit. f oder Art. 9 Abs. 2 DS-GVO erlaubt sein (*Maschmann* BB 2019, 628, 633; *Sander/Schumacher/Kühne* ZD 2017, 105, 108 f.). Beispiele sind Übermittlung von Beschäftigtendaten im Rahmen von **„Due-Diligence-Prüfungen"** beim Kauf von Betrieben oder Unternehmen (*Grau* FS Willemsen, 2018, S. 147, 149), für Big-Data-Analysen (*Götz* Big Data im Personalmanagement, Diss. Regensburg 2020, S. 61), oder für die Konzernrevision (dazu ausf. *Ringel/von Busekist* CCZ 2017, 31).

Persönlich gilt § 26 BDSG für die Verarbeitung personenbezogener Daten von **Beschäftigten**. Wer als Beschäftigter i.S.d. BDSG gilt, bestimmt **§ 26 Abs. 8 BDSG** in abschließender Form. Danach gilt der Beschäftigtendatenschutz außer für Arbeitnehmer i.S.d. § 611a BGB auch für Auszubildende, Rehabilitanden, Beschäftigte in Behindertenwerkstätten, Personen, die Freiwilligendienste oder Zivildienst leisten, arbeitnehmerähnliche Selbständige, Beamte und Richter des Bundes sowie Soldaten. Dieser sehr weit gefasste Schutzbereich muss im Einklang mit der Öffnungsklausel des Art. 88 Abs. 1 DS-GVO stehen. Ob das der Fall ist, erscheint zweifelhaft. Richtigerweise erlaubt die DS-GVO nationales Beschäftigtendatenschutzrecht nur als „klassisches" Arbeitnehmerdatenschutzrecht (ausf. Kühling/Buchner/*Maschmann* DS-GVO Art. 88 Rn. 11 ff.; ebenso *Körner* Beschäftigtendatenschutz im Lichte der DS-GVO, S. 55; für eine weite Auslegung *Franzen* EuZA 2017, 313, 349; *Gola* BB 2017, 1462, 1472; *Kort* ZD 2017, 319, 321; BeckOK DatenschutzR/*Riesenhuber* DS-GVO Art. 88 Rn. 13). Werden personenbezogene Daten von Personen verarbeitet, die nicht unter § 26 BDSG fallen, wie z.B. Vorstände und Geschäftsführer, gilt die DS-GVO direkt, jedenfalls bei automatisierter Datenverarbeitung i.S.d. Art. 2 Abs. 1 DS-GVO. Zu beachten sind dann vor allem die allgemeinen Grundsätze des Art. 5 DS-GVO und die Abwägungsklausel des Art. 6 Abs. 1 lit. f DS-GVO. **15**

3. Allgemeine Grundsätze

a) Rechtmäßigkeit und Zweckbindung der Datenverarbeitung

Die Verarbeitung von personenbezogenen Daten ist nur dann zulässig, wenn dies ausdrücklich gestattet ist. Art. 6 Abs. 1 DS-GVO enthält insoweit ein „Verbot mit Erlaubnisvorbehalt". Für den Beschäftigtendatenschutz enthält § 26 Abs. 1 BDSG eine gesetzliche Verarbeitungsgrundlage. Dabei herrscht der Grundsatz der **strengen Zweckbindung,** der sich unionsrechtlich aus Art. 5 Abs. 1 lit. b DS-GVO ergibt. Dieser verlangt, dass die Daten nur für Zwecke verarbeitet werden dürfen, die bereits vor der Erhebung eindeutig festgelegt sind. Eine Weiterverarbeitung zu anderen Zwecken ist nur dann erlaubt, wenn sie mit den ursprünglichen Zwecken vereinbar ist. Dazu ist ein „Kompatibilitätstest" nach Maßgabe von Art. 6 Abs. 4 DS-GVO erforderlich. Für die Vereinbarkeit spielt u.a. eine Rolle, ob es eine Verbindung zwischen den verschiedenen Zwecken gibt, ob für die Weiterverarbeitung dieselbe Person verantwortlich ist, ferner die Art der Daten, die möglichen Folgen der beabsichtigten Weiterverarbeitung für den Betroffenen sowie schließlich das Vorhandensein geeigneter Garantien, wie z.B. eine Verschlüsse- **16**

lung oder Pseudonymisierung. Werden die Daten bei der betroffenen Person erhoben, müssen ihr die Zwecke zum Zeitpunkt der Datenerhebung nach Maßgabe von Art. 13 Abs. 1 DS-GVO mitgeteilt werden. Sollen sie für einen anderen als für den ursprünglichen Zweck weiterarbeitet werden, ist die betroffene Person vorher zu informieren (Art. 13 Abs. 3 DS-GVO). Der Verantwortliche hat den Verarbeitungszweck in einem Verzeichnis der Verarbeitungstätigkeiten festzuhalten (Art. 30 Abs. 1 S. 2 lit. b DS-GVO). Darin hat er anzugeben, welche technischen und organisatorischen Maßnahmen er getroffen hat, um ein angemessenes Datenschutzniveau zu gewährleisten (Art. 30 Abs. 1 S. 2 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO). Ohne diesen Nachweis ist die Verarbeitung rechtswidrig (Art. 24 Abs. 1 S. 1 DS-GVO). Das Verarbeitungsverzeichnis ist grds. schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann (Art. 30 Abs. 3 DS-GVO). Befreit von dieser Verpflichtung sind zwar Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen. Das gilt allerdings dann nicht, wenn die konkrete Verarbeitung (wie z.B. eine Torkontrolle, Videoüberwachung, Handyortung) entweder ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt oder sie nicht nur gelegentlich erfolgt oder wenn sensitive Daten i.S.d. Art. 9 DS-GVO verarbeitet werden (Art. 30 Abs. 5 DS-GVO). Sind die Voraussetzungen einer der drei Alternativen erfüllt, müssen sogar Kleinbetriebe, Vereine und ähnliche gemeinnützige Organisationen ein Verarbeitungsverzeichnis führen. Der Verstoß gegen die Nachweispflicht kann mit einem Bußgeld von bis zu 10 Mio. EUR oder 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs des Verantwortlichen geahndet werden (Art. 83 Abs. 4 lit. a DS-GVO).

b) Verhältnismäßigkeit

17 Erlaubt ist die Verarbeitung nur, wenn sie **„erforderlich"** ist, um die in § 26 Abs. 1 BDSG genannten Zwecke zu verwirklichen. Das gilt auch für die Datenverarbeitung durch den Betriebsrat (*Gola* BB 2017, 1462, 1466). Nach der Gesetzesbegründung (BT-Drucks. 18/11325, 96) sollen bei der Erforderlichkeitsprüfung die widerstreitenden Grundrechtspositionen zur Herstellung praktischer Konkordanz gegeneinander abgewogen werden. Dazu müssen „die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem Ausgleich gebracht werden, der beide Interessen möglichst weitgehend berücksichtigt". Das entspricht der Vorgabe in Art. 88 Abs. 2 DS-GVO. Danach müssen die Mitgliedstaaten beim Erlass von Vorschriften zum Beschäftigtendatenschutz „angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person" ergreifen. Das Kriterium der Erforderlichkeit stellt sicher, dass ein an sich legitimes Datenverarbeitungsziel nicht zum Anlass genommen wird, überschießend personenbezogene Daten zu verarbeiten (NK-Datenschutzrecht/*Petry* DS-GVO Art. 9 Rn. 42). Der Erforderlichkeitsbegriff ist primär durch datenschutzrechtliche Vorgaben geprägt, nicht durch mitbestimmungsrechtliche (ebenso

Gola BB 2017, 1462, 1466). Dabei ist der **Grundsatz der Verhältnismäßigkeit** zu wahren (*Kort* ZD 2017, 319, 323; *Wybitul* NZA 2017, 413, 415).

Da der Gesetzgeber den Wortlaut des § 32 BDSG a.F. weitgehend in § 26 BDSG übernommen hat und damit – ausweislich der Begründung im Regierungsentwurf (BT-Drucks. 18/11325, 95 f.) und der Gegenäußerung zur Stellungnahme des Bundesrats (BT-Drucks. 18/11655, 53) – die spezialgesetzliche Regelung des § 32 BDSG a.F. fortführen wollte, allerdings angepasst an die Terminologie der DS-GVO, ist davon auszugehen, dass **es bei der bisherigen Rechtslage bleiben soll** (ebenso *Gola* BB 2017, 1462, 1464; *Wybitul* NZA 2017, 413, 415). Dafür spricht nicht zuletzt, dass sich der Gesetzgeber ausdrücklich vorbehalten hat, konkrete Fragen des Beschäftigtendatenschutzes in einem späteren Gesetz zu regeln (BT-Drucks. 18/11325, 95). Der Begriff der „Erforderlichkeit" in § 26 BDSG ist daher genauso zu verstehen wie bisher, d.h. im Sinne einer strikten Geltung des Grundsatzes der Verhältnismäßigkeit. Danach muss die vom Arbeitgeber gewählte Art und Weise einer Datenverarbeitung für die Verwirklichung der (zulässigerweise) verfolgten Zwecke überhaupt geeignet sein. Sie muss zudem das mildeste aller gleich effektiven zur Verfügung stehenden Mittel darstellen. Die Verhältnismäßigkeit im engeren Sinne ist gewahrt, wenn die Schwere des mit der Datenverarbeitung bewirkten Eingriffs in die Persönlichkeitsrechte des Arbeitnehmers bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht (so zum bisherigen Recht *BAG* NZA 2014, 146; NZA 2017, 112, 114 f.; NZA 2017, 394; NZA 2017, 1327; NZA 2019, 893; NZA 2019, 1055; NZA 2019, 1212; NZA 2019, 1218). **18**

c) Beachtung der allgemeinen Verarbeitungsgrundsätze

§ 26 Abs. 5 BDSG ordnet ferner an, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen ergreifen muss, um die Einhaltung der insbesondere in Art. 5 DS-GVO dargelegten Grundsätze für die Verarbeitung von Beschäftigtendaten sicherzustellen. Die dort in Abs. 1 lit. a–f genannten **sechs Prinzipien** sind bereits aus der DSRL und dem BDSG a.F. bekannt: **Rechtmäßigkeit der Datenverarbeitung, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit.** Die Datenverarbeitung muss nicht nur auf rechtmäßige Weise, nach Treu und Glauben und in einer für den Beschäftigten nachvollziehbaren Weise erfolgen, sondern sich auf das für die Zweckerreichung Notwendige beschränken. Lässt sich der Zweck auch ohne Beschäftigtendaten erreichen – etwa durch entspr. Technikgestaltung oder Pseudonymisierung (Art. 25 Abs. 1 DS-GVO) –, ist die Verarbeitung unzulässig. Ferner müssen Beschäftigtendaten unverzüglich berichtigt oder gelöscht werden, falls diese fehlerhaft oder unzulässig verarbeitet wurden (Art. 17 Abs. 1 lit. d DS-GVO). Beschäftigtendaten, die die Identifizierung des Betroffenen erlauben, dürfen überdies nur so lange gespeichert werden, wie dies zur Erreichung der vereinbarten Zwecke erforderlich ist (Art. 5 Abs. 1 lit. e DS-GVO). Danach sind sie zu löschen (zur Speicherdauer von Videoaufzeichnungen *BAG* NZA 2018, 1329). Außerdem müssen sie vor unbefugtem Zugriff geschützt werden. Dabei hat der **19**

Arbeitgeber sicherzustellen, dass Personal, das Zugang zu personenbezogenen Daten hat, diese nur nach seinen Anweisungen verarbeitet (BT-Drucks. 18/11325, 98). Ferner sind die Vorschriften der Art. 32 ff. DS-GVO über die Datensicherheit zu beachten, und es ist der betriebliche Datenschutzbeauftragte (Art. 37 DS-GVO) rechtzeitig vor der Verarbeitung zwecks Folgenabschätzung (Art. 35 DS-GVO) einzubinden.

d) Transparenz der Verarbeitung

20 Weiterhin verpflichtet Art. 88 Abs. 2 DS-GVO die Mitgliedstaaten zu angemessenen und besonderen Maßnahmen im Hinblick auf die Transparenz der Verarbeitung von Beschäftigtendaten. Gemeint sind damit die allgemeinen Informationspflichten nach den Art. 13-15 DS-GVO, über die „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" zu unterrichten ist (Art. 12 Abs. 1 S. 1 DS-GVO). Die Unterrichtung muss „in einer für die betroffene Person nachvollziehbaren Weise" geschehen (Art. 5 Abs. 1 lit. a DS-GVO). Der Beschäftigte muss klar erkennen und nachvollziehen können, ob, von wem und zu welchem Zweck seine personenbezogenen Daten erhoben werden (vgl. EG 58 S. 3 DS-GVO). Das hat zum Zeitpunkt der Erhebung zu erfolgen (Art. 13 Abs. 1 DS-GVO und EG 61 S. 1 DS-GVO).

21 **Nicht offen erkennbare Datenverarbeitungen,** wie etwa heimliche Videoüberwachungen und Schrankkontrollen, Observationen durch Detektive, das Belauschen von Telefongesprächen oder Mitlesen von E-Mails, die nach § 32 BDSG a.F. unter – engen – Voraussetzungen erlaubt waren (*BAG* NZA 2017, 112; NZA 2017, 1327), wären danach **prinzipiell unzulässig,** weil sie dem Transparenzgebot zuwiderlaufen (ebenso *Byers* NZA 2017, 1086, 1088; Kühling/Buchner/*Herbst* DS-GVO Art. 5 Rn. 18) und zudem **gegen Art. 8 EMRK verstoßen** (*EGMR* NZA 2017, 1443; *EGMR* ZD 2018, 263*; EGMR* NZA 2019, 169). Hinzu kommt, dass die Heimlichkeit einer in Grundrechte eingreifenden Maßnahme das Gewicht der Rechtsbeeinträchtigung typischerweise erhöht. Verdeckte Überwachungen und Ermittlungen führen dazu, dass dem Betroffenen vorbeugender Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz erheblich erschwert wird (ebenso *BAG* NZA 2014, 143 Rn. 31; *BAG* NZA 2017, 1327). Die Grundsätze einer fairen und transparenten Verarbeitung machen es deshalb zwingend erforderlich, dass der Beschäftigte darüber unterrichtet wird, dass seine Daten verarbeitet werden und zu welchen Zwecken dies geschieht (EG 60 S. 1–3 DS-GVO). Das hat zum Zeitpunkt der Erhebung zu erfolgen (Art. 13 Abs. 1 DS-GVO und EG 61 S. 1 DS-GVO).

Allerdings erlaubt Art. 23 Abs. 1 DS-GVO auch Beschränkungen des Transparenzprinzips. Das kann beispielweise geschehen, um Straftaten zu verhüten oder aufzudecken oder um zivilrechtliche Ansprüche durchzusetzen. Dass die **Rechtsprechung** unter der Geltung des § 32 BDSG a.F. heimliche Mitarbeiterkontrollen zugelassen hat (vgl. zuletzt *BAG* NZA 2017, 112; NZA 2017, 443), **genügt** nach Inkrafttreten der DS-GVO **nicht mehr.** Denn Art. 23 Abs. 1 DS-GVO ver-

langt ausdrücklich eine gesetzliche Regelung (ausf. Kühling/Buchner/*Bäcker* DS-GVO Art. 23 Rn. 35), für die Art. 23 Abs. 2 DS-GVO detaillierte inhaltliche Vorgaben enthält. **§ 26 Abs. 1 BDSG reicht jedenfalls nicht** aus.

22 Dieses Ergebnis liegt auch auf der Linie der neuesten Rechtsprechung des EGMR zu Art. 8 EMRK. Sie hat insoweit unmittelbare Bedeutung auch für die DS-GVO, als diese im Lichte der grundrechtlichen Gewährleistung zum Schutz des Privatlebens nach Art. 7 GRCh bzw. der personenbezogener Daten nach Art. 8 GRCh auszulegen ist. Art. 52 Abs. 3 GRCh bestimmt weiter, dass die Grundrechte der GRCh – jedenfalls soweit sie den durch die EMRK garantierten Rechten entsprechen – die gleiche Bedeutung und Tragweite haben, wie ihnen die EMRK verleiht. Folglich dürfen die Gewährleistungen der Art. 7 und Art. 8 GRCh das Schutzniveau der EMRK nicht unterschreiten. Schon von daher ist die zu ihrer Auslegung ergangene Rechtsprechung des EGMR zwingend zu beachten (ebenso *Lörcher* AuR 2019, 43, 44). In der Rechtssache ***Barbulescu*** (NZA 2017, 1443) ist die Große Kammer des Gerichtshofs zu der Überzeugung gelangt, dass Art. 8 EMRK den Staat zu Maßnahmen zum Schutze des von dieser Norm gewährleisteten Menschenrechts auf „Privatleben" verpflichte, das auch berufliche Tätigkeiten umfasse, wenn diese durch private Dritte beeinträchtigt würden. Das sei bei Überwachungsmaßnahmen durch den Arbeitgeber ohne weiteres anzunehmen. Zwar sei das Kontrollinteresse des Arbeitgebers grundsätzlich anzuerkennen; der Arbeitgeber dürfe aber nicht missbräuchlich handeln. Wo hier die Grenze verlaufe, hätten die Konventionsstaaten grundsätzlich selbst zu bestimmen, wofür sie einen weiten Ermessensspielraum genössen. Allerdings verlange die EMRK bestimmte Verfahrensgarantien gegen Willkür. Dazu gehöre, dass den Arbeitnehmern der Umstand und die Art und Weise der Überwachung mitzuteilen sei. Das müsse geschehen – und das betont der EGMR dreimal (!) ausdrücklich – **bevor die Überwachung** beginne. Fehle es daran, werde gegen Art. 8 EMRK verstoßen.

23 Diese Grundsätze hat die 3. Kammer des EGMR im Urteil vom 9.1.2018 in der Rechtssache ***Lopez Ribalda*** noch einmal bekräftigt (AuR 2019, 32 mit Anm. *Lörcher* = ZD 2018, 263 mit Anm. *Hembach).* Im dort entschiedenen Fall hatte das Management eines spanischen Supermarkts, in dem monatelang Waren im Wert von mehreren Tausend EUR verschwanden, heimlich Überwachungskameras installiert. Diese zeichneten auf, wie Mitarbeiter selbst Waren entwendeten und Kunden dabei halfen, das Geschäft mit unbezahlter Ware zu verlassen. Die spanischen Gerichte ließen das unbeanstandet und hielten die vom Management ausgesprochenen Kündigungen für rechtmäßig. Dagegen erachtete die 3**. Kammer des EGMR die Videoaufnahmen** schon deshalb für **konventionswidrig**, weil sie **ohne vorherige Ankündigung erfolgten**, obwohl das nach spanischem Recht ausdrücklich vorgesehen war. Deren Verwendung verstoße gegen Art. 8 EMRK, weil die Betroffenen wegen der unterlassenen Information über das Bestehen, das Ziel und die Art einer verdeckten Videoüberwachung die „vernünftige Erwartung" hatten, „dass ihre Privatsphäre geschützt werde", die durch die Verwertung der Aufnahmen enttäuscht wurde.

24 Überraschenderweise hat die **Große Kammer des EGMR** diese Entscheidung zwar mit Urt. v. 17.10.2019, NZA 2019, 1697 kassiert, weil sie – anders als die 3. Kammer des EGMR – in den heimlichen Videoaufnahmen **keinen Verstoß gegen Art. 8 EMRK** erblickte. In großen Teilen der Begründung hat sie aber die bisherige Rechtsprechung bestätigt. Ausdrücklich wurde festgestellt: „Die erforderliche Transparenz und das sich daraus ergebenden Recht auf Unterrichtung haben grundsätzliche Bedeutung, vor allem bei arbeitsrechtlichen Beziehungen, in denen der Arbeitgeber erhebliche Befugnisse gegenüber Arbeitnehmern hat und jeder Missbrauch verhindert werden muss" (*EGMR* NZA 2019, 1697 Rn. 131). Wegen der Bedeutung des Rechts auf Unterrichtung in solchen Kontrollfällen können „nur überwiegende Erfordernisse des Schutzes öffentlicher oder wichtiger Privatinteressen das Unterlassen einer vorherigen Information rechtfertigen" (*EGMR* NZA 2019, 1697 Rn. 134). Der „**geringste Verdacht von Unterschlagungen oder anderen Straftaten seitens des Personals können den Arbeitgeber jedenfalls nicht dazu berechtigen, eine geheime Videoüberwachung einzurichten."** Im entschiedenen Fall lagen nach Ansicht der Großen Kammer die Dinge aber ausnahmsweise anders. Nach Ansicht der Richter wurden schwerwiegende Straftaten begangen, der Umfang der festgestellten Verluste war erheblich, der reibungslose Betrieb des Unternehmens war bedroht, und die Delikte wurden nicht nur von einem einzigen Arbeitnehmer, sondern von mehreren begangen, wodurch ein allgemeines Klima des Misstrauens im Unternehmen entstand (*EGMR* NZA 2019, 1697 Rn. 131). Im Grundsatz hat aber, wie gesagt, auch die **Große Kammer die bisherige Rechtsprechung bestätigt und heimliche Überwachungsmaßnahmen für grundsätzlich unzulässig erklärt.** Ob das möglicherweise anders zu beurteilen ist, wenn sich ein konkreter Tatverdacht gegen eine ganz bestimmte Person richtet, so wie das in der von der 5. Kammer des *EGMR* (Urt. v. 5.10.2010 – 420/07, BeckRS 2011, 81439) entschiedenen Rechtssache *Köpke* der Fall war, ist einstweilen offen. Offen ist auch, ob es genügt, dass der Arbeitgeber zumindest „in a general manner" auf die Möglichkeit einer Überwachung hinweist, so wie es offenbar dem EGMR vorschwebt. Von der für Art. 8 EMRK maßgeblichen „Privatheitserwartung" kann dann nämlich nicht mehr die Rede sein. Freilich würde das Art. 8 EMRK im Ergebnis weitgehend leerlaufen lassen (so zutreffend *Lörcher* AuR 2019, 43).

e) Umgang mit sensiblen Beschäftigtendaten

25 Für die Verarbeitung sensibler Daten i.S.v. Art. 9 Abs. 1 DS-GVO, d.h. **rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische** (Art. 4 Nr. 13 DS-GVO) und **biometrische Daten** zur eindeutigen Identifizierung einer natürlichen Person (Art. 4 Nr. 14 DS-GVO), Gesundheitsdaten (Art. 4 Nr. 15 DS-GVO) sowie **Daten zum Sexualleben und zur sexuellen Orientierung**, trifft Art. 9 Abs. 2 DS-GVO eine Sonderregelung, die auch für sensible Daten von Beschäftigten gilt. Danach sind mitgliedstaatliche Regelungen erlaubt, die die Einzelheiten der Verarbeitung regeln, damit der Verantwortliche seinen sich aus dem Arbeits- und So-

zialrecht ergebenden Pflichten nachkommen und die betroffene Person die ihr daraus erwachsenden Rechte ausüben kann (Art. 9 Abs. 2 lit. b DS-GVO). Eine Regelung durch Kollektivvereinbarung nach dem Recht der Mitgliedstaaten lässt die Vorschrift ausdrücklich zu. Vorausgesetzt wird nur, dass die Verarbeitung erforderlich ist und geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorhanden sind. Soweit die Verarbeitung von genetischen, biometrischen oder von Gesundheitsdaten betroffen ist, können die Mitgliedstaaten sogar zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten (Art. 9 Abs. 4 DS-GVO). Dies gilt ebenfalls für Beschäftigtendaten.

Vor diesem Hintergrund bestimmt **§ 26 Abs. 3 BDSG**, dass die Verarbeitung sensibler Daten i.S.d. Art. 9 Abs. 1 DS-GVO für Zwecke des Beschäftigungsverhältnisses zulässig ist, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Zulässig ist die Verarbeitung ferner dann, wenn sie durch Kollektivvereinbarung erlaubt wird, weil § 26 Abs. 4 S. 1 BDSG diese ausdrücklich als Befugnisnorm erwähnt. Wegen des Verweises in § 26 Abs. 3 S. 3 BDSG auf § 22 Abs. 2 BDSG sind zur Wahrung der Interessen einer Person, deren sensible Daten verarbeitet werden, „angemessene und spezifische Maßnahmen" vorzusehen, die § 22 Abs. 2 S. 2 BDSG beispielhaft aufzählt. Dazu können **technische Vorkehrungen** gehören, mit denen sich feststellen lässt, von wem sensible Daten eingegeben, verändert oder entfernt wurden, aber auch die Sensibilisierung des Personals und die Beschränkung des zugangsbefugten Personenkreises, die Bestellung eines Datenschutzbeauftragten sowie die **Anonymisierung oder Pseudonymisierung** der sensiblen Daten. Die Zulässigkeit einer Datenverarbeitung **zur Beurteilung der Arbeitsfähigkeit** eines Beschäftigten richtet sich direkt nach Unionsrecht (Art. 9 Abs. 2 lit. h DS-GVO). Art. 9 Abs. 3 DS-GVO ordnet an, dass nur Fachpersonal, das einem unionsrechtlich oder mitgliedstaatlich geregelten Berufsgeheimnis unterliegt, diese Daten verarbeiten darf, also Ärzte und sonstiges Personal, das entspr. Geheimhaltungspflichten zu beachten hat, einschließlich Hilfspersonal, das unter ihrer Verantwortung tätig wird (§ 22 Abs. 1 Nr. 1 b BDSG). **26**

f) Kollektivvereinbarungen als Verarbeitungsgrundlage

§ 26 Abs. 4 BDSG gestattet die Verarbeitung von Beschäftigtendaten auch auf der Grundlage von Kollektivvereinbarungen. Diese Befugnis ist von großer Relevanz. Zum einen lassen sich durch Kollektivvertrag die **unbestimmten Rechtsbegriffe des gesetzlichen Datenschutzrechts konzern-, unternehmens- oder betriebsspezifisch konkretisiere**n (BT-Drucks. 18/11325, 98), zum anderen können die Modalitäten eines unternehmens- oder **konzernweiten Datenflusses** regelt werden. Verarbeitet der Arbeitgeber die Beschäftigtendaten mittels technischer Einrichtungen, die in der Lage sind, Verhalten und Leistung der Arbeitnehmer zu kontrollieren, hat der Betriebsrat ohnehin nach § 87 Abs. 1 Nr. 6 BetrVG **mitzubestimmen** **27**

(Richardi BetrVG/*Maschmann* § 87 Rn. 475 ff.; *Wisskirchen/Schiller/Schwindling* BB 2017, 2105). Das geschieht meist durch Abschluss von Betriebsvereinbarungen, weil diese aufgrund ihrer normativen Wirkung (§ 77 Abs. 4 BetrVG) nach früherer Rechtslage auch als Rechtsgrundlage für die Datenverarbeitung i.S.d. § 4 Abs. 4 BDSG a.F. dienen konnten (ständige Rspr., zuletzt *BAG* NZA 2017, 394; GK-BetrVG/*Franzen* § 83 Rn. 58; *Gola/Schomerus* BDSG § 4 Rn. 10; *Simitis* BDSG § 4 Rn. 17). **Dabei bleibt es auch unter Geltung der DS-GVO** (BT-Drucks. 18/11325, 98). Art. 88 Abs. 1 DS-GVO gestattet es den Mitgliedstaaten ausdrücklich, den Erlass von Kollektivverträgen zur Verarbeitung von Beschäftigtendaten zuzulassen. Für diese Befugnis hatte sich im Gesetzgebungsverfahren der EU vor allem Deutschland starkgemacht (zur Historie Art. 88 DS-GVO Rn. 2 ff.; krit. *Körner* ZESAR 2015, 153 Fn. 61). § 26 Abs. 4 BDSG stellt diese datenschutzschutzrechtliche Kollektivgewalt nun ausdrücklich klar (*Kort* ZD 2017, 319, 322; *Kühling* NJW 2017, 1985, 1988), obwohl sie an sich überflüssig ist, weil sie sich bereits aus § 1 Abs. 1 TVG bzw. § 87 Abs. 1 Nr. 6 BetrVG ergibt (ebenso *Gola* BB 2017, 1462, 1469; *Maschmann* DB 2016, 2480, 2482). Sie gilt auch für die Verarbeitung sensibler Daten i.S.d. Art. 9 DS-GVO, für die die Mitgliedstaaten aufgrund von Art. 9 Abs. 2 lit. b DS-GVO Regelungen durch Kollektivvereinbarung zulassen dürfen, jedenfalls dann, wenn die Verarbeitung erforderlich ist und geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorhanden sind.

28 Die inhaltlichen Anforderungen für Betriebsvereinbarungen richten sich vor allem nach den Direktiven des Art. 88 Abs. 2 DS-GVO. Darauf weist § 26 Abs. 4 S. 2 BDSG ausdrücklich hin. Im deutschen Recht entsprechen dem die Vorgaben des **§ 75 Abs. 2 S. 1 BetrVG.** Danach sind die **Betriebsparteien** außer zur Wahrung der grundrechtlich geschützten **Freiheitsrechte** (*BAG* NZA 1999, 546) auch zur **Beachtung des allgemeinen Persönlichkeitsrechts** verpflichtet, und zwar in allen seinen Ausprägungen, wie z.B. dem Recht am gesprochenen Wort und dem Recht am eigenen Bild (*BAG* NZA 2004, 1278 Rn. 14; *BAG* NZA 2013, 1433 Rn. 22). Das Persönlichkeitsrecht kann zwar kraft Betriebsvereinbarung beschränkt werden (*BAG* NZA 1991, 154; NZA 1999, 546; NZA 2004, 1278; NZA 2013, 1433). Die Beschränkung muss aber ihrerseits durch schutzwürdige Belange anderer Grundrechtsträger – beispielsweise des Arbeitgebers – gerechtfertigt sein. Ähnlich wie bei Art. 6 Abs. 1 lit. f DS-GVO ist auch bei § 75 Abs. 2 S. 1 BetrVG eine **Güterabwägung** zwischen den Persönlichkeitsrechten des Arbeitnehmers und dem schutzwürdigen Interesse des Arbeitgebers unter Berücksichtigung der Umstände des Einzelfalls erforderlich (*BAG* NZA 2003, 1193). Dabei ist der **Grundsatz der Verhältnismäßigkeit** zu wahren (*BAG* NZA 1999, 546). Den Betriebsparteien dürfen zur Erreichung des Verarbeitungszwecks keine anderen, gleich wirksamen und das Persönlichkeitsrecht der Arbeitnehmer weniger einschränkende Mittel zur Verfügung stehen. Eine Regelung ist verhältnismäßig im engeren Sinn, wenn die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht (*BAG* NZA 2004, 1278, all das entspricht den Vorgaben der Art. 88 Abs. 2, Art. 6

Abs. 1 lit f. DS-GVO). Außerdem müssen Kollektivvereinbarungen die allgemeinen Grundsätze des Art. 5 DS-GVO beachten, die auch für die Verarbeitung von Beschäftigtendaten gelten (s. Rn. 19).

29 Eine andere Frage ist, ob die **richterrechtlich geprägten** Regeln für die Mitarbeiterüberwachung **kraft Betriebsvereinbarung auch verschärft** werden dürfen. Beispiele hierfür wären ein absolutes Verbot einer heimlichen Videoüberwachung, die Statuierung eines gerichtlichen Verwertungsverbots für mitbestimmungs- oder datenschutzwidrig erlangtes Beweismaterial oder der Ausschluss jeglicher Verhaltens- und Leistungskontrolle, der sich in vielen betrieblichen Regelungen über die Verarbeitung von Beschäftigtendaten findet. Die wohl **h.M. bejaht** das, weil sie Verschärfungen gegenüber der DS-GVO für das gesamte mitgliedstaatliche Beschäftigtendatenschutzrecht erlaubt und dabei nicht zwischen gesetzlichen und kollektivvertraglichen Regelungen differenziert (*Düwell/Brink* NZA 2016, 665, 668; *Gola/Pötters/Thüsing* RDV 2016, 57, 59 f.; *Kort* DB 2015, 711, 714; *ders.* ZD 2017, 319, 322; Paal/*Pauly* Art. 88 Rn. 17; *Taeger/Rose* BB 2016, 819, 831).

30 Überzeugender ist die Annahme, dass die **Union** trotz der Öffnungsklausel des Art. 88 Abs. 2 DS-GVO **auch für den Beschäftigtendatenschutz am Prinzip der Vollharmonisierung** festhält und damit nationale Alleingänge mit strengeren Regeln als den in der DS-GVO vorgesehenen nicht erlaubt, weil sie auf Kosten eines unionsweit freien Datenverkehrs mit neuen Hindernissen für den Binnenmarkt und einem „patchwork" an Regelungen gehen würden (vgl. ausführlich *Maschmann* DB 2016, 2480, 2482 ff.; im Ergebnis ebenso *Franzen* EuZA 2017, 313, 345; *Kühling/Klar/Sackmann* Datenschutzrecht, 5. Aufl. 2021, Rn. 143 ff.; *Wybitul* NZA 2017, 413; **a.A.** *Kort* ZD 2017, 319, 321). Für die DSRL hatte der EuGH in der ASNEF-Entscheidung (NZA 2011, 1409) das Prinzip der Vollharmonisierung ausdrücklich betont. Die Richtlinie wolle auf einem hohen Niveau den freien Verkehr personenbezogener Daten sicherstellen. Dazu diene vor allem Art. 7 DSRL, der abschließend die Fälle aufführe, in denen die Verarbeitung personenbezogener Daten zulässig sei. Die Mitgliedstaaten seien deshalb weder befugt, neue Grundsätze einzuführen noch zusätzliche Bedingungen zu stellen, wenn dadurch die Tragweite der in Art. 7 DSRL genannten Prinzipien verändert würde. Nach hier vertretener Ansicht gelten die vom EuGH in der ASNEF-Entscheidung für Art. 7 DSRL aufgestellten Bedingungen sinngemäß auch für die Öffnungsklauseln der DS-GVO. **Im nationalen Beschäftigtendatenschutz** – zu dem auch kollektivvertragliche Regelungen zählen – wären dann **nur Präzisierunge**n erlaubt, **nicht jedoch zusätzliche Bedingungen,** wenn sie die Tragweite eine der in Art. 6 DS-GVO erwähnten Voraussetzungen verändern, oder kategorische Verarbeitungsverbote für bestimmte Daten. Strikte Kontrollausschlüsse wären mit diesen Vorgaben ebenso wenig vereinbar wie absolute Beweiserhebungs- oder -verwertungsverbote. Sie untersagen die Verarbeitung von Beschäftigtendaten ausnahmslos, ohne zu berücksichtigen, dass es im konkreten Einzelfall sehr wohl zulässig sein kann und muss, vom Erhebungs-, Nutzungs- oder Verwertungsverbot abzuweichen, etwa um Gefahren von Leib und Leben der Beschäftigten abzuwenden oder andere besonders wichtige Interessen zu verfolgen. Ein vollstän-

diger Ausschluss jeder Leistungs- und Verhaltenskontrolle wäre auch aus dem Gesichtspunkt der Compliance nicht hinnehmbar (ebenso *Beckschulze/Fackeldey* RDV 2013, 109, 117). § 130 OWiG verpflichtet den Betriebsinhaber zur Aufsicht über die in seinem Betrieb Beschäftigten. Ohne entsprechende Kontrollmaßnahmen kann der Arbeitgeber diese Anforderungen nicht erfüllen. Sie von vornherein zu verbieten, wäre nach der ASNEF-Rechtsprechung (*EuGH* NZA 2011, 1409) nicht erlaubt.

g) Einwilligung

31 Grundlage für die Verarbeitung von Beschäftigtendaten kann auch die Einwilligung des Betroffenen sein (Art. 6 Abs. 1 lit. a DS-GVO). Die **Mitgliedstaaten** können im Rahmen von Art. 88 DS-GVO hierfür **spezielle Voraussetzungen** festlegen. Das ergibt sich aus EG 155 DS-GVO, der explizit Vorschriften über die Bedingungen erlaubt, „unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen". Das kann **auch durch Kollektivvertrag,** insbesondere durch Betriebsvereinbarung geschehen (*Kort* DB 2016, 711, 715). Unverfügbar für die Mitgliedstaaten sind die durch Art. 4 Nr. 11 DS-GVO unionsrechtlich vorgegebenen Grundelemente einer Einwilligung: eine unmissverständliche („unambiguous") Erklärung oder sonstige eindeutige bestätigende Handlung des Beschäftigten, durch die dieser freiwillig, informiert und für einen bestimmten Fall zu verstehen gibt, dass er mit der Verarbeitung seiner personenbezogenen Daten einverstanden ist. Das Recht des Betroffenen, seine Einwilligung jederzeit zu **widerrufen** (Art. 7 Abs. 3 S. 1 DS-GVO), kann ebenfalls nicht ausgeschlossen werden, auch nicht durch Betriebsvereinbarung. Eine letzte Vorgabe des Unionsrechts ist die **Freiwilligkeit der Einwilligung**. Sie ist nur dann gegeben, wenn der von einer Datenverarbeitung Betroffene in der Lage ist, seine Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (EG 42 S. 4 DS-GVO). Die Einwilligung muss auch im nationalen Beschäftigtendatenschutz als Erlaubnistatbestand ausscheiden, wenn sie zur conditio sine qua non für den Abschluss des Arbeitsvertrags oder für den Erhalt bestimmter Leistungen erhoben wird (Plath/*Stamer/Kuhnke* DS-GVO Art. 88 Rn. 13). Die Einwilligung als Verarbeitungsgrundlage vollkommen auszuschließen, ist den Mitgliedstaaten bereits wegen Art. 8 GRCh verboten, der diese ausdrücklich erlaubt. Das gilt auch für die Betriebsparteien.

32 Vor diesem Hintergrund ist angesichts des **Wiederholungsverbots** (Rn. 9) verständlich, dass § 26 Abs. 2 BDSG nur einige Aspekte der Einwilligung regelt, namentlich deren Freiwilligkeit und bestimmte Formerfordernisse. Hinsichtlich der Freiwilligkeit ordnet § 26 Abs. 2 S. 1 BDSG an, dass zu ihrer Beurteilung insbesondere die im Beschäftigungsverhältnis bestehende **Abhängigkeit der beschäftigten Person** sowie die **Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen sind.** Neben der Art des verarbeiteten Datums und der Eingriffstiefe kann auch der Zeitpunkt, zu dem die Einwilligung erteilt wird, maßgebend sein. Vor Abschluss eines (Arbeits-)Vertrages werden Beschäftigte regelmäßig einer größeren Drucksituation ausgesetzt sein, eine Einwilligung in eine

Datenverarbeitung zu erteilen, als im laufenden Arbeitsverhältnis (BT-Drucks. 18/11325, 97). Entsprechendes gilt für Maßnahmen der **Mitarbeiterüberwachung.** In sie kann nicht wirksam vorab eingewilligt werden. Das dürfte mittlerweile der h.M. entsprechen (DWWS/*Däubler* BDSG § 26 Rn. 226; *Gola* BB 2017, 1462, 1468). Als Beispiel für eine zulässige Einwilligung nennt § 26 Abs. 2 S. 2 BDSG den Fall, dass die Arbeitsvertragsparteien ausnahmsweise einmal gleichgelagerte Interessen verfolgen. Hierzu kann etwa die Aufnahme von Name und Geburtsdatum in eine Geburtstagsliste oder die Nutzung von Fotos für das Intranet zählen (BT-Drucks. 18/11325, 97). Anders als in § 26 Abs. 2 S. 2 BDSG bestimmt, genügt es jedoch nicht, dass der Beschäftigte infolge der Datenverarbeitung einen rechtlichen oder wirtschaftlichen Vorteil erlangt, wie z.B. die Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen (BT-Drucks. 18/11325, 97). Freiwillig ist die Einwilligung jedenfalls dann nicht, wenn dem Beschäftigten der Vorteil verwehrt wird, falls er eine mit der Gewährung des Vorteils verbundene Kontrolle verweigert, bei der personenbezogene Daten erhoben werden.

Die **Einwilligung hat schriftlich oder elektronisch** zu erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist (§ 26 Abs. 2 S. 3 BDSG). Ausweislich der Gesetzesbegründung (BT-Drucks. 19/11181, 19) soll es genügen, dass der Arbeitgeber die Einwilligung als E-Mail abspeichert. Folglich ist das Formerfordernis „schriftlich oder elektronisch" nicht i.S.d. §§ 126, 126a BGB zu verstehen (ebenso *Thüsing/Rombey* NZA 2019, 1399, 1402). Vielmehr genügt bereits das Anklicken eines Kästchens beim Besuch einer Internetseite des Arbeitgebers, so wie es EG 32 S. 2 DS-GVO explizit vorsieht, weil darin eine „eindeutige bestätigende Handlung" i.S.d. Art. 4 Nr. 11 DS-GVO liegt, nicht aber Stillschweigen oder eine bereits vom Arbeitgeber im voraus markierte Schaltfläche (*EuGH* ZD 2021, 89). Stets muss der Arbeitgeber als Verantwortlicher **nachweisen** können, dass der Arbeitnehmer die Einwilligung „in Kenntnis der Sachlage" erteilt hat (Art. 7 Abs. 1 DS-GVO). Das verlangt nach EG 42 S. 2 mindestens Informationen über den Verantwortlichen und für welche Zwecke die Beschäftigtendaten erhoben werden. Nach Ansicht des EuGH hat dies in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu geschehen. Der Arbeitnehmer muss dabei in die Lage versetzt werden, die Konsequenzen seiner Einwilligung leicht ermitteln zu können. Dazu muss er mindestens die nach Art. 13 DS-GVO erforderlichen Hinweise erhalten (*EuGH* ZD 2021, 89 Rn. 40). Eine ausdrückliche Einwilligung ist stets erforderlich bei der Erhebung sensibler Daten (Art. 9 Abs. 2 lit. a DS-GVO, § 26 Abs. 3 S. 2 BDSG n.F.) sowie beim sog. Profiling (Art. 22 Abs. 2 lit. c DS-GVO). Die Einwilligung kann auch vom Arbeitgeber vorformuliert werden. Sie muss dann in einer klaren und einfachen Sprache abgefasst sein und darf keine missbräuchlichen Klauseln enthalten (EG 42 S. 3 DS-GVO). Außerdem muss sie in einer Form präsentiert werden, die sie klar von anderen Vertragsklauseln unterscheidet (*EuGH* ZD 2021, 89 Rn. 47). Sie darf also nicht in anderen AGBs „versteckt" werden. Keinesfalls können die dargelegten Anforderungen abgesenkt werden, auch nicht durch Betriebsvereinbarung. Zudem muss die Einwilligung „für den konkreten Fall" erfol- **33**

gen, was so zu verstehen ist, dass sie sich gerade auf die betreffende Datenverarbeitung beziehen muss und nicht aus einer Willensbekundung mit anderem Gegenstand abgeleitet werden kann (*EuGH* ZD 2021, 89 Rn. 38).

4. Rechte des Betroffenen

34 Die Art. 12 ff. DS-GVO gewähren der von der Verarbeitung ihrer Daten betroffenen Person eine Reihe weiterer individueller Rechte. Adressat dieser Rechte ist der für die Datenverarbeitung Verantwortliche. Das ist nach der Legaldefinition des Art. 4 Nr. 7 DS-GVO derjenige, der über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Dieser Begriff ist weit auszulegen, um einen wirksamen und umfassenden Schutz der betroffenen Person zu gewährleisten (*EuGH* NZA 2018, 919, 920). Zunächst kann sie vom Verantwortlichen Auskunft darüber verlangen, ob sie betr. personenbezogene Daten verarbeitet werden (Art. 15 Abs. 1 DS-GVO). Ist das der Fall, hat sie der Verantwortliche zu unterrichten, und zwar über die Verarbeitungszwecke, die Kategorien der verarbeiteten Daten (z.B. Name, Wohnort, Betriebsabteilung, Alter, Personalnummer), die Empfänger und Zugriffsberechtigten der Daten, die Speicherdauer, das Recht auf Berichtigung, Löschung, Widerspruch und Beschwerde bei der Aufsichtsbehörde sowie über die Herkunft der Daten, falls diese nicht bei der betroffenen Person erhoben wurden. Werden personenbezogene Daten an einen Empfänger in einem „Drittland" außerhalb der EU übermittelt, kann die betroffene Person Auskunft über die hierfür nach Art. 46 DS-GVO erforderlichen Garantien verlangen (Art. 15 Abs. 2 DS-GVO). Überdies hat der Verantwortliche eine kostenlose Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen (Art. 15 Abs. 3 DS-GVO).

35 Das Auskunftsrecht bezieht sich nicht nur auf die **Stammdaten**, die der Arbeitgeber für die Durchführung des Beschäftigungsverhältnisses benötigt, und die weiteren Informationen aus der **Personalakte**, sondern umfasst grundsätzlich **alle Medien, in denen Beschäftigtendaten gespeichert sind,** wie z.B. dienstliche Emails (*LAG Baden-Württemberg* NZA-RR 2019, 242 Rn. 175), ärztliche Unterlagen (*LG Köln* ZD 2019, 313), Videoaufnahmen oder Protokolle von Befragungen im Rahmen unternehmensinterner Ermittlungen. Stets muss aber ein **hinreichender Personenbezug** zum Betroffenen in dem verlangten Medium bestehen. Dazu genügt es nicht, dass ein Betroffener lediglich eine E-Mail versandt oder erhalten hat. Das Medium muss aussagekräftige Informationen über den Betroffenen oder eine vergleichbare Nähe zu seiner Person enthalten (*Härtling* CR 2019, 219, 224). Vor Erteilung einer Auskunft **kann der Arbeitgeber verlangen** – jedenfalls wenn er eine große Menge von Informationen verarbeitet –, dass der **Arbeitnehmer präzisiert**, **auf welche Information oder welche Verarbeitungsvorgänge sich sein Auskunftsersuchen bezieht** (vgl. Art. 63 S. 7 DS-GVO). Auskunftsansprüche können nicht „ins Blaue" geltend gemacht werden. Es muss vielmehr ausreichend dargelegt werden, dass tatsächlich personenbezogene Daten gespeichert sein könnten (*LAG Hessen* ZD 2013, 413 zu § 34 BDSG a.F.).

Der Arbeitgeber kann **die Auskunft verweigern**, wenn dadurch Informationen offenbart würden, die **geheimhaltungsbedürftig** sind (vgl. § 34 Abs. 1, § 29 Abs. 1 S. 2 BDSG), wie z.B. die Hinweise von „Whistleblowern" im Rahmen eines unternehmensinternen Meldesystems. Stets ist aber zwischen dem Geheimhaltungsbedürfnis des Arbeitgebers und dem Auskunftsinteresse des Arbeitnehmers abzuwägen. Das Bestehen eines berechtigten **Geheimhaltungsinteresses hat der Arbeitgeber ihm substantiiert darzulegen** und ggf. zu beweisen (*LAG Baden-Württemberg* NZA-RR 2019, 242 Rn. 180 ff.). Ansonsten hat der Arbeitgeber die verlangten Informationen **binnen eines Monats** zur Verfügung zu stellen, wobei er die Frist um höchstens zwei Monate verlängern kann, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist (Art. 12 Abs. 3 DS-GVO). Bei **offenkundig unbegründeten oder exzessiven Anträgen** – insbesondere im Fall von häufiger Wiederholung – kann der Arbeitgeber die **Auskunft und das Zuverfügungstellen einer Kopie verweigern** oder dem Arbeitnehmer die Kosten dafür in Rechnung stellen (Art. 12 Abs. 5 DS-GVO). Ein hoher Arbeitsaufwand steht dem Anspruch nicht entgegen. Erforderlich ist vielmehr ein **rechtsmissbräuchliches Verhalten** (Kühling/Buchner/*Bäcker* DS-GVO Art. 12 Rn. 37). Das kann bejaht werden, wenn eine Datenkopie ohne jedes Eigeninteresse **(nutzlose Rechtsausübung) oder in reiner Schädigungsabsicht** verlangt wird (*König* CR 2019, 295, 297). Dasselbe gilt, wenn der Arbeitnehmer personenbezogene Daten durch Einblick in den eigenen E-Mail-Account selbst ermitteln kann, er aber eine entsprechende Auskunft in Textform verlangt (*LAG Hessen* ZD 2013, 413). Dagegen kann eine Datenkopie nicht allein deshalb versagt werden, weil der Arbeitnehmer damit ein über die bloße **Rechtmäßigkeitskontrolle** hinausgehenden Zweck verfolgt. So kann er z.B. im Rahmen eines Kündigungsschutzprozesses wegen einer Verdachtskündigung die Herausgabe von Videoaufnahmen verlangen, um hinsichtlich der vom Arbeitgeber vorgetragenen Verdachtsmomente das Bestehen eines prozessualen Sachvortrags- oder Beweisverwertungsverbotes wegen einer Verletzung seines Persönlichkeitsrechts prüfen zu können (*König* CR 2019, 295, 297). Ein solches Verlangen stellt in der Regel keinen Rechtsmissbrauch dar, solange keine weiteren Umstände hinzutreten. Erforderlich ist vielmehr ein zielgerichtetes treuwidriges Verhalten. Die bloße Möglichkeit, mit dem Verlangen Druck auf den Arbeitgeber auszuüben, genügt für sich allein deshalb nicht. **36**

Ungeklärt ist bislang, ob **alle Medien** (E-Mails, sämtlicher Schriftverkehr, Notizen von Vorgesetzten) **in Kopie herauszugeben sind** (*Claus/Reif* RDV 2019, 238, 244; *Dausend* ZD 2019, 103; *Fuhlrott* NZA-RR 2019, 251; *Härting* CR 2019, 219, 225; *König* CR 2019, 295, 297; *Suchan* ZD 2021, 198; *Wybitul/Brams* NZA 2019, 672; *Wybitul/Baus* CR 2019, 494; *Zikesch/Sörup* ZD 2019, 239). Nach Ansicht des *LG Köln* (ZD 2019, 313) bezieht sich der Anspruch weder auf sämtliche internen Vorgänge, noch kann der Betroffene verlangen, den gesamten Schriftverkehr, soweit er ihm bereits bekannt ist, erneut ausgedruckt und übersendet zu erhalten. Der Anspruch aus Art. 15 DS-GVO diene nicht der „vereinfachten Buchführung des Betroffenen", sondern solle sicherstellen, dass dieser den Umfang **37**

und Inhalt der von ihm gespeicherten personenbezogenen Daten beurteilen könne. Zu der mit Art. 15 DS-GVO im wesentlichen vergleichbaren Vorschrift des Art. 12 lit. a DS-RL hat der **EuGH** die Ansicht vertreten, dass es zur Wahrung des dort eingeräumten Auskunftsanspruchs **genüge, dass der Betroffene eine vollständige Übersicht seiner Daten in verständlicher Form erhalte.** Sinn und Zweck des Auskunftsanspruchs sei es, dem Betroffenen die **Kenntnisnahme der über ihn gespeicherten Daten zu ermöglichen, um zu prüfen, ob sie richtig seien und der DS-RL gemäß verarbeitet wurden**, um ggf. vom Verantwortlichen die Berichtigung, Löschung oder Sperrung seiner Daten zu verlangen (*EuGH* EuZW 2009, 546 Rn. 51 ff.; *EuGH* ZD 2014, 515 Rn. 44, 57 f.). Soweit dieses Ziel durch eine andere Form der Mitteilung vollständig erreicht werde, stehe dem Betroffenen kein Recht zu, eine Kopie des Dokuments oder der Originaldatei, in der diese Daten enthalten seien, zu erhalten. Das *OLG Köln* (ZD 2018, 536) und das *AG Dortmund* (NJOZ 2018, 1420) haben den vom EuGH vertretenen Ansatz in jüngsten Entscheidungen für das Auskunftsrecht nach § 34 BDSG a.F. übernommen. Nach Ansicht des *LAG Niedersachsen* (NZA-RR 2020, 571) soll der Anspruch auf Erteilung einer Kopie nicht weiter als die in Art 15 Abs. 1 DS-GVO geregelten **Pflichtangaben gehen**. Das **BAG** hat die **Frage ausdrücklich offengelassen** (Urt. v. 27.4.2021 - 2 AZR 342/20) und statt dessen prozessuale Probleme aufgeworfen. Ein **Klageantrag** auf Überlassung einer Kopie von E-Mails ist nach Ansicht des Gerichts **nicht hinreichend bestimmt** i.S.v. § 253 Abs. 2 Nr. 2 ZPO, wenn die E-Mails, von denen eine Kopie zur Verfügung gestellt werden soll, nicht so genau bezeichnet sind, dass im Vollstreckungsverfahren zweifelhaft bleibt, auf welche E-Mails sich die Verurteilung bezieht. Gegenstand der Verurteilung wäre die Vornahme einer nicht vertretbaren Handlung i.S.v. § 888 ZPO, für die im Zwangsvollstreckungsrecht nicht vorgesehen sei, dass der Schuldner an Eides statt zu versichern habe, sie vollständig erbracht zu haben. Eine andere Frage ist, wo und wie der Auskunfts- und Überlassungsanspruch zu erfüllen ist. Laut *LAG Niedersachsen* (NZA-RR 2020, 571) sei **Leistungsort der Wohnort des Auskunftssuchenden**. Ein Fernzugriff auf ein sicheres System, in dem die Daten direkt abrufbar seien, ersetze die Übersendung im Wege der Schickschuld per Post oder auf elektronischem Wege nur, wenn sich der Anspruchsteller damit einverstanden erklärt habe.

38 Sodann kann die betroffene Person die unverzügliche **Berichtigung** unrichtiger bzw. die Vervollständigung unvollständiger Daten verlangen, indem sie z.B. ergänzende Erklärungen abgibt. Ferner kann sie die unverzügliche **Löschung** ihrer Daten fordern, etwa wenn deren Speicherung für das Erreichen des damit verfolgten Verarbeitungszwecks nicht mehr erforderlich ist, wenn die betroffene Person ihre Einwilligung widerrufen oder Widerspruch gegen die Verarbeitung eingelegt hat oder wenn Daten unrechtmäßig verarbeitet wurden (Art. 17 Abs. 1 DS-GVO). Der Verantwortliche kann dem entgegnen, dass er die Daten zur Ausübung oder zur Verteidigung von Rechtsansprüchen weiter benötigt (Art. 17 Abs. 3 lit. e DS-GVO). Nach Maßgabe von Art. 18 DS-GVO kann die betroffene Person auch die Einschränkung der Verarbeitung fordern, was zur Folge hat, dass die Daten – von

ihrer Speicherung abgesehen – nur mit ihrer Einwilligung oder zur Ausübung bzw. zur Verteidigung von Rechtsansprüchen des Verantwortlichen weiter verarbeitet werden dürfen. Hat die betroffene Person in die Datenverarbeitung eingewilligt, steht ihr ein Recht auf Datenübertragbarkeit nach Maßgabe von Art. 20 DS-GVO zu. Selbst wenn die Daten rechtmäßig verarbeitet werden, kann die betroffene Person jederzeit Widerspruch einlegen, wenn sich Gründe aus ihrer besonderen Situation ergeben. In diesem Fall muss der Verantwortliche nachweisen, dass zwingende Gründe für die Verarbeitung bestehen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen (Art. 21 Abs. 1 DS-GVO). Außerdem kann die betroffene Person fordern, keiner Entscheidung unterworfen zu werden, wenn diese ausschließlich auf einer automatisierten Verarbeitung beruht und ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (Art. 22 Abs. 1 DS-GVO), es sei denn, dass eine solche Entscheidung mit ihrer ausdrücklichen Einwilligung geschieht oder für den Abschluss oder die Erfüllung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person erforderlich ist (Art. 22 Abs. 2 DS-GVO). Die Vorgaben der DS-GVO sind für das deutsche Recht – soweit es die Öffnungsklauseln in den Art. 13 ff. DS-GVO erlauben – durch die §§ 32 ff. BDSG eingeschränkt worden. Ob das erlaubt ist, wird die Rechtsprechung des EuGH klären müssen.

39 Ist einem Beschäftigten wegen eines Verstoßes gegen die DS-GVO ein **materieller** oder **immaterieller Schaden** entstanden, hat er **Anspruch auf Schadenersatz** gegen den Verantwortlichen (Art. 82 Abs. 1 DS-GVO). Der Verantwortliche wird von seiner **Haftung nur dann befreit**, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist (Art. 82 Abs. 3 DS-GVO). Das ist der Fall, wenn er sämtliche Sorgfaltsanforderungen erfüllt hat und **ihm nicht die geringste Fahrlässigkeit vorzuwerfen ist** oder wenn der Schaden ausschließlich auf dem Verhalten der betroffenen Person oder höherer Gewalt beruht (Kühling/Buchner/*Bergt* DS-GVO Art. 82 Rn. 54). Dabei haftet der Verantwortliche auch für das Handeln seiner Mitarbeiter, ohne sich entlasten zu können. Eine unmittelbare Haftung trifft auch den Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 und Art. 28 DS-GVO. Art. 82 DS-GVO gewährt dem Geschädigten – zusätzlich zu den allgemeinen zivilrechtlichen Haftungsansprüchen nach deutschem Recht (§§ 280 Abs. 1, 311 Abs. 2, 823 ff. BGB) – eine weitere, verschuldensunabhängige Anspruchsgrundlage. Der Betroffene trägt nur die Darlegungs- und Beweislast für den Tatbestand der Rechtsverletzung. Der Arbeitgeber hat sich dann zu exkulpieren oder kann die mangelnde Kausalität zwischen der von ihm zu vertretenden Rechtsverletzung und dem Schaden nachweisen. Zur Frage, ob datenschutzrechtliche Schadensersatzansprüche im Musterfeststellungsverfahren geltend gemacht werden können, *Geissler/Ströbel* NJW 2019, 3414.

40 Ein **immaterieller Schaden** i.S.d. Art. 82 DS-GVO entsteht nicht nur, wenn die datenschutzwidrige Verarbeitung zu einer **Diskriminierung**, einem Verlust der Vertraulichkeit, einer **Rufschädigung** oder anderen **gesellschaftlichen Nachteilen** führt, sondern auch, wenn die betroffene Person **um ihre Rechte und Freiheiten gebracht oder daran gehindert wird, die sie betreffenden personenbezogen Da-**

ten zu kontrollieren (*ArbG Dresden* ZD 2021, 54). Kommt daher der Verantwortliche seiner Auskunftspflicht gem. Art. 15 DS-GVO nicht, nicht vollständig oder nicht rechtzeitig nach, kann der Betroffene einen Schadensersatzanspruch gem. Art. 82 Abs. 1 DS-GVO geltend machen, **ohne einen materiellen Schaden darlegen zu müssen** (*ArbG Düsseldorf* ZD 2020, 649). Der **Schadensersatz soll eine abschreckende Wirkung** haben, um der DS-GVO zum Durchbruch zu verhelfen (effet utile). Deshalb kann sich die Bemessung des immateriellen Schadensersatzes auch an **Art. 83 Abs. 2 DS-GVO** orientieren, sodass als **Zumessungskriterien** u.a. Art, Schwere, Dauer des Verstoßes, Grad des Verschuldens, Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens, früher einschlägige Verstöße sowie die Kategorien personenbezogener Daten in Betracht kommen (*LG Köln* ZD 2021, 47; *ArbG Dresden* ZD 2021, 54; *ArbG Düsseldorf* ZD 2020, 649; *ArbG Neumünster* ZD 2021, 171). Die Schwere des immateriellen Schadens ist für die Begründung der Haftung nach Art. 82 Abs. 1 DS-GVO irrelevant; sie wirkt sich nur bei der Höhe des Anspruchs aus (*ArbG Düsseldorf* ZD 2020, 649). Die Beeinträchtigung besteht vor allem in der Ungewissheit über die Verarbeitung der Daten des Betroffenen. Das *ArbG Neumünster* (ZD 2021, 171) hat z.B. 500 EUR für jeden Monat der Verspätung zugesprochen. Handelt es sich um einen Bagatellfall (z.B. einmalige Übersendung eines Kontoauszugs an einen falschen Empfänger), kann auch unter Berücksichtigung der weiteren Umstände des Einzelfalls die **Zuerkennung eines Schmerzensgelds ausgeschlossen** sein (*LG Köln* ZD 2021, 47). Die Bemessung kann sich auch an der Finanzkraft des Verantwortlichen orientieren (*ArbG Düsseldorf* ZD 2020, 649). Die Rechtsprechung ist allerdings noch im Fluss (*Paal/Aliprandi* ZD 2021, 241). Da selbst der EuGH bislang nicht abschließend geklärt hat, unter welchen Voraussetzungen Art. 82 Abs. 1 DS-GVO einen Entschädigungsanspruch gewährt und sich diese Frage auch nicht unmittelbar aus der DS-GVO beantworten lässt, müssen der BGH oder das BAG den EuGH um Vorabentscheidung nach Art. 267 Abs. 3 AEUV anrufen, damit dieser die Vorschrift unionsweit einheitlich auslegen kann. Unterlassen sie dies in einem Rechtsstreit, bei dem die Auslegung des Art. 82 DS-GVO entscheidungserheblich ist, verletzen sie das Recht auf den gesetzlichen Richter (Art. 101 Abs. 1 GG). Ihr letztinstanzliches Urteil kann dann mit der Verfassungsbeschwerde angefochten werden (*BVerfG* ZD 2021, 266).

5. Weitere Sanktionen bei Verstößen gegen das Datenschutzrecht

a) Bußgeld

41 Verstöße gegen die DS-GVO sind mit einem Bußgeld bedroht, dessen Verhängung durch die zuständige Aufsichtsbehörde wirksam, verhältnismäßig und abschreckend zu sein hat (Art. 83 Abs. 1 DS-GVO). Der Sanktionsrahmen wurde im Vergleich zum bisherigen Recht drastisch ausgeweitet und für alle Mitgliedstaaten einheitlich geregelt. Das Bußgeld kann danach bis zu 10 Mio. EUR betragen, falls der Verantwortliche gegen die – eher formalen – Anforderungen der Art. 8, 11, 25–39, 42 und 43 DS-GVO verstößt. Gegen Unternehmen können darüber hi-

naus sogar Bußgelder von bis zu 2 % ihres gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden. Bei Missachtung der materiellen Verarbeitungsgrundsätze nach den Art. 5, 6, 7 und 9 DS-GVO, der Nichtgewährung der Betroffenenrechte nach Art. 12–22 DS-GVO, einer nicht nach den Art. 44 DS-GVO ff. zulässigen Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder bei Verstößen gegen mitgliedstaatliches Datenschutzrecht in Ausfüllung der Öffnungsklauseln – wie etwa für den Beschäftigtendatenschutz in Art. 88 DS-GVO – sowie bei der Nichtbefolgung von Anweisungen der Aufsichtsbehörde gem. Art. 58 DS-GVO kann das Bußgeld bis zu 20 Mio. EUR betragen, bei Unternehmen sogar bis zu 4 % ihres gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, falls dieser Betrag höher liegt. Dabei ist nach EG 150 S. 3 DS-GVO auf den kartellrechtlichen Unternehmensbegriff i.S.d. Art. 101, 102 AEUV abzustellen, d.h. auf den Umsatz der gesamten Unternehmensgruppe. Art. 83 DS-GVO folgt dabei – anders als das deutsche Recht – dem Modell der originären Verbandshaftung. Dieses sanktioniert bei Verstößen gegen die DS-GVO den Rechtsträger unmittelbar, d.h. bei Unternehmen regelmäßig die juristische Person; die Zurechnung von Handlungen natürlicher Personen ist nicht erforderlich (Kühling/Buchner/*Bergt* DS-GVO Art. 83 Rn. 20). Wird die Geldbuße einer natürlichen Person auferlegt, muss die Aufsichtsbehörde das allgemeine Einkommensniveau im jeweiligen Mitgliedstaat und die wirtschaftliche Lage der Person berücksichtigen (EG 150 S. 4 DS-GVO). Bei geringfügigeren Verstößen oder falls voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, kann anstelle einer Geldbuße eine Verwarnung erteilt werden (EG 148 S. 2 DS-GVO). Für die Verhängung und die Höhe des Bußgelds sollen nach Art. 83 Abs. 2 DS-GVO u.a. folgende Gesichtspunkte eine Rolle spielen: Art, Schwere und Dauer des Verstoßes, der vorsätzliche Charakter des Verstoßes, die Maßnahmen zur Minderung des entstandenen Schadens, der Grad der Verantwortlichkeit, die Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde sowie die Einhaltung der gegen den Verantwortlichen angeordneten Maßnahmen. Offen ist, ob Art. 83 DS-GVO die Verhängung von Geldbußen ohne Verschulden vorsieht (Kühling/Buchner/*Bergt* DS-GVO Art. 83 Rn. 34 ff.) und ob für die Verfolgung des Legalitäts- oder das Opportunitätsprinzip gilt (Kühling/Buchner/*Bergt* DS-GVO Art. 83 Rn. 30 ff.). Für die Verhängung des Bußgelds gelten die Vorschriften des OWiG sinngemäß (§ 41 BDSG).

b) Geld- und Freiheitsstrafen

Strafrechtliche Sanktionen bei Verstößen gegen das unionsrechtliche Daten- **42**
schutzrecht enthält die DS-GVO nicht. Art. 84 DS-GVO enthält jedoch eine Öffnungsklausel für entspr. mitgliedstaatliche Regelungen. Der deutsche Gesetzgeber hat von dieser Möglichkeit Gebrauch gemacht und die Vorschrift des § 42 BDSG erlassen. Danach wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein, einem

Dritten übermittelt oder auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt (Abs. 1). Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind, ohne hierzu berechtigt zu sein, verarbeitet oder durch unrichtige Angaben erschleicht und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen (Abs. 2). Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte für den Datenschutz und die Aufsichtsbehörde (Abs. 3).

c) Prozessrechtliche Folgen

43 Während die StPO zahlreiche Vorschriften über die Zulässigkeit der Verwertung von Beweismitteln enthält (§§ 69 Abs. 3, 100d Abs. 5 S. 2, 136a Abs. 3 S. 2, 252 StPO), sind dem ArbGG und der ZPO solche Bestimmungen weitgehend fremd (vgl. aber z.B. § 383 Abs. 3 ZPO). Umfang und Reichweite von entspr. Verwertungsverboten, insbesondere im Hinblick auf Beweise, die unter Verstoß gegen Persönlichkeitsrechte des Arbeitnehmers oder gegen datenschutzrechtliche Bestimmungen gewonnen wurden, sind deshalb **umstritten** (*BAG* NZA 2003, 1193; NZA 2017, 112 Rn. 23 ff.; vgl. aus dem umfangreichen Schrifttum zuletzt *Betz* RdA 2018, 100; *Eufinger* DB 2017, 1266; *Fuhlrott/Schröder* NZA 2017, 278; *Kaiser* NJW 2017, 2790 ff.; *Reitz* NZA 2017, 273 ff.). Eine analoge Anwendung strafprozessualer Normen kommt schon deshalb nicht in Betracht, weil Zivil- und Strafrecht unterschiedlichen Prozessmaximen folgen und der Zivilrichter nicht an ein Strafurteil gebunden ist (§ 14 Abs. 2 Nr. 1 EGZPO). Das geltende Recht wird durch zahllose Entscheidungen des Bundesverfassungsgerichts (*BVerfG* NJW 2007, 753), des Bundesgerichtshofs (zuletzt NJW 2018, 2883) und des Bundesarbeitsgerichts (*BAG* NZA 2011, 571; 2012, 1025; 2014, 143; 2017, 112; 2017, 1179; 2017, 1327; 2019, 1212) bestimmt. Danach steht fest, dass **nicht aus jedem Beweiserhebungsverbot zwangsläufig ein Beweisverwertungsverbot** resultiert (*BGHSt* 19, 325, 331; 38, 214, 219). Wann das der Fall ist, ist bislang nicht abschließend geklärt. Maßgeblich ist stets der Schutzzweck der Norm, gegen die bei der Beweisgewinnung verstoßen wurde (Musielak/*Foerste* § 286 ZPO Rn. 6). Nach der vom BGH vertretenen „Rechtskreistheorie" bleiben jedenfalls Verstöße gegen Beweiserhebungsverbote, die ausschließlich dem Schutz des Staates oder dritter Personen dienen, folgenlos (*BGHSt* 1, 39; 11, 213; *BGH* NStZ 1983, 354).

44 Die Frage eines Beweisverwertungsverbots im Zivilverfahren ist mitunter deshalb problematisch, weil für dieses der **Beibringungsgrundsatz** gilt (*Lunk* NZA 2009, 457; *Musielak* Einl. ZPO Rn. 37 ff.). Stellen die Parteien – auch wider besseres Wissen – den Tatsachenstoff unstreitig, ist das Gericht hieran wie an ein Geständnis gebunden: es darf für unbestrittene Tatsachen weder einen Beweis verlangen noch einen solchen erheben (*BAG* NZA 2008, 1008). Ein „Sachvortragsverwertungsverbot" besteht also grds. nicht (*Heinemann* MDR 2001, 137, 140; Germelmann/*Prütting* § 58 ArbGG Rn. 32). Die Konsequenz ist freilich folgende: Wo das Gericht bei einem unstreitigen Sachverhalt keine Beweise erheben darf, laufen

Beweisverwertungsverbote leer. Dazu kommt, dass der Arbeitnehmer den Sachvortrag des Arbeitgebers aufgrund der in § 138 Abs. 1 ZPO normierten Pflicht zur wahrheitsgemäßen Erklärung nur sehr bedingt bestreiten darf. Der Arbeitnehmer darf keine Erklärungen wider besseres Wissen abgeben (statt aller Musielak/*Stadler* § 138 ZPO Rn. 2 m.w.N.), so dass ein Verbot der prozessualen Lüge gilt. Missachtet er dies, läuft er Gefahr, sich wegen eines versuchten Prozessbetrugs strafbar zu machen. Schweigt er, gilt der Prozessvortrag des Arbeitgebers als zugestanden (§ 138 Abs. 3, 331 Abs. 1 ZPO).

Ob das in diesem Zusammenhang auch Tatsachen betrifft, die der Arbeitgeber unter Verstoß gegen Persönlichkeitsrechte ermittelt hat, ist **zweifelhaft** (*BAG* NZA 2011, 571, 574; *OLG Karlsruhe* NJW 2000, 1577, 1578; Maschmann/*Natter* Beschäftigtendatenschutz in der Reform, S. 133, 151 f.). Die Wahrheitspflicht ist ein Gebot redlichen Verhaltens (*OLG Brandenburg* NJW-RR 2000, 1522), das nicht zum Selbstzweck besteht, sondern eine faire Verfahrensführung ermöglichen soll (*Olzen* ZZP 1985, 403 ff., 419; Musielak/*Stadler* § 138 ZPO Rn. 1). Einige Stimmen wollen dem Arbeitnehmer deshalb ein **„Recht zur Lüge"** zugestehen (so Zöller/*Greger* § 138 Rn. 3; *Heinemann* MDR 2001, 137, 142). Das nützt indes wenig, weil sich der Arbeitnehmer damit dem Vorwurf eines zumindest versuchten Prozessbetrugs aussetzt (so zu Recht *BAG* NZA 2011, 571, 574), abgesehen von der (beschränkten) Überzeugungskraft einer derartigen Verteidigungsstrategie, wenn der Arbeitgeber Augenscheinobjekte (Videoaufzeichnung, E-Mail-Protokolle usw.) vorlegt. Umgekehrt genügt es sicher auch nicht, den Arbeitnehmer schlicht darauf zu verweisen, er hätte den Vortrag nur zu bestreiten brauchen, weil dann eine Beweisaufnahme nötig wäre, bei der die einschlägigen Verwertungsverbote wieder gelten würden (so offenbar aber *LAG Sachsen-Anhalt* 15.4.2008, *LAGE* § 626 BGB Nr. 17; ähnlich *Grimm/Schiefer* RdA 2009, 329, 342; Henssler/Willemsen/Kalb/*Lembke* Vorb. BDSG, Rn. 112). Erst recht scheidet eine solche Pflicht im Falle des § 138 Abs. 4 ZPO aus, wo einfaches Bestreiten nicht genügt und sich der Arbeitnehmer mit einem bewusst falschen Gegenvorbringen belasten müsste. **45**

Aus diesem Grunde soll nach der neueren Rspr. (*BAG* NZA 2017, 112 Rn. 23, 25; NZA 2018, 1329 Rn. 14 ff.) unstreitiger Sachvortrag nicht allein deshalb uneingeschränkt verwertbar sein, weil die durch diesen belastete Partei die Möglichkeit des Bestreitens hatte. Da eine Partei im zivil- und arbeitsgerichtlichen Verfahren der Wahrheitspflicht nach § 138 Abs. 1 und 2 ZPO unterliegt, kann sie nicht gezwungen werden, grundrechtswidrig über sie erlangte Informationen bestreiten zu müssen, um ihre Rechte zu wahren. Daher kann der Schutzzweck der bei der Informationsgewinnung verletzten Norm auch einer gerichtlichen Verwertung *unstreitigen* Sachvortrags entgegenstehen (*BAG* NZA 2017, 1179 Rn. 21; NZA 2011, 571 Rn. 29; NZA 2008, 1008; ähnlich *OLG Karlsruhe* NJW 2000, 1577 [zu II 3 b]; a.A. *Ahrens* Der Beweis im Zivilprozess, Kap. 6 Rn. 29). Das setzt voraus, dass es dem Schutzzweck etwa des allgemeinen Persönlichkeitsrechts zuwiderliefe, selbst den inhaltlichen Gehalt eines Beweismittels in Form von Sachvortrag z.B. in Folge von § 138 Abs. 3 ZPO oder § 331 Abs. 1 S. 1 ZPO zur **46**

Entscheidungsgrundlage zu machen (vgl. *Weber* ZZP 2016, 57, 81). Ein solches **„Sachvortrags-Verwertungsverbot“** ist Ausfluss der Grundrechtsbindung der Gerichte, deren Beachtung ihnen unabhängig davon obliegt, ob sich eine Partei darauf beruft. Hat das **Gericht** Anhaltspunkte dafür, dass für den Rechtsstreit relevante Erkenntnisse unter Verletzung des allgemeinen Persönlichkeitsrechts einer Partei gewonnen wurden, muss es **von Amts wegen prüfen, ob es das Vorbringen, selbst wenn es unbestritten bleibt, bei der Feststellung des Tatbestands berücksichtigen darf.** Hiervon besteht dann eine Ausnahme, wenn die Partei auf die Geltendmachung der Rechtsverletzung wirksam verzichtet hat (*BAG* NZA 2017, 112 Rn. 25). Ob ein Verwertungsverbot eingreift, muss allerdings nur dann geprüft werden, wenn entsprechende Anhaltspunkte dazu Anlass geben. Ergeben sich nicht schon aus dem Vorbringen des Arbeitgebers – einschließlich der Beweisantritte – Zweifel an der Verwertbarkeit des Vorgetragenen, ist es Sache des Arbeitnehmers, die relevanten Umstände für eine möglicherweise grundrechtswidrige Erkenntnis- oder Beweismittelgewinnung aufzuzeigen. Insofern bleibt es also beim Beibringungsgrundsatz (*BAG* NZA 2018, 1329 Rn. 17). Das Gericht muss jedoch begründeten Zweifeln durch Hinweise und Auflagen an die Parteien nachgehen und gegebenenfalls Beweis zu den tatsächlichen Voraussetzungen für das Vorliegen eines Verwertungsverbots erheben. So wird es regelmäßig Grund zu der Nachfrage haben, aus welchem Anlass und auf welche Weise eine Videoaufzeichnung zustande gekommen ist, deren Inaugenscheinnahme als (einziger) Beweis angeboten wird (*BAG* NZA 2018, 1329 Rn. 17; *Niemann* JbArbR Bd. 55, S. 41, 63?ff.). Besteht – wie im Regelfall – ein Verwertungsverbot, umfasst dieses nicht nur das unrechtmäßig erlangte Beweismittel selbst, wie z.B. eine Inaugenscheinnahme der Videoaufzeichnungen, sondern auch dessen mittelbare Verwertung wie etwa die Vernehmung eines Zeugen über den Inhalt des Bildmaterials (*BAG* NZA 2017, 112 Rn. 24).

47 Ob es eine **Fernwirkung** eines Beweisverwertungsverbots gibt, wie die *fruit of the poisonous tree*-Doktrin behauptet, ist offen (*Bergwitz* NZA 2012, 353, 358; *Dzida/Grau* NZA 2010, 1201, 1206). Der BGH hat sie bekanntlich nur für das Strafverfahren abgelehnt (*BGH* NJW 1988, 1223), weil damit die richterliche Pflicht, den Sachverhalt umfassend von Amts wegen zu erforschen, zu stark beschränkt würde. Im Zivilprozess gilt die Instruktionsmaxime dagegen nicht, weshalb die Gerichte hier von Fall zu Fall anders entscheiden (*BGH* NJW 2006, 1657; NJW 2018, 2883)*BAG* NZA 2011, 571, 574 f.; NZA 2017, 112). Im Zweifel unterbleibt die Verwertung nur, wenn durch sie ein verfassungsrechtlich geschütztes Recht der einen Partei verletzt würde, ohne dass dies zur Gewährleistung eines ebenfalls geschützten Rechtsguts der anderen Partei notwendig wäre. Erforderlich ist also auch hier eine am Grundsatz der Verhältnismäßigkeit orientierte **Abwägung** der betroffenen Rechtsgüter (*BGH* NJW 2006, 1657, 1659).

48 Entscheidend dürfte damit sein, dass in der gerichtlichen Verwertung eines persönlichkeitsrechtswidrig erlangten Beweismittels ein **erneuter Eingriff in das Persönlichkeitsrecht** liegt, der einer sachlichen Rechtfertigung unter Beachtung des Verhältnismäßigkeitsprinzips und damit einer umfassenden **Abwägung** bedarf

(*BVerfG* NJW 2002, 3619, 3624; *BGH* 15.5.2018 – VI ZR 233/17, Rn. 44 ff.; *BAG* NZA 2003, 1193; NZA 2017, 112 Rn. 23 ff.; ausf. *Betz* RdA 2018, 100 ff.). Das allgemeine Interesse an einer funktionstüchtigen Zivilrechtspflege kann für sich allein den Eingriff ebenso wenig rechtfertigen (*BAG* NZA 2012, 1025; NZA 2017, 1327 Rn. 41) wie das Bedürfnis, sich ein Beweismittel für zivilrechtliche Ansprüche zu sichern (*BAG* NZA 2011, 571, 2014, 143; NZA 2017, 112, Rn. 24; NZA 2017, 1327 Rn. 41). Vielmehr müssen weitere Umstände hinzutreten, bei deren Vorliegen das Interesse an der Beweiserhebung schwerer als die Persönlichkeitsbeeinträchtigung wiegt (*BAG* NZA 2003, 1193, 1195; NZA 2017, 112 Rn. 24; NZA 2017, 1327 Rn. 41). Das hat die **Rechtsprechung** ausnahmsweise angenommen, wenn eine an sich verbotene Maßnahme das einzig mögliche Mittel ist, den Täter zu überführen (*BGH* NJW 1988, 277) oder wenn die Beweisnot der beweisbelasteten Partei ausgenutzt wird (*BVerfG* NJW 2002, 3619, 3624; *BAG* NZA 2003, 1193, 1196), etwa bei offenbarer Verletzung der Wahrheits- (§ 138 ZPO) oder Vorlagepflicht (§§ 422, 423 ZPO). Unter diesen Umständen wird man allerdings schon die Beweiserhebung für zulässig halten müssen. Umgekehrt gilt: War der mit der privaten Beweiserhebung verbundene Eingriff in das Persönlichkeitsrecht gerechtfertigt, spricht nichts dagegen, das so gewonnene Beweismittel auch im Prozess zu verwerten (*BAG* NZA 2017, 112 Rn. 35 ff.). Die materiellen Rechtfertigungsgründe, die dem Arbeitgeber bei der Beweisgewinnung zur Seite standen, wirken in einem späteren Prozess fort. Das gilt auch für „Zufallsfunde". Ist nämlich eine Videoüberwachung zulässig, so sind durch sie bewirkte Eingriffe in die Persönlichkeitsrechte mitbetroffener Arbeitnehmer ebenfalls durch den Aufklärungszweck gerechtfertigt. Zeigt sich bei einer solchen Videoüberwachung ein strafbares Verhalten eines Mitarbeiters, der nicht zum Kreis der Verdächtigen gehört, können die Aufnahmen im Prozess gegen ihn verwendet werden (*BAG* NZA 2017, 112 Rn. 35 ff.). Noch großzügiger ist die Rechtsprechung bei der Verwertung von Aufnahmen im allgemeinen Straßenverkehr, die mittels einer „Dash-Cam" angefertigt werden. Diese ist angesichts der notorischen Beweisnot in Unfallprozessen und der relativen Geringfügigkeit des Eingriffs in das Recht am eigenen Bild grds. zulässig (*BGH* NJW 2018, 2883 Rn. 47 ff.) und stellt nach Ansicht des EGMR auch keine Verletzung des Art. 8 EMRK dar (*EGMR* NJW 2015, 1079).

IV. Mitarbeiterüberwachung

Werden Mitarbeiter kontrolliert, kann darin eine Verarbeitung personenbezogener Daten liegen. Allerdings eröffnet nicht jede Kontrolle den Anwendungsbereich der DS-GVO bzw. des § 26 BDSG. Die DS-GVO gilt nicht, wenn Mitarbeiter nur um Angaben zum Stand der ihnen übertragenen Aufgaben gebeten werden. Die erteilten Auskünfte stellen nämlich nicht allein deshalb personenbezogen Daten i.S.d. DS-GVO dar, weil sie von einer „identifizierten oder identifizierbaren natürlichen Person" (Art. 4 Nr. 1 DS-GVO) stammen. Vielmehr kann es sich auch um **rein „sachbezogene Daten"** handeln, deren Erhebung keiner datenschutzrechtlichen Erlaubnis bedarf (Gola/*Gola* DS-GVO, Art. 4 Rn. 11). Das ist **49**

der Fall, wenn der Mitarbeiter ausschließlich um Mitteilungen über gewisse Umstände, Vorfälle, Zustände usw. gebeten wird. Beschäftigtendaten liegen erst dann vor, wenn es um Einzelangaben über bestimmte „persönliche oder sachliche Verhältnisse" des Betroffenen geht (vgl. § 3 Abs. 1 BDSG a.F.). Das setzt **einen *konkreten* Personenbezug** der Angabe voraus (ähnlich *Art.-29-Datenschutzgruppe* WP 136 v. 20.6.2007, S. 10 ff.) Dieser besteht, wenn die Information auch *inhaltlich* die Person betrifft, die sie erteilt (ebenso *Krügel* ZD 2017, 455, 459). Das ist zu bejahen, wenn der Vorgesetzte Angaben über das Verhalten des ihm unterstellten Mitarbeiters oder seiner Kollegen verlangt, gleichviel ob es bereits abgeschlossen oder erst geplant ist, oder es um Informationen über bestimmte persönliche Merkmale und Eigenschaften des Unterstellten geht.

50 Für diese sowie auch für viele andere Überwachungsformen erlaubt Art. 88 Abs. 1 DS-GVO die Verarbeitung von Beschäftigtendaten ausdrücklich auch zum Schutz des Eigentums des Arbeitgebers oder der Kunden. Darüber hinaus erwähnt Art. 88 Abs. 2 DS-GVO die **„Überwachungssysteme am Arbeitsplatz",** d.h. alle offen oder verdeckt durchgeführten Maßnahmen zur Kontrolle von Mitarbeitern, wie etwa die Zugangskontrolle (→ Rn. 55), Videoüberwachung (→ Rn. 60), die Erfassung von Telefondaten (→ Rn. 84), die Kontrolle des E-Mail-Verkehrs und der sonstigen Internetnutzung (→ Rn. 72), die Aufzeichnung von Bewegungsdaten per RFID, Handy-Ortung und GPS sowie die Verarbeitung von Körperdaten durch in die Arbeitskleidung integrierte Sensoren, sog. „Wearables" (→ Rn. 92). Da es sich um Beschäftigtendaten handelt, spielt es keine Rolle, ob diese Daten automatisch durch eine technische Einrichtung (z.B. durch eine Videoanlage) erhoben und verarbeitet werden oder von einem Menschen (§ 26 Abs. 7 BDSG). Stets bedarf es einer Verarbeitungsgrundlage i.S.d. Art. 6 Abs. 1 DS-GVO. Wird der Mitarbeiter überwacht, um das Beschäftigungsverhältnis durchzuführen oder zu beenden oder um eine Straftat aufzudecken, liefert § 26 Abs. 1 BDSG die dafür notwendige Verarbeitungsgrundlage. Dient die Kontrolle anderen Zwecke – etwa der Durchsetzung des Hausrechts – ist Art. 6 Abs. 1 lit. f DS-GVO einschlägig.

51 Richtschnur für sämtliche Kontrollen ist der **Grundsatz der Verhältnismäßigkeit** (*BAG* AP Nr. 36, 41 zu § 87 BetrVG 1972 Überwachung), der auf zwei Ebenen relevant wird: Zum einen, wenn zu bestimmen ist, aus welchen **Anlässen** kontrolliert werden darf; zum anderen, wenn es um die **konkrete Durchführung** einer Überprüfung geht. Das Übermaßverbot gilt folglich für das „Ob" und das „Wie" einer Maßnahme. Eine Rolle spielt dabei, wie viele Personen einer Kontrolle ausgesetzt sind, ob sie hierfür einen Anlass gegeben haben, ob sie als Personen anonym bleiben, welche Umstände und Inhalte ihrer Kommunikation bei einer Überprüfung erfasst werden können und welche Nachteile aus der Überwachungsmaßnahme drohen (ständige Rspr., vgl. *BGH* 15.5.2018 – VI ZR 233/17, Rn. 18 ff. 26; *BAG* NZA 2017, 1179 Rn. 32 ff.; NZA 2017, 1327 Rn. 31 ff.). Intensive Grundrechtseingriffe sind nur zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft

sind, und der Einsatz des noch verbleibenden Mittels insgesamt als nicht unverhältnismäßig erscheint (*BAG* AP Nr. 41 zu § 87 BetrVG 1972 Überwachung; NZA 2017, 394 Rn. 30 m.w.N.).

52 Offene Überwachungsmaßnahmen, die der Verhinderung von Pflichtverletzungen dienen, können sich nach der neueren Rechtsprechung des BAG schon aufgrund des **Vorliegens einer abstrakten Gefahr** als verhältnismäßig erweisen, wenn sie **keinen solchen psychischen Anpassungsdruck erzeugen, dass die Betroffenen bei objektiver Betrachtung in ihrer Freiheit, ihr Handeln aus eigener Selbstbestimmung zu planen und zu gestalten, wesentlich gehemmt** sind (*BAG* NZA 2017, 1205 Rn. 20 und Rn. 28 ff.; *BAG* NZA 2019, 1212 Rn. 37). Dazu gehören z.B. Tor- und Taschenkontrollen beim Verlassen des Betriebs, wenn sie nach abstrakten Kriterien durchgeführt werden und keinen Arbeitnehmer besonders unter Verdacht stellen, offene Videoüberwachungen, soweit eine lückenlose, dauerhafte oder sehr detaillierte Erfassung des gesamten Verhaltens der Mitarbeiters ausgeschlossen ist, das Einsehen von nicht als privat gekennzeichneten Dateien, die auf einem Dienstrechner gespeichert sind, sowie das spontane Aufsuchen des Arbeitnehmers an seinem Arbeitsplatz zu Kontrollzwecken. Sie sollen nach § 26 Abs. 1 S. 1 zulässig sein. Die Entscheidungen sind zwar noch zu § 32 BDSG a.F. ergangen. Da die Norm aber wortlautgetreu in § 26 aufgegangen ist, ist davon auszugehen, dass das BAG auch unter der Geltung der DS-GVO und des BDSG 2018 daran festhält. Das gilt umso mehr, als das Gericht der Auffassung ist, dass seine Auslegung des § 32 I 1 BDSG a.F. sowohl der DS-RL als auch Art. 7 EU-GRC und Art. 8 EMRK entspricht (*BAG* NZA 2018, 1329 Rn. 25; *BAG* NZA 2019, 893 Rn. 52; *BAG* NZA 2019, 1212 Rn. 51).

53 Ausgangspunkt ist die Annahme, dass von § 32 Abs. 1 S. 2 BDSG a.F., der die Verarbeitung von Beschäftigtendaten zur Aufdeckung von Straftaten nur unter sehr restriktiven Bedingungen zulässt, **angeblich keine Sperrwirkung für anlassbezogene Datenerhebungen zu anderen Zwecken entfalte**. Vielmehr gestatte § 32 Abs. 1 S. 1 BDSG a.F. ausdrücklich die Verarbeitung auch zur Durchführung und zur Beendigung des Arbeitsverhältnisses. Dabei gehöre zur „Durchführung die Kontrolle, ob der Arbeitnehmer seinen Pflichten nachkommt", zur Beendigung im Sinne der Kündigungsvorbereitung „die Aufdeckung einer Pflichtverletzung, die die Kündigung des Arbeitsverhältnisses rechtfertigen kann" (*BAG* NZA 2017, 1327 Rn. 28; *BAG* NZA 2017, 1179 Rn. 26; *BAG* NZA 2019, 1212 Rn. 35.) Ausgehend von dieser Prämisse ist es nur ein kleiner Schritt, die Anforderungen noch weiter abzusenken und **sogar präventive Kontrollmaßnahmen zur Verhinderung von Pflichtverletzungen zuzulassen** (zustimmend *Gola* in Beschäftigtendatenschutz-Hdb Rn. 1213; abl. *Brink/Joos* jurisPR-ArbR 38/2019 Anm. 1; 1 *Däubler* Gläserne Belegschaften Rn. 312 b), jedenfalls solange die Überwachung **keinen „psychischen Anpassungsdruck"** erzeugt. **Unzulässig** ist eine offene Überwachung **erst dann**, wenn das **Verhalten „lückenlos, dauerhaft sowie sehr detailliert"** erfasst wird, so dass die betroffene Person „davon ausgehen muss, dass jede ihrer Bewegungen überwacht wird" und deshalb – vergleichbar mit der Situation einer verdeckten Überwachung – **„keine Möglichkeit einer unbewachten und ungestörten**

Wahrnehmung ihres Persönlichkeitsrechts“ mehr besteht (*BAG* NZA 2019, 1212 Rn. 38; ähnlich *Gola* in Beschäftigtendatenschutz-Hdb Rn. 1216: „keine Vollkontrolle“; *Wedde* in DWWS § 26 BDSG Rn. 119: „keine Totalkontrolle“). **Nicht mehr notwendig** ist nach der Rechtsprechung ein durch konkrete Tatsachen belegter **„einfacher Anfangsverdacht“ einer Straftat oder Arbeitspflichtverletzung;** es genügt bereits die „abstrakte Gefahr“ für eine Verletzung arbeitsvertraglicher Pflichten (*BAG* NZA 2017, 1327 Rn. 31; *BAG* NZA 2019, 1212 Rn. 37). Das überzeugt nicht. Denn damit verschwimmen die Grenzen zwischen präventiver und repressiver Überwachung, die in § 26 Abs. 1 BDSG durch die jeweils unterschiedlichen Voraussetzungen in S. 1 und 2 ausdrücklich errichtet hat (ebenso *Brink/Joos* jurisPR-ArbR 38/2019 Anm. 1). Vor diesem Hintergrund sollen im Folgenden die für die Praxis wichtigsten Kontrollmaßnahmen erörtert werden.

1. Spontanes Aufsuchen am Arbeitsplatz

54 Ein spontanes Aufsuchen des Mitarbeiters am Arbeitsplatz ist **ohne weiteres zulässig** (allgemeine Meinung, vgl. nur MünchArbR/*Reichold* 4. Aufl. 2018, § 55 Rn. 32 m.w.N.). Einschlägig ist **§ 26 Abs. 1 S. 1 BDSG**. Danach ist eine mit dem Kontrollbesuch verbundene Erhebung von Beschäftigtendaten – auch wenn sie nicht automatisiert erfolgt (§ 26 Abs. 7 BDSG) – erlaubt, wenn sie für die Durchführung des Arbeitsverhältnisses erforderlich ist. Das ist grds. zu bejahen (statt aller *Däubler* Rn. 292). Der Arbeitgeber darf, wie jeder Gläubiger einer Dienstleistung, von Zeit zu Zeit prüfen, ob die Arbeitspflicht ordnungsgemäß erfüllt wird. Überdies hat er nach **§ 130 OWiG** zumindest stichprobenweise zu kontrollieren, ob seine Mitarbeiter straf- oder bußgeldbewehrte Rechtsvorschriften einhalten (vgl. *BGHSt* 9, 319, 323; *BGH* NJW 1973, 1511; *OLG Köln* wistra 1994, 115; *Senge* § 130 OWiG Rn. 15; KK-OWiG/*Rogall* § 130 Rn. 60). Solche Kontrollen gehören zu den **unvermeidlichen Einschränkungen des Persönlichkeitsrechts**. Eines konkreten Anlasses bedarf es ebenso wenig wie einer vorherigen Ankündigung, jedenfalls solange die Überwachung **keinen „psychischen Anpassungsdruck“** erzeugt. **Unzulässig** ist nach aktueller Rechtsprechung nur die **„lückenlose, dauerhafte sowie sehr detaillierte“ Überwachung, bei der der Überwachte „keine Möglichkeit einer unbewachten und ungestörten Wahrnehmung ihres Persönlichkeitsrecht“** mehr hat (*BAG* NZA 2019, 1212 Rn. 38). Ehrverletzende, **diskriminierende oder den Arbeitnehmer schikanierende Kontrollen sind ebenfalls unzulässig.** Soweit sich der Arbeitgeber auf konkret-individuelle Überprüfungen bestimmter Arbeitnehmer an deren Arbeitsplätzen beschränkt und diese weder systematisch noch mittels technischer Hilfsmittel durchführt, ist auch der Betriebsrat nicht zu beteiligen. Es handelt sich nicht um sog. Ordnungsverhalten i.S.d. **§ 87 Abs. 1 Nr. 1 BetrVG**, sondern um Anordnungen bezüglich des Arbeitsverhaltens, d.h. der Erbringung der Arbeitsleistung (ständige Rspr., vgl. *BAG* NZA 2012, 687, 689). Zum Zugriff auf Akten, Briefe und sonstige Schriftstücke s. Rn. 85, zum Zugriff auf den PC am Arbeitsplatz s. Rn. 73.

2. Zugangs- und Taschenkontrollen

55 Kraft seines Weisungsrechts (§ 106 S. 2 GewO) kann der Arbeitgeber **einseitig anordnen,** dass sich Arbeitnehmer Zugangskontrollen zu unterziehen haben (*BAG* NZA 2014, 551, 555 f.), die der Personenkontrolle und der Überprüfung mitgeführter Gegenstände dienen (*BAG* NZA 2008, 1008 zur Taschenkontrolle; BT-Drucks. 14/8796, 24). Die Kontrolle kann **präventiv** oder **repressiv**, **stichprobenartig** ohne konkrete Verdachtsmomente gegenüber einer Person **oder anlassbezogen** erfolgen (*BAG* NZA 2013, 1433, 1436; anders aber gegenüber Betriebsfremden, wie z.B. Kunden, bei denen verdachtsunabhängige Sichtkontrollen von Einkauftaschen unzulässig sind, *BGH* NJW 1996, 2574). Stets ist dabei billiges Ermessen zu wahren. Da bei ihr üblicherweise personenbezogene Daten erhoben werden („Herr X war zum Zeitpunkt Y am Tor Z und führte unerlaubt Alkohol, Drogen, Betriebsmittel usw. mit sich"), ist der Anwendungsbereich des Datenschutzrechts eröffnet. Dient die Kontrolle der **Durchführung des Arbeitsverhältnisses, ist § 26 Abs. 1 S. 1 BDSG einschlägige Verarbeitungsgrundlage**, dient sie der Verteidigung des Hausrechts, kommt Art. 6 Abs. 1 lit. f DS-GVO in Betracht. Der mit der Maßnahme verbundene Eingriff in das allgemeine Persönlichkeitsrecht des Arbeitnehmers muss gegen das Überwachungsinteresse des Arbeitgebers abgewogen werden (*Joussen* NZA 2010, 254, 256; zur Abwägung: *BAG* NZA 2008, 1008 Rn. 58 m.w.N.). Geschieht die Torkontrolle stichprobenartig, muss sie alle Arbeitnehmer gleichermaßen erfassen (*BAG* NZA 2014, 551, 555 f.), d.h. auf dem **Zufallsprinzip** beruhen, und darf nicht gezielt (und ggf. wiederholt) bestimmte Arbeitnehmer betreffen (HK-ArbR/*Boemke/Kreuder* BGB § 611 Rn. 526; *Grobys/Panzer/Panzer-Heemeier* Rn. 15). Für eine abweichende Auswahl müssen sachliche Gründe vorliegen (Schaub/*Linck* § 53 Rn. 25). Für eine **anlassbezogene Kontrolle muss ein hinreichender Tatverdacht** bestehen. Das bloße objektiv grundlose „für verdächtig Halten" durch die Prüfperson genügt nicht (*LAG Mannheim* AP § 611 BGB Torkontrolle Nr. 1). Soll der Inhalt mitgeführter Taschen oder die Kleidung des Arbeitnehmers überprüft werden, ist der Eingriff in die von Art. 2 Abs. 1 GG geschützten Rechte (*BAG* NZA 2013, 1433 Rn. 42) nur dann zulässig, wenn damit Diebstähle in erheblichem Umfang aufgedeckt werden sollen, die zu kontrollierenden Personen nach dem Zufallsprinzip ausgewählt werden, die Kontrolle in einem nicht einsehbaren Raum erfolgt und ihre Intensität nach konkreten Verdachtsumständen gestaffelt wird (*BAG* NZA 2013, 1433 Rn. 47; vgl. zum räumlichen Bereich von Torkontrollen: *LAG Hessen* BeckRS 2011, 78545). Die Kontrolle kann auch noch im (direkten) Anschluss an die bereits beendete Arbeit, d.h. außerhalb der regulären Arbeitszeit durchgeführt werden (*LAG Hessen* BeckRS 2011, 78545; *LAG Nürnberg* NZA-RR 2007, 136). Sie ist auf das Öffnen von mitgeführten Behältnissen und unter Umständen das Abtasten der Oberbekleidung zu beschränken. Für weitergehende Maßnahmen bedarf der Arbeitgeber die Inanspruchnahme der zuständigen Behörden. In keinem Fall darf das Ehr- und Schamgefühl der Untersuchten verletzt werden (Schaub/*Linck* § 53 Rn. 25). Neben Kontrollen kommt auch die Einführung von Werksausweisen und anderen Zugangssicherungssystemen zu Über-

wachungs- und Kontrollzwecken in Betracht (*Hümmerich/Boecken/Düwell/Boecken* Rn. 36). Bei allen Maßnahmen hat der Betriebsrat mitzubestimmen (§ 87 Abs. 1 Nr. 1 BetrVG). Entsprechend abgeschlossene Betriebsvereinbarungen zur Torkontrolle (s. Arbeitshilfe 2402) genießen Vorrang vor den Regelungen des BDSG (vgl. § 26 Abs. 4 BDSG). Sie müssen jedoch die oben erwähnten Vorgaben des Art. 88 Abs. 2 DS-GVO erfüllen. Außerdem haben die Betriebsparteien die Persönlichkeitsrechte der Arbeitnehmer zu wahren haben (§ 75 Abs. 2 BetrVG). Keiner Mitbestimmung unterliegt die Taschenkontrolle bei einem konkret Tatverdächtigen in einem Einzelfall (*BAG* NZA 1991, 729).

56 Bei Zugangskontrollen mittels **Erfassung biometrischer Daten (Iris-Scan, Fingerprint usw.)** i.S.d. Art. 9 DS-GVO ist zusätzlich § 26 Abs. 3 S. 3 BDSG zu beachten. Die Erhebung solcher Daten ist zulässig, wenn sie zur Ausübung von Rechten aus dem Arbeitsverhältnis erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Darüber hinaus sind **angemessene** und **spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person** vorzusehen (§ 22 Abs. 2 i.V.m. § 26 Abs. 3 S. 3 BDSG). Dazu gehören u.a. technisch organisatorische Maßnahmen, insbesondere solche, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt wurden, sodann die Sensibilisierung der an den Verarbeitungsvorgängen Beteiligten, die Benennung eines Datenschutzbeauftragten, die Beschränkung des Zugangs zu den personenbezogenen Daten, die Pseudonymisierung bzw. Verschlüsselung personenbezogener Daten sowie – ganz allgemein – die Einführung eines Verfahrens, mit dem regelmäßig überprüft und bewertet wird, ob die technischen und organisatorischen Maßnahmen genügen, um die Einhaltung der Vorgaben der DS-GVO und des BDSG sicherzustellen. Ob und welche Maßnahmen zu ergreifen sind, richtet sich nach dem jeweiligen Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten des Betroffenen.

57 In Zeiten der **Corona-Pandemie** werden vor dem Betreten des Betriebsgeländes vermehrt **Gesundheitskontrollen** durchgeführt. Da eine SARS-CoV-2-Infektion teilweise mit einer spezifisch erhöhten Körpertemperatur der infizierten Person einhergeht, werden **elektronische Geräte zur Temperaturerfassung** eingesetzt. Die Messung erfolgt kontaktlos mittels einer Infrarot-Wärmebildkamera. Nachdem auch **„Coronatests"** in verschiedenen Formen (PCR- und PCR-Schnelltest, Antigen- und Antikörpertests) ausreichend und preisgünstig zur Verfügung stehen, werden auch diese eingesetzt. Dass der Arbeitgeber den Zugang zum Arbeitsplatz ohne Corona-Test verweigert, kann zulässig sein (*ArbG Offenbach* BB 2021, 627). Die Auswahl und Durchführung dieser Kontrollmaßnahmen unterliegt nicht der Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG. Die Testergebnisse bilden weder ein konkretes Verhalten oder eine konkrete Leistung eines Arbeitnehmers ab noch lassen sie auf solche schließen. Dass ein positives Testergebnis Folgen

für die Beschäftigung hat, genügt für sich allein nach der Rechtsprechung nicht (*BAG* NZA 2018, 673). In Betracht kommt aber – wenn der Test verpflichtend ausgestaltet wird – eine Mitbestimmung nach § 87 Abs. 1 Nr. 1 BetrVG, soweit darin eine Zugangskontrolle liegt.

Temperaturmessungen sind generell zweifelhaft: eine COVID-19-Infektion kann auch fieberlos ablaufen, nicht jedes Fieber geht auf COVID-19 zurück (Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) v. 10.9.2020 zum Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie). Auch Corona-Schnelltests dürfen **nicht anlasslos, sondern nur bei konkreten Verdachtsmomenten im Betrieb** oder bei der kontrollierten Person erfolgen. Befürwortet werden sie auch für Arbeitsumgebungen mit besonders engem Kontakt sowie für Beschäftigte in Einrichtungen, die für die akute Versorgung der Bevölkerung unverzichtbar sind, wie etwa Krankenhäuser. Verarbeitet werden darf nur die Information, dass aufgrund eines positiven Ergebnisses bei einer Gesundheitskontrolle der Zugang zum Betrieb verweigert wurde, nicht aber die einzelnen Krankheitssymptome (*Sander/Hilberg/Bings* COVuR 2020, 347, 351). Stets muss der Arbeitgeber angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person ergreifen (§ 26 Abs. 3 S. 3 i.V.m. § 22 Abs. 2 BDSG). Das gilt auch in Krisenzeiten. Dazu gehört im Regelfall auch eine **Datenschutz-Folgeabschätzung** nach Art. 35 DS-GVO. Nicht mehr für die benannten Zwecke benötigte personenbezogene Daten sind **unverzüglich zu löschen.** Die betroffenen Personen müssen in verständlicher Weise über die Verarbeitung ihrer Daten i**nformiert** werden. Liegen die Voraussetzungen des § 26 Abs. 3 BDSG vor, bedarf es keiner Einwilligung der von einem „Coronatest" betroffenen Beschäftigten. Sie kann sogar gegen seinen Willen durchgeführt werden. 58

3. Spindkontrollen

Ein dem Arbeitnehmer zugeordneter Schrank **(„Spind")** und dessen Inhalt sind **Teil der von Art. 2 Abs. 1 GG geschützten Privatsphäre,** die der Arbeitgeber selbst dann zu wahren hat, wenn er zur Überlassung eines Schranks verpflichtet ist (vgl. § 6 Abs. 2 ArbStättVO i.V.m. Nr. 4.1 Abs. 3 des Anhangs). Eine Spindkontrolle kommt jedoch in Betracht, wenn dort **Gegenstände aufbewahrt werden,** die dem Arbeitgeber oder Kollegen **entwendet** wurden oder von denen **Gefahren ausgehen**, die der Arbeitgeber abzuwenden verpflichtet ist (*BAG* NZA 2014, 143). Auch in diesem Fall muss der Arbeitnehmer darauf vertrauen können, dass sein Spind **ausschließlich mit seiner Einwilligung geöffnet** und dort eingebrachte persönliche Sachen allein mit seinem Einverständnis durchsucht werden. Nur so kann er auf die Durchführung der Kontrolle Einfluss nehmen und sie durch freiwillige Herausgabe gesuchter Gegenstände sogar ganz abwenden. Eine heimliche Spinddurchsuchung ist daher unzulässig. Sie verstößt nach Inkrafttreten der DS-GVO gegen das Transparenzgebot. Die dort sichergestellten Beweismittel sind in einem anschließenden Gerichtsverfahren nicht verwertbar (*BAG* NZA 2014, 59

143). Das gilt erst recht, wenn die heimliche Kontrolle die Überführung eines Tatverdächtigen bei einer späteren Torkontrolle nur „vorbereiten soll". Dass ein bei einer offenen Kontrolle ertappter Arbeitnehmer einwenden kann, er hätte die im Spind aufgefundene, unbezahlte Ware vor Verlassen des Betriebs noch bezahlen wollen, rechtfertigt keine andere Beurteilung. Eine solche Einlassung ist selbst bei einer heimlichen Kontrolle nicht auszuschließen.

4. Videoüberwachung

60 Die Überwachung **öffentlich zugänglicher Räume,** wie etwa von Verkaufsräumen, mit optisch-elektronischen Einrichtungen („Videoüberwachung") ist erlaubt, soweit sie zur Wahrnehmung des Hausrechts oder anderer, konkret festgelegter und berechtigter Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen (§ 4 Abs. 1 BDSG; vgl. im Einzelnen Kühling/Buchner/*Buchner* BDSG § 4 Rn. 6 ff.). Der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind durch geeignete Maßnahmen zum frühest möglichen Zeitpunkt erkennbar zu machen (§ 4 Abs. 2 BDSG). Der Gedanke hinter dieser Norm ist einfach (*BAG* AP § 87 BetrVG 1972 Überwachung Nr. 42): Wer weiß, dass er überwacht wird, kann von dem überwachten Ort wegbleiben, wenn er die Videokontrolle vermeiden möchte. Arbeitnehmer können das nicht.

61 Dass für die **Videoüberwachung öffentlich zugänglicher Räume an sich § 4 BDSG gilt**, der gegenüber § 26 BDSG hinausgehende Bedingungen aufstellt, umschifft die Rechtsprechung durch die Annahme, dass es sich bei **§ 26 BDSG um eine eigenständige, von den Voraussetzungen des § 4 BDSG unabhängige Erlaubnisnorm** handelt (*BAG* NZA 2018, 1329 Rn. 23; *BAG* NZA 2019, 1212 Rn. 49 zu den wortlautgleichen Vorgängernormen der §§ 6b, 32 BDSG a.F.). Sei eine bestimmte Datenverarbeitung nach § 26 BDSG rechtmäßig, komme es im Verhältnis zu den betroffenen Arbeitnehmern nicht darauf an, ob die Anforderungen des § 4 BDSG erfüllt seien. Während § 4 BDSG die Allgemeinheit vor einer ausufernden Videoüberwachung im öffentlichen Raum schützen wolle, solle § 26 BDSG die widerstreitenden Interessen der Arbeitsvertragsparteien in Bezug auf den Beschäftigtendatenschutz ausgleichen. Für die Eigenständigkeit des § 26 BDSG spreche auch, dass die Videoüberwachung nicht öffentlich zugänglicher (Arbeits-) Räume im BDSG nicht gesondert geregelt sei. Ihre Zulässigkeit richte sich daher, soweit Arbeitnehmer betroffen sind, allein nach § 26 BDSG. Es erschiene aber wenig plausibel, wenn bezogen auf den Beschäftigtendatenschutz von Arbeitnehmern, die in öffentlich zugänglichen Räumen arbeiten, andere Maßstäbe gelten sollten als für Arbeitnehmer, die dies nicht tun (*BAG* NZA 2017, 112 Rn. 43). Freilich lässt sich auch genau umgekehrt argumentieren: wenn bereits die Überwachung öffentlicher Räume allein nach Maßgabe von § 4 BDSG erlaubt ist, kann für die Kontrolle von Beschäftigten in Bereichen, die für die Öffentlichkeit unzugänglich sind, kein anderer, jedenfalls kein geringerer Maßstab gelten (*Däubler* Gläserne Belegschaften Rn. 312 b; *Wedde* in DWWS § 26 BDSG Rn. 120). Abge-

sehen davon kann eine Videoüberwachung durch eine nicht öffentliche Stelle, die damit Interessen verfolgt, die nicht unter die öffentlichen Interessen i.S.d. Art. 6 Abs. 1 lit e, Abs. 3 DS-GVO fallen, ohnehin nicht auf § 4 BDSG, sondern allenfalls auf Art. 6 Abs. 1 lit f DS-GVO gestützt werden (*BVerwG* 27.3.2019, ZD 2019, 372; Kühling/*Buchner* BDSG § 4 Rn. 3, 4, 11).

62 Nach früherer Rechtsprechung (*BAG* NZA 2003, 1193; *BAG* NZA 2004, 1278) war eine (offene) Videoüberwachung nur erlaubt, wenn das Kontrollinteresse des Arbeitgebers das Persönlichkeitsrecht des Arbeitnehmers eindeutig überragt (ausf. *Grimm/Schiefer* RdA 2009, 329 ff.; *Maties* NJW 2008, 2219 ff.; *Müller* Die Zulässigkeit der Videoüberwachung am Arbeitsplatz, 2008). Dazu genügte es nicht, dass der Arbeitgeber schlicht überprüfen wollte, ob und wie gearbeitet wird. Vielmehr mussten **rechtlich geschützte Güter des Arbeitgebers schwerwiegend beeinträchtigt** sein, etwa durch gegen ihn gerichtete Straftaten (Diebstahl, Unterschlagung, Verrat von Betriebs- und Geschäftsgeheimnissen usw.). Weiterhin war ein konkreter Tatverdacht in Bezug auf eine konkrete strafbare Handlung oder andere schwere Verfehlung zu Lasten des Arbeitgebers gegen einen zumindest räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern erforderlich. Er durfte sich zwar nicht auf die allgemeine Mutmaßung beschränken, es könnten Straftaten begangen werden, musste sich aber nicht notwendig nur gegen einen einzelnen, bestimmten Arbeitnehmer richten (*BAG* NZA 2017, 112, 114 m.w.N.) Der „Generalverdacht" gegen die gesamte Belegschaft eines Betriebs oder einer Abteilung genügte nicht (*LAG Baden-Württemberg* BB 1999, 1439). Die tatsächlichen Anhaltspunkte für den Verdacht waren zu dokumentieren (§ 32 Abs. 1 S. 2 BDSG a.F.). Inventurdifferenzen bei Betrieben des Einzelhandels sollten für sich allein noch keinen hinreichenden Anfangsverdacht begründen, solange der Arbeitgeber nicht andere Ursachen für ein bestehendes Manko – z.B. Fehlbuchungen, Entwendung nicht im Verkaufs-, sondern im Lagerbereich – ausgeschlossen hatte (*BAG* NZA 2014, 243, 249). Es bedurfte konkreter Feststellungen, warum eine Videoüberwachung das praktisch einzig verbliebene Mittel darstellte, Unregelmäßigkeiten aufzuklären oder einen Verdacht in personeller Hinsicht weiter einzugrenzen (*BAG* NZA 2014, 243, 249).

63 Die **neuere Rechtsprechung** ist – zu Unrecht – **deutlich großzügiger**. § 26 Abs. 1 S. 1 BDSG gestatte ausdrücklich die Verarbeitung auch zur Durchführung und zur Beendigung des Arbeitsverhältnisses. Dabei gehöre zur „Durchführung die Kontrolle, ob der Arbeitnehmer seinen Pflichten nachkommt", zur Beendigung i.S.d. Kündigungsvorbereitung „die Aufdeckung einer Pflichtverletzung, die die Kündigung des Arbeitsverhältnisses rechtfertigen kann" (*BAG* NZA 2017, 1327 Rn. 28; *BAG* NZA 2017, 1179 Rn. 26; *BAG* NZA 2019, 1212 Rn. 35). Ausgehend von dieser Prämisse ist es nur ein kleiner Schritt, die Anforderungen noch weiter abzusenken und **sogar präventive Kontrollmaßnahmen zur Verhinderung von Pflichtverletzungen zuzulassen,** jedenfalls solange die Überwachung **keinen „psychischen Anpassungsdruck"** erzeugt. Das ist nach der Rechtsprechung **erst dann der Fall, wenn die Überwachten „in ihrer Freiheit, ihr Handeln aus eigener Selbstbestimmung zu planen und zu gestalten wesentlich gehemmt sind"** (*BAG*

NZA 2017, 1327 Rn. 31; *BAG* NZA 2019, 1212 Rn. 37). Bei ohne weiteres erkennbaren Videoüberwachungen muss dem betroffenen Arbeitnehmer nicht einmal ausdrücklich eröffnet werden, dass er überhaupt kontrolliert wird und welches Verhalten dabei besonders relevant ist. Wird z.B. der Kassenbereich überwacht, muss das Kassenpersonal damit rechnen, dass mithilfe der Videoaufzeichnungen vorsätzliche Pflichtverletzungen verhindert bzw. aufgedeckt und verfolgt werden. **Unzulässig** ist eine offene Videoüberwachung **erst dann**, wenn das **Verhalten „lückenlos, dauerhaft sowie sehr detailliert"** erfasst wird, so dass die betroffene Person „davon ausgehen muss, dass jede ihrer Bewegungen überwacht wird" und deshalb – vergleichbar mit der Situation einer verdeckten Überwachung – **„keine Möglichkeit einer unbewachten und ungestörten Wahrnehmung ihres Persönlichkeitsrecht"** mehr besteht (*BAG* NZA 2019, 1212 Rn. 38). In einem Kündigungsschutzverfahren muss der verantwortliche Arbeitgeber daher nur darlegen, welcher räumliche Bereich des überwachten Betriebs in welchem Umfang durch die einzelnen Videokameras konkret erfasst wird, ob alle oder nur ein Teil der von den Überwachten ausgeführten Tätigkeiten aufzeichnet werden und ob es den betroffenen Arbeitnehmern bekannte Zonen gibt, in denen sie sich während der Arbeitsschichten überwachungsfrei aufhalten können und wie groß diese Zonen gegebenenfalls sind (*BAG* NZA 2019, 1212 Rn. 41). **Nicht mehr notwendig** ist nach der Rechtsprechung ein durch konkrete Tatsachen belegter **„einfacher Anfangsverdacht" einer Straftat oder Arbeitspflichtverletzung;** es genügt bereits die „abstrakte Gefahr" für eine Verletzung arbeitsvertraglicher Pflichten (*BAG* NZA 2017, 1327 Rn. 31; *BAG* NZA 2019, 1212 Rn. 37).

64 Wird bei Beschäftigten im Zuge einer an sich gegen andere Personen gerichteten, zulässigen Videoüberwachung „zufällig" ein Fehlverhalten entdeckt, können die Aufzeichnung als Beweismittel auch gegen sie verwendet werden. Es kommt nicht darauf an, ob der Arbeitgeber alle anderen zumutbaren Aufklärungsmaßnahmen auch bezüglich des zufällig aufgedeckten Fehlverhaltens bereits ausgeschöpft hat, weil dies, falls es noch keinen Anfangsverdacht gab, weder möglich noch geboten ist (*BAG* NZA 2017, 112, 116; a.A. *Eylert* NZA-Beil. 2015, 100, 107). Beschäftigte, die sich unter Verletzung eines Zutrittsverbots in einem überwachten Bereich aufhalten, können sich zwar auch auf ihr allgemeines Persönlichkeitsrecht berufen; doch ist ihr Interesse, nicht von einer verdeckten Videoüberwachung erfasst zu werden, erheblich gemindert (*BAG* NZA 2017, 443, 447).

65 Nach wie vor hohe Anforderungen gelten auch nach der neueren Rechtsprechung (*BAG* NZA 2019, 1212 Rn. 38) für **heimliche Videoüberwachungen.** Denn ihnen ist sich der Arbeitnehmer gar nicht bewusst, weshalb er auch keine Abwehrstrategien entwickeln kann. Trotz der Hinweispflicht auf Videokontrollen in öffentlich zugänglich Räumen (§ 4 Abs. 2 BDSG) sind sie vor Inkrafttreten der DS-GVO auch dort in verdeckter Form erlaubt gewesen (*BAG* NZA 2012, 1025; NZA 2014, 243; NZA 2017, 112, 115 f.), weil sich nach Ansicht der Rechtsprechung ein auf Heimlichkeit angelegtes Verhalten kaum durch offen angekündigte Beobachtungen entdecken ließ (*BAG* NZA 2003, 1193, 1195). Außerdem hielt es die Rechtsprechung

für widersprüchlich, wenn für den Datenschutz von Personen, die in öffentlich zugänglichen Räumen arbeiteten, andere Vorschriften gelten sollten, als für Arbeitnehmer, die in für die Öffentlichkeit versperrten Bereichen tätig würden und wandte deshalb nur § 32 Abs. 1 BDSG a.F. an (*BAG* NZA 2017, 112, 115). Freilich galt auch damals im Grundsatz der Vorrang der offen erkennbaren vor einer heimlichen Überwachung (*BAG* NZA 2003, 1193, 1195; NZA 2017, 112, 114). Als ***ultima ratio*** kam die heimliche Videoüberwachung deshalb nur in Betracht, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers bestand, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft waren oder keinen Erfolg versprachen – z.B. bei Ladenangestellten der Einsatz von Ladendetektiven (*BAG* NZA 2003, 1193, 1195; NZA 2004, 1278, 1283) – und die verdeckte Überwachung praktisch das einzig verbleibende Mittel darstellte (*BAG* NZA 2003, 1193). Zudem musste sie sich auf den Ort beschränken, an dem der Täter vermutet wird, und durfte auch zeitlich nicht über Gebühr ausgedehnt werden (*BAG* NZA 2003, 1193, 1195; NZA 2004, 1278, 1281). Unangemessen war die Kontrolle nicht, wenn sie allein den räumlichen Bereich, auf den sich der Verdacht erstreckte, betraf und sie zeitlich begrenzt durchgeführt wurde (*BAG* NZA 2003, 1193, 1195; NZA 2017, 112, 114).

Mit Geltung der DS-GVO sind heimliche Mitarbeiterkontrollen grundsätzlich unzulässig. Sie bedürfen nach Art. 23 DS-GVO einer ausdrücklichen gesetzlichen Regelung. § 26 BDSG genügt hierfür nicht (Rn. 21). Das liegt im Übrigen auch auf der Linie des EGMR. In der Rechtssache *Barbulescu* (NZA 2017, 1143) hatte der Gerichtshof die heimliche Überwachung der Privatnutzung der Betriebs-IT wegen Verstoßes gegen Art. 8 EMRK für unzulässig erklärt. In der Entscheidung *Lopez Ribalda* (*EGMR* v. 9.1.2018 1874/13 und 8567/13) hatte der EGMR die heimliche Videoüberwachung eines Supermarktes, bei der Arbeitnehmer dabei gefilmt wurden, wie sie Waren entwendeten, ebenfalls für unzulässig erklärt, weil sie verdachtsunabhängig, anlasslos und zeitlich unbeschränkt erfolgte (Rn. 67 ff. des Urteils). **66**

Tabu für jede Videoüberwachung ist die **Intimsphäre der im Betrieb Beschäftigten.** Sie wird seit 2015 auch strafrechtlich besonders geschützt. Seitdem stellt § 201a StGB die unbefugte **Bildaufnahme** einer anderen Person, die sich in einem gegen Einblick besonders geschützten Raum befindet, unter Strafandrohung. Damit sind Überwachungen von Beschäftigten in **Toiletten, geschlossenen Sanitärbereichen (Duschräumen) und Umkleidekabinen** passé (vgl. BT-Drucks. 15/2466, 5). Zur Intimsphäre zählen auch der Schutz höchstpersönlicher Geheimnisse, wie etwa „Selbstgespräche", die nicht aufgezeichnet werden dürfen (*BGH* NJW 2012, 945), und Tagebucheinträge als adressatenlose schriftliche Aufzeichnungen (*BVerfG* NJW 1990, 563), nicht aber **Chatprotokolle** (dazu *EGMR* NZA 2017, 1443 – Barbulescu). **Nicht zur Intimsphäre** gehören der **Spind** und ähnliche unter Verschluss des Beschäftigten befindliche Behältnisse, z.B. Schubladen im Schreibtisch, die (nur) im Beisein des Besitzers geöffnet werden dürfen (*BAG* NZA 2014, 143), wie auch **Taschen**, die bei einer anlasslosen und verdachts- **67**

unabhängigen Torkontrolle kontrollierbar sind (*BAG* NZA 2014, 551, 555 f.). Zu den Kontrollmöglichen im Homeoffice *Frank/Heine* BB 2021, 248.

68 Eine andere Frage ist, **wie lange rechtmäßige Videoaufzeichnungen gespeichert werden dürfen** (dazu *Brink/Schwab* jurisPR-ArbR 6/2019 Anm. 5; *Goetz* SAE 2019, 54; *Grages/Plath* CR 2017, 791; *Grimm* ArbRB 2018, 258; *Meyer-Michaelis* DB 2018, 2821; *Stähler* DSB 2019, 291; *Tiedemann* ZD 2019, 230). Das bemisst sich nach Art. 17 DS-GVO. Eine Löschung personenbezogener Daten kann danach nicht verlangt werden, solange die weitere Verarbeitung (d.h. Speicherung und Nutzung) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist (Kühling/Buchner/*Herbst* DS-GVO Art. 17 Rn. 19, 83). Auch hier verfährt die arbeitsgerichtliche Rechtsprechung zum bisherigen Recht denkbar großzügig (*BAG* NZA 2018, 1329; deutlich restriktiver aber die Vorinstanz *LAG Hamm* ZD 2018, 494). **Das BAG hält die Speicherung für erforderlich, bis der Zweck der Erhebung „erreicht, aufgegeben oder nicht mehr erreichbar ist**." Der Arbeitgeber könne mit Blick auf mögliche „heimliche" Verletzungen seines Eigentums durch eigene Beschäftigte nicht darauf verwiesen werden, die gesamten Aufzeichnungen nach kurzer Zeit unbesehen überschreiben zu lassen. Würden die Speicherintervalle so kurz bemessen, dass die Aufzeichnungen bei Bekanntwerden von Vorfällen üblicherweise schon gelöscht sind, wäre die Videoüberwachung insoweit praktisch wirkungslos und damit jedenfalls unverhältnismäßig. Umgekehrt sei der rechtmäßig aufgenommene Vorsatztäter in Bezug auf die Aufdeckung und Verfolgung seiner materiell-rechtlich noch verfolgbaren Tat nicht schutzwürdig. Er werde dies auch nicht durch bloßen Zeitablauf, weil das durch Art. 12 und Art. 14 GG geschützte Verarbeitungs- und Nutzungsinteresse des Arbeitgebers nicht an Gewicht verliere, solange die Rechtsverfolgung materiell-rechtlich nicht ausgeschlossen ist. Das allgemeine Persönlichkeitsrecht könne nicht zu dem alleinigen Zweck in Anspruch genommen werden, sich vor dem Eintritt von Verfall, Verjährung oder Verwirkung der Verantwortung für vorsätzlich rechtswidriges Handeln zu entziehen **(„Datenschutz ist nicht Tatenschutz").** Dem widerspräche es, wenn der Arbeitgeber gezwungen wäre, die Aufzeichnungen aus einer offenen, vorrangig zu präventiven (Verhinderung von Pflichtverletzungen) und nur bei Verfehlung dieses Primärziels zu repressiven Zwecken (Aufklärung und Verfolgung von Pflichtverletzungen) eingesetzten Videoüberwachung laufend vollumfänglich einzusehen, um relevante Sequenzen weiterverarbeiten zu dürfen. Das hielte ihn zu ständigem Misstrauen an. Zugleich würde durch einen faktischen Zwang zu zeitnaher Aufdeckung und „Sanktionierung" von Pflichtverletzungen der Arbeitnehmerschutz durch die Vorgaben des Datenschutzrechts in sein Gegenteil verkehrt. **Folgerichtig hält das BAG sogar wochen- und monatelange Speicherintervalle für zulässig**, wenn Straftaten oder erhebliche Pflichtverletzungen erst bei aufwendigen Überprüfungen oder Abrechnungsmaßnahmen entdeckt werden können. Die Speicherung – nach wie vor – erforderlicher Sequenzen könne deshalb nur unangemessen sein, wenn das Verhalten des Arbeitgebers objektiv den Schluss zulasse, er wolle diese Passagen nicht allein zur Rechtsverfolgung verwenden. Das soll nach der Rechtsprechung aber

nur dann der Fall sein, wenn die „greifbare Gefahr eines Missbrauchs personenbezogener Daten" besteht. Vor diesem Hintergrund wäre es nach Meinung des BAG unzulässig, das gesamte Bildmaterial zunächst über einen längeren Zeitraum vorzuhalten, um es sodann ohne konkreten Anlass in Augenschein zu nehmen. Erst unter diesen Umständen dürfte sich die – unvermeidliche – Einsichtnahme (auch) in die irrelevanten Aufzeichnungsteile als unverhältnismäßig darstellen. Die **Ansicht des BAG widerspricht allerdings den Grundsätzen der Datenminimierung und Speicherbegrenzung**, die in Art. 5 DS-GVO als dem maßgeblichen und nicht durch Art. 88 DS-GVO verdrängten europäischen Recht ihren Niedersachlag gefunden haben (im Ergebnis wie hier *LAG Hamm* ZD 2018, 494 mit Anm. *Tiedemann*; *Brink/Schwab* jurisPR-ArbR 6/2019 Anm. 5; *Brink/Joos* jurisPR-ArbR 38/2019 Anm. 1). Nach Ansicht der Datenschutzaufsichtsbehörden sind Videoaufzeichnungen stets unverzüglich zu sichten und dann rasch, d.h. regelmäßig binnen 48 Stunden zu löschen (DSK, Kurzpapier Nr. 15).

69 Die Installation einer Videoüberwachungsanlage – gleichgültig ob sie offen oder verdeckt erfolgen soll – ist **mitbestimmungspflichtig** nach **§ 87 Abs. 1 Nr. 6 BetrVG** (*BAG* NJW 1974, 2023; NZA 2003, 1193, 1196), auch wenn die Mitarbeiterkontrolle bloßer Nebeneffekt ist. Es genügt, wenn der Einsatz objektiv zu deren Überwachung geeignet ist (*BAG* NJW 1974, 2023, 2024; NZA 1985, 669, 670). Der Betriebsrat hat mitzubestimmen bei der Einführung der Videoüberwachung wie auch bei ihrer Anwendung. Bei seinen Überlegungen hat er die berechtigten Belange des Arbeitgebers gegen die Interessen der Arbeitnehmer auf Schutz ihres Persönlichkeitsrechts abzuwägen (*BAG* NZA 1986, 643, 647). Die Zustimmung des Betriebsrats zu einer geplanten Überwachungsmaßnahme rechtfertigt allerdings noch nicht ihre Durchführung. Deren Zulässigkeit richtet sich allein nach materiellen Kriterien. Es empfiehlt sich der Abschluss einer Betriebsvereinbarung (s. Arbeitshilfe 2403).

70 Umstritten ist die Frage, ob Videoaufnahmen, die unter **Verletzung von Mitbestimmungsrechten erstellt wurden, gerichtlich verwertbar sind.** Verstöße gegen Beweiserhebungsverbote führen nur dann zu Beweisverwertungsverboten, wenn der Schutzzweck der verletzten Norm dies verlangt (*Maschmann* NZA 2002, 13, 21 m.w.N.). Bei § 87 Abs. 1 Nr. 6 BetrVG ist das nach Ansicht des BAG nicht der Fall (*BAG* NZA 2008, 1008; NZA 2017, 112 Rn. 33; im Ergebnis ebenso *Altenburg/Leister* NJW 2006, 469, 470; *Haußmann/Krets* NZA 2005, 259, 263 f. m.w.N.; *Lunk* NZA 2009, 457, 459; *Schlewing* NZA 2004, 1071, 1072 f.). Das Mitbestimmungsrecht flankiere nur den individuellen Schutz des Persönlichkeitsrechts, reiche jedoch nicht darüber hinaus. Gehe die Videoaufnahme individualarbeitsrechtlich in Ordnung, reduziere sich die unterlassene Mitbestimmung auf einen rein formalen Verstoß gegen die betriebsverfassungsrechtliche Kompetenzverteilung, die der Betriebsrat zwar beanstanden und zu unterbinden suchen könne, die aber keinesfalls zu einem Beweisverwertungsverbot führe (*Grosjean* DB 2003, 2650, 2653; *Wiese* FS Lorenz, S. 915, 938, 940). Wahrheitsfindung rangiere vor Mitbestimmung, so das BAG. Damit wird das Gericht allerdings der von ihm selbst vertretenen (*BAG* AP BetrVG 1972 § 23 Nr. 25; Nr. 23; AP BetrVG

1972 § 87 Lohngestaltung Nr. 52; Nr. 51) „Theorie der Wirksamkeitsvoraussetzung" nicht gerecht, und so sehen es auch einige Landesarbeitsgerichte (*LAG Hamm* BeckRS 2006, 42354; *LAG Bremen* BeckRS 2005, 43027; *LAG Baden-Württemberg* BB 1999, 1439). Die zwingende Beteiligung des Betriebsrats schon im Vorfeld einer Überwachung soll helfen, unzulässige Aufnahmen zu vermeiden und erlaubte auf das Maß des Unvermeidlichen zu reduzieren. Die Mitbestimmung würde leerlaufen, wenn der Arbeitgeber am Betriebsrat vorbei heimlich Aufnahmen anordnen könnte (ebenso *Däubler* Gläserne Belegschaften, Rn. 838g; *Fischer* BB 1999, 154, 155; *Kaltenmaier* Betriebsverfassungsrechtliches Beweisverwertungsverbot, S. 162; DKW/*Klebe* § 87 Rn. 6; Schaub/*Ahrendt* § 235 Rn. 21; HK-BetrVG/*Kohte* § 87 Rn. 75; *Wolter* RdA 2006, 137, 143). Denn mangels Kenntnis der Aufnahme würde dem Betriebsrat der von der Rechtsprechung (*BAG* AP BetrVG 1972 § 87 Überwachung Nr. 40 mit Anm. *Wiese*; *BAG* AP BetrVG 1972 § 23 Nr. 23 mit Anm. *Richardi*) entwickelte Unterlassungsanspruch bei § 87 BetrVG jedenfalls bei heimlichen Aufnahmen nichts nützen.

71 Es verwundert nicht, dass Betriebsräte auf diese wenig mitbestimmungsfreundliche Rechtsprechung reagiert haben, und zwar mit der **Aufnahme von Beweisverwertungsverboten in Betriebsvereinbarungen über die Videoüberwachung** von Mitarbeitern (*Däubler* Gläserne Belegschaften, Rn. 838g). An diese sind nach § 77 Abs. 4 BetrVG beide Arbeitsvertragsparteien gebunden, und sie sind auch von den Gerichten zu beachten. Denn der Verzicht auf dieses Schutzrecht ist nicht ohne weiteres möglich, sondern bedarf der Zustimmung des Betriebsrats (§ 77 Abs. 4 S. 2 BetrVG). Ob solche unbedingten Beweisverwertungsverbote unionsrechtlich zulässig sind, ist allerdings zweifelhaft (Kühling/Buchner/*Maschmann* § 26 BDSG Rn 71). Ob die Betriebsparteien gegenüber den Gerichten über das formelle Recht hinausgehende Verwertungsverbote begründen oder zumindest dem Arbeitgeber die Berufung auf einen Sachvortrag in einem Rechtsstreit mit dem betreffenden Arbeitnehmer wirksam versagen können, hat die Rechtsprechung ausdrücklich offengelassen (*BAG* NZA 2019, 893 Rn. 68).

5. Überwachung der IT-Nutzung

72 Ähnliche Überlegungen wie bei der Videoüberwachung gelten, wenn der Arbeitgeber durch den Einsatz eines **Software-Keyloggers** verdeckt überprüfen will, ob der Arbeitnehmer seinen Dienst-PC vorschriftsgemäß benutzt. Ein Computerprogramm, mit dem sämtliche Tastatureingaben des Arbeitnehmers protokolliert werden können, darf zum Zwecke der Mitarbeiterkontrolle nur dann eingesetzt werden, wenn ein auf einen bestimmten Arbeitnehmer bezogener, durch konkrete Tatsachen begründeter Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung besteht. Eine Überwachung „ins Blaue hinein" verletzt das Grundecht auf informationelle Selbstbestimmung (*BAG* NZA 2017, 1327). Zwar berührt der Einsatz eines Keyloggers grds. nicht das Recht am eigenen Bild, insbesondere ist er regelmäßig nicht geeignet, Verhaltensweisen optisch zu erfassen, die von dem Betroffenen als peinlich empfunden werden. Jedoch wird mit der

Datenerhebung durch einen Keylogger massiv in das Recht des Betroffenen auf informationelle Selbstbestimmung eingegriffen. Es werden – für den Benutzer irreversibel – alle Eingaben über die Tastatur eines Computers einschließlich des Zeitpunkts der Eingabe sowie des zeitlichen Abstands zwischen zwei Eingaben erfasst und gespeichert. Die auf diese Weise gewonnenen Daten ermöglichen es, ein nahezu umfassendes und lückenloses Profil sowohl von der privaten als auch dienstlichen Nutzung durch den Betroffenen zu erstellen. Dabei werden nicht nur gespeicherte Endfassungen und ggf. Zwischenentwürfe bestimmter Dokumente sichtbar, sondern es lässt sich jeder Schritt der Arbeitsweise des Benutzers nachvollziehen. Darüber hinaus können hochsensible Daten wie z.B. Benutzernamen, Passwörter für geschützte Bereiche, Kreditkartendaten, PIN-Nummern etc. protokolliert werden, ohne dass dies für die verfolgten Kontroll- und Überwachungszwecke erforderlich wäre. Ebenso hat der betroffene Arbeitnehmer weder Veranlassung noch die Möglichkeit, bestimmte Inhalte als privat oder gar höchstpersönlich zu kennzeichnen und damit ggf. dem Zugriff des Arbeitgebers zu entziehen (*BAG* NZA 2017, 1327).

73 Eine andere Frage ist, ob der Arbeitgeber auf einem **von einem Arbeitnehmer benutzten Dienstrechner gespeicherte Dateien einsehen darf,** um zu prüfen, ob dieser seine vertraglichen Pflichten vorsätzlich verletzt hat. Das hat die Rechtsprechung bejaht (*BAG* NZA 2019, 893 Rn. 54), wenn die **Überprüfung** aus einem **nicht willkürlichen Anlass** geschieht – wobei ein durch Tatsachen begründeter Anfangsverdacht einer Pflichtverletzung nicht zwingend erforderlich ist –, sie **offen** erfolgt und der **Arbeitnehmer im Vorfeld darauf hingewiesen** wurde, welche legitimen Gründe eine Einsichtnahme in – vermeintlich – dienstliche Ordner und Dateien erfordern können (vgl. *EGMR* NZA 2017, 1443 – Barbulescu). Außerdem muss der Arbeitnehmer darauf **hingewiesen** worden sein, dass er **Ordner und Dateien durch eine Kennzeichnung als „privat"** von einer Einsichtnahme ohne „qualifizierten" Anlass ausschließen kann (*EGMR* NZA 2018, 1609 – Libet). Unter diesen Umständen muss der Arbeitnehmer dann billigerweise mit einem jederzeitigen Zugriff auf die vermeintlich rein dienstlichen Daten rechnen. Das hält die Rechtsprechung für unproblematisch, weil er „private" Daten in einen gesicherten Bereich verbringen kann. Die **Einsichtnahme** in die Datei muss **weder im Beisein des Mitarbeiters** noch unter Heranziehung eines Mitglieds des **Betriebsrats** oder des **Datenschutzbeauftragten** erfolgen. Der Arbeitgeber darf die Festplatte des Dienstrechners zum Zweck der computerforensischen Untersuchung kopieren, wenn dadurch weder der Inhalt der Dateien nicht verändert wird noch die Gefahr einer missbräuchlichen Verwendung der Daten steigt (*BAG* NZA 2019, 893 Rn. 59).

74 Nutzen Beschäftigte die Betriebs-IT, um damit im Internet zu surfen oder E-Mails zu versenden, speichert der E-Mail-/Internet-Server (Internet-Server können mit verschiedenen Funktionalitäten betrieben werden, z.B. als Proxy-Server oder Web-Server) die ID- und Zugriffsdaten (Verkehrsdaten) aller Benutzer sowie Daten zur Nutzungshistorie. Außerdem können E-Mails, die an Beschäftigte gerichtet sind, vom Arbeitgeber zur Kenntnis genommen werden, wenn sie auf ein be-

triebliches E-Mail-Konto eingehen („Hans.Meier@Firma.de). Solange sie sich auf dem Mailserver des Arbeitgebers oder eines von ihm beauftragten Providers befinden, fehlen dem Beschäftigten die technischen Möglichkeiten, den Zugriff, die Vervielfältigung oder die Weitergabe an Dritte zu verhindern (zu den praxisrelevanten Fallgruppen des POP3-Verfahrens und des IMAP-Verfahrens ausf. *Hoppe/Braun* MMR 2010, 80, 82). Entsprechendes gilt, wenn über den betrieblichen Festnetz-, Mobilfunk oder Breitband-Internetanschluss Bilder oder SMS ausgetauscht oder über die sog. OTT- („Over The Top"-) Dienste – wie etwa WhatsApp und Facebook – Nachrichten gesendet werden. Werden auf betrieblichen Endgeräten Internetseiten aufgerufen, lassen sich die Aufrufe protokollieren. Ferner können die vom Nutzer in Suchmaschinen eingegebenen Begriffe gespeichert und ihm persönlich zugeordnet werden (vgl. nur *BVerfG* ZD 2017, 132 mit Anm. *Bär*). Ob der Arbeitgeber die Nutzung der von ihm zu dienstlichen Zwecken bereitgestellten Betriebs-IT (PC, Tablet-PC, Smartphone usw.) überwachen darf, hängt davon ab, ob er eine Privatnutzung durch den Arbeitnehmer ausdrücklich gestattet oder zumindest geduldet hat (s. im Einzelnen *Bloesinger* BB 2007, 2177; *Füllbier/Splittgerber* NJW 2012, 1995; *Hoppe/Braun* MMR 2010, 80; *Kempermann* ZD 2017, 12; *Mengel* NZA 2017, 1494, 1495 ff.; *Singelnstein* NStZ 2012, 593; *Stück* CCZ 2018, 88; *Wybitul/Böhm* CCZ 2015, 133).

75 Hat der Arbeitgeber den **Privatgebrauch kraft Weisungsrechts generell untersagt,** sind Kontrollen grds. zulässig, schon um die Einhaltung des Verbots zu überprüfen (*BAG* NZA 2017, 1327; *Joussen* NZA Beilage 2011/1, 35, 39). Das gilt jedenfalls dann, wenn die Mitarbeiter vorab über die Möglichkeit von Kontrollen informiert wurden (vgl. *EGMR* NZA 2017, 1443, 1447 – Barbulescu). Beschränkungen durch das Telekommunikationsrecht bestehen nicht (*Härting* ITRB 2008, 88, 89). Das unbefugte Abhören und Mitschneiden von Telefonaten – sogar wenn diese im Betrieb geführt werden – ist nach § 201 StGB strafbar, nicht aber das Mithören (*BAG* EzA § 87 BetrVG 1972 Kontrolleinrichtung Nr. 16). Grenzen für die Überwachung der Internetnutzung zieht § 26 BDSG (*Kramer* ArbRAktuell 2010, 164). Eingehende E-Mails darf er einsehen, da diese als Geschäftsbriefe i.S.v. § 257 HGB angesehen werden (*Oberwetter* NJW 2011, 417, 419). In jedem Fall muss der **Verhältnismäßigkeitsgrundsatz** gewahrt bleiben (vgl. § 26 Abs. 1 BDSG; ausführlich dazu *Wybitul* BB 2010, 1085). Eine dauerhafte Kontrolle ist unzulässig. Die vorübergehende Speicherung und stichprobenartige Kontrolle der Verlaufsdaten eines Internetbrowsers kann zulässig sein, um die Einhaltung des Verbots oder einer Beschränkung der Privatnutzung von IT-Einrichtungen des Arbeitgebers zu kontrollieren (*BAG* NZA 2017, 1327), wenn dabei lediglich die Adressen und Titel der aufgerufenen Seiten und der Zeitpunkt des Aufrufs protokolliert und damit nicht mehr Daten gespeichert als benötigt werden, um einen möglichen inhaltlichen oder zeitlichen Missbrauch der Nutzungsrechte festzustellen (*LAG Berlin-Brandenburg*, BB 2016, 891 zu B I 4 a aa (8) (d) der Gründe). Würden die gespeicherten Verlaufsdaten nicht zumindest stichprobenartig überprüft, könnten Zuwiderhandlungen gegen das Verbot oder die Beschränkung der Privatnutzung von IT-Einrichtungen des Arbeitgebers nicht geahndet werden

und könnte die Datenerhebung ihre verhaltenslenkende Wirkung nicht entfalten. Chat-Protokolle, die der Arbeitgeber von der Internetkommunikation seiner Beschäftigten erstellt, sind nur zulässig, wenn er diese vorab über die Möglichkeit von Kontrollen sowie über deren Art, Anlass und Ausmaß informiert. Die Kontrolle darf nicht grundlos geschehen und muss das mildeste Überwachungsmittel darstellen (*EGMR* Große Kammer NZA 2017, 1443). Sollen Straftaten aufgedeckt werden, ist § 26 Abs. 1 S. 2 BDSG zu beachten. Unzulässig ist auch die **anlassunabhängige Ortung eines dem Arbeitnehmer überlassenen Mobilfunkgeräts,** insbesondere, wenn dadurch auch der Privatbereich erfasst wird (zum Ganzen: *Gola* NZA 2007, 1139, 1143 f.; *Lunk* NZA 2009, 457, 461; *Oberwetter* NZA 2008, 609, 611).

Von ein- und ausgehenden **dienstlichen E-Mails** seiner Mitarbeiter darf der Arbeitgeber im selben Maße Kenntnis nehmen wie von deren dienstlichem Schriftverkehr (*Thüsing* Arbeitnehmerdatenschutz und Compliance, Rn. 322). Verfügt das Unternehmen nur über eine elektronische Firmenadresse (z.B. info@firma.de), so ist die gesamte über die Adresse abgewickelte Post als betriebliche Korrespondenz zu werten. Der Vorgesetzte darf also anordnen, dass ihm jede ein- oder ausgehende E-Mail seiner Mitarbeiter zur Kenntnis zu geben ist. Gleiches gilt, wenn eine Adresse eindeutig als Adresse einer bestimmten Unterabteilung der Firma zu qualifizieren ist (z.B. personalabteilung@firma.de). Bei **E-Mail-Adressen, die den Namen eines Arbeitnehmers enthält** (z.B. hans.schulze@firma.de), wird der Mitarbeiter zwar direkt und unmittelbar angesprochen; das nimmt dieser E-Mail jedoch ebenfalls nicht ihren dienstlichen Charakter. Enthält die E-Mail-Adresse einen Firmenzusatz, handelt es sich jedenfalls stets um eine dienstliche Adresse, die nur direkt zu bestimmten Accounts der Mitarbeiter weitergeleitet wird (so mit Recht *Beckschulze* DB 2001, 1491, 1994; a.A. *Ernst* NZA 2002, 585, 589). Will der Absender eine Einsicht durch den Arbeitgeber vermeiden, muss er die E-Mail als „persönlich/vertraulich" kennzeichnen und entsprechend verschlüsseln. Fehlt es an solchen ausdrücklichen Vermerken, ist vom dienstlichen Charakter der E-Mail auszugehen. Einem umfassenden Kontrollverbot unterliegen allerdings die **E-Mail-Adressen von Geheimnisträgern** wie dem Betriebsrat und – sofern vorhanden – einem Betriebsarzt bzw. Betriebspsychologen. Auch diese dürfen ihre Stellungnahmen per E-Mail abgeben, insbesondere wenn sie bereits zuvor vom Mitarbeiter angeschrieben wurden. Aus Gründen des besonderen Geheimnisschutzes darf der Arbeitgeber hier auch nicht erfassen, wer Absender und Adressat der Korrespondenz ist (*Ernst* NZA 2002, 585, 590 m.w.N.). **76**

Hat der Arbeitgeber die **private Nutzung ausdrücklich gestattet oder duldet er sie zumindest,** gilt der Arbeitgeber als Anbieter von Telekommunikationsdiensten i.S.d. § 2 Abs. 2 Nr. 1 TTDSG. Inhalts- sowie Verbindungsdaten der elektronischen Kommunikation unterfallen damit dem Telekommunikationsgeheimnis nach § 3 TTDSG, § 206 StGB (str.; wie hier *LAG Hamm* 4.2.2004 – 9 Sa 502/03; *ArbG Hannover* NZA-RR 2005, 420; *Dann/Gastell* NJW 2008, 2945; *Deutsch/Diller* DB 2009, 1462, 1465; *Hoppe/Braun* MMR 2010, 80, 81; *Koch* NZA 2008, 911, 912; *Kratz/Gubbels* NZA 2009, 652, 654 f.; *Mengel* BB 2004, 2014, 2017; **77**

Schmidl MMR 2005, 343; a.A. *LAG Berlin-Brandenburg* NZA-RR 2011, 342; *LAG Niedersachsen* NZA-RR 2010, 406, 408; *Scheben/Klos/Geschonneck* CCZ 2012, 13; *Löwisch* DB 2009, 2782; *Thüsing* Arbeitnehmerdatenschutz und Compliance, Rn. 220 ff.; *Walther/Zimmer* BB 2013, 2933). Nach Auffassung des **BVerfG** erstreckt sich das **Fernmeldegeheimnis** allerdings nicht auf die außerhalb eines laufenden Kommunikationsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Kommunikation. Der **Schutz des Fernmeldegeheimnisses endet insoweit in dem Moment, in dem die E-Mail beim Empfänger angekommen und der Übertragungsvorgang beendet ist** (*BVerfG* NJW 2009, 2431 Rn. 68). Zur Begründung verweist das Gericht auf das ebenfalls unter Art. 10 Abs. 1 GG fallende Briefgeheimnis. Dort entspricht es allgemeiner Ansicht, dass der grundrechtlich vermittelte Schutz nur so lange währt, wie sich der Brief im Herrschaftsbereich des Beförderers befindet, also zwischen Absendung und Ankunft. Sobald der Empfänger den Brief erhalten habe, bestünden die spezifischen Gefahren, die mit einer räumlich-distanzierten Kommunikation einhergehen, nicht mehr. Der Adressat könne in seinem Herrschaftsbereich eigene Schutzvorkehrungen treffen, um zu verhindern, dass Dritte ungewollt auf seine Daten zugreifen (BeckOK-GG/*Ogorek* GG Art. 10 Rn. 45.1). Übertragen auf den Versand von E-Mails bedeutet dies: Solange diese auf dem Server des Arbeitgebers oder eines von ihm beauftragten Providers gespeichert sind, liegen sie außerhalb des Herrschaftsbereichs des Arbeitnehmers, und zwar auch dann, wenn sie auf dem Server des Arbeitgebers nur zwischengespeichert werden, dort also nur „ruhen" (*BVerfG* NJW 2009, 2431 Rn. 47). Der Kommunikationsprozess ist noch nicht abgeschlossen. Der Arbeitgeber, aber auch die Ermittlungsbehörden können die auf dem Mailserver gespeicherten E-Mails jederzeit abrufen. Der Adressat ist daher auf den Schutz des Fernmeldegeheimnisses angewiesen (*BVerfG* NJW 2009, 2431 Rn. 46). Der Schutz des Fernmeldegeheimnisses endet erst, wenn der Arbeitnehmer von einer eingehenden E-Mail tatsächlich Kenntnis genommen hat und er einen Zugriff des Arbeitgebers verhindern kann (*Hoppe/Braun* MMR 2010, 80, 82). Das ist der Fall, wenn er empfangene E-Mails an einer selbst gewählten Stelle im betrieblichen TK-System archiviert oder speichert (ebenso *VG Frankfurt/Main* WM 2009, 948; *Nolte/Becker* CR 2009, 125; *Schöttler* juris-PR_ITR 4/2009 Rn. 2).

78 Noch nicht abschließend geklärt ist, ob es Normen gibt, die dem Arbeitgeber einen Zugriff auf die an sich von Art. 10 GG geschützten Daten erlauben. Weitgehend einig ist man sich darin, dass eine Betriebsvereinbarung keine solche Erlaubnisnorm darstellt. Sie kann die individuelle Zustimmung zu Eingriffen in die TK-Freiheit nicht ersetzen, sondern ist das Instrument zur Ausübung und Wahrung der Mitbestimmungsrechte nach § 87 Abs. 1 Nr. 6 BetrVG (*Wronka/Gola/Pötters* Handbuch Arbeitnehmerdatenschutz, 7. Aufl. 2016, Rn. 1330; *Kempermann* ZD 2012, 12, 14; *Kort* DB 2011, 2092, 2093; a.A. *Schaar* RDV 2002, 4, 10). Anders sieht es mit der Einwilligung aus. Sowohl in Beschränkungen von Art. 10 GG als auch in § 3 TTDSG kann eingewilligt werden. Nach h.M. ist der Schutz des Fernmeldegeheimnisses nämlich verzichtbar (Maunz/Dürig/*Durner*

GG Art. 10 Rn. 1; Sachs/*Pagenkopf* GG Art. 10 Rn. 43. Beck TKG/*Bock* § 8 Rn. 44). Umstritten ist allerdings, ob für Zugriffe des Arbeitgebers auf die Kommunikationsinhalte des E-Mail-Verkehrs nur die Einwilligung des Empfängers oder auch die des Absenders nötig ist. Letzteres wird von einem Teil der Literatur verlangt (Beck TKG/*Bock* § 8 Rn. 44; Maunz/Dürig/*Durner* GG Art. 10 Rn. 127; Spindler/Schuster/*Eckhardt* TKG § 88 Rn. 28 m.w.N.; Sachs/*Pagenkopf* GG Art. 10 Rn. 43). Andere (Plath/*Jenny* TKG § 88 Rn. 11; *Kempermann* ZD 2012, 12, 14) bestreiten das mit Recht. Wer einen Arbeitnehmer unter seiner dienstlichen E-Mail-Adresse kontaktiert, muss damit rechnen, dass der Arbeitgeber auf diese E-Mail zugreifen kann, wenn sie unverschlüsselt versendet werden. Die Rechtsprechung hat – soweit ersichtlich – über diese Frage noch nicht entschieden. In der „Fangschaltungsentscheidung" ist das BVerfG allerdings zu dem Ergebnis gekommen, dass der eine Partner eines Telefongesprächs nicht mit Wirkung für den anderen ohne dessen Einverständnis auf die Wahrung des Fernmeldegeheimnisses verzichten kann. Jedenfalls folge dies nicht bereits daraus, dass jeder Fernsprechteilnehmer ohne Grundrechtsverstoß Dritte von seinen Telefongesprächen unterrichten dürfe (vgl. *BVerfG* NJW 1992, 1875). Mit Inkrafttreten des TTDSG am 1.12.2021 regelt § 25 den Schutz der Privatsphäre in diesem Fall. Danach sind die Speicherung von Informationen in der „Endeinrichtung" des Nutzers sowie der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, nur zulässig, wenn der Nutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Als „Endeinrichtung" in diesem Sinne gilt dabei jede direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten (§ 2 Abs. 2 Nr. 6 TTDSG). Die Information des Nutzers und die Einwilligung haben gemäß der DS-GVO zu erfolgen (§ 25 Abs. 1 TTDSG).

Maßgeblich für die Einwilligung ist Art. 7 DS-GVO (Buchner/Kühling/*Kühling/Raab* DS-GVO Art. 95 Rn. 10). Knackpunkt ist dabei – wie so oft – die Freiwilligkeit (Art. 4 Nr. 11 DS-GVO, § 26 Abs. 2 BDSG). An dieser fehlt es, wenn der Beschäftigte außerstande ist, seine Einwilligung ohne Rechtsnachteile zu verweigern (a.A. *Brink/Schwab* ArbR 2018, 111, 114 f., die darauf abstellen, dass der Arbeitnehmer, der nach seiner Einwilligung in die Kontrollbefugnisse die Erlaubnis zur Privatnutzung der Betriebs-IT erhält, damit seine Handlungsmöglichkeiten ja erweitere). Problematisch ist daher der auch von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vorgeschlagene Weg, die Privatnutzung der Betriebs-IT von vornherein davon abhängig zu machen, dass die Beschäftigen durch individuell erteilte Einwilligungserklärungen dem Arbeitgeber den Zugriff auf das E-Mailkonto zu Kontrollzwecken zu erlauben (DSK, Orientierungshilfe zu datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, Stand: Jan. 2016, S. 8 ff.). Auch § 26 BDSG scheidet als Erlaubnisnorm aus. Nach h.M. ist die Kontrolle des Inhalts von E-Mails nur dann erlaubt, wenn tatsächliche Anhaltspunkte für eine Leistungserschleichung i.S.v. § 265a StGB oder eine sonstige rechtswidrige Inanspruchnahme von Telekommunikationsnetzen und – diensten bestehen. Nicht erfasst ist damit die Ver- **79**

wendung des betrieblichen Accounts zur Planung, Ausführung und Vorbereitung von anderen Straftaten zulasten des Arbeitgebers oder Dritten (*Mengel* NZA 2017, 1494, 1497).

80 Noch schwieriger wird es, wenn die „Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation" (ePrivacyVO) in Kraft tritt. Diese soll die ePrivacyRL ablösen und die nationalen Vorschriften zu ihrer Umsetzung. In Deutschland sind das das TelemedienG und das TelekommunikationsG, die beide verdrängt würden und mit ihnen das deutsche Telekommunikationsgeheimnis. Für die ePrivacyVO hat die EU-Kommission am 10.1.2017 einen offiziellen Entwurf unterbreitet (COM [2017] 10 final 2017/0003 [COD]). Sie soll für die Verarbeitung elektronischer Kommunikationsdaten, die in Verbindung mit der Bereitstellung und Nutzung elektronischer Kommunikationsdienste erfolgt, anwendbar sein (Art. 2 Abs. 1 ePrivacyVO) und Vorrang vor der DS-GVO haben, deren Vorschriften sie „präzisieren und ergänzen" soll (Art. 1 Abs. 3 ePrivacyVO). Sie würde auch für den Arbeitgeber gelten, der seinen Mitarbeitern die Privatnutzung der Betriebs-IT ermöglicht. In Art. 5 erhält sie das bekannte Telekommunikationsgeheimnis. Allerdings ist dieses – wie das allgemeine Datengeheimnis als „Verbot mit Erlaubnisvorbehalt" formuliert: „Elektronische Kommunikationsdaten sind vertraulich. Eingriffe in elektronische Kommunikationsdaten wie Mithören, Abhören, Speichern, Beobachten, Scannen oder andere Arten des Abfangens oder Überwachens oder Verarbeitens elektronischer Kommunikationsdaten durch andere Personen als die Endnutzer sind untersagt, sofern sie nicht durch diese Verordnung erlaubt werden". Erlaubnistatbestände enthält dann v.a. Art. 6 ePrivacyVO. Die Verarbeitung elektronischer Kommunikationsdaten ist danach auch dann zulässig, falls der betr. Endnutzer seine Einwilligung für die Verarbeitung erteilt hat (Art. 6 Abs. 2 lit. c ePrivacyVO). Für die Einwilligung gelten dann aber wieder die Bedingungen der DS-GVO, vgl. Art. 9 Abs. 1 ePrivacyVO. Neu ist auch der in Art. 8 ePrivacyVO vorgesehene Schutz der in Endeinrichtungen der Endnutzer gespeicherten oder sich auf diese beziehenden Informationen. Danach wäre jede vom Endnutzer nicht selbst vorgenommene Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer, auch über deren Software und Hardware, grds. untersagt. Konkret hieße das, dass eine Untersuchung von auf dem Rechner des Mitarbeiters eingegangenen E-Mails künftig grds. ausgeschlossen wäre. Auch hier kann aber seine Einwilligung einen Zugriff rechtfertigen. Für sie gelten jedoch die strengen Vorgaben der DS-GVO. Wann die ePrivacyVO in Kraft tritt, ist allerdings ungewiss. Ursprünglich hatte die Kommission beabsichtigt, die ePrivacyVO zeitgleich mit der DS-GVO zum 25.5.2018 ohne jede Übergangsfrist in Kraft treten zu lassen. Der Entwurf ist aber auf heftigen Widerstand im EU-Parlament gestoßen, aus dem es nicht weniger als 827 Änderungsanträge gab. Der Rat der EU hat am 10.2.2021 seinen Standpunkt zum Entwurf der e-PrivacyVO festgelegt (https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf) und ein Man-

dat erteilt, um mit dem EU-Parlament weiterzuverhandeln. Der Ausgang des Verfahrens ist offen. Es bleibt daher vorerst bei der derzeitigen Rechtslage.

Im Ergebnis führt die Erlaubnis der Privatnutzung zu einer massiven Beschränkung der arbeitgeberseitigen Kontrollbefugnisse. Befinden sich auf dem Rechner eines Mitarbeiters sowohl dienstliche als auch private E-Mails, die unter den Schutz von Art. 10 GG fallen, schlägt das Kontrollverbot für die privaten E-Mails auf die i.Ü. zulässige Kontrolle der dienstlichen E-Mails durch (*Mengel* NZA 2017, 1494, 1496). Für den kontrollierenden Arbeitgeber bleibt zumeist unklar, welche Art von E-Mail bei einer Kontrolle betroffen ist. Das gilt jedoch nicht, wenn die Beschäftigten angehalten werden, dienstliche und private E-Mails in getrennten Postfächern abzuspeichern. Unter dieser Bedingung kann der Arbeitgeber auf das Postfach mit den dienstlichen E-Mails so wie im Falle einer verbotenen Privatnutzung zugreifen. Entsprechendes gilt, wenn bei einer erlaubten Privatnutzung private E-Mails gesondert gekennzeichnet oder nach bestimmten Fristen gelöscht sein müssen (im Ergebnis ebenso *EGMR* ZD 2018, 263 mit Anm. *Hembach* = MMR 2018, 301 mit Anm. *Hoeren*). **81**

Die Kontrollmaßnahmen unterliegen der **Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG.** Beim Einsatz von Software sowie deren Änderung genügt für das Mitbestimmungsrecht, dass ein Personenbezug durch die damit verbundenen Daten (etwa Log-Dateien bzw. Protokolldaten) mit noch vertretbarem Aufwand hergestellt werden kann (*Däubler* Rn. 759; *Kort* NZA 2011, 1319, 1321). Die Mitbestimmungspflicht besteht auch, wenn private mobile Endgeräte zu dienstlichen Zwecken eingesetzt werden (Bring Your Own Device; dazu *Arning/Moos/Becker* CR 2012, 592, 593; *Göpfert/Wilke* NZA 2012, 765, 769 f.). I.Ü. gelten die Ausführungen zur Videoüberwachung. **82**

6. Datenscreening

Datenscreening meint den automatisierten Abgleich von Beschäftigtendaten und betrifft damit die Fälle, bei denen Beschäftigtendaten quasi im Wege der „Rasterfahndung" gegen andere Daten „quergelesen" werden, etwa um herauszufinden, ob Zahlungen unbekannten Inhalts an Beschäftigte geleistet wurden (zu den verschiedenen Formen eines Datenabgleichs: *Bierekoven* CR 2010, 203; *Brink/Schmidt* MMR 2010, 592; *Gola/Wronka* Handbuch zum Arbeitnehmerdatenschutz, Rn. 1203). In der Compliance-Debatte ist es aber mitnichten ausgemacht, dass die Anforderungen an die Korruptionsbekämpfung dem Datenschutz vorgehen. *De lege lata* zieht § **26 Abs. 1 BDSG** dem „Datenscreening" Grenzen, soweit es sich als unverhältnismäßig erweist, gleichgültig, ob es zu präventiven oder repressiven Zwecken erfolgt (*Salvenmoser/Hauschka* NJW 2010, 331, 333; *Wybitul* BB 2009, 1582, 1984). Die Einzelheiten sind freilich umstritten (eher restriktiv *Däubler* Rn. 427a ff.; *Steinkühler* BB 2009, 1294; eher bejahend *Diller* BB 2009, 438, 439; differenzierend *Heldmann* DB 2010, 1235, 1237 f.; *Kort* DB 2011, 651, 653). Nach wohl h.M. widersprechen jedenfalls verdachtsunabhängige und permanente Screenings dem Verbot der Totalüberwachung (*Kock/Franke* **83**

NZA 2009, 646, 648). Geschehen sie heimlich, wird gegen das Transparenzgebot (Art. 5 Abs. 1 lit. a, Art. 13 DS-GVO) verstoßen. Darin liegt zugleich ein Verstoß gegen Art. 8 EMRK (*EGMR* NZA 2017, 1443; *EGMR* MMR 2018 mit Anm. *Hoeren* = ZD 2018,265 mit Anm. *Hembach*)

7. Telefonüberwachung

84 Das **Abhören** von Telefongesprächen sowie jedes anderen, nicht öffentlich gesprochenen Wortes und dessen **Aufzeichnung** sind nach § 201 StGB strafbar (*BGH* NJW 1991, 1180). Vertrauliche Kommunikation kann nämlich auch an allgemein zugänglichen Arbeitsplätzen stattfinden, und fällt daher in den Schutzbereich des § 201 StGB. Kein Abhören ist die Benutzung einer Telefonaufschaltanlage, mit der sich der Arbeitgeber deutlich wahrnehmbar in ein laufendes Gespräch einschalten kann (*BAG* NJW 1973, 1247). Auf **Notwehr (§ 32 StGB)** kann sich der Arbeitgeber nur berufen, wenn ein zur Zeit des Abhörens noch andauernder rechtswidriger Angriff auf ein rechtlich geschütztes Gut des Arbeitgebers vorliegt (*BGHSt* 34, 39, 51). **Notstand** (§ 34 StGB) wird als Rechtfertigungsgrund regelmäßig ausscheiden, weil die Einholung staatlicher Hilfe nach den §§ 100a ff. StPO für die Überwachung der Telekommunikation vorrangig ist (*Dann/Gastell* NJW 2008, 2945, 2946). Nicht strafbar ist das heimliche **Mithörenlassen**, d.h. das Belauschen eines Mitarbeitergesprächs durch einen Dritten, das unter Kenntnis und Billigung des Gesprächspartners erfolgt, mit dem sich der Mitarbeiter unterhält (*BGH* NJW 1994, 596; *OLG Düsseldorf* NJW 2000, 1578). Gleichwohl kann das Persönlichkeitsrecht des Mitarbeiters verletzt sein (*BVerfG* NZA 1992, 307, 308). Das gilt auch dann, wenn der Arbeitnehmer vom Vorhandensein einer Mithöreinrichtung weiß, weil er nicht damit rechnen muss, dass von dieser Möglichkeit auch Gebrauch gemacht wird (*BVerfG* NZA 1992, 307). Wer jemanden mithören lassen will, hat seinen Gesprächspartner vorher darüber zu informieren. Dieser ist nicht gehalten, sich seinerseits vorsorglich zu vergewissern, dass niemand mithört (*BAG* NZA 1998, 307). Keine Rolle spielt, ob im Gespräch persönliche Angelegenheiten oder sogar persönlichkeitssensible Daten erörtert wurden (*BVerfG* NJW 2002, 3619). Das Persönlichkeitsrecht ist i.d.R. nur dann nicht verletzt, wenn der Gesprächspartner einwilligt oder positiv weiß, dass sein Gespräch mitgehört wird (*BAG* NZA 2009, 974). Die Inhalte eines rechtswidrig mitgehörten Telefonats dürfen in einem Prozess nur dann verwertet werden, wenn sich der Arbeitgeber in einer Notwehrsituation oder einer notwehrähnlichen Lage befindet (vgl. *BGHZ* 27, 284, 289 f.) Das Interesse, sich ein Beweismittel für zivilrechtliche Ansprüche zu sichern, genügt für sich allein nicht (*BGH* NJW 1982, 277; NJW 1988, 1016, 1018; NJW 1998, 155). Konnte ein Dritter zufällig, ohne dass der beweispflichtige Arbeitgeber etwas dazu beigetragen hat, den Inhalt eines Telefongesprächs mithören, ist das allgemeine Persönlichkeitsrecht des Gesprächspartners nicht verletzt. In diesem Fall kann der Dritte zum Inhalt des Telefongesprächs als Zeuge vernommen werden (*BAG* NZA 2009, 974).

8. Öffnen von Briefen und verschlossenen Schriftstücken

Der Arbeitgeber hat das Briefgeheimnis zu wahren. Das unbefugte Öffnen von Briefen und verschlossenen Schriftstücken, die nicht zu seiner Kenntnis bestimmt sind, ist nach § 202 StGB **strafbar**. Geschützt ist jedoch nur die **Privatpost**. Dienstpost, bei der als Absender oder Empfänger der Arbeitgeber selbst angegeben ist, fällt nicht unter den Anwendungsbereich der Strafnorm und darf vom Arbeitgeber geöffnet und gelesen werden (Schönke/Schröder/*Lenckner-Eisele* StGB § 202 Rn. 12). Dies gilt ungeachtet dessen, ob sein Name als Adressat neben der Firmenadresse vermerkt ist (*LAG Hamm* NZA-RR 2003, 346). Ist **Dienstpost** zugleich an den Mitarbeiter adressiert, kann ein die Strafbarkeit ausschließendes Einverständnis vorliegen, wenn es betrieblicher Übung entspricht, dass solche Briefe allgemein geöffnet werden. Etwas anderes gilt in Parallelität zur Überwachung der IT-Nutzung dann, wenn der Brief von vornherein einen Vertraulichkeitsvermerk trägt (K/R/T/*Schuster* 11. Kap. Rn. 124). Auch wenn sich nach dem Öffnen erkennbar ergibt, dass dieser Brief einen solchen Vermerk hätte tragen müssen (z.B. Anwaltspost in einer privaten Angelegenheit an die Firmenadresse), muss der Brief sofort nach dem Öffnen vertraulich behandelt werden. **Telefaxe** unterliegen als Dienstpost dem Zugriff des Arbeitgebers. Jedoch gilt auch hier, dass ein Fax von erkennbar privater Natur (ein Rechtsanwalt leitet ein Fax zum Scheidungsverfahren des Arbeitnehmers versehentlich an die dienstliche Faxnummer) selbst dann vertraulich zu behandeln ist, wenn sein Inhalt für jeden offenkundig ist. **85**

9. Zuverlässigkeitstests

Bei einem **Zuverlässigkeitstest** (zur Frage psychologischer Eignungstests vgl. *Franzen* NZA 2013, 1 ff.) prüft der Arbeitgeber, ob sich der Mitarbeiter in einer alltäglichen Standardsituation zur Begehung einer Straftat verleiten lässt (ausf. *Maschmann* NZA 2002, 13). Bekanntestes Beispiel ist die „Wechselgeldfalle". Hierbei wird einer Verkäuferin absichtlich zu viel Wechselgeld in die Kasse gelegt, um zu kontrollieren, ob sie den „überzähligen" Kassenbestand ordnungsgemäß erfasst und für den Arbeitgeber verbucht oder das Geld einfach an sich nimmt. Auf die Probe stellen darf der Arbeitgeber einen Mitarbeiter nur, wenn gegen ihn der konkrete Verdacht einer Straftat oder einer schweren Arbeitspflichtverletzung besteht (*BAG* NZA 2000, 418, 420). Zuverlässigkeitstests ohne konkreten Kontrollanlass sind dagegen nur zulässig, wenn der Arbeitgeber keine andere Möglichkeit hat, sich von der Rechtschaffenheit seiner im Außendienst oder vergleichbar „unbeaufsichtigt" tätigen Mitarbeiter zu überzeugen. Ansonsten sind „prophylaktische" Zuverlässigkeitstests, die ohne jeden Anhaltspunkt womöglich nur zur Abschreckung durchgeführt werden, unzulässig (im Ergebnis ähnlich EGMR 9.1.2018 App. 1874/13 und 8567/13 Rn. 68 ff.; großzügiger *Ricken* RdA 2001, 52, 53, der lediglich verlangt, dass Zuverlässigkeitstests mit der konkreten Arbeitssituation in Zusammenhang stehen müssen). Der Mitarbeiter darf nicht nur mit dem Ziel auf die Probe gestellt werden, ihn „hereinzulegen". Unzulässig ist die Anwendung **86**

strafbarer oder sonst verwerflicher Mittel. Der Arbeitgeber darf dem Mitarbeiter zwar die günstige Gelegenheit zur Begehung einer Straftat verschaffen; er darf ihn aber nicht anstiften. Die Grenze zwischen noch erlaubter „Herausforderung" und unzulässiger „Verführung" lässt sich nur im Einzelfall unter Berücksichtigung sämtlicher Umstände bestimmen.

87 Nach dem BAG kann die „Tatprovokation" nicht ohne Einfluss auf die Auswahl der Sanktionen bleiben, die der Arbeitgeber nach einem nicht bestandenen Zuverlässigkeitstest verhängen darf. Im Einzelfall kann es ihm sogar verwehrt sein, eine außerordentliche Tat- oder Verdachtskündigung auszusprechen; er muss sich dann mit einer Abmahnung begnügen (*BAG* NZA 2000, 381, 383). Von Bedeutung ist in diesem Zusammenhang, ob der Arbeitgeber auf die mögliche Durchführung von Ehrlichkeitskontrollen **hingewiesen** hat (*EGMR* NZA 2017, 1443; *EGMR* 9.1.2018 App. 1874/13 und 8567/13 Rn. 68 ff.). Bei Außendienstlern, die auch ohne konkrete Verdachtsmomente jederzeit auf die Probe gestellt werden dürfen, gebietet es die Fairness, wenigstens den Zeitraum zu nennen, innerhalb dessen mit „Routine-Kontrollen" zu rechnen ist. Eine andere Frage ist, ob der Betriebsrat von dem Test benachrichtigt werden muss. Das ist zu bejahen, wenn ihm ein zwingendes Mitbestimmungsrecht zukommt, was nur unter besonderen Umständen der Fall ist (s. im Einzelnen *Maschmann* NZA 2002, 13, 18).

88 Da alle Zuverlässigkeitstests in der entscheidenden Phase ohne Zugriff des Arbeitgebers ablaufen, muss für ein aussagekräftiges Ergebnis gesorgt werden, das **störenden Einflüssen Dritter entzogen** ist. So hat der Arbeitgeber sicherzustellen, dass die zu überführende Mitarbeiterin im Verkauf alleinigen Zugang zur Kasse hat, dass der Lagerarbeiter den einzigen Schlüssel für das Depot besitzt, dass der Zahlstellenmitarbeiter die Wertmarken allein verwaltet usw. Anderenfalls riskiert der Arbeitgeber, dass sich der ertappte Arbeitnehmer auf die Möglichkeit eines ihn entlastenden alternativen Geschehensablaufs beruft. Überdies ist mit den üblichen Schutzbehauptungen zu rechnen, etwa Wechselgeld nur an sich genommen zu haben, um es später zu registrieren usw. Hier ist es Sache des Arbeitgebers, für einen **klaren und eindeutigen Betriebsablauf** zu sorgen. Insbesondere muss er dem Mitarbeiter mitteilen, wie er in der vom Normalfall abweichenden Ausnahmesituation zu verfahren hat, beispielsweise, dass überzähliges Wechselgeld sofort zu verbuchen ist. Unklare Handlungsanweisungen gehen im Zweifel zu Lasten des Arbeitgebers.

10. Einsatz von Detektiven

89 Die Observation von Arbeitnehmern durch den Einsatz von Detektiven bedeutet einen schwerwiegenden Eingriff in das allgemeine Persönlichkeitsrecht (*BAG* NZA 2017, 1179). Ein von einer verdeckten Überwachung Betroffener wird in der Befugnis, selbst über die Preisgabe und Verwendung persönlicher Daten zu befinden, beschränkt, indem er zum Ziel einer nicht erkennbaren systematischen Beobachtung durch einen Dritten gemacht wird und dadurch auf sich beziehbare Daten über sein Verhalten preisgibt, ohne den mit der Beobachtung verfolgten

Verwendungszweck zu kennen. Darin liegt zugleich ein schwerwiegender Eingriff in Art. 8 EMRK (vgl. *EGMR* NZA 2017, 1443; MMR 2018, 301 = ZD 2018, 263). Dies gilt unabhängig davon, ob Fotos, Videoaufzeichnungen oder Tonmitschnitte angefertigt werden und damit zugleich ein Eingriff in das Recht am eigenen Bild bzw. Wort vorliegt. Ein Eingriff in das Recht auf informationelle Selbstbestimmung setzt auch nicht notwendig voraus, dass die Privatsphäre des Betroffenen ausgespäht wird. Zwar muss der Einzelne außerhalb des thematisch und räumlich besonders geschützten Bereichs der Privatsphäre damit rechnen, Gegenstand von Wahrnehmungen beliebiger Dritter zu werden, grds. aber nicht, Ziel einer verdeckten und systematischen Beobachtung zur Beschaffung konkreter, auf die eigene Person bezogener Daten zu sein (*BAG* NZA 2015, 994; NZA 2017, 1179, 1181). Erfolgt diese heimlich oder durch Nutzung einer Legende (z.B. getarnt als Kunde, neuer Kollege, Lieferant), wird damit gegen das Transparenzgebot (Art. 5 Abs. 1 lit. a, Art. 13 DS-GVO) verstoßen. Vor Inkrafttreten der DS-GVO hielt die Rechtsprechung einen (verdeckten) Detektiveinsatz für zulässig, wenn ein auf Tatsachen beruhender konkreter Verdacht einer Straftat oder einer schwerwiegenden Pflichtverletzung des Arbeitnehmers bestand (*BAG* NZA 2015, 994; 2017, 1179). Das hatte die Rechtsprechung z.B. angenommen für eine unerlaubte Konkurrenztätigkeit, für die sich ein Verdacht aus einer vom Arbeitgeber verfolgten E-Mail-Korrespondenz des Arbeitnehmers ergab (*BAG* NZA 2017, 1179). Im Hinblick auf das Vortäuschen einer Arbeitsunfähigkeit als einer eine Überwachung rechtfertigende Straftat hatte sie den Nachweis „begründeter Zweifel an der Richtigkeit einer ärztlichen Arbeitsunfähigkeits-Bescheinigung" verlangt (*BAG* NZA 2015, 994). Mit Inkrafttreten der DS-GVO kann daran nicht mehr festgehalten werden, jedenfalls solange der deutsche Gesetzgeber keine den Vorgaben des Art. 23 DS-GVO entspr. Vorschrift erlässt, die eine heimliche Observation zulässt. Selbst dann muss der Einsatz **verhältnismäßig** sein und ist auf das unbedingt Erforderliche zu beschränken (vgl. weiter *EGMR* NZA 2017, 1443; MMR 2018, 301 = ZD 2018, 263). Eine **verdeckte Ermittlung „ins Blaue hinein",** ob ein Arbeitnehmer sich pflichtwidrig verhält, ist nach aktueller Rechtsprechung des *LAG Berlin-Bbg* (ZD 2021, 170) **unzulässig.** Ein Informationsinteresse bezüglich des Verhaltens eines Arbeitnehmers oder **Zweifel, ob jemand weiterhin so gut wie möglich arbeite, reichten nicht aus**, um eine **Überwachung durch einen Detektiv** zu rechtfertigen. Daran ändern auch nachträgliche Feststellungen im Zuge einer Überwachung nichts; sie genügen nicht, um den erforderlichen zuvor bestehenden auf konkrete Tatsachen gestützten Verdacht zu begründen. Der rechtswidrige Detektiveinsatz führe zu einem **Sachvortrags- und Beweisverwertungsverbot hinsichtlich des unerlaubt gewonnenen Ermittlungsmaterials.** Stets verboten ist das nachhaltige Ausspähen der Privat- oder gar Intimsphäre des Arbeitnehmers; sie steht sogar unter der Strafandrohung des § 201a StGB. Fertigt der Detektiv heimlich Bild- oder Tonaufnahmen oder hört er Telefongespräche ab oder mit, gelten die **bereits dargestellten Grundsätze**.

Die **Kosten**, die durch das Tätigwerden eines Detektivs entstehen, hat der Arbeitnehmer zu ersetzen, wenn gegen ihn ein konkreter Tatverdacht bestand und er **90**

später einer vorsätzlichen vertragswidrigen Handlung überführt wird (*BAG* NZA 1998, 1334). Die Kosten müssen sachdienlich und notwendig sein und zum Streitgegenstand in einem angemessenen Verhältnis stehen (*LAG Hamm* DB 1996, 279). **„Vorsorgekosten"**, wie etwa die Personalaufwendungen für einen angestellten Hausdetektiv, sind nicht erstattungsfähig, weil sie sich nicht einer konkreten Pflichtverletzung eines Mitarbeiters zurechnen lassen (*BAG* 3 AZR 277/84 n.v.). Dass der Detektiveinsatz auch einer gerichtsfesten Aufklärung des Sachverhalts dient, stellt den notwendigen Bezug zu einem späteren Rechtsstreit noch nicht her, weil offen ist, ob sich der Arbeitnehmer wegen der gegen ihn verhängten Sanktionen gerichtlich zu Wehr setzt (*LAG Frankfurt/Main* NZA-RR 1999, 322).

91 Die **reine Beobachtung eines Mitarbeiters,** etwa durch einen Detektiv, **unterliegt keiner Mitbestimmung** nach § 87 Abs. 1 Nr. 1 BetrVG, jedenfalls soweit dabei keine technischen Einrichtungen i.S.v. § 87 Abs. 1 Nr. 6 BetrVG verwendet werden (*BAG* NZA 2000, 418, 421; *LAG Schleswig-Holstein* 4 TaBV 5/83 n.v.; *LAG Rheinland-Pfalz* 5 TaBV 27/97 n.v.; a.A. *LAG Frankfurt/Main* 5 TaBV 97/99). Die Beobachtung dient nämlich nicht der Beeinflussung des Mitarbeiters, sondern allein der Aufdeckung einer von ihm begangenen Straftat oder Arbeitsvertragsverletzung (*BAG* NZA 1991, 729). Werden Detektive „wie Arbeitnehmer" in den Betriebsablauf eingegliedert, um verdeckt ermitteln zu können, ist der Betriebsrat nach § 99 BetrVG zu beteiligen (*BAG* NZA 1991, 729). Dabei ist ihm die Ermittlungstätigkeit des Detektivs mitzuteilen, über die er Stillschweigen zu bewahren hat.

11. Elektronische Ortung

92 Die **elektronische Ortung von Beschäftigten** durch den Arbeitgeber mittels **GPS (Global Positioning System), Diensthandy oder RFID-Chips** (zum Ganzen *Göpfert/Papst* DB 2016, 1015; *Gola* NZA 2007, 1139, 1143 f.; *Lunk* NZA 2009, 457, 461; *Oberwetter* NZA 2008, 609, 611**)** ist nur dann erlaubt, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist (Plath/*Stahmer/Kunke* § 26 BDSG Rn. 130). Das kann z.B. der Fall sein, wenn Wachpersonal, Feuerwehrleute oder Beschäftigte auf einer Bohrinsel durch GPS gesichert werden sollen (NK-ArbR/*Brink* § 32 BDSG, 2016, Rn. 121; Däubler/Klebe/*Wedde*/Weichert BDSG, 5. Aufl. 2016, § 32 Rn. 108), oder wenn der Arbeitgeber den Arbeitseinsatz von Arbeitnehmern im Außendienst (Fahrer, Monteure, Vertreter usw.) koordinieren will (*Beckschulze/Natzel* BB 2010, 2368, 2373) oder wenn es um den Schutz von wertvollem Eigentum des Arbeitgebers (LKW mit Ladung) oder von diesem anvertrauten Gegenständen (Geld in einem Werttransporter) geht (Simitis/*Seifert* § 32 BDSG a.F. Rn. 82). Dafür gelten aber strenge Anforderungen. Zunächst muss der Zweck der Ortungsdaten klar dokumentiert und kommuniziert werden (NK-ArbR/*Brink*, § 32 BDSG Rn. 122). Eine nachträgliche Zweckänderung – etwa zur Leistungs- und Verhaltenskontrolle der Beschäftigten – kommt nur nach vorheriger Information gem. Art. 13 Abs. 3 DS-GVO in Betracht, damit der Überwachte vor der Weiterverarbeitung zu geänderten Zwecken

Einwände erheben kann (Kühling/Buchner/*Bäcker* DS-GVO Art. 13 Rn. 38 ff.). Die heimliche Erstellung von Bewegungsprofilen der Beschäftigten mittels GPS ist nach hier vertretener Ansicht grds. ausgeschlossen (ebenso Plath/*Stamer/Kuhnke* BDSG § 26 Rn. 130; a.A. *Gola* ZD 2012, 308; Simitis/*Seifert* § 32 BDSG a.F. Rn. 82, der heimlich erstellte Bewegungsprofile für zulässig hält, wenn die Voraussetzungen des § 26 Abs. 1 S. 2 BDSG erfüllt sind, d.h. bei Vorliegen eines konkreten Tatverdachtes gegen den betroffenen Beschäftigten, der Erforderlichkeit des angefertigten Bewegungsprofils für die Klärung der Beweisfrage sowie des Fehlens milderer Mittel, die zur Herbeiführung desselben Erfolges vom Arbeitgeber eingesetzt werden könnten; ähnlich Däubler/Klebe/*Wedde*/Weichert BDSG, § 32 BDSG Rn. 106). Stets muss der Einsatz eines Ortungssystems kenntlich gemacht werden (Art. 13 Abs. 1 DS-GVO), etwa durch eine Benachrichtigung des Überwachten per SMS oder eine entspr. Anzeige. Lässt sich der Aufenthaltsort eines Beschäftigten auch durch einen Anruf auf seinem Mobiltelefon ermitteln, kann eine automatisierte Datenerhebung unverhältnismäßig sein (NK-ArbR/*Brink* § 32 Rn. 124; Däubler/Klebe/*Wedde*/Weichert BDSG, § 32 BDSG Rn. 109). Die zulässige Intensität einer Ortung bemisst sich ebenfalls nach dem Grundsatz der Erforderlichkeit. Genügt es, das Ortungssystem erst dann zu aktivieren, wenn dafür ein konkretes Bedürfnis besteht, wäre eine dauerhafte Ortung unverhältnismäßig (Ebenso Däubler/Klebe/*Wedde*/Weichert BDSG, § 32 BDSG Rn. 108, der Ausnahmen allenfalls in Bereichen zulassen will, bei denen Beschäftigte besonderen Sicherheitsrisiken ausgesetzt sind, wie z.B. Fahrer von Geldtransporten; ähnlich Plath/*Stamer/Kuhnke* BDSG § 26 Rn. 130). Die anlasslose Ortung von Kraftwagen einer Fahrzeugflotte ist unzulässig, wenn sie unabhängig von notwendigen Dispositionen erfolgt (NK-ArbR/*Brink* § 32 BDSG Rn. 123). Selbst im Falle einer gestatteten oder auch nur geduldeten Privatnutzung von Dienstwagen besteht kein pauschales Bedürfnis für eine Erhebung von auch außerhalb der Arbeitszeit anfallenden Daten durch ein im Fahrzeug installiertes Ortungssystem. Für einen präventiven Diebstahlsschutz sind Ortungssysteme mit ständiger anlassloser Erhebung der Positionsdaten völlig ungeeignet. Für das Wiederauffinden eines womöglich entwendeten Dienstwagens genügt eine anlassbezogene Ortung, sobald der Verlust festgestellt wurde (*VG Lüneburg* ZD 2019, 331; ebenso *Hrube* jurisPR-ITR 23/2019 Anm. 3; *Jacobi* ArbRB 2019, 175; *Stück* AuA 2019, 556; *Shindova* DSB 2019, 111; *Bartsch/Müller* IR 2019, 191. Sind Ortungssysteme mit Arbeitsmitteln (LKW/Bagger) verbunden, gilt § 26 Abs. 1 BDSG, wenn sie einem bestimmten Beschäftigten zugeordnet werden können (NK-ArbR/*Brink* § 32 BDSG Rn. 121). Dienstfahrzeuge, die auch privat genutzt werden dürfen, müssen nach Dienstschluss vom Ortungssystem abgemeldet werden (NK-ArbR/*Brink* § 32 BDSG Rn. 124). Unzulässig ist auch die **anlassunabhängige Ortung eines dem Arbeitnehmer überlassenen Mobilfunkgeräts,** insbesondere wenn dadurch auch der Privatbereich erfasst wird. Der Einsatz von Ortungsgeräten unterliegt der Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG, soweit damit die Möglichkeit eröffnet ist, die Leistung und das Verhalten von Beschäftigten zu überwachen (Plath/*Stamer/Kuhnke* BDSG § 26 Rn. 130). Das ist bei der Verwendung von RFID-Chips zur Sicherung von beweglichen Sachen (z.B. Bücher einer

Bibliothek, Waren in einem Kaufhaus) nicht der Fall, so lange diese nicht einzelnen Mitarbeitern zuzuordnen sind (*Gola* NZA 2007, 1139, 1141; Plath/*Stamer/Kuhnke* BDSG § 26 Rn. 130). Die Verarbeitung von „Wearable-Sensordaten" bei Beschäftigten, die z.B. durch in die Arbeitskleidung eingebaute Sender ermittelt und übertragen werden, ist nur unter strenger Beachtung des Erforderlichkeitsprinzips zulässig, weil hierbei auch sensible Daten i.S.d. Art. 9 DS-GVO erhoben und genutzt werden (ausf. *Weichert* NZA 2017, 565).

V. Sanktionen

1. Überblick

93 Verstoßen Arbeitnehmer gegen Compliance-Vorschriften, kommt als Sanktion zunächst die **Abmahnung** in Betracht. Massivere Verfehlungen werden sich – wenn der überführte Mitarbeiter keinen Aufhebungsvertrag zu schließen bereit ist (s. dazu unten Rn. 119) – nur mit einer **Kündigung** beantworten lassen. Ist die ordentliche Kündigung ausgeschlossen oder scheidet eine Weiterbeschäftigung des Arbeitnehmers bis zum Ablauf der Kündigungsfrist wegen Unzumutbarkeit aus, ist an eine **außerordentliche** Kündigung zu denken. Sie kann als **Tatkündigung** erklärt werden, wenn der Verstoß gegen Compliance-Vorschriften bereits erwiesen ist. Besteht nur ein begründeter Verdacht, wird der Arbeitgeber eine **Verdachtskündigung** erklären, wenn das für das Arbeitsverhältnis unverzichtbare Vertrauensverhältnis zwischen den Arbeitsvertragsparteien erheblich gestört ist (unten Rn. 113 ff.). Wird ein Aufhebungsvertrag geschlossen, stellt sich die Frage nach seiner Wirksamkeit (unten Rn. 120 ff.). Können Arbeitnehmer nicht fristlos gekündigt werden, ist zumindest ihre **Suspendierung von der Arbeit** in Erwägung zu ziehen (unten Rn. 123 ff.). Verstöße gegen die betriebliche Ordnung wurden früher auch durch **Betriebsbußen** (*BAG* NZA 1990, 193) geahndet. Sie sind außer Gebrauch gekommen, weil die Verhängung von Bußen durch nichtstaatliche Stellen dem Rechtsempfinden widerspricht. Aus Gründen der Compliance erfreuen sie sich seit kurzem aber wieder größerer Beliebtheit.

2. Abmahnung

94 Mit der Abmahnung beanstandet der Arbeitgeber in einer für den Arbeitnehmer hinreichend deutlich erkennbaren Weise die Verletzung einer Vertragspflicht und verbindet damit den Hinweis, dass im Wiederholungsfall der Inhalt oder der Bestand des Arbeitsverhältnisses gefährdet ist (*BAG* NZA 2013, 91). Beruht die **Vertragspflichtverletzung auf steuerbarem Verhalten des Arbeitnehmers,** ist grds. davon auszugehen, dass sein künftiges Verhalten schon durch die Androhung von Folgen für den Bestand des Arbeitsverhältnisses positiv beeinflusst werden kann (*BAG* NZA 2010, 1227; *Schlachter* NZA 2005, 433, 436). Deshalb hat der Arbeitgeber den Arbeitnehmer **bei Störungen im Leistungsbereich sowie bei Verstößen gegen die betriebliche Ordnung grds. abzumahnen, bevor er eine verhaltensbedingte Kündigung ausspricht.** Eine fruchtlose Abmahnung rechtfertigt zugleich

die Prognose, dass der Arbeitnehmer sich auch in Zukunft nicht vertragsgerecht verhalten wird (*BAG* 2008, 589; 2010, 1227). Diese Prognose ist Voraussetzung für eine verhaltensbedingte Kündigung. Einer **Abmahnung bedarf es** nur dann **nicht**, wenn bereits **ex ante erkennbar** ist, dass eine **Verhaltensänderung in Zukunft auch nach Abmahnung nicht zu erwarten steht**, oder es sich um eine **so schwere Pflichtverletzung** handelt, dass **selbst deren erstmalige Hinnahme dem Arbeitgeber nach objektiven Maßstäben unzumutbar und damit offensichtlich** – auch für den Arbeitnehmer erkennbar – **ausgeschlossen** ist (*BAG* NZA 2019, 445). Das hat die Rspr. zuletzt angenommen für die unerwünschte Zusendung pornografischer Videos über einen Messenger-Dienst (WhatsApp) an eine Arbeitskollegin (*LAG MV* NZA-RR 2020, 419) sowie bei einer Entwendung einer Einliterflasche Desinfektionsmittel, die der Arbeitgeber seinen Arbeitnehmern während der Corona-Pandemie zur Verfügung gestellt hatte (*LAG Düsseldorf* 14.1.2021 - 5 Sa 483/20).

95 Bei der Abmahnung handelt es sich um die Ausübung eines arbeitsvertraglichen Gläubigerrechts (*BAG* AP Nr. 8 zu § 611 BGB Nebentätigkeit). Als Gläubiger der Arbeitsleistung weist der Arbeitgeber den Arbeitnehmer auf seine vertraglichen Pflichten hin und macht ihn darauf aufmerksam, dass er sie verletzt hat, sog. **Rüge- bzw. Dokumentationsfunktion** (*BAG* AP Nr. 34 zu § 1 KSchG 1969 Verhaltensbedingte Kündigung). Zugleich fordert er ihn für die Zukunft zu einem vertragsgetreuen Verhalten auf und droht ihm für den Fall erneuter Pflichtverletzung individualrechtliche Konsequenzen an, die bis zur Kündigung reichen können, sog. **Warnfunktion** (*BAG* AP Nr. 4 zu § 78 BetrVG 1972). Der dem Arbeitnehmer vorgeworfenen Vertragsverstoß muss dabei so genau bezeichnet werden, dass der Arbeitnehmer den Inhalt der nach Auffassung des Arbeitgebers verletzten Pflicht erkennen kann (*AP* KSchG 1969 § 1 Abmahnung Nr. 5). **Abmahnungsberechtigt** sind der Arbeitgeber und die von ihm Bevollmächtigten. Dazu gehören regelmäßig die kündigungsberechtigten Personen und die Mitarbeiter, die nach ihrer Aufgabe befugt sind, Anweisungen zu Ort, Zeit und Art und Weise der Arbeitsleistung zu erteilen, d.h. sowohl die zu Personalentscheidungen befugten Dienstvorgesetzten („Disziplinarvorgesetzter") als auch die Fachvorgesetzten.

96 Für die Abmahnung kommt es nicht darauf an, ob dem Arbeitnehmer die Pflichtverletzung subjektiv vorgeworfen werden kann; **es reicht aus,** wenn der Arbeitgeber einen **objektiven Verstoß des Arbeitnehmers gegen seine arbeitsvertraglichen Pflichten** rügt (*BAG* AP Nr. 84 zu § 37 BetrVG 1972). Die Abmahnung ist jedoch **ungerechtfertigt,** wenn sie **unrichtige Tatsachenbehauptungen** enthält (*BAG* AP Nr. 93 zu § 611 BGB Fürsorgepflicht), das Verhalten des Arbeitnehmers unzutreffend bewertet wird, oder wenn die Abmahnung eine **unangemessene Reaktion** auf eine nur geringfügige Pflichtverletzung darstellt und sie damit den Grundsatz der Verhältnismäßigkeit verletzt (*BAG* AP Nr. 98 zu § 37 BetrVG 1972).

97 Vor Erteilung einer Abmahnung ist weder der Arbeitnehmer (*BAG* NZA 2009, 894) noch der Betriebsrat **anzuhören** (APS/*Kiel* § 1 KSchG Rn. 366a m.w.N.). Ein

Mitbestimmungsrecht des Betriebsrats besteht ebenfalls nicht (*BAG* AP Nr. 25 zu § 1 KSchG 1969 Verhaltensbedingte Kündigung). Das gilt selbst dann, wenn der Arbeitgeber wegen einer Vertragsverletzung abmahnt, durch die die Ordnung des Betriebs gestört wurde (§ 87 Abs. 1 Nr. 1 BetrVG). Der Arbeitgeber macht lediglich von einem vertraglichen Recht Gebrauch: er fordert einen konkreten Arbeitnehmer zur Erfüllung seiner arbeitsvertraglichen Verpflichtungen auf.

98 Da es für die Abmahnung **keine Ausschlussfrist gibt**, kann der Arbeitgeber sie auch noch einige Zeit nach dem Pflichtverstoß erklären. Der Arbeitgeber **verwirkt** (§ 242 BGB) jedoch **sein Recht zur Abmahnung**, wenn er durch sein Nichthandeln beim Arbeitnehmer das berechtigte Vertrauen erweckt, er werde wegen der Verfehlung nicht mehr belangt (*BAG* AP Nr. 17 zu § 1 KSchG 1969 Verhaltensbedingte Kündigung). Ob eine vorangegangene Abmahnung zeitlich so weit zurückliegt, dass sich eine bei einem neuerlichen Pflichtverstoß ausgesprochene Kündigung als unverhältnismäßig darstellt, ist eine Frage des Einzelfalls. Eine diesbezügliche **Regelfrist** gibt es **nicht**. Hat der Arbeitgeber vor dem Ausspruch einer verhaltensbedingten Kündigung eine Abmahnung auszusprechen, ist eine Abmahnung nicht nur dann einschlägig, wenn sie **genau denselben Pflichtenverstoß** betrifft, der auch der nachfolgenden Kündigung zugrunde liegt, sondern ebenfalls dann, wenn es um eine **Pflichtverletzung geht, die mit dem der Kündigung zugrundeliegenden Vorwurf auf einer Ebene liegt** (*LAG Rheinland-Pfalz* 8.7.2016 – 1 Sa 57/16). **Mehrere Abmahnungen** wegen gleichartiger Pflichtverletzungen, **denen keine weiteren Konsequenzen folgen**, können die Warnfunktion der Abmahnungen abschwächen. Der Arbeitgeber muss dann die letzte Abmahnung vor Ausspruch einer Kündigung besonders eindringlich gestalten, um dem Arbeitnehmer klar zu machen, dass weitere derartige Pflichtverletzungen nunmehr zur Kündigung führen werden (*BAG* AP Nr. 4 zu § 1 KSchG 1969 Abmahnung). Eine unwirksame Kündigung kann als Abmahnung ausgelegt werden (*BAG* DB 1990, 790).

99 Hat der Arbeitgeber die Abmahnung zu den Personalakten genommen, so kann der Arbeitnehmer verlangen, dass eine Gegendarstellung zu den Akten genommen wird (§ 83 Abs. 2 BetrVG, § 26 Abs. 2 S. 4 SprAuG). Entsprechend §§ 242, 1004 Abs. 1 S. 1 BGB kann er darüber hinaus verlangen, dass der Arbeitgeber eine ungerechtfertigte Abmahnung aus der Personalakte entfernt (ständige Rspr., vgl. *BAG* NZA 2014, 803). Zudem besteht ein datenschutzrechtlicher Löschungsanspruch aus Art. 17 DS-GVO (*LAG Sachsen-Anhalt* ZD 2019, 424). Der Arbeitnehmer kann den Anspruch mit der Leistungsklage verfolgen. Er kann sich aber auch darauf beschränken, in einem eventuellen Kündigungsschutzprozess die Pflichtwidrigkeit zu bestreiten (*BAG* EzA § 611 BGB Abmahnung Nr. 5, 24). **Mit einer Abmahnung verzichtet der Arbeitgeber auf sein Kündigungsrecht**. Er kann dem Arbeitnehmer wegen derselben Pflichtwidrigkeit nicht mehr kündigen (*BAG* NZA 2010, 823). Der Arbeitgeber gibt mit einer Abmahnung zu erkennen, dass er das Arbeitsverhältnis noch nicht als so gestört ansieht, als dass er es nicht mehr fortsetzen könnte. Dies gilt allerdings dann nicht, wenn gem. §§ 133, 157 BGB der Abmahnung selbst oder den Umständen zu entnehmen ist, dass der Arbeit-

geber die Angelegenheit mit der Abmahnung nicht als „erledigt" ansieht. Für die Frage, ob das **Verhalten des Arbeitnehmers** i.S.v. § 1 Abs. 2 S. 1 KSchG eine **Kündigung „bedingt"**, gilt ein **objektiver Maßstab**. Maßgeblich ist nicht, ob ein bestimmter Arbeitgeber meint, ihm sei die Fortsetzung des Arbeitsverhältnisses nicht zuzumuten, und ob er weiterhin hinreichendes Vertrauen in einen Arbeitnehmer hat. Es kommt vielmehr darauf an, ob dem Kündigenden die Weiterbeschäftigung – bei der ordentlichen Kündigung auch über den Ablauf der Kündigungsfrist hinaus – aus der Sicht eines objektiven und verständigen Betrachters unter Berücksichtigung der Umstände des Einzelfalls zumutbar ist oder nicht (*BAG* NZA 2016, 540). Setzt der Arbeitnehmer allerdings trotz der Abmahnung sein pflichtwidriges Verhalten fort oder begeht er eine neue vergleichbare Pflichtverletzung, dann eröffnet die Abmahnung dem Arbeitgeber den Weg zur Kündigung.

100 War die **Abmahnung zulässig**, kann der Arbeitnehmer ihre **Entfernung** nur dann verlangen, **wenn sie unter keinem rechtlichen Gesichtspunkt mehr Bedeutung für das Arbeitsverhältnis haben kann** und der Arbeitgeber sie auch nicht mehr zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen i.S.d. Art. 17 Abs. 3 lit. e DS-GVO benötigt (*BAG* NZA 2013, 91; *Nebeling/Lankes* DB 2017, 2542). Das durch die Abmahnung gerügte Verhalten muss für das Arbeitsverhältnis in jeder Hinsicht rechtlich bedeutungslos geworden sein. Das ist nicht der Fall, solange eine zu Recht erteilte Abmahnung etwa für eine zukünftige Entscheidung über eine Versetzung oder Beförderung und die entsprechende Eignung des Arbeitnehmers, für die spätere Beurteilung von Führung und Leistung in einem Zeugnis oder für die im Zusammenhang mit einer möglichen späteren Kündigung erforderlich werdende Interessenabwägung von Bedeutung sein kann (*BAG* NZA 2013, 91). Darüber hinaus kann es im berechtigten Interesse des Arbeitgebers liegen, die Erteilung einer Rüge im Sinne einer Klarstellung der arbeitsvertraglichen Pflichten weiterhin dokumentieren zu können. Allerdings muss ein solches Dokumentationsinteresse nicht zwangsläufig für die gesamte Dauer des Arbeitsverhältnisses bestehen. So kann ein hinreichend lange zurückliegender, nicht schwerwiegender und durch beanstandungsfreies Verhalten faktisch überholter Pflichtenverstoß seine Bedeutung für eine später erforderlich werdende Interessenabwägung gänzlich verlieren. Eine nicht unerhebliche Pflichtverletzung im Vertrauensbereich wird demgegenüber eine erhebliche Zeit von Bedeutung sein (*BAG* NZA 2013, 91). **Nach Beendigung des Arbeitsverhältnisses** kann der Erhalt der Abmahnung in der Personalakte notwendig sein, soweit dies zur Abwehr von etwaigen Ansprüchen des Arbeitnehmers oder zur Begründung eigener Ansprüche gegen den Arbeitnehmer erforderlich erscheint. Ist das nicht der Fall, kann der Arbeitnehmer Löschung nach § 17 DS-GVO verlangen, ohne objektive Anhaltspunkte darlegen zu müssen, dass ihm die Abmahnung noch schaden könnte (*LAG Sachsen-Anhalt* NZA-RR 2019, 355; ebenso *Möllenkamp* NZA-RR 2019, 357).

3. Außerordentliche Kündigung

a) Wichtiger Grund

101 Eine außerordentliche, in der Regel fristlose Kündigung ist zulässig, wenn ein wichtiger Grund i.S.d. § 626 BGB vorliegt. Ob ein solcher besteht, ist nach der Rechtsprechung des BAG in **zwei Schritten** zu prüfen (*BAG* NZA 2014, 1197, 1200 m.w.N.; NZA 2017, 1121; NZA 2018, 845; NZA 2019, 445). Zunächst ist festzustellen, ob ein Sachverhalt unabhängig vom Einzelfall **„an sich"** geeignet ist, einen Kündigungsgrund zu bilden. Ist das zu bejahen, erfolgt in einem zweiten Schritt eine **umfassende Interessenabwägung**, bei der sämtliche Umstände des Einzelfalles zu berücksichtigen sind. Die systematische Trennung der Prüfung dient der Rechtssicherheit und der Rechtsklarheit, weil für die vorrangige Frage, ob ein bestimmter Grund an sich eine außerordentliche Kündigung zu rechtfertigen vermag, allgemeine Grundsätze aufgestellt werden können, die die Anwendung des Rechtsbegriffs des wichtigen Grundes erleichtern (*BAG* AP Nr. 28 zu § 626 BGB Verdacht strafbarer Handlung).

102 **Kontrovers** beurteilt wird die Frage, ob eine einmalige Pflichtverletzung des Arbeitnehmers, die zu einer lediglich **geringfügigen Schädigung des Arbeitgebers** führt, eine außerordentliche Kündigung „an sich" rechtfertigen kann. Während vereinzelt vertreten wird, dass etwa der Diebstahl oder die Unterschlagung solcher Sachen nicht einmal die Schwelle des wichtigen Grundes erreichen (*LAG Köln* NZA-RR 2001, 83; *LAG Hamburg* NZA-RR 1999, 469), wird das vom *BAG* (NZA 1985, 91; 2000, 421; 2008, 1008; 2010, 1227) im Einklang mit der h.L. (statt aller KR/*Fischermeier* § 626 BGB Rn. 445) zu Recht anders gesehen. Das von der Mindermeinung (MK-BGB/*Henssler* § 626 Rn. 77) angesprochene Ungleichgewicht zwischen der Störung der Hauptleistungspflicht durch Arbeitsverweigerung, die beharrlich sein muss, um einen wichtigen Grund bilden zu können, und der Verletzung der Nebenpflicht, Eigentum und Vermögen des Arbeitgebers zu wahren, besteht nicht. Wer einer einmaligen und geringfügigen Pflichtverletzung von vornherein die Bedeutung eines „an sich" tauglichen Grundes für eine außerordentliche Kündigung abspricht, läuft zudem Gefahr, die systematische Zweiteilung des § 626 Abs. 1 BGB, die der Rechtssicherheit dient, zu verfehlen. Ob ein Schaden als geringfügig zu betrachten ist, ist bereits eine Wertungsfrage. Das spricht dafür, das Ausmaß der Pflichtverletzung und die Schadenshöhe im Rahmen der Interessenabwägung zu berücksichtigen. Der Umfang des dem Arbeitgeber zugefügten Schadens kann vor allem im Hinblick auf die Stellung des Arbeitnehmers und die besonderen Verhältnisse des Betriebs unterschiedliches Gewicht für die Beurteilung der Zumutbarkeit des Pflichtverstoßes aufweisen. Objektive Kriterien für eine allein an der Schadenshöhe ausgerichtete Abgrenzung in ein für eine außerordentliche Kündigung grds. geeignetes und ein nicht geeignetes Verhalten lassen sich nicht aufstellen (*BAG* AP Nr. 28 zu § 626 BGB Verdacht strafbarer Handlung). Auch geringfügige (objektive) Pflichtverletzungen vermögen deshalb eine außerordentliche Kündigung „an sich" zu rechtfertigen (*BAG* NZA 2010, 1227). Der Pflichtenverstoß setzt nach der Rechtspre-

chung kein Verschulden voraus; die Frage des Verschuldens im Sinne einer subjektiven Vorwerfbarkeit ist erst bei der Interessenabwägung zu berücksichtigen (*BAG* NZA 1999, 863).

Die Rechtfertigung einer **„Tatkündigung"** hängt allein davon ab, ob im Kündigungszeitpunkt objektiv Tatsachen vorlagen, die zu der Annahme berechtigen, dem Kündigenden sei die Fortsetzung des Arbeitsverhältnisses – im Fall der außerordentlichen Kündigung bis zum Ablauf der Kündigungsfrist – unzumutbar gewesen. Vor diesem Hintergrund mag eine umfassende, der Kündigung vorausgehende Sachverhaltsaufklärung im eigenen Interesse des Arbeitgebers liegen. Unterlässt er sie, geht er aber „nur" das Risiko ein, die behauptete Pflichtverletzung im Prozess nicht beweisen zu können (*BAG* NZA 2016, 161). Anders als bei der **Verdachtskündigung** (s. unten Rn. 113) ist der Arbeitgeber vor Ausspruch einer „Tatkündigung" nicht verpflichtet, alle zumutbaren Anstrengungen zur Aufklärung des Sachverhalts – auch mit Blick auf den Arbeitnehmer möglicherweise entlastende Umstände – zu unternehmen. Im Kündigungsschutzprozess obliegt dem Arbeitgeber die volle Darlegungs- und Beweislast für das Vorliegen eines Kündigungsgrundes. Für Umstände, die das Verhalten des Arbeitnehmers rechtfertigen oder entschuldigen könnten, ist seine Darlegungslast allerdings abgestuft. Der Arbeitgeber darf sich zunächst darauf beschränken, den objektiven Tatbestand einer Arbeitspflichtverletzung vorzutragen. Er muss nicht jeden erdenklichen Rechtfertigungs- oder Entschuldigungsgrund vorbeugend ausschließen. Es ist vielmehr Sache des Arbeitnehmers, für das Eingreifen solcher Gründe – soweit sie sich nicht unmittelbar aufdrängen – zumindest greifbare Anhaltspunkte zu benennen. Schon auf der Tatbestandsebene des wichtigen Grundes kann den Arbeitnehmer darüber hinaus eine sekundäre Darlegungslast treffen. Dies kommt insbesondere dann in Betracht, wenn der Arbeitgeber als primär darlegungsbelastete Partei außerhalb des fraglichen Geschehensablaufs steht, während der Arbeitnehmer aufgrund seiner Sachnähe die wesentlichen Tatsachen kennt. In einer solchen Situation – kann der Arbeitnehmer gehalten sein, dem Arbeitgeber durch nähere Angaben weiteren Sachvortrag zu ermöglichen. Kommt er in einer solchen Prozesslage seiner sekundären Darlegungslast nicht nach, gilt das tatsächliche Vorbringen des Arbeitgebers – soweit es nicht völlig „aus der Luft gegriffen" ist – i.S.v. § 138 Abs. 3 ZPO als zugestanden (*BAG* NZA 2016, 161). **103**

b) Umfassende Interessenabwägung

Ob dem Arbeitgeber die Weiterbeschäftigung eines Arbeitnehmers trotz eines an sich vorliegenden wichtigen Kündigungsgrundes noch zugemutet werden kann, beurteilt sich nach den Umständen des Einzelfalls (ständige Rechtsprechung seit *BAG* AP Nr. 1 zu § 123 GewO). Dabei sind der *ultima ratio*-Grundsatz, das Prognoseprinzip und das Übermaßverbot zu beachten (Staudinger/*Preis* § 626 BGB Rn. 82 ff.). **104**

aa) Ultima ratio-Grundsatz

105 Die außerordentliche Kündigung muss das unausweichlich letzte Mittel – die *ultima ratio* – sein, um die eingetretene Vertragsstörung zu beseitigen. Nur wenn alle anderen nach den Umständen des Einzelfalles möglichen, geeigneten und angemessenen Mittel erschöpft sind, die in ihren Wirkungen „milder" sind als eine außerordentliche Kündigung, darf das Arbeitsverhältnis auch außerordentlich gekündigt werden (*BAG* NZA 2014, 243). Mildere Mittel sind im Allgemeinen die Abmahnung, die Versetzung, die einvernehmliche Änderung des Vertrages und die ordentliche Beendigungskündigung (*BAG* NZA 2016, 417 Rn. 46; NZA 2016, 1527 Rn. 30; NZA 2017, 1121 Rn. 27 f.).

bb) Prognoseprinzip

106 Die außerordentliche Kündigung will weder den Gekündigten für eine Verfehlung „bestrafen" (die Kündigung ist keine Sanktion: *BAG* AP Nr. 25 zu § 1 KSchG 1969 Verhaltensbedingte Kündigung) noch eine in der Vergangenheit eingetretene Leistungsstörung abwickeln, sondern dem Kündigenden die Möglichkeit geben, sich wegen der **künftigen Auswirkungen** gegenwärtiger oder vergangener Ereignisse sofort vom Arbeitsvertrag zu lösen (*BAG* NZA 2017, 1121 Rn. 27 f.). § 626 BGB stellt nicht schlechthin auf Unzumutbarkeit ab, sondern auf die Unzumutbarkeit der Fortsetzung des Arbeitsverhältnisses in der Zukunft (MK-BGB/*Henssler* § 626 Rn. 109). Das Prognoseprinzip hat in der Rechtsprechung ursprünglich vor allem bei krankheitsbedingten Kündigungen eine Rolle gespielt (*BAG* AP Nr. 3, 8 zu § 626 BGB Krankheit). Mittlerweile hat es sich auch bei der verhaltensbedingten Kündigung durchgesetzt (*BAG* NZA 1997, 487). Das Prognoseprinzip verlangt eine **zweistufige Prüfung**. Zunächst ist die in der Vergangenheit liegende schwerwiegende Störung des Arbeitsverhältnisses festzustellen. Danach ist zu prüfen, ob das Arbeitsverhältnis auch künftig erheblich beeinträchtigt sein wird (**„Negativprognose"**; vgl. *BAG* EzA § 1 KSchG Verhaltensbedingte Kündigung Nr. 41). Schwerwiegende Störungen in der Vergangenheit stützen in aller Regel die Prognose, dass das Arbeitsverhältnis auch in Zukunft nicht störungsfrei verlaufen wird. Der Betroffene kann die Vermutungswirkung jedoch ausräumen, etwa durch eine glaubwürdige Entschuldigung oder Wiedergutmachung eines Schadens (*Backmeister/Trittin* KSchR, § 626 BGB Rn. 14).

cc) Übermaßverbot

107 Die außerordentliche Kündigung muss schließlich auch das angemessene Mittel zur Beseitigung der Störung sein. Sie darf **keine übermäßige Reaktion** auf die Störung des Arbeitsverhältnisses darstellen. Bei der Abwägung aller in Betracht kommenden Umstände muss das Interesse an der sofortigen Beendigung des Arbeitsverhältnisses das Bestandsschutzinteresse überwiegen (Staudinger/*Preis* § 626 BGB Rn. 75). In die Abwägung sind alle, aber auch nur die Umstände einzubeziehen, die konkret mit dem Arbeitsverhältnis zusammenhängen (Erman/*Belling* § 626 BGB Rn. 38 ff.). Auf Seiten des Arbeitgebers sind grds. sämtliche betriebs-

und unternehmensbezogenen Interessen zu berücksichtigen, wie z.B. **Ordnung im Betrieb, Betriebsfrieden, Arbeitsablauf, wirtschaftliche Lage** (KR/*Fischermeier* § 626 BGB Rn. 240). Auf Seiten des Arbeitnehmers kommen in Betracht die **Dauer der Betriebszugehörigkeit** (*BAG* AP Nr. 81 zu § 626 BGB), das **Alter** (*BAG* EzA § 1 KSchG Krankheit Nr. 5), **Ansehensverlust, Art, Schwere und Folgen des Pflichtverstoßes und das Verschulden** (*BAG* NZA 2019, 445), insbesondere auch die Frage der **Entschuldbarkeit eines Rechtsirrtums** (*BAG* DB 1996, 2134; NZA 2016, 417; NZA 2017, 394; NZA 2018, 845). Unterhaltspflichten können nur im Ausnahmefall berücksichtigt werden (*BAG* AP Nr. 101 zu § 626 BGB). Stehen die Umstände fest, so sind die Einzelinteressen zu gewichten. Da die außerordentliche Kündigung nicht der Sanktion pflichtwidrigen Verhaltens in der Vergangenheit dient, kann bei der Interessenabwägung nicht auf die Grundsätze der Strafzumessung gem. § 46 StGB abgestellt werden (*BAG* NZA 2019, 445 Rn. 38). Zu Lasten des zu Kündigenden geht aber ein bewusstes, kollusives Zusammenwirken mit anderen Beschäftigten, wenn es zum Nachteil des Arbeitgebers geschieht (*BAG* AP BGB § 626 Nr. 274).

108 Bei gleich gelagerten Pflichtverletzungen mehrerer Arbeitnehmer darf der Arbeitgeber **einzelne Mitarbeiter nicht „herausgreifend" kündigen**, wenn es hierfür an sachlichen Gründen mangelt. I.Ü. ist der Gleichbehandlungsgrundsatz nach h.M. nicht unmittelbar heranzuziehen, weil er mit dem Gebot der umfassenden Abwägung der Umstände des Einzelfalles kollidiert (*BAG* EzA § 133b GewO Nr. 1). Dem Arbeitgeber ist es also erlaubt, einem Arbeitnehmer wegen einer Verfehlung zu kündigen und einem anderen wegen derselben Verfehlung nicht, wenn bei ihm aufgrund der Interessenabwägung der „an sich" gegebene Kündigungsgrund nicht für eine außerordentliche Kündigung ausreicht.

c) Kündigungserklärungsfrist

109 Die außerordentliche Kündigung muss innerhalb einer **Ausschlussfrist von zwei Wochen erklärt werden** (§ 626 Abs. 2 S. 1 BGB). Nach Ablauf dieser Frist gilt die **unwiderlegbare Vermutung,** dass die Fortsetzung des Arbeitsverhältnisses nicht unzumutbar ist (*BAG* EzA § 626 BGB n.F. Nr. 16). Das Arbeitsverhältnis kann dann mit gleicher Begründung **allenfalls noch ordentlich gekündigt werden** (*BAG* AP Nr. 4 zu Art. 140 GG). Die Ausschlussfrist dient der Rechtsklarheit und dem Rechtsfrieden; sie konkretisiert das Institut der Verwirkung. Die Frist schützt den Arbeitnehmer, weil er nach ihrem Ablauf nicht mehr mit einer außerordentlichen Kündigung zu rechnen braucht (*BAG* AP Nr. 1, 3 zu § 626 BGB Ausschlussfrist). Sie kann vertraglich weder ausgeschlossen noch verkürzt noch verlängert werden (*BAG* AP Nr. 6, 13 zu § 626 BGB Ausschlussfrist).

110 Die **Frist beginnt** mit dem Zeitpunkt, in dem der Kündigungsberechtigte von den für die Kündigung maßgebenden Tatsachen Kenntnis erlangt (§ 626 Abs. 2 S. 2 BGB). **Kündigungsberechtigter** ist, wer befugt ist, im konkreten Fall die Kündigung auszusprechen (*BAG* AP Nr. 1, 3, 20 zu § 626 BGB Ausschlussfrist). Das sind die Vertragsparteien selbst sowie ihre gesetzlichen und bevollmächtigten

Vertreter. Bei Gesamtvertretung können zwar nur alle Vertreter gemeinsam kündigen; die Ausschlussfrist läuft jedoch schon dann, wenn auch nur einer von ihnen den Kündigungsgrund kennt (*BAG* EzA § 626 BGB n.F. Nr. 92). Die **Kenntnis eines Dritten** muss sich der Kündigungsberechtigte entsprechend **§ 166 BGB** zurechnen lassen, wenn dieser eine ähnlich selbständige Stellung innehat wie ein gesetzlicher oder bevollmächtigter Vertreter und seine Position ihn zur Feststellung der für eine außerordentliche Kündigung entscheidenden Umstände verpflichtet. Dritte in diesem Sinne sind vor allem Betriebs- und Abteilungsleiter. Ihre Stellung lässt erwarten, dass sie den Kündigungsberechtigten informieren (*BAG* AP Nr. 3, 11 zu § 626 BGB Ausschlussfrist). Mängel im internen Informationsfluss gehen zu Lasten des Arbeitgebers (*BAG* AP Nr. 11 zu § 626 BGB Ausschlussfrist). Kenntnis bedeutet zuverlässiges und möglichst umfassendes Wissen über die Tatsachen, die für die Kündigungsentscheidung benötigt werden; dazu gehören sowohl die be- als auch die entlastenden Umstände (*BAG* DB 1989, 282). Selbst grob fahrlässige Unkenntnis genügt nicht (*BAG* NZA 1991, 141). Kündigungsgründe, die bei Ausspruch einer Kündigung vorliegen, dem Kündigenden jedoch nicht bekannt sind, können nach Ablauf der Ausschlussfrist noch nachgeschoben werden (*BAG* AP Nr. 5 zu § 626 BGB Nachschieben von Kündigungsgründen). § 626 Abs. 2 BGB bildet weder in direkter noch in entsprechender Anwendung eine Schranke für das Nachschieben von Kündigungsgründen, die bei Zugang der betreffenden außerordentlichen Kündigung bereits objektiv vorlagen, aber dem Kündigungsberechtigten seinerzeit noch nicht bekannt waren. Es kommt insbesondere nicht darauf an, ob der Grund, auf den die Kündigung zunächst gestützt wurde, bei ihrem Zugang noch nicht verfristet war. Die Kündigung kann grundsätzlich sogar „blanko" erklärt worden sein (*BAG* NZA 2021, 710).

111 Der Lauf der Frist ist gehemmt, solange der Kündigungsberechtigte die zur Aufklärung des Sachverhalts nach pflichtgemäßem Ermessen notwendig erscheinenden Maßnahmen mit der gebotenen Eile durchführt (*BAG* AP Nr. 27, 32 zu § 626 BGB Ausschlussfrist). Allerdings trifft den Arbeitgeber keine Obliegenheit, den Arbeitnehmer belastende und den Sachverhalt gegebenenfalls erst in den Bereich des wichtigen Grundes hebende Tatsachen zu ermitteln. Das widerspräche dem Grundsatz, dass eine – sogar grob – fahrlässige Unkenntnis der maßgeblichen Tatsachen nicht genügt, um die Kündigungserklärungsfrist auszulösen und läge auch nicht im Interesse des Arbeitnehmers (*BAG* NZA 2020, 1405). Der Arbeitgeber kann den Arbeitnehmer vor der Kündigung anhören, das muss allerdings innerhalb einer kurz zu bemessenden Frist geschehen (im Regelfall binnen einer Woche nach Bekanntwerden von Anhaltspunkten für den Kündigungssachverhalt, *BAG* AP Nr. 3, 6, 27 zu § 626 BGB Ausschlussfrist; *BAG* NZA 2019, 1415). Die Frist kann sich verlängern, wenn ein Arbeitnehmer, der dem Arbeitgeber den maßgeblichen Sachverhalt mitgeteilt hat, darum bittet, zunächst keine Anhörung des Kündigungsgegners durchzuführen und der Arbeitgeber dieser Bitte nachkommt, um seiner Rücksichtnahmepflicht aus § 241 II BGB gegenüber dem Informanten zu entsprechen. Will sich der Arbeitgeber die Möglichkeit einer außerordentlichen Kündigung erhalten, muss er den Arbeitnehmer auffordern, innerhalb einer

angemessen kurzen Frist zu erklären, ob er auf die Vertraulichkeit der Mitteilung verzichtet (*BAG* NZA 2019, 1415). Der Arbeitgeber kann auch den Ausgang des erstinstanzlichen Strafverfahrens oder den Eintritt der Rechtskraft abwarten (*BAG* NZA 2000, 1282, 1288). Entschließt er sich zum Abwarten, so kann er später nicht spontan und unvermittelt kündigen, wenn er zuvor trotz hinreichenden Anfangsverdachts von eigenen Ermittlungen abgesehen hat (*BAG* AP Nr. 31 zu § 626 BGB Ausschlussfrist). Weder der Verdacht strafbarer Handlungen noch eine begangene Straftat stellen Dauerzustände dar, die es dem Arbeitgeber ermöglichen, bis zur strafrechtlichen Verurteilung des Arbeitnehmers zu irgendeinem beliebigen Zeitpunkt eine fristlose Kündigung auszusprechen (*BAG* AP Nr. 31 zu § 626 BGB Ausschlussfrist).

d) Anhörung der Belegschaftsvertretungen

112 **Vor der Kündigung** hat der Arbeitgeber den **Betriebsrat anzuhören** (§ 102 Abs. 1 S. 1 BetrVG). Soll ein leitender Angestellter (§ 5 Abs. 3 BetrVG) gekündigt werden, ist der Sprecherausschuss anzuhören (§ 31 Abs. 2 S. 1 SprAuG). Entsprechendes gilt für einen schwerbehinderten Menschen, vor dessen Kündigung die Schwerbehindertenvertretung anzuhören ist (§ 178 Abs. 2 SGB IX). Dabei sind die **Personalien des zu kündigenden Arbeitnehmers, die Beschäftigungsdauer, die Kündigungsart sowie die Kündigungsgründe mitzuteilen.** Das Anhörungsverfahren hat über die reine Unterrichtung hinaus den Sinn, dem Betriebsrat Gelegenheit zu geben, seine Überlegungen zu der Kündigungsabsicht zur Kenntnis zu bringen. Die Anhörung soll in geeigneten Fällen dazu beitragen, dass es gar nicht zum Ausspruch einer Kündigung kommt (*BAG* AP Nr. 29 zu § 102 BetrVG 1972). Daraus folgt für den Arbeitgeber die Verpflichtung, die Gründe für seine Kündigungsabsicht so mitzuteilen, dass der Betriebsrat eine nähere Umschreibung des für die Kündigung maßgeblichen Sachverhalts erhält. Der Betriebsrat muss in die Lage versetzt werden, ohne eigene Nachforschungen selbst die Stichhaltigkeit der Kündigungsgründe zu prüfen und sich ein Bild zu machen. Es genügt nicht, den Kündigungssachverhalt nur pauschal, schlagwort- oder stichwortartig zu umschreiben oder lediglich ein Werturteil abzugeben, ohne die für seine Bewertung maßgeblichen Tatsachen mitzuteilen (*BAG* AP Nr. 37 zu § 626 BGB Verdacht strafbarer Handlung). Die Anforderungen an die Mitteilungspflicht sind weniger streng als die Darlegungslast im Kündigungsschutzprozess. Im Anhörungsverfahren gilt der **Grundsatz der subjektiven Determinierung.** Danach wird der Betriebsrat ordnungsgemäß angehört, wenn der Arbeitgeber die aus seiner Sicht tragenden Gründe darlegt (ständige Rechtsprechung, vgl. nur *BAG* AP Nr. 37 zu § 626 BGB Verdacht strafbarer Handlung). Bei einer Verdachtskündigung sind auch die Sozialdaten des Arbeitnehmers mitzuteilen, obwohl es sich um Umstände handelt, die nicht das beanstandete Verhalten des Arbeitnehmers selbst betreffen. Nach Sinn und Zweck der Anhörung dürfen persönliche Umstände des Arbeitnehmers, die sich im Rahmen der Interessenabwägung entscheidend zu seinen Gunsten auswirken können, nicht vorenthalten werden (*BAG* EzA BGB § 626 Unkündbarkeit Nr. 7). Das gilt nur dann nicht, wenn es dem Arbeitgeber

wegen der Schwere der Kündigungsvorwürfe auf die genauen Daten ersichtlich nicht ankommt und der Betriebsrat die ungefähren Daten ohnehin kennt und daher die Kündigungsabsicht des Arbeitgebers ausreichend beurteilen kann (*BAG* EzA BGB § 626 Unkündbarkeit Nr. 7). Im Zweifel sollte der Arbeitgeber den Betriebsrat ausführlicher informieren. Eine Kündigung ist wegen § 102 Abs. 1 S. 3 BetrVG nicht erst unwirksam, wenn die Unterrichtung ganz unterblieben ist, sondern schon dann, wenn der Unterrichtungspflicht nicht richtig, insbesondere nicht ausführlich genug nachgekommen wurde (*BAG* EzA BGB § 626 Unkündbarkeit Nr. 7).

4. Verdachtskündigung

a) Abgrenzung zur Tatkündigung

113 Ausnahmsweise kann schon der **bloße Verdacht** einer **strafbaren Handlung oder einer anderen schwerwiegenden Vertragsverletzung** eine außerordentliche Kündigung rechtfertigen, wenn dem Arbeitsverhältnis dadurch die **Vertrauensgrundlage entzogen** ist (ständige Rspr., vgl. *BAG* NZA 2008, 636; NZA 2018, 1405). Da eine schuldhafte Verfehlung nicht wirklich vorliegen muss, handelt es sich bei einer Verdachtskündigung nicht um eine verhaltens-, sondern um eine **personenbedingte Kündigung.** Steht nach der Überzeugung des Arbeitgebers die Verfehlung fest, so kann er eine „Tatkündigung" aussprechen (*BAG* AP Nr. 23, 27 zu § 626 BGB Verdacht strafbarer Handlung). Dazu ist er aber selbst bei „erdrückenden" Verdachtsmomenten nicht gehalten, weil stets ein Beweisrisiko verbleibt (*BAG* NZA 2005, 1056, 1058 m.w.N.). Umgekehrt hängt die Wirksamkeit der Verdachtskündigung nicht von der strafgerichtlichen Würdigung ab, sondern von der Beeinträchtigung des für das Arbeitsverhältnis erforderlichen Vertrauens (*BAG* AP Nr. 27 zu § 626 BGB Verdacht strafbarer Handlung). Der Ausgang des Strafverfahrens ist weder für die Zivil- noch für die Arbeitsgerichte bindend (§ 14 EGZPO). Steht nach Überzeugung des Arbeitsgerichts die Pflichtverletzung fest, so ist es nicht gehindert, die nachgewiesene Pflichtverletzung als Kündigungsgrund anzuerkennen, selbst wenn der Arbeitgeber sich nicht darauf beruft (*BAG* NZA 2014, 243). Maßgeblicher Zeitpunkt für die Beurteilung der Rechtmäßigkeit ist der Zugang der Kündigung. Be- und Entlastungsvorbringen will das BAG bis zum Schluss der letzten mündlichen Verhandlung in der Tatsacheninstanz berücksichtigen (*BAG* AP Nr. 24 zu § 626 BGB Verdacht strafbarer Handlung). Damit rückt die Verdachtskündigung sehr in die Nähe einer Tatkündigung. Die wohl h.L. lehnt deshalb diese Rechtsprechung ab (Ascheid/Preis/Schmidt/*Dörner* § 626 BGB Rn. 355 ff.; Kittner/Däubler/Zwanziger/*Däubler* KSchR-Kündigungsschutzrecht, 9. Aufl. 2014, § 626 BGB Rn. 152). Erweist sich die Unschuld des Arbeitnehmers erst nach Abschluss eines Kündigungsschutzprozesses – oder, wenn man der h.L. folgt, nach Zugang der Kündigung –, kann dem Arbeitnehmer ein **Wiedereinstellungsanspruch** zustehen (ständige Rechtsprechung, vgl. *BAG* AP Nr. 27 zu § 626 BGB Verdacht strafbarer Handlung). Stützt der Arbeitgeber die Kündigung erst nach ihrem Ausspruch auf den Verdacht einer strafbaren Hand-

lung, **schiebt er damit einen andersartigen Kündigungsgrund nach.** Das ist prozessrechtlich möglich, unterliegt aber kollektivrechtlichen Beschränkungen. Besteht im Betrieb ein Betriebsrat, der nach § 102 Abs. 1 BetrVG vor der Kündigung zu hören ist, kann der Verdachtsgrund selbst bei unverändert gebliebenem Sachverhalt nicht nachgeschoben werden, falls dem Betriebsrat dieser Kündigungsgrund nicht im Rahmen des Anhörungsverfahrens mitgeteilt worden ist (*BAG* AP Nr. 22, 23 zu § 102 BetrVG 1972).

b) Voraussetzungen

aa) Dringender Tatverdacht

Um die Kündigung eines Unschuldigen nach Möglichkeit zu verhindern, stellt die h.M. an die Verdachtskündigung zu Recht hohe Anforderungen. Der Verdacht muss sich auf **objektive Tatsachen** gründen; bloße Vermutungen genügen nicht (*BAG* AP Nr. 25, 27 zu § 626 BGB Verdacht strafbarer Handlung; NZA 2018, 1405). Die Pflichtverletzung, derer der Arbeitnehmer verdächtigt wird, muss so erhebliche Auswirkungen auf das Arbeitsverhältnis haben, dass sie – ihre Erweislichkeit unterstellt – eine außerordentliche Kündigung rechtfertigen würde (*BAG* NZA 2014, 243; NZA 2015, 429; NZA 2018, 1405). Der Verdacht eines Verstoßes gegen eine Haupt- oder Nebenpflicht und der damit verbundene Vertrauensverlust muss das zur Fortsetzung des Arbeitsverhältnisses notwendige **Vertrauen des Arbeitgebers in die Redlichkeit des Arbeitnehmers zerstört** und damit zu einer unerträglichen Belastung des Arbeitsverhältnisses geführt haben (*BAG* NZA 2014, 301: „Vertrauenskündigung"). Der Tatverdacht ist nur dann dringend, wenn eine **große Wahrscheinlichkeit für die Täterschaft spricht** (*BAG* NZA 2008, 636). Mathematische Wahrscheinlichkeitsgrade spielen keine Rolle, selbst wenn die Wahrscheinlichkeit für eine Tatbeteiligung kleiner als die gegen eine solche ist (*BAG* NZA 2008, 219). Dass die dem Arbeitnehmer zur Last gelegte Handlung nicht mit letzter Sicherheit erwiesen ist, schließt eine Verdachtskündigung nicht aus, weil es bei ihr nicht darauf ankommt, ob die Tat erwiesen ist, sondern ob die vom Arbeitgeber vorgetragenen Tatsachen den Verdacht rechtfertigen (Schlüssigkeit, Rechtsfrage) und, falls ja, ob sie tatsächlich zutreffen (Tatsachenfrage, vgl. *BAG* NZA 2005, 1056). Der Vortrag, die Strafverfolgungsbehörden hätten einen dringenden Tatverdacht bejaht, genügt nicht; der Arbeitgeber muss selbst Indizien darlegen (*BAG* NZA 2013, 371). **114**

bb) Vorherige Anhörung

Vor Ausspruch einer Verdachtskündigung muss der Arbeitgeber alles ihm Zumutbare zur Aufklärung des Sachverhalts unternehmen (*BAG* AP Nr. 25, 27 zu § 626 BGB Verdacht strafbarer Handlung; NZA 2018, 1405). Insbesondere hat er den verdächtigen Arbeitnehmer anzuhören. Die **Anhörung ist Wirksamkeitsvoraussetzung** für die Verdachtskündigung, und zwar auch dann, wenn sie objektiv zu keinem anderen Ergebnis geführt hätte oder die Möglichkeit ausgeschlossen ist, dass sie für den Arbeitgeber neue, den Arbeitnehmer entlastende Momente er- **115**

geben hätte (*Eylert* NZA-RR 2014, 393). Die Anhörung hat im Zuge der gebotenen Aufklärung des Sachverhalts zu erfolgen, jedoch nicht zwingend erst nach Abschluss der Ermittlungen (*BAG* AP Nr. 25 zu § 626 BGB Verdacht strafbarer Handlung). Ihr Umfang richtet sich nach den Umständen des Einzelfalles (*BAG* NZA 2013, 137). Die Anforderungen sind weniger streng als bei einer Anhörung des Betriebsrats gem. § 102 Abs. 1 BetrVG (*BAG* NZA 2018, 1405), weil beide Anhörungen unterschiedlichen Zwecken dienen und schon im Ansatz nicht vergleichbar sind. Allerdings genügt es nicht, den Arbeitnehmer lediglich mit einer unsubstantiierten Wertung zu konfrontieren. **Notwendig ist der Vorwurf eines konkretisierten Sachverhalts,** da der Beschuldigte sonst keine Möglichkeit hat, sich zum Verdachtsvorwurf und den ihn tragenden Verdachtsmomenten substantiiert zu äußern. Dabei darf der Arbeitgeber Erkenntnisse, die er im Anhörungszeitpunkt bereits besitzt, nicht zurückhalten, sondern muss alle relevanten Umstände angeben, aus denen er den Verdacht ableitet (*Busch* MDR 1995, 217, 218; *Schönfeld* NZA 1999, 299, 300). Andernfalls würden die Einlassungs- und Verteidigungsmöglichkeiten des Arbeitnehmers unzulässig beschränkt (*BAG* AP Nr. 37 zu § 626 BGB Verdacht strafbarer Handlung). Der Arbeitnehmer muss erkennen können, zur Aufklärung welchen Sachverhalts ihm Gelegenheit gegeben werden soll. Er muss die Möglichkeit haben, bestimmte, zeitlich und räumlich eingegrenzte Tatsachen gegebenenfalls zu bestreiten oder den Verdacht entkräftende Tatsachen aufzuzeigen und so zur Aufhellung der für den Arbeitgeber im Dunkeln liegenden Geschehnisse beizutragen (*BAG* NZA 2018, 1405).

116 **Verletzt** der Arbeitgeber **schuldhaft** die sich aus der Aufklärungspflicht ergebende **Anhörungspflicht,** so kann er sich im Prozess nicht auf den Verdacht einer strafbaren Handlung oder einer Pflichtverletzung des Arbeitnehmers berufen. Eine hierauf gestützte **Kündigung ist unwirksam** (*BAG* AP zu § 626 Nr. 25 BGB Verdacht strafbarer Handlung; BAG NZA 2018, 1405). An einer schuldhaften **Verletzung der Anhörungspflicht fehlt es,** wenn der **Arbeitnehmer von vornherein nicht bereit war,** sich auf die gegen ihn erhobenen Vorwürfe einzulassen und nach seinen Kräften an der Aufklärung **mitzuwirken** (*BAG* NZA 2014, 1015). Bestreitet der Arbeitnehmer den Tatvorwurf pauschal, obwohl die ihm bislang bekannten und vorgehaltenen Tatsachen eine konkrete Einlassung ermöglichen würden, lässt dies regelmäßig den Schluss zu, der Arbeitnehmer sei an einer Mitwirkung an der Aufklärung des Verdachts nicht interessiert (*BAG* AP Nr. 25 zu § 626 BGB Verdacht strafbarer Handlung). Erklärt der Arbeitnehmer sogleich, er werde sich zum Vorwurf nicht äußern und nennt er auch für seine Verweigerung keine relevanten Gründe, muss ihn der Arbeitgeber nicht näher über die Verdachtsmomente informieren (*BAG* AP Nr. 19, 37 zu § 626 BGB Verdacht strafbarer Handlung). Ist der Arbeitnehmer krankheitsbedingt längerfristig auch an einer schriftlichen Stellungnahme auf ihm übermittelte Fragen verhindert, muss der Arbeitgeber nicht notwendig die Zeit abwarten, zu der sich der Arbeitnehmer wieder äußern kann (*BAG* NZA 2014, 1015). Lässt sich der Arbeitnehmer zu den vorgehaltenen Verdachtsmomenten konkret ein, so dass der Verdacht zerstreut wird oder aus der Sicht des Arbeitgebers für eine Kündigung nicht mehr ausreicht, und

führen erst die daraufhin durchgeführten weiteren Ermittlungen aus der Sicht des Arbeitgebers zu einer Widerlegung des Entlastungsvorbringens des Arbeitnehmers, so ist dieser vor Ausspruch der Verdachtskündigung erneut anzuhören (*BAG* AP zu § 626 Nr. 25 BGB Verdacht strafbarer Handlung). Hat sich der Arbeitnehmer erst im Prozess zur Sache geäußert, müssen die Gerichte seinem Vortrag, mit dem er sich von dem ihm gegenüber vorgebrachten Verdacht reinigen will, durch eine vollständige Aufklärung des Sachverhalts nachgehen (*BAG* AP Nr. 32 zu § 626 BGB Verdacht strafbarer Handlung).

cc) Ausschlussfrist

117 Der **Beginn** der Ausschlussfrist des § 626 Abs. 2 BGB ist **gehemmt**, solange der Kündigungsberechtigte die zur **Aufklärung des Kündigungssachverhalts** nach pflichtgemäßem Ermessen notwendig erscheinenden **Maßnahmen mit der gebotenen Eile durchführt.** Ob diese Voraussetzungen erfüllt sind, hängt von den Umständen des Einzelfalles ab (zum Fristbeginn bei der Aufklärung komplexer Sachverhalt der Wirtschaftskriminalität s. *Dzida* NZA 2014, 809; *Göpfert/Drägert,* CCZ 2011, 25). Eine Regelfrist gilt, anders als für die Anhörung des Kündigungsgegners, für die Durchführung der übrigen Ermittlungen nicht (*BAG* AP Nr. 27 zu § 626 BGB Ausschlussfrist). Ist eine vom Arbeitgeber ausgesprochene Verdachtskündigung rechtskräftig für unwirksam erklärt worden, weil die den Verdacht begründenden Umstände dem Arbeitgeber beim Zugang der Kündigung länger als zwei Wochen bekannt gewesen und daher nach § 626 Abs. 2 BGB verfristet sind, so hindert die Rechtskraft dieses Urteils den Arbeitgeber nicht, nach dem Abschluss des gegen den Arbeitnehmer eingeleiteten Strafverfahrens eine nunmehr auf die Tatbegehung gestützte außerordentliche Kündigung auszusprechen, selbst wenn das Strafverfahren nicht zu einer Verurteilung des Arbeitnehmers geführt hat, sondern gegen Zahlung eines Geldbetrages nach § 153a Abs. 2 StPO eingestellt worden ist. Die zweiwöchige Ausschlussfrist des § 626 Abs. 2 BGB für eine solche auf die Tatbegehung gestützte außerordentliche Kündigung beginnt jedenfalls dann nicht vor dem Abschluss des Strafverfahrens gegen den Arbeitnehmer, wenn der Arbeitgeber vorher zwar Verdachtsumstände kannte, diese Verdachtsumstände aber noch keine jeden vernünftigen Zweifel ausschließende sichere Kenntnis der Tatbegehung begründeten (*BAG* AP Nr. 19 zu § 626 BGB Verdacht strafbarer Handlung).

c) Ordentliche Verdachtskündigung

118 Die Verdachtskündigung kann auch als ordentliche Kündigung erklärt werden. Sie ist als personenbedingte Kündigung nur dann durch den bloßen Verdacht pflichtwidrigen Verhaltens i.S.v. § 1 Abs. 2 KSchG aus Gründen in der Person des Arbeitnehmers „bedingt", wenn das Verhalten, dessen der Arbeitnehmer verdächtig ist, – wäre es erwiesen – sogar eine sofortige Beendigung des Arbeitsverhältnisses gerechtfertigt hätte (*BAG* NZA 2019, 893). Anders als für eine außerordentliche Verdachtskündigung besteht keine starre Frist, innerhalb derer der Arbeitgeber das

Recht zur ordentlichen Verdachtskündigung ausüben müsste. Allerdings kann ein längeres Zuwarten zu der Annahme berechtigen, die Kündigung sei nicht i.S.v. § 1 Abs. 2 KSchG durch den Verlust des vertragsnotwendigen Vertrauens „bedingt". Daneben kommt eine Verwirkung des Kündigungsrechts nach § 242 BGB in Betracht (*BAG* NZA 2019, 893).

5. Aufhebungsvertrag

119 Bei massiven Compliance-Verstößen werden die Parteien das Arbeitsverhältnis häufig einvernehmlich auflösen. Der Aufhebungsvertrag ist schriftlich zu schließen (§ 623 BGB), und zwar auch dann, wenn in dem Vertrag die Worte „Auflösung oder Aufhebung" nicht verwendet werden (ErfK-ArbR/*Müller-Glöge* § 623 BGB Rn. 4). Die Auflösung kann mit sofortiger Wirkung, aber auch für einen Termin in der Zukunft oder – wenn das Arbeitsverhältnis bereits außer Vollzug gesetzt war (*BAG* AP Nr. 77 zu § 7 BUrlG Abgeltung) – in der Vergangenheit vereinbart werden.

120 Wird der Arbeitnehmer zum Vertragsschluss gedrängt, etwa unter Ankündigung einer sonst drohenden Strafanzeige, kommt eine **Anfechtung nach § 123 BGB** in Betracht. Die Drohung mit einer außerordentlichen Kündigung ist unzulässig, wenn ein verständiger Arbeitgeber eine solche Kündigung nicht ernsthaft in Erwägung ziehen durfte (*BAG* NZA 1996, 1030). Die Widerrechtlichkeit der Kündigungsandrohung kann sich regelmäßig nur aus der Inadäquanz von Mittel und Zweck ergeben. Hat der Drohende an der Erreichung des verfolgten Zwecks – die Eigenkündigung oder den Abschluss eines Aufhebungsvertrags – kein berechtigtes Interesse oder ist die Drohung nach Treu und Glauben nicht mehr als angemessenes Mittel zur Erreichung des Zwecks anzusehen, so ist die Drohung widerrechtlich (*BAG* AP BGB § 123 Nr. 42). Dabei ist es nicht erforderlich, dass die angedrohte Kündigung, wenn sie ausgesprochen worden wäre, sich in einem Kündigungsschutzprozess als rechtsbeständig erwiesen hätte, weil von einem verständigen Arbeitgeber nicht generell verlangt werden kann, dass er bei seiner Abwägung die Beurteilung des Tatsachengerichts „trifft". Die Drohung ist jedoch dann unzulässig, wenn eine außerordentliche Kündigung bei der gebotenen Abwägung aller Umstände des Einzelfalls höchstwahrscheinlich unwirksam wäre (*BAG* AP ZPO § 286 Nr. 33).

121 Ist ein Anfechtungsgrund gegeben, kann der Aufhebungsvertrag **innerhalb** der **Jahresfrist** des § 124 Abs. 1 BGB **angefochten werden.** Die 2-Wochen-Frist des § 626 Abs. 2 BGB findet keine entspr. Anwendung (*BAG* AP BGB § 123 Nr. 25). Eine Verwirkung des Anfechtungsrechts ist im Hinblick auf den eigenen Verstoß des Arbeitgebers nur unter ganz außergewöhnlichen Umständen anzunehmen. Bei der Prüfung des erforderlichen Zeitmoments ist zu berücksichtigen, dass der Gesetzgeber dem Bedrohten schon für die Anfechtung in § 124 BGB eine Überlegungsfrist von einem Jahr einräumt. Der Drohende muss sich deshalb nach Treu und Glauben regelmäßig damit abfinden, dass der Bedrohte die Nichtigkeit des

Rechtsgeschäfts auch noch einige Monate nach der Anfechtung und Klageandrohung klageweise geltend macht (*BAG* AP Nr. 45 zu § 242 BGB Verwirkung).

122 Ein Aufhebungsvertrag ist **unwirksam**, wenn er unter **Missachtung des Gebots fairen Verhandelns zustande gekommen ist** (*BAG* NZA 2019, 688). Dieses Gebot ist eine bei den Vertragsverhandlungen zu beachtende Nebenpflicht. Sie wird verletzt, wenn eine Seite eine **psychische Drucksituation** schafft oder ausnutzt, die eine freie und überlegte Entscheidung des Vertragspartners über den Abschluss eines Aufhebungsvertrags erheblich erschwert oder unmöglich macht. Das ist noch nicht der Fall, wenn der Arbeitgeber dem Arbeitnehmer weder eine Bedenkzeit noch ein Rücktritts- oder Widerrufsrecht einräumt (vgl. *BAG* NZA 1996, 811). Auch eine Ankündigung des Unterbreitens einer Aufhebungsvereinbarung ist nicht erforderlich (vgl. *BAG* NZA 1994, 209). **Schädlich** ist jedoch die **Schaffung besonders unangenehmer Rahmenbedingungen, die erheblich ablenken oder sogar den Fluchtinstinkt wecken** (vgl. *LAG Thüringen* NZA-RR 1999, 399). Entsprechendes gilt für die die Ausbeutung einer objektiv erkennbaren körperlichen oder psychischen Schwäche oder unzureichender Sprachkenntnisse. Auch die plötzliche Überrumpelung kann die Entscheidungsfreiheit des Vertragspartners beeinträchtigen. Letztlich ist die konkrete Situation im jeweiligen Einzelfall am Maßstab des § 241 Abs. 2 BGB zu bewerten und von einer bloßen Vertragsreue abzugrenzen (*BAG* NZA 2019, 688 Rn. 34).

6. Freistellen von der Arbeit (Suspendierung)

123 Der Arbeitgeber ist grds. **nicht berechtigt,** den **Arbeitnehmer einseitig von der Arbeit freizustellen** und ihm die weitere Tätigkeit im Betrieb zu verbieten („Suspendierung"). Vielmehr hat der Arbeitnehmer das Recht, vom Arbeitgeber nicht nur bezahlt, sondern auch tatsächlich beschäftigt zu werden (*BAG* AP BGB § 611 Beschäftigungspflicht Nr. 14). Dieser Beschäftigungsanspruch steht allen Arbeitnehmern zu, nicht nur denen, die ein besonderes Interesse an der tatsächlichen Verrichtung ihrer Arbeit haben, wie etwa Journalisten, Schauspieler, Piloten oder Wissenschaftler. Die tatsächliche Beschäftigung soll es ermöglichen, Fähigkeiten und Fertigkeiten zu erhalten und zu erweitern und die in der Arbeit liegende Chance zur Entfaltung der Persönlichkeit zu nutzen (*BAG* AP BGB § 611 Beschäftigungspflicht Nr. 14). Der **Beschäftigungsanspruch entfällt,** wenn das Interesse des Arbeitgebers an einer Nichtbeschäftigung überwiegt. Davon ist auszugehen, wenn ein **wichtiger Grund** vorliegt, der den Arbeitgeber zu einer außerordentlichen Kündigung des Arbeitsverhältnisses nach § 626 BGB berechtigt (*BAG* DB 1976, 2308; 1972, 1878). Die Suspendierung kann dann entweder als – vorübergehendes – milderes Mittel zur Vermeidung einer sofortigen außerordentlichen Kündigung in Betracht (ErfK-ArbR/*Preis* BGB § 611a Rn. 567) oder wenn eine ordentliche Kündigung gesetzlich (z.B. § 15 Abs. 1 KSchG, § 17 MuSchG) oder (kollektiv-)vertraglich ausgeschlossen ist (MK-BGB/*Müller-Glöge* § 611 Rn. 976). Die tatsächliche Beschäftigung muss für den Arbeitgeber unzumutbar sein. Das ist sie, wenn die Weiterarbeit Schäden hervorrufen würde – z.B. beim Verrat von

Betriebs- und Geschäftsgeheimnissen (Ascheid/Preis/Schmidt/*Preis* Grundlagen K. Rn. 76). Bei einem Arbeitnehmer in exponierter Stellung, der zur Konkurrenz abwandern will und Einblick in wichtige Geschäftsgeheimnisse hat, kann eine Suspendierung während der gesamten, auch längeren Kündigungsfrist gerechtfertigt sein (*LAG Hamm* LAGE BGB § 611 Beschäftigungspflicht Nr. 36), bei tätlichen Auseinandersetzungen zwischen Arbeitskollegen (Zöllner/Loritz/*Hergenröder* ArbR § 17 II 1) und in Fällen sexueller Belästigung, sodann bei Verdacht einer strafbaren Handlung bzw. einer schwerwiegenden Pflichtverletzung sowie bei Bestehen eines Beschäftigungsverbots (vgl. *BAG* NZA 2009, 611).

124 Die Suspendierung unterliegt keiner Mitbestimmung nach § 95 Abs. 3 i.V.m. § 99 BetrVG (*BAG* NZA 2000, 1355). Die einseitige Freistellung beseitigt die Vergütungspflicht selbst dann nicht, wenn sie zulässig ist (*BAG* BB 1964, 1045). In ihr liegt regelmäßig die Ablehnung der Annahme weiterer Arbeitsleistungen des Arbeitnehmers, die zum Annahmeverzug des Arbeitgebers führt (ErfK-ArbR/*Preis* BGB § 611a Rn. 571; MK-BGB/*Müller-Glöge* BGB § 611 Rn. 979). Nur in extremen Ausnahmefällen, etwa bei besonders schwerwiegendem Fehlverhalten des Arbeitnehmers, kann auch die Vergütungspflicht entfallen (*LAG Bremen* NZA-RR 2000, 632), vor allem dann, wenn eine sofortige Beendigung des Arbeitsverhältnisses durch fristlose Kündigung – wie z.B. bei Betriebsratsmitgliedern – nicht möglich ist (*LAG Hessen* NZA-RR 2000, 633). Der Beschäftigungsanspruch ist dispositiv. Auf ihn kann der Arbeitnehmer im Falle einer konkreten Freistellung verzichten. Ob ein solcher Verzicht auch im Voraus in einem vorformulierten Arbeitsvertrag möglich ist, ist streitig (bejahend *LAG Hamburg* LAGE BGB § 611 Beschäftigungspflicht Nr. 37; *Bauer* NZA 2007, 409; a.A. *LAG Hessen* NZA-RR 2011, 419; *ArbG Berlin* BeckRS 2009, 68151; Wolf/Lindacher/Pfeiffer/*Stoffels* BGB Anh. zu § 310 Rn. 152). Zutreffend ist die Annahme, dass es sich bei der Beschäftigungspflicht um eine aus den Grundrechten abgeleitete Kardinalpflicht handelt, die wegen § 307 Abs. 1 BGB jedenfalls in einem ungekündigten Arbeitsverhältnis nicht abbedungen werden kann (*LAG Hessen* NZA-RR 2011, 419). Denkbar sind allenfalls Vertragsklauseln, die für eine Freistellung ausdrücklich ein gewichtiges Arbeitgeberinteresse voraussetzen und dieses ggf. präzisieren. Die konkrete Ausübung des Freistellungsrechts unterliegt einer gerichtlichen Billigkeitskontrolle nach § 315 BGB (ErfK-ArbR/*Preis* BGB § 611a Rn. 568). In einem gekündigten Arbeitsverhältnis wird eine Freistellung allgemein für zulässig erachtet, weil der Arbeitgeber im Regelfall ein berechtigtes Interesse daran hat (vgl. z.B. *LAG München* LAGE BGB 2002 § 307 Nr. 2; a.A. ErfK-ArbR/*Preis* BGB § 611a Rn. 570 m.w.N.).

7. Betriebsbuße

125 Betriebsbußen können verhängt werden, wenn sich Arbeitnehmer gemeinschaftswidrig verhalten, d.h., wenn sie gegen verbindliche Verhaltensregeln zur Sicherung des ungestörten Arbeitsablaufs oder des reibungslosen Zusammenlebens und Zusammenwirkens im Betrieb verstoßen (*BAG* AP BetrVG 1972 § 87 Be-

triebsbuße Nr. 1). Die Betriebsbuße hat Strafcharakter, denn sie enthält ein Unwerturteil über ein Fehlverhalten (*BAG* AP BetrVG 1972 § 87 Betriebsbuße Nr. 12; Nr. 2). Formen der Betriebsbuße sind **Verwarnung** (bei geringeren Verstößen), **Verweis**, häufig mit Kündigungsandrohung (für schwerere oder wiederholte leichtere Verstöße) und **Geldbuße**. Betriebsbußen dürfen nicht mit Vertragsstrafen verwechselt werden, denen der Strafcharakter fehlt. Diese lässt sich der Arbeitgeber für den Fall versprechen, dass der Arbeitnehmer vertragsbrüchig wird, also seine Arbeitspflicht nicht oder schlecht erfüllt oder eine auf die Arbeitspflicht bezogene Nebenpflicht missachtet. Fällig wird dann ein bestimmter Geldbetrag (vgl. *BAG* NZA 2011, 89).

126 Die Verhängung von Betriebsbußen setzt das Bestehen einer ordnungsgemäß bekannt gemachten **Bußordnung** voraus. Bußordnungen beruhen in aller Regel auf **Betriebsvereinbarungen**. Das **Weisungsrecht** des Arbeitgebers **genügt** als Rechtsgrundlage **nicht** (*BAG* AP BetrVG 1972 § 87 Betriebsbuße Nr. 12). Die Tatbestände, bei deren Verwirklichung die Betriebsbuße droht, müssen abstrakt formuliert und eindeutig bestimmt sein. Außerdem müssen die Art und der Umfang der Bußen sowie das Verfahren zur Verhängung geregelt sein (*BAG* AP BetrVG § 56 Betriebsbuße Nr. 1).

127 Die Betriebsbuße darf nur in einem rechtsstaatlichen Grundsätzen entspr., **ordnungsgemäßen Verfahren** verhängt werden. Dazu gehört, dass dem **Arbeitnehmer rechtliches Gehör** gewährt wird und dass er sich durch den Betriebsrat, einen Gewerkschaftssekretär oder einen Rechtsanwalt vertreten lassen darf (*BAG* AP BetrVG 1972 § 87 Betriebsbuße Nr. 1). Die Verhängung einer Betriebsbuße setzt voraus, dass der Arbeitnehmer rechtswidrig und schuldhaft gegen die Bußordnung verstoßen hat. Dabei gilt das **Opportunitätsprinzip**. Die Betriebsbuße kann verhängt werden, sie muss es aber nicht. Die Verhängung der Betriebsbuße unterliegt in jeglicher Hinsicht der gerichtlichen Kontrolle (*BAG* AP BetrVG 1972 § 87 Betriebsbuße Nr. 1). Gegen einen Verweis oder eine Verwarnung ist die Feststellungsklage im Urteilsverfahren die richtige Klageart (§§ 2 Abs. 1 Nr. 3a, Abs. 5, 46 Abs. 2 ArbGG, § 256 ZPO). Die Rechtmäßigkeit einer Geldbuße wird regelmäßig inzident im Rahmen einer Zahlungsklage geprüft, weil der Arbeitgeber sie zumeist in Form eines Lohnabzugs einbehalten wird. Bei der Verhängung der Betriebsbuße hat der **Betriebsrat** ein erzwingbares Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG (*BAG* AP BetrVG 1972 § 87 Betriebsbuße Nr. 12; Nr. 1). Dieses Mitbestimmungsrecht besteht neben dem Mitbestimmungsrecht bei der Aufstellung der Bußordnung. In größeren Betrieben ist die Verhängung von Betriebsbußen häufig einem gemeinsamen Ausschuss (§ 28 Abs. 1 BetrVG) übertragen. Können sich Betriebsrat und Arbeitgeber nicht einigen, entscheidet die betriebliche Einigungsstelle (§ 76 BetrVG).

Weiterführende Literatur: *Asgari* Datenschutz im Arbeitsverhältnis – Offenbarungspflicht/Fragerecht, Mitarbeiter-Screening und Datenschutzgrundverordnung, DB 2017, 1325; *Aßmus/Winzer* Mitarbeiterfotos im Internet, auf Webseiten und in sozialen Netzwerken.

Anforderungen an Einwilligung und Widerruf nach dem KUG und der DS-GVO, ZD 2018, 508; *Bartz/Grotenrath* „Bring Your Own Device"-Geräte in internen Ermittlungen, CCZ 2019, 184; *Beckschulze/Fackeldey* Systematischer Aufbau von Betriebsvereinbarungen zum Schutze von Beschäftigtendaten, RDV 2013, 109; *Behling* Neues EGMR-Urteil zur Überwachung der elektronischen Kommunikation am Arbeitsplatz: Datenschutzrechtliche Implikationen für deutsche Arbeitgeber, BB 2018, 52; *Bettinghausen/Wiemers* Bewerberdatenschutz nach neuem Datenschutzrecht, DB 2018, 1277; *Betz* Automatisierte Sprachanalyse zum Profiling von Stellenbewerbern, ZD 2019, 148; *Bissels/Mayer-Michaelis/Schiller* Arbeiten 4.0: Big Data-Analysen im Personalbereich, DB 2016, 3042; *Bork/Servos* Einsatz von Dashcams in Fahrzeugflotten. Technische Zukunft oder unzulässige Überwachungsmöglichkeit?, AuA 2018, 338; *Byers* Die Zulässigkeit heimlicher Mitarbeiterkontrollen nach dem neuen Datenschutzrecht, NZA 2017, 1086; *Brink/Schwab* Die private E-Mail-Nutzung am Arbeitsplatz, ArbR 2018, 111; *Byers/Wenzel* Videoüberwachung am Arbeitsplatz nach dem neuen Datenschutzrecht, BB 2017, 2036; *Broy* Der Umgang mit Bewerberdaten aus Internetquellen, 2017; *Culik/Döpke* Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen, ZD 2017, 226; *Chandna-Hoppe* Beweisverwertung bei digitaler Überwachung am Arbeitsplatz unter Geltung des BDSG 2018 und der DS-GVO – Der gläserne Arbeitnehmer?, NZA 2018, 614; *Conze* Der neu geregelte Beschäftigtendatenschutz – am Beispiel des Fragerechts des öffentlichen Arbeitgebers gegenüber Bewerbern bei der Vertragsanbahnung, öAT 2018, 89; *Däubler* Informationsbedarf versus Persönlichkeitsschutz – was muss, was darf der Arbeitgeber wissen?, NZA 2017, 1481; *Dausend* Der Auskunftsanspruch in der Unternehmenspraxis, ZD 2019, 103; *Diercks* Video-Interviews in Personalauswahlverfahren, DuD 2017, 750; *Dombrowsky* Praktische Probleme von Datenschutz und Beschäftigtendatenschutz im Betrieb, ZfA 2019, 5; *Düwell/Brink* Die EU-Datenschutz-Grundverordnung und der Beschäftigtendatenschutz, NZA 2016, 665; *dies.* Beschäftigtendatenschutz nach der Umsetzung der Datenschutz-Grundverordnung: Viele Änderungen und wenig Neues, NZA 2017, 1081; *Dzida* Big Data und Arbeitsrecht, NZA 2017, 541; *ders.* Der neue Beschäftigtendatenschutz – Erste Erfahrungen aus der Praxis, BB 2018, 2677; *Dzida/Grau* Beschäftigtendatenschutz nach der Datenschutzgrundverordnung und dem neuen BDSG, DB 2018, 189; *Dzida/Groh* People Analytics im Personalbereich. Rechtliche Risiken beim Einsatz von Algorithmen im Betrieb, ArbRB 2018, 179; *Faas/Henseler* Speicherdauer und Aufbewahrungsfristen unter der DS-GVO, BB 2018, 2292; *Faulhaber/Scheurer* Pics or it didn't happen?!" – Die Fotodokumentation betrieblicher Veranstaltungen aus datenschutzrechtlicher Perspektive jM 2019, 2; *Feige* Personaldaten(über)fluss – Konzerne als illegal Datensammler? Datenübermittlungen in Konzern- und Matrixstrukturen innerhalb Europas, ZD 2015, 116; *Fischer* Datenschutzrechtliche Stolperfallen im Arbeitsverhältnis und nach dessen Beendigung, NZA 2018, 8; *Franck* Das System der Betroffenenrechte nach der DS-GVO, RDV 2016, 111; *Franzen* DS-GVO und Arbeitsrecht, EuZA 2017, 313; *Franzen* Persönlichkeitsrecht und Datenschutz im Arbeitsverhältnis ZfA 2019, 18; *Fuhlrott/Oltmanns* Arbeitnehmerüberwachung und interne Ermittlungen im Lichte der Datenschutz-Grundverordnung, NZA 2019, 1105; *Fuhlrott/Oltmanns* Auskunftsanspruch, Schadensersatz und Bußgelder. DS-GVO: Risiken für Personaler?, AuA 2021, 8; *Gaul/Pitzer* Das Gesetz zur Anpassung des Datenschutzrechts an die DS-GVO. Was ändert sich im Beschäftigtendatenschutz?, ArbRB 2017, 241; *Giesen/Kersten* Arbeiten im Privaten und Privatisieren am Arbeitsplatz. Verflechtung und Entflechtung von Lebenssphären in der digitalisierten Arbeitswelt, DB 2017, 2865; *Göpfert/Papst* Digitale Überwachung mobiler Arbeit, DB 2016, 1015; *Götz* Datenschutz ist nicht Tatenschutz" – Kein Verwertungsverbot bei offener rechtmäßiger Videoüberwachung SAE 2019, 54; *Gola* Datenschutz bei der Kontrolle „mobiler" Arbeitnehmer – Zu-

lässigkeit und Transparenz, NZA 2007, 1139; *ders.* Der „neue" Beschäftigtendatenschutz nach § 26 BDSG n.F., BB 2017, 1462; *ders.* Das Internet als Quelle von Bewerberdaten, NZA 2019, 654; *Gola/Jaspers* Zweckänderungen bei der Weiterverarbeitung von Beschäftigtendaten, RDV 2018, 145; *Gomez Hernández/Lincke* Videoüberwachung von Beschäftigten zwischen Weisungsrecht und Persönlichkeitsschutz, ZESAR 2018, 271; *Grages/Plath* Black Box statt Big Brother: Datenschutzkonforme Videoüberwachung unter BDSG und DS-GVO CR 2017, 791; *Grimm* Die „Rahmenbetriebsvereinbarung-DS-GVO" als Mittel zur Umsetzung der neuen Datenschutzvorgaben, ArbRB 2018, 78 und 122; *Grimm/Göbel* Das Arbeitnehmerdatenschutzrecht in der DS-GVO und dem BDSG neuer Fassung, jM 2018, 278; *Grimm/Kühne* Löschkonzept nach der DS-GVO. Alle Aufbewahrungspflichten und -rechte sowie Löschfristen bei Beschäftigtendaten im Überblick, ArbRB 2018, 144; *Grimm/Kühne* Die vorsorgliche Global-Einwilligung des Arbeitnehmers in die Datenverarbeitung, ArbRB 2018, 218; *Groß/Platzer* Whistleblowing: Keine Klarheit beim Umgang mit Informationen und Daten, NZA 2017, 1097; *Gundelach* Die datenschutzrechtliche Zulässigkeit von anlasslosen automatisierten Anti-Terror-Mitarbeiterscreenings, NZA 2018, 1606; *Härting* Was ist eigentlich eine „Kopie"? Zur Auslegung des Art. 15 Abs. 3 Satz 1 DS-GVO, CR 2019, 219; *Haußmann/Karwatzki/Ernst* Datenschutzrechtliche Löschfristen in der Personalverwaltung. Von der Bewerbung über die Personalentwicklung bis zur Beendigung eines Arbeitsverhältnisses – und danach?, DB 2018, 2697; *Herrmann/Zeidler* Arbeitnehmer und interne Untersuchungen – ein Balanceakt, NZA 2017, 1499; *Hofmann* Smart Factory – Arbeitnehmerdatenschutz in der Industrie 4.0, ZD 2016, 12; *Hodis-Mayer* Datenverarbeitung im Beschäftigungsverhältnis zur Aufdeckung von Straftaten, RDV 2019, 164; *Huff/Götz* Evidenz statt Bauchgefühl? – Möglichkeiten und rechtliche Grenzen von Big Data im HR-Bereich, NZA-Beilage 2019 (zu Heft 24), 73; *Jaspers/Jacquemain* Künstliche Intelligenz und ihre Auswirkungen auf den Beschäftigtendatenschutz, RDV 2019, 232; *Jessolat* Verdeckte Videoüberwachung am Arbeitsplatz und Auswertung eines Dienstcomputers durch den AG – Zulässige Eingriffe in das Privatleben?, ArbuR 2019, 38; *Jung/Hansch* Die Verantwortlichkeit in der DS-GVO und ihre praktischen Auswirkungen, ZD 2019, 143; *König* Das Recht auf eine Datenkopie im Arbeitsverhältnis, CR 2019, 295; *Kainer/Weber* Datenschutzrechtliche Aspekte des „Talentmanagements", BB 2017, 2740; *Kamps/Bonanni* Die datenschutzrechtliche Einwilligung im Beschäftigtenverhältnis nach der DS-GVO. Risiken und Chancen eines datenschutzrechtlichen Gestaltungsinstruments, ArbRB 2018, 50; *Karthaus* Mangelnde Beteiligungsfähigkeit des Algorithmus im betriebsverfassungsrechtlichen Beschlussverfahren. Steht dem Betriebsrat bei digitalisierten Produktionsmethoden ein Unterlassungsanspruch gegen fremde Arbeitgeber zu?, NZA 2017, 558; *Klaas* Mehr Beteiligungsrechte des Verdächtigen. Der Einfluss des Transparenzgrundsatzes der DS-GVO auf die Durchführung interner Ermittlungen, CCZ 2018, 242; *Kleinebrink* Die Einwilligung im Beschäftigungsverhältnis nach neuem Datenschutzrecht, DB 2018, 1729; *Klösel/Mahnhold* Die Zukunft der datenschutzrechtlichen Betriebsvereinbarung, NZA 2017, 1428; *König* Das Recht auf eine Datenkopie im Arbeitsverhältnis. Ein Leitfaden zur Handhabung in der betrieblichen Praxis, CR 2019, 295; *Körner* Die Datenschutz-Grundverordnung und nationale Regelungsmöglichkeiten für Beschäftigtendatenschutz, NZA 2016, 1383; *dies.* Beschäftigtendatenschutz in Betriebsvereinbarungen unter der Geltung der DS-GVO, NZA 2019, 1389; *dies.* EGMR relativiert Verbot der Videoüberwachung, NZA 2020, 25; *Korinth* Datenschutz-Grundverordnung – Was ändert sich für den Betriebsrat?, ArbRB 2018, 47; *Kort* Arbeitnehmerdatenschutz gemäß der EU-Datenschutz-Grundverordnung, DB 2016, 771; *ders.* Eignungsdiagnose von Bewerbern unter der Datenschutz-Grundverordnung, NZA-Beilage 2016, 62; *ders.* Der Beschäftigtendatenschutz nach § 26 BDSG-neu, ZD 2017, 319; *ders.* Die Bedeutung der neueren arbeits-

rechtlichen Rechtsprechung für das Verständnis des neuen Beschäftigtendatenschutzes, NZA 2018, 1097; *ders.* Neuer Beschäftigtendatenschutz und Industrie 4.0. Grenzen einer „Rundumüberwachung" angesichts der Rechtsprechung, der DS-GVO und des BDSG nF, RdA 2018, 24; *Kramer (Hrsg.)* IT-Arbeitsrecht, 2. Aufl. 2019; *Kramer* Folgen der EGMR-Rechtsprechung für eine IT-Kontrolle bei Privatnutzungsverbot, NZA 2018, 637; *Künzl* Facebook, Twitter & Co – Persönlichkeitsrechte in sozialen Netzwerken und Mitbestimmung des Betriebsrats, BB 2021, 436; *Laber/Santon* Die Auswertung von Browserverläufen zur Überwachung der Internetnutzung am Arbeitsplatz, ArbRB 2019, 60; *Lentz* Arbeitgeberseitige Risiken im Kündigungsschutzprozess nach Inkrafttreten der DS-GVO, ArbRB 2018, 374; *Lepperhoff* Gehaltsdaten für Benchmarks übermitteln – zulässig?, RDV 2017, 242; *Lörcher* Offene Videoüberwachung am Arbeitsplatz Universität, ArbuR 2019, 43; *Maschmann* Datenschutzgrundverordnung: Quo vadis Beschäftigtendatenschutz?, DB 2016, 2488; *ders.* Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA Beilage 2018 Nr 4, 115; *ders.* Verarbeitung personenbezogener Entgeltdaten und neuer Datenschutz, BB 2019, 628; *Maschmann/Fritz* Matrixorganisationen. Gesellschaftsrecht. Arbeitsrecht. Datenschutz, 2019; *Mengel* Internal Investigations – Arbeitsrechtliche Lessons Learned und Forderungen an den Gesetzgeber, NZA 2017, 1494; *Middel* Beschäftigtendatenschutz im Lichte der DS-GVO und unter Berücksichtigung des BDSG (neu), AuR 2018, 411; *Müller* Beschäftigtendatenschutz im Arbeitsrecht: dienstliche und private E-Mail-Nutzung, öAT 2019, 1; *Nebel* Big Data und Datenschutz in der Arbeitswelt. Risiken der Digitalisierung und Abhilfemöglichkeiten, ZD 2018, 520; *Nebeling/Lankes* Das neue BDSG und die Personalakte 2.0 – ein Recht auf Vergessen?, DB 2017, 2542; *Niklas/Thurn* Arbeitswelt 4.0 – Big Data im Betrieb, BB 2017, 1589; *Niklas/Peter* WhatsApp & Co. – Die Messenger-Nutzung auf Diensthandys. Rechtliche Grundlagen, Risiken und Gestaltungsmöglichkeiten, ArbRB 2019, 50; *Niemann* Keylogger & Co: Verwertungsverbote infolge grundrechtswidriger Arbeitgebermaßnahmen, JbArbR 55 (2018) 41; *Oberthür* Die anderweitige Verwertung von Erkenntnissen aus dem Betrieblichen Eingliederungsmanagement. DS-GVO und BDSG n.F. setzen enge Grenzen, ArbRB 2018, 309; *Paal/Aliprandi* Immaterieller Schadensersatz bei Datenschutzverstößen, ZD 2021, 241; *Pfrang* Die „nicht-dateimäßige" Verarbeitung von Beschäftigtendaten, DuD 2018, 380; *Piltz* Datenübertragbarkeit im Beschäftigungsverhältnis – Arbeitgeberwechsel: Und die Daten kommen mit?, RDV 2018, 3; *Pötters* Grundrechte und Beschäftigtendatenschutz, 2013; *Ringel/von Busekist* Konzernrevision und Datenschutz, CCZ 2017, 31; *Rudkowski* „Predictive policing" am Arbeitsplatz , NZA 2019, 72; *Sander/Schumacher/Kühne* Weitergabe von Arbeitnehmerdaten in Unternehmenstransaktionen, ZD 2017, 105; *Schneider* Schließt Art. 9 DS-GVO die Zulässigkeit der Verarbeitung bei Big Data aus?, ZD 2017, 303; *ders.* Das Rückgriffsverbot im Datenschutz – kein „best of both worlds"? Zum Verhältnis zwischen Einwilligung und gesetzlicher Erlaubnis am Beispiel von Arbeitnehmerdaten, CR 2017, 568; *Schrey/Kielkowski* Die datenschutzrechtliche Betriebsvereinbarung in DS-GVO und BDSG 2018 – Viel Lärm um Nichts?, BB 2018, 629; *Schulte/Welge* Der datenschutzrechtliche Kopieanspruch im Arbeitsrecht, NZA 2019, 1110; *T. Schulz* Ist der Betriebsrat Verantwortlicher i.S.d. Europäischen Datenschutz-Grundverordnung?, ZESAR 2019, 323; *Schwarz* Datenschutzrechtliche Zulässigkeit des Pre-Employment Screening, ZD 2018, 353; *Söbbing* Künstliche Intelligenz im HR-Recruiting-Prozess: Rechtliche Rahmenbedingungen und Möglichkeiten, InTeR 2018, 64; *Ströbel/Böhm/Breunig/Wybitul* Beschäftigtendatenschutz und Compliance: Compliance-Kontrollen und interne Ermittlungen nach der EU-Datenschutz-Grundverordnung und dem neuen Bundesdatenschutzgesetz, CCZ 2018, 14; *Stück* Datenschutzrechtliche Aspekte einzelner Mitbestimmungsrechte, ZD 2019, 346; *ders.* Präventive und repressive Compliance: Datenschutz- und arbeitsrechtliche Aspekte nach DS-GVO sowie

BDSG 2018, ArbR 2019, 216; *ders.* Unternehmensinterne Untersuchungen im Spannungsfeld von Arbeitsrecht, Compliance, Datenschutz, Haftungsrecht und Strafrecht GmbHR 2019, 156; *ders.* Aufbewahrungspflichten und Löschfristen nach neuem Datenschutzrecht, AuA 2019, 695; *Suchan* Der „qualitative Exzess" nach Art. 15 DS-GVO ZD 2021, 198; *Thüsing/Rombey* Der verdeckte Einsatz von Privatdetektiven zur Kontrolle von Beschäftigten nach dem neuen Datenschutzrecht, NZA 2018, 1105; *dies.* Die „schriftlich oder elektronisch" erteilte Einwilligung des Beschäftigten nach dem neuen Formerfordernis in § 26 II 3 BDSG, NZA 2019, 1399; *Thüsing/Fütterer/Jänsch* Petzen ist doof. Zu den datenschutzrechtlichen Grenzen des Whistleblowings, RDV 2018, 133; *Thüsing/Schmidt* Zulässige Pauschalierung bei der Rechtfertigung präventiver Überwachungsmaßnahmen des Arbeitgebers, NZA 2017, 1027; *Tiedemann* Offene Videoüberwachung – Verdachtskündigung – Beweisverwertungsverbot, ZD 2019, 230; *Tinnefeld/Conrad* Die selbstbestimmte Einwilligung im europäischen Recht, ZD 2018, 391; *Uecker* Die Einwilligung im Datenschutzrecht und ihre Alternativen, ZD 2019, 248; *Ullrich* Datensparsamkeit im Arbeitsverhältnis, ZMV 2018, 176; *Venetis* Neues zum Thema offene Videoüberwachung, AnwBl BE 2018, 459; *Wisskirchen/Schiller/Schwindling* Die Digitalisierung – eine technische Herausforderung für das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG, BB 2017, 2105; *Weichert* Die Verarbeitung von Wearable-Sensordaten bei Beschäftigten, NZA 2017, 565; *Wybitul* Betriebsvereinbarungen im Spannungsverhältnis von arbeitgeberseitigem Informationsbedarf und Persönlichkeitsschutz des Arbeitnehmers, NZA 2017, 1488; *ders.* Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte?, ZD 2016, 203; *ders.* EU-Datenschutz-Grundverordnung in der Praxis – Was ändert sich durch das neue Datenschutzrecht?, BB 2016, 1077; *ders.* Der neue Beschäftigtendatenschutz nach § 26 BDSG und Art. 88 DS-GVO, NZA 2017, 413; *Wybitul/Brams* Welche Reichweite hat das Recht auf Auskunft und auf eine Kopie nach Art. 15 I DS-GVO?, NZA 2019, 672; *Wybitul/Baus* Wie weit geht das Recht auf Auskunft und Kopie nach Art. 15 DS-GVO?, CR 2019, 494; *Wybitul/Brink/Albrecht* Beschäftigtendatenschutz nach der DS-GVO, NZA 2018, 285; *Wybitul/Ströbel/Ruess* Übermittlung personenbezogener Daten in Drittländer, ZD 2017, 503; *Zikesch/Sörup* Der Auskunftsanspruch nach Art. 15 DS-GVO, ZD 2019, 239; *Zöll/Schönbach* Die digitale Personalakte. Digitalisierung und Datenschutz, AuA 2018, 217.