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.

3 Zum dritten kommt das Arbeitsrecht ins Spiel, wenn es um die Grenzen der Verhaltenssteuerung geht. Diese werden vor allem bei der **Mitarbeiterkontrolle** aktu-

ell, 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.

Endlich entscheidet das Arbeitsrecht darüber, welche **Sanktionen** der Arbeitgeber **4**
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. 68). 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. 47).

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 Arbeitgeber einseitig kraft Direktionsrechts aufstellen. Eines Einverständnisses oder einer Bestätigung seitens des Arbeitnehmers bedarf er hierzu nicht. Im Regelfall **5**

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 (§ 17 UWG) 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 Direk-

tionsrechts 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 Erhebung, Verarbeitung, Übermittlung und Nutzung perso- **8**
nenbezogener Daten richtet sich seit dem 25.5.2018 nach der Datenschutz-Grundverordnung (DSGVO) 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 DSGVO. 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 DSGVO). 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 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 DSGVO 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 DSGVO 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 DSGVO 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 DSGVO 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 DSGVO 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, dh 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 TKG 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 DSGVO in der jeweils geltenden Fas-

sung, unmittelbar gilt. Darauf weist § 1 Abs. 5 BDSG noch einmal ausdrücklich hin, obwohl sich diese Rechtsfolge bereits aus Art. 288 Abs. 2 AEUV ergibt.

Konkrete Regelungen zum Schutz von Beschäftigtendaten treffen weder die DSGVO noch das BDSG. Art. 88 DSGVO 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* DSGVO Art. 88 Rn. 63, 65). Seitens des Bundesrats wurde deshalb erneut der Erlass eines Beschäftigtendatenschutzgesetzes angemahnt (BT-Drucks. 18/11655, S. 24). Der Koalitionsvertrag vom Februar 2018 stellt ein solches für die 19. Legislaturperiode in Aussicht (Koalitionsvertrag S. 42). Die inhaltlichen Vorgaben und Grenzen für ein solches Gesetz 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 DSGVO, sondern wacht zudem darüber, dass die Mitgliedstaaten beim Erlass ihres nationalen Datenschutzrechts die inhaltlichen Vorgaben des Art. 88 Abs. 2 DSGVO einhalten. **11**

2. Anwendbarkeit des des deutschen Beschäftigtendatenschutzrechts (§ 26 BDSG)

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 DSGVO legaldefiniert.** Darunter sind alle Informationen zu verstehen, die sich auf eine „identifizierte oder identifizierbare natürliche Person beziehen". Identifizierbar ist eine natürliche Personen, 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 DSGVO** geregelt. Das Unionsrecht versteht darunter – weiter als das bisherige deutsche Recht – „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". Während die DSGVO nur für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten (dazu zuletzt *EuGH* NZA 2018, 931) Anwendung findet (Art. 2 Abs. 1 DSGVO), 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), wie z.B. bei Befragungen von Bewerbern und Be- **12**

schäftigten, Tor-, Taschen- und Spindkontrollen oder bei rein tatsächlichen Beobachtungen von Arbeitnehmern durch Wach- und Sicherheitspersonal (s. zum bisherigen Recht *BAG* 20.6.2013, NZA 2014, 143; *Gola/Schomerus* BDSG § 32 Rn. 7; Simitis/*Seifert* BDSG § 32 Rn. 14, 100). Mit dem den Anwendungsbereich der DSGVO überschießenden Bereich wird § 26 Abs. 7 BDSG als nationale Sondervorschrift nicht von der DSGVO verdrängt (*Kort* ZD 2017, 319, 323; *Wybitul* NZA 2017, 413, 418).

13 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, die dem § 32 Abs. 1 S. 2 BDSG a.F. entspricht. Sie gilt – wie bisher – 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 DSGVO genannten Zwecken schließt § 26 Abs. 1 BDSG nicht aus. Sie können nach Art. 6 Abs. 1 lit. f oder Art. 9 Abs. 2 DSGVO erlaubt sein. Beispiele sind Übermittlung von Beschäftigtendaten im Rahmen von **„Due-Diligence-Prüfungen"** beim Kauf von Betrieben oder Unternehmen oder die **Ansprache von Mitarbeitern zu Werbezwecken,** die nichts mit dem Beschäftigungsverhältnis zu tun haben (*Gola/Schomerus* BDSG § 32 Rn. 46), oder für die Konzernrevision (dazu ausf. *Ringel/von Busekist* CCZ 2017, 31).

14 **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. Die Vorschrift übernimmt im Wesentlichen die bisher in § 3 Abs. 11 BDSG a.F. definierten Begriffe in einer redaktionell überarbeiteten 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 (§ 26 Abs. 8 S. 1 BDSG). Dieser sehr weit gefasste Schutzbereich muss im Einklang mit der Öffnungsklausel des Art. 88 Abs. 1 DSGVO stehen. Ob das der Fall ist, erscheint zweifelhaft. Richtigerweise erlaubt die DSGVO nationales Beschäftigtendatenschutzrecht nur als „klassisches" Arbeitnehmerdatenschutzrecht (ausf. Kühling/Buchner/*Maschmann* DSGVO Art. 88 Rn. 11 ff.; ebenso *Körner* Beschäftigtendatenschutz im Lichte der DSGVO, S. 55; für eine weite Auslegung *Franzen* EuZA 2017, 313 (349); *Gola* BB 2017, 1462 (1472); *Kort* ZD 2017, 319 (321); BeckOK DatenschutzR/*Riesenhuber* DSGVO Art. 88 Rn. 13). Werden personenbezogene Daten von Personen verarbeitet, die nicht unter § 26 BDSG fallen, wie z.B. Vorstände und Geschäftsführer, gilt die DSGVO direkt, jedenfalls bei automatisierter Datenverarbeitung i.S.d. Art. 2 Abs. 1 DSGVO. Zu beachten sind dann vor allem die allgemeinen Grundsätze des Art. 5 DSGVO und die Abwägungsklausel des Art. 6 I f DSGVO.

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 DSGVO enthält insoweit ein „Verbot mit Erlaubnisvorbehalt". Für den Beschäftigtendatenschutz enthält § 26 Abs. 1 BDSG eine gesetzliche Verarbeitungsgrundlage. Dabei herrscht – wie bisher – der Grundsatz der **strengen Zweckbindung,** der sich unionsrechtlich aus Art. 5 Abs. 1 lit. b DSGVO 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, die mit den ursprünglichen nicht vereinbar sind, ist verboten. Werden die Daten bei der betroffenen Person erhoben, müssen ihr die Zwecke zum Zeitpunkt der Datenerhebung nach Maßgabe von Art. 13 Abs. 1 DSGVO mitgeteilt werden. Sollen sie für einen anderen als für den ursprünglichen Zweck weiterarbeitet werden, ist die betroffene Person vorher zu informieren (§ 13 Abs. 3 DSGVO). Der Verantwortliche hat den Verarbeitungszweck in einem Verzeichnis der Verarbeitungstätigkeiten festzuhalten (Art. 30 Abs. 1 S. 2 lit. b DSGVO). 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 DSGVO). Ohne diesen Nachweis ist die Verarbeitung rechtswidrig (Art. 24 Abs. 1 S. 1 DSGVO). Das Verarbeitungsverzeichnis ist grds. schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann (Art. 30 Abs. 3 DSGVO). 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 DSGVO verarbeitet werden (Art. 30 Abs. 5 DSGVO). 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 DSGVO). **15**

b) Verhältnismäßigkeit

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 be- **16**

rücksichtigt". Das entspricht der Vorgabe in Art. 88 Abs. 2 DSGVO. 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. Dabei ist der **Grundsatz der Verhältnismäßigkeit** zu wahren (*Kort* ZD 2017, 319, 323; *Wybitul* NZA 2017, 413, 415).

17 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 DSGVO, 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).

c) Beachtung der allgemeinen Verarbeitungsgrundsätze

18 § 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 DSGVO 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 DSGVO) –, 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 DSGVO). Ob damit eine ständige Prüfungspflicht gemeint ist, ist streitig. Es dürfte wohl genügen, eine Pflicht zur Einleitung eines Korrekturprozesses nur dann anzunehmen, wenn eine Datenunrich-

tigkeit bekannt wird (ebenso *Wybitul/Sürup/Pötters* ZD 2015, 559, 562). 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 DSGVO). Außerdem müssen sie vor unbefugtem Zugriff geschützt werden. Dabei hat der 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. DSGVO über Datensicherheit und beachten, und es ist der betriebliche Datenschutzbeauftragte (Art. 37 DSGVO) rechtzeitig vor der Verarbeitung zwecks Folgenabschätzung (Art. 35 DSGVO) einzubinden.

d) Transparenz der Verarbeitung

19 Weiterhin verpflichtet Art. 88 Abs. 2 DSGVO 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 DSGVO, 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 DSGVO). Die Unterrichtung muss „in einer für die betroffenen Person nachvollziehbaren Weise" geschehen (Art. 5 Abs. 1 lit. a DSGVO). 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 DSGVO). Das hat zum Zeitpunkt der Erhebung zu erfolgen (Art. 13 Abs. 1 DSGVO und EG 61 S. 1 DSGVO).

Nicht offen erkennbare Datenverarbeitungen, wie etwa heimliche Videoüberwachungen und Schrankkontrollen, Observationen durch Detektive, das Belauschen von Telefongesprächen oder Mitlesen von E-Mail, 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* DSGVO Art. 5 Rn. 18). Allerdings erlaubt Art. 23 Abs. 1 DSGVO auch Beschränkungen des Transparenzprinzips. Das kann beispielweise geschehen, um Straftaten zu verhüten oder aufzudecken oder um zivilrechtliche Ansprüche durchzusetzen. Solche Beschränkungen dürfen die Mitgliedstaaten aber nur durch Gesetz anordnen. Dabei müssen der Wesensgehalt der Grundrechte und Grundfreiheiten sowie der Grundsatz der Verhältnismäßigkeit beachtet werden (Art. 23 Abs. 1 DSGVO). **§ 26 Abs. 1 BDSG als Befugnisnorm genügt hierfür nicht.** Zwar spricht § 26 Abs. 1 S. 2 BDSG – ähnlich wie die Vorgängernorm – von besonderen Bedingungen, wenn Beschäftigtendaten „zur Aufdeckung von Straftaten" verarbeitet werden sollen. Von heimlichen Verarbeitungen ist dort aber gerade nicht die Rede, auch wenn die in der Vorschrift genannten Erhebungsvoraussetzungen darauf hindeuten, dass der Gesetzgeber gerade diese im Blick gehabt hatte (*BAG* NZA 2015, 741; NZA 2017, 1179 Rn. 27; NZA 2017, 1327). Selbst wenn das der Fall gewesen sein sollte, kann die Zulassung heimlicher Überwachungsmaßnahmen nicht

einfach in § 26 Abs. 1 S. 2 BDSG hineingelesen werden (ebenso *Byers* NZA 2017, 1086, 1089). Dagegen sprechen nicht nur der Wortlaut und das Fehlen entspr. Belege in den Gesetzgebungsmaterialien, sondern auch der Umstand, dass die 2010 in Angriff genommene Regelung des Beschäftigtendatenschutzes gerade am fehlenden Konsens über die Zulässigkeit heimlicher Überwachungsmaßnahmen gescheitert war. 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 DSGVO **nicht mehr.** Denn Art. 23 Abs. 1 DSGVO verlangt ausdrücklich eine gesetzliche Regelung (ausf. Kühling/Buchner/*Bäcker* DSGVO Art. 23 Rn. 35), für die Art. 23 Abs. 2 DSGVO detaillierte inhaltliche Vorgaben enthält. Die Ausnahmevorschrift des § 32 BDSG ist nicht einschlägig (ebenso *Byers* NZA 2017, 1086, 1089), weil er nur die Weiterverarbeitung von personenbezogenen Daten zu einem anderen als den Erhebungszweck betrifft (Begr. RegE, BT-Drucks. 18/11325, 102) und nicht die (heimliche) Erhebung (das übersieht *Gola* BB 2017, 1462, 1466). Ebenso wenig greift § 33 Abs. 1 Nr. 2a BDSG, weil auch eine verdeckte Mitarbeiterkontrolle eine Datenerhebung bei der betroffenen Person i.S.d. Art. 13 DSGVO darstellt und keine Erhebung bei einem Dritten (ebenso Kühling/Buchner/*Bäcker* DSGVO Art. 13 Rn. 14). § 33 BDSG a.F., der eine Benachrichtigung des Betroffenen vorsah, falls personenbezogene Daten „ohne Kenntnis des Betroffenen gespeichert" wurden, wurde im BDSG n.F. nicht übernommen. **Erst recht nicht** können derartige Beschränkungen (allein) auf einen **Kollektivvertrag** gestützt werden. Betriebsvereinbarungen über heimliche Videokontrollen wären ab dem 25.5.2018 ebenfalls unzulässig. Dem steht nicht entgegen, dass § 33 BDSG n.F. eine erst nachträgliche Information des Betroffenen zulässt, denn diese gilt – so wie Art. 14 DSGVO – nur, falls die Daten nicht beim Betroffenen selbst, sondern bei einem Dritten erhoben wurden.

e) Umgang mit sensiblen Beschäftigtendaten

20 Für die Verarbeitung sensibler Daten i.S.v. Art. 9 Abs. 1 DSGVO, d.h. **rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische** (Art. 4 Nr. 13 DSGVO) und **biometrische Daten** zur eindeutigen Identifizierung einer natürlichen Person (Art. 4 Nr. 14 DSGVO), Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) sowie **Daten zum Sexualleben und zur sexuellen Orientierung**, trifft Art. 9 Abs. 2 DSGVO 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 Sozialrecht ergebenden Pflichten nachkommen und die betroffene Person die ihr daraus erwachsenden Rechte ausüben kann (Art. 9 Abs. 2 lit. b DSGVO). 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 zusätz-

liche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten (Art. 9 Abs. 4 DSGVO). Dies gilt ebenfalls für Beschäftigtendaten.

Vor diesem Hintergrund bestimmt **§ 26 Abs. 3 BDSG** – in bewusst enger textlicher Anlehnung an § 28 Abs. 6 Nr. 3 BDSG a.F. – dass die Verarbeitung sensibler Daten i.S.d. Art. 9 Abs. 1 DSGVO 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 DSGVO). Art. 9 Abs. 3 DSGVO 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). **21**

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 (**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 nach neuem Recht (**BT-Drucks. 18/ **22**

11325, 98**)**. Art. 88 Abs. 1 DSGVO 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 DSGVO 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 DSGVO, für die die Mitgliedstaaten aufgrund von Art. 9 Abs. 2 lit. b DSGVO Regelungen durch Kollektivvereinbarung zulassen dürfen, jedenfalls dann, wenn die Verarbeitung erforderlich ist und geeignete Garantien für die Grundrechte und die Interessen des betroffenen Person vorhanden sind. **Kollektivvereinbarungen** zur Datenverarbeitung, die bei Inkrafttreten der DSGVO bereits bestehen, **gelten fort.** Sie müssen der Kommission nicht nach Art. 88 Abs. 3 DSGVO gemeldet werden, weil diese Verpflichtung nur für die von den Mitgliedstaaten selbst erlassene Rechtsvorschriften gilt (*Gola/Pötters/Thüsing* RDV 2016, 57, 59; BeckOK DatenschutzR/*Riesenhuber* DSGVO Art. 88 Rn. 93; Ehmann/Selmayr/*Selk* DSGVO Art. 88 Rn. 125; Sydow/*Tiedemann* DSGVO Art. 88 Rn. 26; Schantz/*Wolff* Das neue Datenschutzrecht, 2017, Rn. 1341; a.A. Plath/*Stamer/Kuhnke* DSGVO Art. 88 Rn. 11). Ob sie weiter genutzt werden können, hängt davon ab, ob sie den inhaltlichen Anforderungen der DSGVO genügen. Das ist im jeweiligen Einzelfall zu prüfen (*Klösel/Mahnhold* NZA 2017, 1428, 1430; *Von dem Bussche* DB 2016, 1359, 1362 f.; *Wybitul/Pötters* ZD 2016, 10, 15).

23 Die inhaltlichen Anforderungen für Betriebsvereinbarungen richten sich vor allem nach den Direktiven des Art. 88 Abs. 2 DSGVO. 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 DSGVO 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. DSGVO). Außerdem müssen Kollektivvereinbarungen die allgemeinen Grundsätze des Art. 5 DSGVO beachten, die auch für die Verarbeitung von Beschäftigtendaten gelten (s. Rn. 18).

g) Einwilligung

24 Grundlage für die Verarbeitung von Beschäftigtendaten kann auch die Einwilligung des Betroffenen sein (Art. 6 Abs. 1 lit. a DSGVO). Die **Mitgliedstaaten** können im Rahmen von Art. 88 DSGVO hierfür **spezielle Voraussetzungen** festlegen. Das ergibt sich aus EG 155 DSGVO, 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 DSGVO 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 DSGVO), 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 DSGVO). 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* DSGVO 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.

25 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 deren Schriftform. 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 (ebenso *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 verweigert wird, falls er eine mit der Gewährung des Vorteils verbundene Kontrolle verweigert, bei der personenbezogene Daten erhoben werden.

26 Ferner bestimmt § 26 Abs. 2 BDSG, dass der Arbeitgeber den Beschäftigten vor einer Einwilligung über den **Zweck der Datenverarbeitung** und über sein **Widerrufsrecht** nach Art. 7 Abs. 3 DSGVO aufzuklären hat (Musterformulierungen bei *Kleinebrink,* DB 2018, 1729 ff.). Das kann in Textform (§ 126a BGB) geschehen, also z.B. per E-Mail, wenn der Arbeitgeber nachweisen kann, dass sie der Mitarbeiter erhalten hat. Unionswidrig ist, dass § 26 Abs. 2 BDSG für eine wirksame Einwilligung grds. die Schriftform verlangt. Denn damit geht der deutsche Gesetzgeber unzulässig über die Vorgabe in Art. 4 Nr. 11 DSGVO hinaus (ebenso *Krohm* ZD 2016, 368, 371; a.A. *Kort* ZD 2017, 319, 321). **Mündliche und konkludente Einwilligungen sind danach möglich,** wenn sie unmissverständlich erteilt wurden (*Albrecht* CR 2016, 88, 91; *Härting* ITRB 2016, 36, 39; *Kort* DB 2016, 711, 715). Dass § 26 Abs. 2 BDSG die Schriftform ausnahmsweise für entbehrlich erklärt, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist, genügt nicht, weil damit das Regel-Ausnahme-Prinzip des Art. 7 Abs. 3 DSGVO in sein Gegenteil verkehrt wird. Allerdings muss der Verantwortliche nachweisen können, dass der Arbeitnehmer die Einwilligung „in Kenntnis der Sachlage" erteilt hat (Art. 7 Abs. 1 DSGVO). Das verlangt nach EG 42 S. 2 mindestens Informationen über den Verantwortlichen und für welche Zwecke die Beschäftigtendaten erhoben werden, so wie es früher in § 4a BDSG a.F. angeordnet war (*Kort* DB 2016, 711, 715). Das reine Schriftformgebot ist hierfür unbehelflich, weil damit dem eigentlichen Defizit der datenschutzrechtlichen Einwilligung nicht begegnet werden kann: der Transparenz in die Reichweite der Erklärung. Pauschale Einwilligungen sind daher stets unwirksam. Sie widersprechen der Vorgabe, dass eine Einwilligung nur für einen bestimmten Zweck erteilt werden kann (*Kühling/Buchner* DSGVO Art. 7 Rn. 61 ff.). Eine **ausdrückliche Einwilligung** ist stets erforderlich bei der **Erhebung sensibler Daten** (Art. 9 Abs. 2 lit. a DSGVO, § 26 Abs. 3 S. 2 BDSG) sowie beim sog. **Profiling** (Art. 22 Abs. 2 lit. c DSGVO). 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 DSGVO). Keinesfalls können die dargelegten Anforderungen abgesenkt werden, auch nicht durch Betriebsvereinbarung.

4. Rechte des Betroffenen

Die Art. 12 ff. DSGVO 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 DSGVO 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 DSGVO). 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 DSGVO erforderlichen Garantien verlangen (Art. 15 Abs. 2 DSGVO). Überdies hat der Verantwortliche eine kostenlose Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen (Art. 15 Abs. 3 DSGVO). 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 DSGVO). Der Verantwortliche kann dem entgegnen, dass er die Daten zur Ausübung oder zur Verteidigung von Rechtsansprüchen weiter benötigt (Art. 17 Abs. 3 lit. e DSGVO). Nach Maßgabe von Art. 18 DSGVO 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 DSGVO 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 DSGVO). 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 DSGVO), es sei denn, dass

27

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 DSGVO). Die Vorgaben der DSGVO sind für das deutsche Recht – soweit es die Öffnungsklauseln in den Art. 13 ff. DSGVO erlauben – durch die §§ 32 ff. BDSG eingeschränkt worden. Ob das erlaubt ist, wird die Rechtsprechung des EuGH klären müssen.

28 Ist einem Beschäftigten wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden, hat er Anspruch auf Schadenersatz gegen den Verantwortlichen (Art. 82 Abs. 1 DSGVO). 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 DSGVO). 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* DSGVO 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. 28 DSGVO). Art. 82 DSGVO 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.

5. Weitere Sanktionen bei Verstößen gegen das Datenschutzrecht

a) Bußgeld

29 Verstöße gegen die DSGVO sind mit einem Bußgeld bedroht, dessen Verhängung durch die zuständige Aufsichtsbehörde wirksam, verhältnismäßig und abschreckend zu sein hat (Art. 83 Abs. 1 DSGVO). 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 bis 39, 42 und 43 DSGVO verstößt. Gegen Unternehmen können darüber hinaus 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 DSGVO, der Nichtgewährung der Betroffenenrechte nach Art. 12 bis 22 DSGVO, einer nicht nach den Art. 44 DSGVO 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 DSGVO – sowie bei der Nichtbefolgung von Anweisungen der Aufsichtsbehörde gem. Art. 58 DSGVO 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 DSGVO auf den kartellrechtlichen Unternehmensbegriff i.S.d. Art. 101, 102 AEUV abzustellen, d.h. auf den Umsatz der gesamten Unternehmensgruppe. Art. 83 DSGVO folgt dabei – anders als das deutsche Recht – dem Modell der originären Verbandshaftung. Dieses sanktioniert bei Verstößen gegen die DSGVO den Rechtsträger unmittelbar, d.h. bei Unternehmen regelmäßig die juristische Person; die Zurechnung von Handlungen natürlicher Personen ist nicht erforderlich (Kühling/Buchner/*Bergt* DSGVO Art. 83 Rn. 20). Wird die Geldbuße einer natürlichen Personen auferlegt, muss die Aufsichtsbehörde das allgemeine Einkommensniveau im jeweiligen Mitgliedstaat und die wirtschaftliche Lage der Person berücksichtigen (EG 150 S. 4 DSGVO). 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 DSGVO). Für die Verhängung und die Höhe des Bußgelds sollen nach Art. 83 Abs. 2 DSGVO 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 DSGVO die Verhängung von Geldbußen ohne Verschulden vorsieht (Kühling/Buchner/*Bergt* DSGVO Art. 83 Rn. 34 ff.) und ob für die Verfolgung des Legalitäts- oder das Opportunitätsprinzip gilt (Kühling/Buchner/*Bergt* DSGVO 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- **30**
schutzrecht enthält die DSGVO nicht. Art. 84 DSGVO 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

31 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 Urt. v. 15.5.2018 – VI ZR 233/17) und des Bundesarbeitsgerichts (*BAG* NZA 2011, 571; 2012, 1025; 2014, 143; 2017, 112; 2017, 1179; 2017, 1327) 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).

32 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. **33**

Aus diesem Grunde soll nach neuester Rspr. (*BAG* NZA 2017, 112 Rn. 23, 25) 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 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 nur dann eine Ausnahme, wenn die Partei auf die Geltendmachung der Rechtsverletzung wirksam verzichtet hat (*BAG* NZA 2017, 112 Rn. 25). Besteht – wie im Regelfall – ein Verwertungs- **34**

verbot, 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).

35 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; *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).

36 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.). 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" anfertigt werden. Diese ist angesichts der notorischen Beweisnot in Unfallprozessen und der relativen Geringfügigkeit des Eingriffs in das Recht am eigenen Bild grds. zulässig (*BGH* 15.5.2018 – VI ZR 233/17 Rn. 47 ff.) und stellt nach Ansicht des EGMR auch keine Verletzung des Art. 8 EMRK dar (EGMR NJW 2015, 1079).

IV. Mitarbeiterüberwachung

Werden Arbeitnehmer kontrolliert, ist damit regelmäßig eine Erhebung personenbezogener Daten i.S.d. Art. 4 Nr. 2 DSGVO verbunden, denn dazu rechnen *„alle Informationen, die sich auf eine identifizierbare natürliche Person beziehen"* (Art. 4 Nr. 1 DSGVO). 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 DSGVO. Art. 88 Abs. 1 DSGVO erlaubt die Verarbeitung von Beschäftigtendaten ausdrücklich auch zum Schutz des Eigentums des Arbeitgebers und der Kunden. Darüber hinaus erwähnt Art. 88 Abs. 2 DSGVO die „Überwachungssysteme am Arbeitsplatz", d.h. die offen oder verdeckt durchgeführten Maßnahmen der Mitarbeiterkontrolle, wie etwa die Videoüberwachung, die Kontrolle des E-Mail-Verkehrs und der sonstigen Internetnutzung, die Erfassung von Telefondaten, die Aufzeichnung von Bewegungsdaten per RFID, Handy-Ortung und GPS sowie die Verarbeitung von Körperdaten durch in die Kleidung von Arbeitnehmern integrierte Sensoren („Wearables"). Wird der Mitarbeiter überwacht, um das Beschäftigungsverhältnisses 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 DSGVO einschlägig. **37**

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. zuletzt *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 **38**

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.). Vor diesem Hintergrund sollen im Folgenden die für die Praxis wichtigsten Kontrollmaßnahmen erörtert werden.

1. Spontanes Aufsuchen am Arbeitsplatz

39 Ein spontanes Aufsuchen des Mitarbeiters am Arbeitsplatz ist **ohne weiteres zulässig** (allgemeine Meinung, vgl. nur MünchArbR/*Reichold* 3. Aufl. 2009, § 86 Rn. 7). 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. Ehrverletzende, **diskriminierende oder den Arbeitnehmer schikanierende Kontrollen sind 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 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, Brief und sonstige Schriftstücke s. Rn. 60, zum Zugriff auf den PC am Arbeitsplatz s. Rn. 49.

2. Tor- und Taschenkontrollen

40 Kraft seines Weisungsrechts (§ 106 S. 2 GewO) kann der Arbeitgeber **einseitig anordnen,** dass sich Arbeitnehmer Torkontrollen 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 Einkaufstaschen unzulässig sind, *BGH* NJW 1996, 2574). Stets ist dabei billiges Ermessen zu wahren. 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 Überwachungs- 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 DSGVO 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).

Bei Zugangskontrollen mittels **Erfassung biometrischer Daten (Iris-Scan, Fingerprint usw.)** i.S.d. Art. 9 DSGVO 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 **41**

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 Datenschutbeauftragten, 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 DSGVO 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.

3. Spindkontrollen

42 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 DSGVO gegen das Transparenzgebot. Die dort sichergestellten Beweismittel sind in einem anschließenden Gerichtsverfahren nicht verwertbar (*BAG* NZA 2014, 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

43 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. Sie müssen sich dort aufhalten, wo es der Arbeitgeber anordnet. Überdies wird der Arbeitnehmer durch die ständige Beobachtung einem „Anpassungszwang" ausgesetzt, dem er sich während seiner Tätigkeit nicht entziehen kann (*BAG* NZA 2003, 1193). Darin liegt ein Verstoß gegen das **allgemeine Persönlichkeitsrecht.** Dieses schützt den Arbeitnehmer vor einer lückenlosen technischen Überwachung am Arbeitsplatz. Folglich kann eine permanente Videoüberwachung weder auf das Direktionsrecht noch auf das Hausrecht des Arbeitgebers gestützt werden (*BAG* NZA 2004, 1278, 1283; NZA 2005, 839; *Bayreuther* NZA 2005, 1038, 1040; *Richardi/Kortstock* RdA 2005, 381, 382; *Tinnefeld/Viethen* NZA 2003, 468, 472). Die Aufnahmen sind nur dann 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 genügt es nicht, dass der Arbeitgeber schlicht überprüfen will, ob und wie gearbeitet wird. Vielmehr müssen **rechtlich geschützte Güter des Arbeitgebers schwerwiegend beeinträchtigt** sein, etwa durch gegen ihn gerichtete Straftaten (Diebstahl, Unterschlagung, Verrat von Betriebs- und Geschäftsgeheimnissen usw.). Weiterhin ist 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 darf sich zwar nicht auf die allgemeine Mutmaßung beschränken, es könnten Straftaten begangen werden, muss 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 genügt nicht (*LAG Baden-Württemberg* BB 1999, 1439). Die tatsächlichen Anhaltspunkte für den Verdacht sind zu dokumentieren (§ 26 Abs. 1 S. 2 BDSG). Inventurdifferenzen bei Betrieben des Einzelhandels begründen für sich allein noch keinen hinreichenden Anfangsverdacht, solange der Arbeitgeber nicht andere Ursachen für ein bestehendes Manko – z.B. Fehlbuchungen, Entwendung nicht im Verkaufs-, sondern im Lagerbereich – ausgeschlossen hat (*BAG* NZA 2014, 243, 249). Es bedarf konkreter Feststellungen, warum eine Videoüberwachung das praktisch einzig verbliebene Mittel darstellt, Unregelmäßigkeiten aufzuklären oder einen Verdacht in personeller Hinsicht weiter einzugrenzen (*BAG* NZA 2014, 243, 249). Befinden sich die zu überwachenden Arbeitsplätze in nicht öffentlich zugänglichen Räumen (z.B. Büros, Lagerräumen), gilt statt § 4 BDSG der § 26 Abs. 1 BDSG, der aber keine weitergehenden Voraussetzungen enthält (offengelassen von *BAG* NZA 2014, 243). 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).

44 Noch höher liegen die Anforderungen 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 DSGVO 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; zustimmend *Schlewing* NZA 2004, 1071; *Tinnefeld/Viethen* NZA 2002, 468, 472; tendenziell restriktiver *Däubler* Gläserne Belegschaften Rn. 299 ff.) – 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 DSGVO sind heimliche Mitarbeiterkontrollen unzulässig.** Sie bedürfen nach Art. 23 DSGVO einer ausdrücklichen gesetzlichen Regelung. § 26 BDSG genügt hierfür nicht (Rn. 19). 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 Video-

überwachung 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).

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 verdachtsunabhängigen und Torkontrolle kontrollierbar sind (*BAG* NZA 2014, 551, 555 f.). **45**

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). **46**

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 (*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.) nicht der Fall. 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 Kompetenzvertei- **47**

lung, 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. 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. 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. 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).

48 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).

5. Überwachung der IT-Nutzung

49 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 betriebliches 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-Verfahren 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 Whats-App 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).

50 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).

51 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.).

Hat der Arbeitgeber die **private Nutzung ausdrücklich gestattet oder duldet er sie zumindest,** gilt der Arbeitgeber als Anbieter von Telekommunikationsdiensten i.S.d. § 3 Nr. 6 TKG bzw. von Telemedien i.S.d. § 2 Nr. 1, § 11 TMG. Inhalts- sowie Verbindungsdaten der elektronischen Kommunikation unterfallen damit dem Telekommunikationsgeheimnis nach § 88 TKG, § 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; *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 Herrschaftsbereich 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 tatsäch- **52**

lich 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.).

53 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 § 88 TKG 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). Telekommunikationsrechtlich enthält § 94 TKG zwar eine Sondernorm für die notwendige Einwilligung. Mit Inkrafttreten der DSGVO gelten aber für die Unterrichtung und die Einwilligung – auch soweit die Verarbeitung von Beschäftigtendaten zu Überwachungszwecken betroffen ist – die Vorschriften der DSGVO. Zwar ermöglicht Art. 95 die weitere Anwendung der §§ 91 ff. TKG. Allerdings gilt dies nur für Vorschriften, die auf der Datenschutzrichtlinie für die elektronische Kommunikation (RL 2002/58/EG v. 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ePrivacy-RL) beruhen. Die Regelung über die elektronische Einwilligung (§ 94 TKG) gehört nicht dazu, weil sie sich darauf beschränkt, auf die Vorgaben der DSRL zu verweisen. Auch die e-Privacy-RL enthält keine eigenständige Regelung.

Maßgeblich für die Einwilligung ist also Art. 7 DSGVO (Buchner/Kühling/*Kühling/Raab* DSGVO Art. 95 Rn. 10). Knackpunkt ist dabei – wie so oft – die Freiwilligkeit (Art. 4 Nr. 11 DSGVO, § 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. Das ergibt sich aus § 88 Abs. 3 S. 3 TKG. Danach ist es dem Arbeitgeber als Anbieter von TK-Leistungen nur soweit erlaubt, sich Kenntnis vom Inhalt der TK verschaffen, wie dies für die Erbringung der Dienstleistung erforderlich ist. Für andere Zwecke dürfen diese Kenntnisse nicht verwendet werden, es sei denn, dass das TKG selbst oder eine andere gesetzliche Vorschrift dies erlaubt. Diese andere Vorschrift muss sich auf ausdrücklich auf TK-Vorgänge beziehen. Das ist aber nur selten der Fall. Das „kleine Zitiergebot" des § 88 Abs. 3 S. 3 TKG (Spindler/*Schuster* TKG § 88 Rn. 35) wird derzeit lediglich vom „G-10-Gesetz", den §§ 100a, 100b, und 100g ZPO und dem ZollfahndungsG beachtet. § 26 Abs. 1 BDSG erwähnt das TKG nicht und kommt deshalb als Zugriffsgrundlage nicht in Betracht. Dasselbe gilt für die Regelungen im TKG. § 88 Abs. 4 TKG scheidet regelmäßig aus, weil er nur die Anzeige bevorstehender Verbrechen erfasst, nicht aber die Aufklärung von Vergehen, zu denen die Delikte im Bereich der Wirtschaftskriminalität überwiegend gehören. Ebenso wenig zielführend ist § 100 Abs. 3 TKG. 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 Verwendung des betrieblichen Accounts zur Planung, Ausführung und Vorbereitung von anderen Straftaten zulasten des Arbeitgebers oder Dritten (*Mengel* NZA 2017, 1494, 1497). **54**

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 Vor- **55**

rang vor der DSGVO haben, deren Vorschriften sie „präzisieren und ergänzen" soll (Art. 1 Abs. 3 ePrivacyVO). Sie würde auch für den Arbeitgeber gelten, der seinen Leuten 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 DSGVO, 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 DSGVO. Wann die ePrivacyVO in Kraft tritt, ist allerdings ungewiss. Ursprünglich hatte die Kommission beabsichtigt, die ePrivacyVO zeitgleich mit der DSGVO 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. Wie ist weitergeht, ist zum Zeitpunkt der Drucklegung dieses Einführungstextes vollkommen offen. Es bleibt daher vorerst bei der derzeitigen Rechtslage.

56 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*).

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. **57**

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* NZA 2009, 646, 648). Geschehen sie heimlich, wird gegen das Transparenzgebot (Art. 5 Abs. 1 lit. a, Art 13 DSGVO) 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*) **58**

7. Telefonüberwachung

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, **59**

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

60 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 Dienst-

post 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.

9. Zuverlässigkeitstests

61 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 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.

62 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).

63 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

64 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 DSGVO) verstoßen. Vor Inkrafttreten der DSGVO 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 Vortäu-

schen 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 DSGVO kann daran nicht mehr festgehalten werden, jedenfalls solange der deutsche Gesetzgeber keine den Vorgaben des Art. 23 DSGVO 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). 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**.

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

66 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

67 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/Kun-*

ke § 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 DSGVO in Betracht, damit der Überwachte vor der Weiterverarbeitung zu geänderten Zwecken Einwände erheben kann (Kühling/Buchner/*Bäcker* DSGVO 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 erfüllt sind, dh 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 DSGVO), 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). Sind Ortungssysteme mit Arbeitsmitteln (Lkw/Bagger) verbunden, gilt § 26 Abs. 1, 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 unter-

liegt 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 DSGVO erhoben und genutzt werden (ausf. *Weichert* NZA 2017, 565).

V. Sanktionen

1. Überblick

Verstoßen Arbeitnehmer gegen Compliance-Vorschriften, kommt als Sanktion zu- **68**
nächst die **Abmahnung** in Betracht. Massivere Verfehlungen werden sich – wenn der überführte Mitarbeiter keinen Aufhebungsvertrag zu schließen bereit ist (s. dazu unten Rn. 92) – 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. 75 ff.). Wird ein Aufhebungsvertrag geschlossen, stellt sich die Frage nach seiner Wirksamkeit (unten Rn. 87 ff.). Können Arbeitnehmer nicht fristlos gekündigt werden, ist zumindest ihre **Suspendierung von der Arbeit** in Erwägung zu ziehen (unten Rn. 92 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

Mit der Abmahnung beanstandet der Arbeitgeber in einer für den Arbeitnehmer **69**
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.

70 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). **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.

71 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).

72 Vor Erteilung einer Abmahnung ist der Arbeitnehmer **anzuhören** (*BAG* AP Nr. 28 zu § 1 KSchG 1969 Verhaltensbedingte Kündigung). Ein Mitbestimmungsrecht des Betriebsrats besteht 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.

73 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 Verhaltensbeding-

te 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 zugrunde liegenden 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).

74 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). Dasselbe gilt, wenn das gerügte Verhalten für das Arbeitsverhältnis in jeder Hinsicht bedeutungslos geworden ist. Eine feste Frist gibt es dafür nicht. Entscheidend ist die Schwere der Pflichtverletzung (*BAG* NZA 2013, 91). Der Arbeitnehmer kann den Anspruch auf Entfernung 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 Arbeitgeber 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.

3. Außerordentliche Kündigung

a) Wichtiger Grund

75 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). 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).

76 **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 Rechtsprechung 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. 87) 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). **77**

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.). **78**

aa) Ultima ratio-Grundsatz

79 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

80 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

81 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**, 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.

82 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

83 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).

84 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 au-

ßerordentliche 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).

85 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). Der Arbeitgeber kann den Arbeitnehmer vor der Kündigung **anhören** – allerdings innerhalb einer kurz zu bemessenden Frist (im Regelfall binnen einer Woche, *BAG* AP Nr. 3, 6, 27 zu § 626 BGB Ausschlussfrist) – oder 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

86 **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 Kün-

digungsgründe 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

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). 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

87

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 Handlung, **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

88 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). 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). 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).

bb) Vorherige Anhörung

89 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). 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 ergeben 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* AP zu § 626 Nr. 25 BGB Verdacht strafbarer Handlung), 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).

90 **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). 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.** 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). 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

91 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).

5. Aufhebungsvertrag

92 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.

93 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).

94 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).

6. Freistellen von der Arbeit (Suspendierung)

95 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, § 9 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 Abs. 2 S. 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).

96 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 kon-

krete 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

97 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 Betriebsbuße 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).

98 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).

99 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: Zum Beschäftigtendatenschutz nach Inkrafttreten der DSGVO:

Asgari Datenschutz im Arbeitsverhältnis – Offenbarungspflicht/Fragerecht, Mitarbeiter-Screening und Datenschutzgrundverordnung, DB 2017, 1325; *Bettinghausen/Wiemers* Bewerberdatenschutz nach neuem Datenschutzrecht, DB 2018, 1277; *Bissels/Mayer-Michaelis/Schiller* Arbeiten 4.0: Big Data-Analysen im Personalbereich, DB 2016, 3042; *Byers* Die Zulässigkeit heimlicher Mitarbeiterkontrollen nach dem neuen Datenschutzrecht, NZA 2017, 1086; *Culik/Döpke* Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen, ZD 2017, 226; *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; *Dzida/Grau* Beschäftigtendatenschutz nach der Datenschutzgrundverordnung und dem neuen BDSG, DB 2018, 189; *Ehmann/Selmayr* Datenschutz-Grundverordnung. 2. Aufl. 2018; *Forst* Wer ist „Beschäftigter" i.S.d. § 3 Abs. 11 BDSG?, RDV 2014, 128; *Franck* Das System der Betroffenenrechte nach der DSGVO, RDV 2016, 111; *Franzen* DSGVO und Arbeitsrecht, EuZA 2017, 313; *Gaul/Pitzer* Das Gesetz zur Anpassung des Datenschutzrechts an die DSGVO. Was ändert sich im Beschäftigtendatenschutz?, ArbRB 2017, 241; *Göpfert/Papst* Digitale Überwachung mobiler Arbeit, DB 2016, 1015; *Gola* Datenschutz-Grundverordnung, 2. Aufl. 2018; *ders.* Der „neue" Beschäftigtendatenschutz nach § 26 BDSG n.F., BB 2017, 1462; *Gola/Jaspers* § 32 Abs. 1 BDSG – eine abschließende Regelung?, RDV 2009, 212; *Gola/Pötters/Thüsing* Art. 82 DSGVO: Öffnungsklausel für nationale Regelungen zum Beschäftigtendatenschutz – Warum der deutsche Gesetzgeber jetzt handeln muss, RDV 2016, 57; *Groß/Platzer* Whistleblowing: Keine Klarheit beim Umgang mit Informationen und Daten, NZA 2017, 1097; *Hromadka/Maschmann* Arbeitsrecht 2, 7. Aufl. 2016; *Körner* Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung, 2014; *dies.* Die Datenschutz-Grundverordnung und nationale Regelungsmöglichkeiten für Beschäftigtendatenschutz, NZA 2016, 1383; *Kort* Arbeitnehmerdatenschutz gemäß der EU-Datenschutz-Grundverordnung, DB 2016, 771; *ders.* Der Beschäftigtendatenschutz nach § 26 BDSG-neu, ZD 2017, 319; *Kühling/Buchner* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DSGVO/BDSG, 2. Aufl. 2018; *N. Maier* Der Beschäftigtendatenschutz nach der Datenschutz-Grundverordnung. Getrennte Regelungen für den öffentlichen und nicht öffentlichen Bereich?, DuD 2017, 169; *Maschmann* Datenschutzgrundverordnung: Quo vadis Beschäftigtendatenschutz?, DB 2016, 2488; *Paal/Pauly* Datenschutz-Grundverordnung Bundesdatenschutzgesetz. Kommentar, 2. Aufl. 2018; *Plath* DSGVO/BDSG, 3. Aufl. 2018; *Schmidl/Tannen* Das neue BDSG: die wichtigsten Regelungen für die Unternehmenspraxis, DB 2017, 1633; *Schneider* Schließt Art. 9 DSGVO die Zulässigkeit der Verarbeitung bei Big Data aus?, ZD 2017, 303; *Schrey/Kielkowski* Die datenschutzrechtliche Betriebsvereinbarung in DS-GVO und BDSG 2018 - Viel Lärm um Nichts?, BB 2018, 629-635; *Sörup* Gestaltungsvorschläge zur Umsetzung der Informationspflichten der

DSGVO im Beschäftigtenkontext, ArbRAktuell 2016, 207; *Sörup/Marquardt* Auswirkungen der EU-Datenschutzgrundverordnung auf die Datenverarbeitung im Beschäftigtenkontext, ArbRAktuell 2016, 103; *Spelge* Der Beschäftigtendatenschutz nach Wirksamwerden der Datenschutz-Grundverordnung (DSGVO). Viel Lärm um Nichts?, DuD 2016, 775; *Täger/Rose* Zum Stand des deutschen und europäischen Beschäftigtendatenschutzes, BB 2016, 819; *Thüsing* Beschäftigtendatenschutz und Compliance, 2. Aufl. 2014; *ders.* Umsetzung der Datenschutz-Grundverordnung im Beschäftigungsverhältnis: Mehr Mut zur Rechtssicherheit!, BB 2016, 2165; *Thüsing/Schmidt* Zulässige Pauschalierung bei der Rechtfertigung präventiver Überwachungsmaßnahmen des Arbeitgebers, NZA 2017, 1027; *Venetis/Oberwetter* Videoüberwachung von Arbeitnehmern, NJW 2016, 1051; *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; *Wurzberger* Anforderungen an Betriebsvereinbarungen nach der DSGVO, ZD 2017, 258; *Wybitul* 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 DSGVO, NZA 2017, 413; *Wybitul/Fladung* EU-Datenschutz-Grundverordnung – Überblick und arbeitsrechtliche Betrachtung des Entwurfs, BB 2012, 509, 515; *Wybitul/Pötters* Der neue Datenschutz am Arbeitsplatz, RDV 2016, 10; *Wybitul/Sörup/Pötters* Betriebsvereinbarungen und § 32 BDSG: Wie geht es nach der DSGVO weiter? – Handlungsempfehlungen für Unternehmen und Betriebsräte, ZD 2015, 559; *Zikesch/Reimer* Datenschutz und präventive Korruptionsbekämpfung – kein Zielkonflikt, DuD 2010, 96.

Zu weiteren Themen:
Altenburg/Leister Die Verwertbarkeit mitbestimmungswidrig erlangter Beweismittel im Zivilprozess, NJW 2006, 469; *Bauckhage-Hoffer/Katko* Compliance-Systeme und Datentransfer im Konzern, WM 2012, 486; *Bergwitz* Prozessuale Verwertungsverbote bei unzulässiger Videoüberwachung, NZA 2012, 353; *Bierekoven* Korruptionsbekämpfung vs. Datenschutz nach der BDSG-Novelle, CR 2010, 203; *Bloesinger* Grundlagen und Grenzen privater Internetnutzung am Arbeitsplatz, BB 2007, 2177; *Bongers* Mitarbeiterdatenscreening zur Terrorismusbekämpfung, ArbRAktuell 2009, 81; *Brink/Schmidt* Die rechtliche (Un-)Zulässigkeit von Mitarbeiterscreenings – Vom schmalen Pfad der Legalität, MMR 2010, 592; *Bürkle* Weitergabe von Informationen über Fehlverhalten in Unternehmen (Whistleblowing) und Steuerung auftretender Probleme durch ein Compliance-System, DB 2004, 2158; *Byers* Initiativrecht des Betriebsrats bei technischer Überwachung am Arbeitsplatz, RdA 2014, 37; *Dann/Gastell* Geheime Mitarbeiterkontrollen, NJW 2008, 2945; *Darsow/Schuster* Einführung von Ethikrichtlinien durch Direktionsrecht, NZA 2005, 273; *Däubler* Gläserne Belegschaften, 7. Aufl. 2017; *Däubler/Hjort/Schubert/Wolmerath* Handkommentar Arbeitsrecht, 4. Aufl. 2017; *Dölling (Hrsg.)* Handbuch der Korruptionsprävention, 2007, S. 87; *Dzida* Mitbestimmung des Konzernbetriebsrats bei Ethik-Richtlinien, NZA 2008, 1265; *Dzida/Grau* Verwertung von Beweismitteln bei Verletzung des Arbeitnehmerdatenschutzes, NZA 2010, 1201; *Erfurth* Die Betriebsvereinbarung im Arbeitnehmerdatenschutz, DB 2011, 1275; *Ernst* Social Networks und Arbeitnehmer-Datenschutz, NJOZ 2011, 953; *Etzel/Bader/Fischermeier* KR-Gemeinschaftskommentar zum Kündigungsschutzgesetz und zu sonstigen kündigungsschutzrechtlichen Vorschriften, 11. Aufl. 2016, zitiert: KR/*Bearbeiter*; *Forst* Beschäftigtendatenschutz im Kommissionsvorschlag einer EU-Datenschutzverordnung, NZA 2012, 364; *ders. Garding/Maier* Einsatz eines Privatdetektivs im Arbeitsrecht, DB 2010, 559; *Gastell/Dann* Geheime Mitarbeiterkontrollen, Straf- und arbeitsrechtliche Risiken bei

unternehmensinterner Aufklärung, NJW 2008, 2945; Germelmann/Matthes/Prütting Arbeitsgerichtsgesetz, 9. Aufl. 2017; *Gilch/Pelz* Compliance-Klauseln – gut gemeint aber unwirksam?, CCZ 2008, 131; *Grimm/Schiefer* Videoüberwachung am Arbeitsplatz, RdA 2009, 329; *Grimm/Strauf* Anmerkung zu BAG 24.03.2011, ZD 2011, 188; *Heinemann* Rechtswidrig erlangter Tatsachenvortrag im Zivilprozess, MDR 2001, 137; *Heldmann* Betrugs- und Korruptionsbekämpfung zur Herstellung von Compliance – Arbeits- und datenschutzrechtliche Sicht, DB 2010, 1235; *ders.* Betrugs- und Korruptionsbekämpfung zur Herstellung von Compliance – Arbeits- und datenschutzrechtliche Sicht, DB 2010, 1235; *Henssler/Willemsen/Kalb* Arbeitsrecht, 8. Aufl. 2018; *Kock/Francke* Mitarbeiterkontrolle durch systematischen Datenabgleich zur Korruptionsbekämpfung, NZA 2009, 646; *Kuhlen/Kudlich/Ortiz de Urbina* Compliance und Strafrecht, 2013; *Lingemann/Göpfert* Der Einsatz von Detektiven im Arbeitsrecht, DB 1997, 374; *Lunk* Prozessuale Verwertungsverbote im Arbeitsrecht, NZA 2009, 457; *Mahnhold* Compliance und Arbeitsrecht, 2003; *Maschmann (Hrsg.)* Beschäftigtendatenschutz in der Reform, 2012; *ders.* Compliance versus Datenschutz, NZA-Beilage 2012, 50; *ders.* Corporate Compliance und Arbeitsrecht, 2009;; *Maschmann/Sieg/Göpfert* Vertragsgestaltung im Arbeitsrecht, 2012; *Mengel* Arbeitsrechtliche Besonderheiten der Implementierung von Compliance-Programmen in internationalen Konzernen, CCZ 2008, 85; *Mengel/Hagemeister* Compliance und arbeitsrechtliche Implementierung, BB 2007, 1386; *Morgenroth* Verfassungsrechtliche Überlegungen zu Verwertungsverboten im Arbeitsrecht, NZA 2014, 408; *Müller* Die Zulässigkeit der Videoüberwachung am Arbeitsplatz, 2008; *Musielak/Voith* ZPO, 15. Aufl. 2018; *Mysliwiec/Löwisch* Soziale Netzwerke im Fadenkreuz des Arbeitsrechts, NJW 2011, 417; *Neufeld/Knitter* Mitbestimmung des Betriebsrats bei Compliance-Systemen, BB 2013, 821; *Salvenmoser/Hauschka* Korruption, Datenschutz und Compliance, NJW 2010, 331; *Schaub* Arbeitsrechts-Handbuch, 17. Aufl. 2017; *Scheben/Klos* Analyse von Chatprotokollen und E-Mails, CCZ 2013, 88; *Schlewing* Prozessuales Verwertungsverbot für mitbestimmungswidrig erlangte Erkenntnisse aus einer heimlichen Videoüberwachung?, NZA 2004, 1071; *Schmidt* E-Mail Compliance – revisionssichere Archivierung, DUD 2010, 96; *Schreiber* Das Sachvortragsverwertungsverbot, ZZP 2009, 227; *ders.* Implementierung von Compliance-Richtlinien, NZA-RR 2010, 617; *Schuster/Darsow* NZA 2005, 273, 275; *Simitis* BDSG, 8. Aufl. 2014; *Spindler/Schuster* Recht der elektronischen Medien, 2. Aufl. 2011; *Splittgerber/Fülbier* Keine (Fernmelde-)Geheimnisse vor dem Arbeitgeber?, NJW 2012, 1995; *Stück* Überwachung und Kontrolle von Arbeitnehmern nach neuer Rechtsprechung – Empfehlungen für Arbeitgeber im Brennpunkt von Compliance, Datenschutz und Arbeitsrecht, CCZ 2018, 88; *Wagner* Ethikrichtlinien – Implementierung und Mitbestimmung, 2008; *Wiese* Internet und Meinungsfreiheit des Arbeitgebers, Arbeitnehmers und Betriebsrats, NZA 2012, 1; *Wilke/Göpfert* Recherchen des Arbeitgebers in Sozialen Netzwerken nach dem geplanten Beschäftigtendatenschutzgesetz, NZA 2010, 1329.