Reihe | **Arbeitsrecht**

# BESCHÄFTIGTENDATEN-SCHUTZ UND DATENSCHUTZ-GRUNDVERORDNUNG IN DER PRAXIS


GESAMTMETALL
Die Arbeitgeberverbände der Metall- und Elektro-Industrie

# BESCHÄFTIGTEN-DATENSCHUTZ UND DATENSCHUTZ-GRUNDVERORDNUNG IN DER PRAXIS

1. Auflage

Reihe | Arbeitsrecht

**BESCHÄFTIGTENDATENSCHUTZ UND DATENSCHUTZ-GRUNDVERORDNUNG IN DER PRAXIS**

1. Auflage

von

**Eva Barlage-Melber**
BDA | Bundesvereinigung der Deutschen Arbeitgeberverbände
**Dr. Christoph Bausewein**
Rechtsanwalt und Syndikusrechtsanwalt | Konzerndatenschutzbeauftragter mit internationalem Zuständigkeitsbereich
**Martin Beckschulze**
Rechtsanwalt (Syndikusrechtsanwalt) | Fachanwalt für Arbeitsrecht
Arbeitgeberverbände Ruhr/Westfalen, Bochum
**Tobias Hohenadl**
Rechtsanwalt (Syndikusrechtsanwalt)
Arbeitgeberverband der Versicherungsunternehmen in Deutschland
**Manfred Monreal**
**Stephanie Montfort**
Rechtsanwältin
**Thomas Prinz**
Rechtsanwalt
BDA | Bundesvereinigung der Deutschen Arbeitgeberverbände
**Sibylle Talkenberg**
Gesamtmetall

Herausgegeben von:

**BDA | DIE ARBEITGEBER**
Bundesvereinigung der
Deutschen Arbeitgeberverbände, Berlin

**Arbeitgeberverband Gesamtmetall,** Berlin

Stand: Januar 2018

# VORWORT

Das Datenschutzrecht in der EU und damit auch in Deutschland ist im Umbruch. Nach fast vierjährigen Verhandlungen haben der Rat, das Europäische Parlament und die EU-Kommission sich im Dezember 2015 auf einen gemeinsamen Text für ein neues europäisches Datenschutzrecht geeinigt – die Datenschutz-Grundverordnung. Den Unternehmen wird zwei Jahre Zeit gegeben, sich auf die neue Rechtslage einzustellen. Die Vorgaben der Datenschutz-Grundverordnung müssen ab dem 25. Mai 2018 angewendet werden. Bis zu diesem Datum müssen die Unternehmen nicht nur ihre Prozesse zum Umgang mit personenbezogenen Daten von Kunden an die neue Rechtslage angepasst haben, sondern auch im Hinblick auf den Beschäftigtendatenschutz den Vorgaben genügen.

Der Beschäftigtendatenschutz ist ein Bereich, den der europäische Gesetzgeber den Mitgliedstaaten zur fakultativen spezifischeren Ausgestaltung anvertraut hat. Der deutsche Gesetzgeber hat diese Möglichkeit ergriffen und im Rahmen des „Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU" nationale Regelungen geschaffen, die ebenfalls ab dem 25. Mai 2018 geltendes Recht sein werden.

Die neue Rechtslage für den Schutz personenbezogener Daten verlangt den Unternehmen einiges ab. Eine sorgfältige Auseinandersetzung mit den neuen Rahmenbedingungen ist für die Arbeitgeber ein Muss. Bislang ist das nationale Datenschutzrecht der Dreh- und Angelpunkt, um personenbezogene Daten rechtssicher zu erheben, zu verarbeiten und zu nutzen. Zukünftig ist eine intensive Auseinandersetzung mit den Vorgaben der Datenschutz-Grundverordnung und des deutschen Rechts unumgänglich.

Auch wenn es an verschiedenen Stellen Neuerungen gibt, so bestehen gleichzeitig viele Parallelen zur bisherigen Rechtslage, so dass viele Prozesse aktualisiert, aber nicht neu aufgesetzt werden müssen. Diese Ausarbeitung soll hierbei unterstützen. Es werden verschiedenste Aspekte praxisnah beleuchtet, die für den Beschäftigtendatenschutz relevant sind. Alle Autoren und Autorinnen haben ihre Expertise im Datenschutzrecht eingebracht, um umfassend über die Herausforderungen für den Beschäftigtendatenschutz durch die neue Rechtslage zu informieren.

Berlin, im Januar 2018

# INHALTSVERZEICHNIS

**1. Neues Beschäftigtendatenschutzrecht – wo besteht wesentlicher Handlungsbedarf? ..... 11**

**2. Europäische Datenschutz-Grundverordnung im Überblick ..... 13**

**a. Ziele der DS-GVO – Art. 1 DS-GVO ..... 14**

**b. Sachlicher Anwendungsbereich der Datenschutz-Grundverordnung – Art. 2 DS-GVO. ..... 15**

**c. Räumlicher Anwendungsbereich der Datenschutz-Grundverordnung – Art. 3 DS-GVO. ..... 16**

**d. Grundsätze der Datenverarbeitung – Art. 5 DS-GVO. ..... 16**

aa. Rechtmäßigkeit. ..... 17
bb. Transparenz ..... 18
cc. Zweckbindung. ..... 18
dd. Datenminimierung ..... 19
ee. Richtigkeit ..... 20
ff. Speicherbegrenzung ..... 21
gg. Integrität und Vertraulichkeit ..... 22
hh. Rechenschaftspflicht ..... 22

**e. Rechtmäßigkeit der Verarbeitung – Art. 6 DS-GVO ..... 23**

aa. Verarbeitungen von personenbezogenen Daten im Beschäftigtenkontext ..... 26
(1) Die Erfüllung des (Arbeits-)Vertrags mit der betroffenen Person bzw. einer vorvertraglichen Verpflichtung – Art. 6 Abs. 1 lit. b) DS-GVO. ..... 26
(2) Der Rechtsgrund der Wahrnehmung berechtigter Interessen – Art. 6 Abs. 1 lit. f) DS-GVO ..... 27
(3) Einwilligung der betroffenen Person – Art. 6 Abs. 1 lit. a) DS-GVO ..... 28
(4) Weiterverarbeitung nach einer Zweckänderung ..... 28

**f. Besondere Kategorien personenbezogener Daten – Art. 9 DS-GVO ..... 29**

**g. Rechte der betroffenen Person – Art. 12 ff. DS-GVO ..... 30**

**h. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen – Art. 25 DS-GVO ..... 30**

**i. Gemeinsam für die Verarbeitung Verantwortliche – Art. 26 DS-GVO . . . . . 32**
**j. Auftragsverarbeiter – Art. 28, 29 DS-GVO . . . . . 35**
**k. Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO . . . . . 36**
**l. Meldung von Verletzungen des Schutzes personenbezogener Daten – Art. 33, 34 DS-GVO . . . . . 37**
**m. Datenschutz-Folgenabschätzung – Art. 35 DS-GVO . . . . . 39**
**n. Datenverarbeitung im Beschäftigungskontext – Art. 88 DS-GVO . . 42**
aa. Mitgliedstaatliche Regelungen zum Beschäftigtendatenschutz . . . . . 42
bb. Inhaltliche Ausgestaltung . . . . . 43
**o. Verhängung von Geldbußen – Art. 83 DS-GVO . . . . . 45**

**3. Grundlagen des Beschäftigtendatenschutzes ab Mai 2018 . . . . . 48**
**a. Geltungsbereich des Beschäftigtendatenschutzes . . . . . 48**
aa. Beschäftigtenbegriff – § 26 Abs. 8 BDSG . . . . . 48
bb. Datenverarbeitung ohne Dateisystem – § 26 Abs. 7 BDSG . . . . . 50
**b. Die Verarbeitung personenbezogener Daten von Beschäftigten. . . 52**
aa. Verarbeitung von Beschäftigtendaten – § 26 Abs. 1 BDSG . . . . . 52
(1) Der in Art. 88 DS-GVO gesetzte Rahmen für spezifischere nationale Regelungen . . . . . 52
(2) Zulässige Verarbeitungszwecke . . . . . 53
(3) Der Verarbeitungsbegriff . . . . . 58
(4) Erforderlichkeit als Prüfungsmaßstab . . . . . 58
(5) Verhältnis des § 26 BDSG zu anderen bundesrechtlichen Regelungen zum Datenschutz . . . . . 59
bb. Videoüberwachung von Mitarbeitern . . . . . 59
(1) Offene Videoüberwachung öffentlich zugänglicher Räume . . . . . 59
(2) Offene Videoüberwachung nicht öffentlich zugänglicher Räume . . . . . 61
(3) Verdeckte Videoüberwachung öffentlich zugänglicher Räume . . . . . 62
(4) Verdeckte Videoüberwachung nicht öffentlich zugänglicher Räume . . . . . 63

**c. Regelung der Datenverarbeitung durch Kollektivvereinbarungen . . . . . 63**

**d. Datenverarbeitung auf der Grundlage einer Einwilligung – Art. 7 DS-GVO, § 26 Abs. 2 BDSG . . . . . 69**

aa. Zulässigkeit . . . . . 69
bb. Freiwilligkeit . . . . . 70
cc. Regelbeispiele des § 26 Abs. 2 BDSG . . . . . 72
dd. Inhalt – Informierte Einwilligung . . . . . 73
ee. Form der Einwilligung . . . . . 76
(1) Regelungsbefugnis des deutschen Gesetzgebers . . . . . 77
(2) Ausnahme von der Schriftform . . . . . 78
ff. Widerrufsrecht . . . . . 79
gg. Verhältnis zum Fragerecht des Arbeitgebers . . . . . 80
hh. Schicksal bereits vor dem 25. Mai 2018 erteilter Einwilligungen . . . . . 81
ii. Ausgewählte Praxisfragen . . . . . 82
(1) Betriebliches Eingliederungsmanagement – BEM . . . . . 82
(2) Arbeitsschutzrechtliche Untersuchungen . . . . . 84
(3) Private Internet- und E-Mailnutzung . . . . . 89
(4) Bewerbungsgespräche via videobasiertem Internetangebot . . . . . 92

**e. Umgang mit besonderen Kategorien personenbezogener Daten . . . . 93**

aa. Begriffsbestimmung . . . . . 93
bb. Rechtsgrundlage für den Umgang mit besonderen Kategorien personenbezogener Beschäftigtendaten in Deutschland . . . . . 94
cc. Bedingungen für den Umgang mit besonderen Kategorien personenbezogener Beschäftigtendaten . . . . . 95
dd. Einwilligung des Beschäftigten in die Verarbeitung sensitiver Daten . . . . . 99
ee. Verarbeitung von sensitiven Beschäftigtendaten durch Auftragsverarbeiter . . . . . 102

**4. Rechte der betroffenen Person ..... 104**

**a. Grundsätze für die Realisierung der Rechte der betroffenen Personen nach der DS-GVO ..... 104**

aa. Vorgaben zur Kommunikation mit den Betroffenen ..... 104

bb. Anträge auf Grundlage der Art. 15 bis 22 DS-GVO – Identitätsprüfung ..... 106

cc. Erleichterung der Rechtsausübung – Art. 12 Abs. 2 Satz 1 DS-GVO ..... 107

dd. Frist für die Bearbeitung von Anträgen ..... 107

ee. Grundsätzliche Kostenfreiheit – Art. 12 Abs. 5 DS-GVO ..... 108

ff. Benachrichtigung von Datenempfängern über getroffene Maßnahmen – Art. 19 DS-GVO ..... 109

**b. Informationspflichten des Verantwortlichen ..... 109**

aa. Informationsinhalte bei der Direkterhebung – Art. 13 DS-GVO ..... 110

bb. Ausnahmen von der Informationspflicht nach Art. 13 DS-GVO ..... 114

cc. Informationsinhalte und Frist bei der indirekten Erhebung – Art. 14 DS-GVO ..... 114

dd. Ausnahmen von der Informationspflicht nach Art.14 Abs. 5 DS-GVO ..... 114

ee. Nationale Ausnahmen ..... 115

ff. Weiterverarbeitung bei Zweckänderung ..... 115

(1) Grundsätzliche Pflicht zur Information über Zweckänderung, Art. 13 Abs. 3 und Art. 14 Abs. 4 DS-GVO ..... 115

(2) Ausnahmen gemäß § 32 BDSG ..... 115

**c. Wichtige Betroffenenrechte ..... 116**

aa. Auskunftsrecht – § 34 BDSG, Art. 15 DS-GVO ..... 116

bb. Art. 16 DS-GVO – Recht auf Berichtigung ..... 118

cc. Recht auf Löschung – § 35 BDSG, Art. 17 DS-GVO ..... 119

(1) Neue und alte Löschungsrechte ..... 119

(2) Weiterentwicklung des Rechts auf „Vergessenwerden" ... 121

(3) Keine Regel ohne Ausnahme ..... 122

(4) Umsetzung der Löschungsverpflichtung ..... 123

dd. Einschränkung der Datenverarbeitung – § 35 BDSG, Art. 18 DS-GVO ..... 124

ee. Art. 20 DS-GVO – Recht auf Datenübertragbarkeit ..... 125

**5. Verarbeitung von Beschäftigtendaten durch Auftragsverarbeiter ... 126**
**a. Die europäische Konzeption der Auftragsverarbeitung ... 127**
**b. Auswahl eines qualifizierten Auftragsverarbeiters ... 127**
**c. Vertrag als Grundlage der Auftragsverarbeitung ... 128**
**d. Weitere Auftragsverarbeiter – Unterbeauftragung ... 130**
**e. Teilweise neue weitere Pflichten des Auftragsverarbeiters ... 131**
**f. Bußgelder ... 131**

**6. Übermittlung von Beschäftigtendaten im Konzern ... 132**
**a. „Konzern" im Sinne der Datenschutz-Grundverordnung ... 132**
**b. Konzerninterne Datenübermittlung bei Funktionsübertragung ... 132**
**c. Auftragsverarbeitung ... 134**
**d. Gemeinsame Verantwortlichkeit ... 134**
**e. Konzerndatenschutzbeauftragter ... 135**

**7. Übermittlung von Beschäftigtendaten in Drittländer ... 136**
**a. Länder mit einem adäquaten Datenschutzniveau – Art. 46 DS-GVO ... 138**
**b. Übermittlungen auf der Grundlage von „geeigneten Garantien" – Art. 46 DS-GVO ... 139**
**c. Gesetzliche Ausnahmetatbestände – Art. 49 DS-GVO ... 140**

**8. Der betriebliche Datenschutzbeauftragte ... 142**
**a. Benennungspflicht ... 142**
**b. Verantwortliche bei der Einhaltung des Datenschutzes ... 144**
**c. Stellung des Datenschutz-Beauftragten – Art. 38 DS-GVO ... 146**
**d. Rechtsfolgen bei Verstoß ... 146**
**e. Anforderungen an die Benennung ... 146**
aa. Qualifikationen und persönliche Voraussetzungen; Benennung des Datenschutzbeauftragten – Art. 37 DGSVO ... 146
bb. Form und Dauer der Benennung ... 148
cc. Möglichkeit der externen Benennung ... 149
dd. Möglichkeit der Benennung eines Konzern-Datenschutzbeauftragten ... 149

**f. Stellung des Datenschutzbeauftragten ..... 150**
aa. Unabhängigkeit ..... 150
bb. Abberufungsschutz und Benachteiligungsverbot ..... 151
cc. Unterstützung, Einbindung und Fortbildung ..... 153
dd. Geheimhaltungspflicht und Vertraulichkeit ..... 154
**g. Aufgaben ..... 154**
aa. Unterrichtung und Beratung ..... 154
bb. Überwachung der Einhaltung des Datenschutzes ..... 155
cc. Datenschutz-Folgenabschätzung ..... 155
dd. Zusammenarbeit mit der Aufsichtsbehörde ..... 156
ee. Pflicht zur risikoorientierten Tätigkeit ..... 156

**9. Die Rolle des Betriebsrats bei der Datenverarbeitung .... 156**
**a. Die datenschutzrechtliche Verantwortung des Betriebsrats ..... 156**
**b. Beteiligungsrechte der Interessenvertretung – § 26 Abs. 6 BDSG ..... 158**
**c. Datenverarbeitung durch den Betriebsrat ..... 161**

**10. Anhang 1 – Synopse BDSG bis Mai 2018, BDSG ab Mai 2018, DS-GVO ..... 164**

## Weitere Anhänge:

**Anhang 2 – Muster für ein Informationsblatt zur Verarbeitung von Beschäftigtendaten**

**Anhang 3 – Muster für eine Rahmenbetriebsvereinbarung zur Anpassung des betrieblichen Datenschutzes an die DS-GVO und das BDSG**

**Anhang 4 – Muster für eine Rahmenbetriebsvereinbarung im Hinblick auf die Vorgaben der DS-GVO und des BDSG**

**Anhang 5 – Muster für eine Verpflichtung auf das Datengeheimnis und Merkblatt**

**Anhang 6 – Prozessbeschreibung zu den Themen Auskunftsanspruch, Löschung, Berichtigung**

**Anhang 7 – Muster für eine Rahmenbetriebsvereinbarung über die Einführung und Nutzung von DVM**

**Anhang 8 – Muster für eine Betriebsvereinbarung zur privaten und betrieblichen Nutzung einzelner DVM**

# 1. NEUES BESCHÄFTIGTENDATENSCHUTZRECHT – WO BESTEHT WESENTLICHER HANDLUNGSBEDARF?

Ab dem 25. Mai 2018 wird die Datenschutz-Grundverordnung (DS-GVO) anzuwenden sein. Gleichzeitig wird das angepasste Bundesdatenschutzgesetz (BDSG) in Kraft treten. In dieser Ausarbeitung wird das Bundesdatenschutzgesetz, das ab dem 25. Mai 2018 anzuwenden ist, als „BDSG" bezeichnet. Demgegenüber wird das Bundesdatenschutzgesetz, das bis zu diesem Datum gilt, als „BDSG a. F." bezeichnet.

Viele der dort vorgesehenen Pflichten sind Unternehmen bereits aus dem BDSG unmittelbar oder zumindest in modifizierter Form bekannt. Gleichzeitig sehen die rechtlichen Vorgaben auch Neuerungen vor, die bei der Anpassung der unternehmensinternen Regelungen zu berücksichtigen sind.

Bei folgenden Punkten sollten Sie prüfen, ob sich hieraus aufgrund der DS-GVO bzw. des BDSG ein Handlungsbedarf für Sie ergibt:

- **Personalverwaltungsprozesse:** Alle Personalverwaltungsprozesse sind zu überprüfen und ggf. anzupassen.
- **Betriebsvereinbarungen:** Arbeitgeber sollten alle bestehenden Betriebsvereinbarungen auf die DS-GVO hin überprüfen und ggf. anpassen - hier erscheint eine Rahmenbetriebsvereinbarung sinnvoll.
- **Rechtsgrundlagen von Verarbeitungsvorgängen:** Es sind die Rechtsgrundlagen zu prüfen, auf die die Verarbeitung gestützt wird. Dies ist notwendig, um die Betroffenen entsprechend informieren zu können.
- **Rechenschaftspflicht:** Der Arbeitgeber muss nachweisen können, dass er die Vorgaben der DS-GVO einhält.
- **Einwilligung:** Alte Einwilligungen sind zu prüfen, insbesondere auf Freiwilligkeit, Zweckbindung und unkonditioniertes Widerspruchsrecht. Neue Einwilligungen sind anhand der Checkliste unter (Kapitel 3, d. dd.) zu gestalten.
- **Besondere Kategorien personenbezogener Daten:** Arbeitgeber müssen die Verarbeitung genetischer und biometrischer Daten zur eindeutigen Identifizierung einer Person (z. B. Authentifizierungs- und Zutrittskontrollsysteme) künftig auf die Einwilligung Art. 6 Abs. 1 lit. a) und Art. 9 Abs. 2 lit a) DS-GVO stützen. Alternativ kann geprüft werden, ob eine solche Datenverarbeitung auf eine andere Rechtsgrundlage i. S. v. Art. 6 DS-GVO gestützt werden kann und Art. 9 Abs. 2 lit. b) DS-GVO i. V. m. § 26 Abs. 3 BDSG vorliegt.

- **Behandlung von Eingaben:** Arbeitgeber sollten einen Prozess zur Behandlung von Eingaben der Betroffenen schaffen. Dabei sollten Eingangskanäle und Verantwortlichkeiten definiert werden, um sicherzustellen, dass die Eingaben innerhalb der gesetzlich vorgesehenen Frist bearbeitet werden.
- **Informationspflichten:** Insbesondere im Rahmen der bestehenden Arbeitsverträge und in der Bewerbungsphase ist die Erweiterung der Informationspflichten gegenüber dem Betroffenen zu beachten.
- **Löschung:** Bestehende Löschkonzepte im Beschäftigtenbereich sind zu überprüfen.
- **Gemeinsam für die Verarbeitung Verantwortliche:** Mehrere Verantwortliche können gemeinsam Zwecke und Mittel der Verarbeitung festlegen.
- **Verarbeitung im Auftrag:** Sind Auftragsverarbeiter eingeschaltet oder ist dies geplant, ist mit diesen eine schriftliche Vereinbarung über die Details des Auftrags abzuschließen.
- **Verzeichnis von Verarbeitungstätigkeiten:** Arbeitgeber und Auftragsverarbeiter haben ein Verzeichnis zu führen, in das alle Verarbeitungen eingetragen werden, für die sie zuständig sind.
- **Meldung von Datenschutzverstößen:** Es bestehen umfangreiche Meldeverpflichtungen innerhalb der kurzen Frist von 72 Stunden bei Datenschutzverletzungen, die voraussichtlich zu einem Risiko für Rechte und Freiheiten natürlicher Personen führen werden.
- **Datenschutz-Folgenabschätzung:** Führt die Datenverarbeitung zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen, das nicht eingedämmt wird, folgt ein Konsultationsverfahren mit der Aufsichtsbehörde, in welchem umfassende Informationen zur Verfügung gestellt werden müssen. Arbeitgeber sollten sich deshalb frühzeitig Gedanken über die Risiken machen, die die Verarbeitung für die Rechte und Freiheiten der betroffenen Person haben kann.
- **Verhängung von Geldbußen:** Es werden hohe Geldbußen von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes eines Unternehmens eingeführt und Kriterien festgelegt, an denen sich Aufsichtsbehörden bei der Festsetzung der Höhe der Geldbuße orientieren. Auch der Verstoß gegen die Pflichten zur Ergreifung geeigneter technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten stellt eine Ordnungswidrigkeit dar.
- **Videoüberwachung öffentlich zugänglicher Räume:** Bei der Videoüberwachung bestimmter Anlagen und Einrichtungen wie Einkaufszentren gelten der Schutz von Leben, Gesundheit, Freiheit dort aufhältiger Personen als besonders wichtiges Interesse.
- **Beschäftigtenbegriff – Leiharbeitnehmer:** Die Datenerhebung in Bezug auf Leiharbeitnehmer ist gleichlaufend mit Beschäftigten des Stammbetriebes zu gestalten und entsprechend in das Verzeichnis für Verarbeitungstätigkeiten aufnehmen.

- **Benennung Datenschutzbeauftragter:** Aufgrund der Ausweitung der Benennungspflicht sollten auch Unternehmen mit weniger als zehn Mitarbeitern prüfen, ob sie zukünftig verpflichtet sind, einen Datenschutzbeauftragten zu bestellen. Zudem sollte ggf. dokumentiert werden, warum ein Datenschutzbeauftragter nicht bestellt wird und regelmäßig überprüft werden, ob die Voraussetzungen für die Benennung eines Datenschutzbeauftragten entstehen. Die Kontaktdaten des Datenschutzbeauftragten müssen veröffentlicht und der Aufsichtsbehörde mitgeteilt werden.

## 2. EUROPÄISCHE DATENSCHUTZ-GRUNDVERORDNUNG IM ÜBERBLICK

Die DS-GVO ersetzt die aus dem Jahr 1995 stammende Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Diese Richtlinie wird mit Wirkung zum 25. Mai 2018 aufgehoben werden. Selbiges gilt für die auf ihrer Grundlage geschaffenen nationalen Datenschutzgesetze, wie das BDSG a. F.

Die DS-GVO gilt als Verordnung in allen europäischen Mitgliedstaaten unmittelbar und vorrangig vor nationalen Regelungen. Damit genießt sie Anwendungsvorrang vor dem nationalen Recht. Der europäische Gesetzgeber hat in der DS-GVO Öffnungsklauseln vorgesehen, die den Mitgliedstaaten die Möglichkeit geben, eigenständige nationale Regelungen in bestimmten Bereichen zu treffen. So können z. B. auf der Grundlage von Art. 88 DS-GVO die Mitgliedstaaten spezifischere Vorschriften zur Datenverarbeitung im Beschäftigungskontext vorsehen.

**PRAXISTIPP**
§ 1 Abs. 5 BDSG regelt, dass das BDSG nur dann anzuwenden ist, wenn die DS-GVO nicht unmittelbar gilt. Deshalb muss der erste Blick des Unternehmens in die DS-GVO gehen. Wenn es um einen Sachverhalt geht, der dort ohne Öffnungsmöglichkeit für die Mitgliedstaaten geregelt ist, wie z. B. die Auftragsverarbeitung in Art. 28 DS-GVO oder das Führen eines Verzeichnisses von Verarbeitungstätigkeiten in Art. 30 DS-GVO, regelt die DS-GVO unmittelbar, was zu tun ist. Für andere Bereiche muss zusätzlich das BDSG herangezogen werden. Das gilt gerade für den Beschäftigtendatenschutz, für den insbesondere § 26 BDSG relevant ist. Wie bislang gehen andere Rechtsvorschriften des Bundes über den Datenschutz den Vorschriften des BDSG vor, wie z. B. die Vorgaben in den Sozialgesetzbüchern und der Abgabenordnung, so dass auch diese Regelungen zu berücksichtigen sind.

Dieser Systematik entsprechend sind Ausführungen des Düsseldorfer Kreises als Gremium insbesondere zur Koordinierung der deutschen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich für den Beschäftigtendatenschutz im Hinblick auf das deutsche Recht wichtig. Im Hinblick auf die Auslegung der DS-GVO insgesamt ist aber bislang die Artikel-29-Datenschutzgruppe maßgeblich. Sie ist das gesetzlich vorgesehene Gremium der Datenschutzbehörden aus den EU-Mitgliedstaaten, das insbesondere beratende und prüfende Funktionen erfüllt. Durch die DS-GVO wird die Artikel-29-Datenschutzgruppe durch den „Europäischen Datenschutzausschuss" ersetzt werden, der für die einheitliche Anwendung der DS-GVO zuständig ist.

Zur Zeit läuft noch der Übernahmeprozess der DS-GVO in das Abkommen über den Europäischen Wirtschaftsraum, der neben den EU-Mitgliedstaaten Island, Liechtenstein und Norwegen umfasst. Solange der Übernahmeprozess nicht abgeschlossen ist, ist für diese drei Länder jeweils ihr nationales Datenschutzrecht maßgeblich.

Neben der Kernregelung zum Beschäftigtendatenschutz in der Datenschutz-Grundverordnung – Art. 88 DS-GVO – und insbesondere den auf dieser Grundlage erlassenen Regelungen im BDSG müssen Arbeitgeber auch die weiteren Vorgaben der DS-GVO beachten, um den Festsetzungen zum Datenschutz zu genügen. Dieses Kapitel geht auf wichtige Teilbereiche der DS-GVO ein und bietet einen ersten Überblick über die Vorschriften, die ab dem 25. Mai 2018 angewendet werden müssen. Dabei wird immer wieder auch auf die Erwägungsgründe zur DS-GVO hingewiesen. Bei den Erwägungsgründen handelt es sich um die Begründung für die Artikel der DS-GVO. Sie erläutern, auf der Grundlage welcher Überlegungen die Artikel verfasst wurden. Die Erwägungsgründe dienen deshalb der Auslegung der Artikel der DS-GVO, ohne dass aus ihnen unmittelbare Rechtsfolgen abgeleitet werden können.

## a. Ziele der DS-GVO – Art. 1 DS-GVO

Die DS-GVO zielt gemäß Art. 1 darauf ab, den Schutz von personenbezogenen Daten innerhalb der Europäischen Union sicherzustellen. Gleichzeitig soll die DS-GVO den freien Datenverkehr innerhalb der Europäischen Union gewährleisten. Damit werden zwei gleichrangige Ziel verfolgt: Der Schutz der Grundrechte und Grundfreiheiten, insbesondere das Recht auf Schutz personenbezogener Daten auf der einen Seite und die Vollendung des Binnenmarkts durch Gewährleistung des freien Verkehrs auf der anderen Seite.

## b. Sachlicher Anwendungsbereich der Datenschutz-Grundverordnung – Art. 2 DS-GVO

Art. 2 DS-GVO geht auf den sachlichen Anwendungsbereich der Verordnung ein. Danach ist die DS-GVO zunächst für die automatisierte Verarbeitung personenbezogener Daten anzuwenden. Die Definition von „personenbezogene Daten" findet sich in Art. 4 Nr. 1 DS-GVO. Ob die personenbezogenen Daten vollständig oder nur teilweise automatisiert verarbeitet werden, spielt dabei keine Rolle, beide Fälle werden vom Anwendungsbereich der Verordnung erfasst.

Die nichtautomatisierte Verarbeitung personenbezogener Daten fällt unter die Vorgaben der Datenschutz-Grundverordnung, wenn diese Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Was unter einem „Dateisystem" zu verstehen ist, wird in Art. 4 Nr. 6 DS-GVO definiert. Danach handelt es sich hierbei um „jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird". Voraussetzung ist also, dass eine strukturierte Sammlung vorliegt. Aus Erwägungsgrund 15 DS-GVO ergibt sich, dass dementsprechend Akten oder Aktensammlungen sowie ihre Deckblätter nicht vom Anwendungsbereich der Verordnung umfasst sind, sofern sie nicht nach bestimmten Kriterien geordnet sind.

**HINWEIS**

Für den Beschäftigtendatenschutz in Deutschland muss allerdings eine Besonderheit beachtet werden. Die Vorgaben von § 26 Abs. 1 bis 6 BDSG für die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses sind auch dann anzuwenden, wenn personenbezogene Daten von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen.[1] Diese ausdrückliche Vorgabe ergibt sich aus § 26 Abs. 7 BDSG. Das bedeutet, dass unstrukturierte Sammlungen von Beschäftigtendaten, wie z. B. spontane handschriftliche Aufzeichnungen in Vorstellungsgesprächen oder in einer sogenannten „Meisterkladde", wie bisher nur dann zulässig sind, wenn sie gemäß § 26 Abs. 1 BDSG zur Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich sind.

Für weitere Ausführungen hierzu siehe „Datenverarbeitung ohne Dateisystem" Seite 50.

[1] Siehe hierzu auch DSK, Kurzpapier Nr. 14 zu "Beschäftigtendatenschutz", abzurufen unter: https://www.lda.bayern.de/media/dsk_kpnr_14_beschaeftigtendatenschutz.pdf.

## c. Räumlicher Anwendungsbereich der Datenschutz-Grundverordnung – Art. 3 DS-GVO

Mit der Datenschutz-Grundverordnung wird der Anwendungsbereich des europäischen Datenschutzrechts erheblich ausgeweitet.

**HINWEIS**
Das bedeutet, dass die Änderungen des EU-Datenschutzrechts durch die DS-GVO auch außerhalb der EU relevant sein können. Findet die Verarbeitung personenbezogener Daten in einer Niederlassung außerhalb der EU statt, müssen international agierende Unternehmen deshalb prüfen, ob die Vorgaben der Datenschutz-Grundverordnung auf sie Anwendung finden.

Nach dem in Art. 3 Abs. 2 DS-GVO neu geregelten „Marktortprinzip" muss die DS-GVO auch dann angewendet werden, wenn Verantwortlicher oder Auftragsverarbeiter zwar keine Niederlassung in der EU haben, die Verarbeitung der personenbezogenen Daten durch den Verantwortlichen oder Auftragsverarbeiter aber dazu dient, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten.[2] Das kann entgeltlich oder unentgeltlich erfolgen. Die DS-GVO findet auch dann Anwendung, wenn Verantwortlicher oder Auftragsverarbeiter das Verhalten der betroffenen Person in der EU beobachten. Nach Erwägungsgrund 24 Satz 2 DS-GVO ist darunter zu verstehen, ob ihre Internetaktivitäten nachvollzogen werden. Somit erfasst die Datenschutz-Grundverordnung jede Form des Webtrackings z. B. durch Cookies oder Social Plug-ins soweit das Verhalten der Personen in der EU erfolgt.[3]

## d. Grundsätze der Datenverarbeitung – Art. 5 DS-GVO

Art. 5 DS-GVO ist eine der zentralen Vorschriften der Datenschutz-Grundverordnung. Hier werden Grundsätze formuliert, an denen sich jede Datenverarbeitung ausrichten muss. Viele dieser Vorgaben sind bereits aus dem bisherigen Datenschutzrecht bekannt. Hierzu zählen z. B. die Grundsätze der Rechtmäßigkeit und der Datensparsamkeit. Neu hinzugekommen ist insbesondere die in Art. 5 Abs. 2 DS-GVO geregelte Rechenschaftspflicht des Verantwortlichen, der die Einhaltung

[2] Siehe hierzu DSK, Kurzpapier Nr. 7 zu „Marktortprinzip", abzurufen unter: https://www.lda.bayern.de/media/dsk_kpnr_7_marktortprinzip.pdf.

[3] Ehrmann/Selmayr/*Zerdick,* DS-GVO, Art. 3 Rn. 19.

der Grundsätze der Datenverarbeitung nachweisen können muss. Ein Verstoß gegen die Vorgaben von Art. 5 DS-GVO kann gravierende Folgen haben. Gemäß Art. 83 Abs. 5 DS-GVO kann er mit Geldbußen bis zu 20 Mio. Euro oder im Falle eines Unternehmens mit bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes sanktioniert werden, je nachdem, welcher der Beträge höher ist.

**PRAXISTIPP**
Die DS-GVO sieht keine Verpflichtung auf das Datengeheimnis vor. Gleichwohl ist zu empfehlen, die bisherige Praxis der Verpflichtung der Mitarbeiter auf die einzuhaltenden Regeln wegen der Rechenschaftspflicht beizubehalten. Eine Verpflichtung auf das Datengeheimnis, wie es § 5 BDSG a. F. vorsieht, gibt es nach der DS-GVO zwar nicht. Die in Art. 5 Abs. 2 DS-GVO vorgesehene Rechenschaftspflicht wird aber insbesondere in Art. 24 DS-GVO konkretisiert. Danach muss die verantwortliche Stelle geeignete technische und organisatorische Maßnahmen ergreifen, um sicherzustellen und den Nachweis erbringen zu können, dass die Verarbeitung gemäß der DS-GVO erfolgt. Eine dieser Maßnahmen kann auch die Verpflichtung der Mitarbeiter auf die einzuhaltenden Regeln sein. Zudem ergibt sich aus Art. 29 DS-GVO, dass dem Verantwortlichen unterstellte Personen personenbezogene Daten nur auf Weisung des Verantwortlichen verarbeiten dürfen. Für Auftragsverarbeiter ergibt sich eine solche Verpflichtung zudem aus Art. 28 Abs. 3 lit. b) DS-GVO, wonach sie sicherzustellen haben, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet sind.

Für ein Muster hierzu siehe Anhang 5.

Die grundlegende Bedeutung dieser Regelung hat den deutschen Gesetzgeber bewogen, in § 26 Abs. 5 BDSG ausdrücklich auf Art. 5 der Datenschutz-Grundverordnung hinzuweisen. Danach muss im Bereich des Beschäftigtendatenschutzes der Verantwortliche geeignete Maßnahmen ergreifen, um insbesondere die Verarbeitungsgrundsätze in Art. 5 DS-GVO sicherzustellen.

**aa. Rechtmäßigkeit**

Die personenbezogenen Daten müssen „auf rechtmäßige Weise" verarbeitet werden, Art. 5 Abs. 1 lit. a) DS-GVO. Wann das der Fall ist, ergibt sich aus Art. 6 Abs. 1 DS-GVO. Eine Verarbeitung ist dann rechtmäßig, wenn einer der in Art. 6 Abs. 1 DS-GVO vorgesehenen Erlaubnistatbestände vorliegt, andernfalls ist die Verarbei-

tung verboten. An diesem aus dem BDSG bereits bekannten „Verbot mit Erlaubnisvorbehalt" ändert sich durch die Datenschutz-Grundverordnung somit nichts. Zudem sieht die Datenschutz-Grundverordnung weitere Vorschriften für besondere Verarbeitungssituationen vor. Für den Beschäftigtendatenschutz ist Art. 88 DS-GVO von zentraler Bedeutung, auf dessen Grundlage Deutschland in § 26 BDSG spezifischere Vorschriften für den Beschäftigtendatenschutz geschaffen hat.

Für weitere Ausführungen zu Art. 6 DS-GVO siehe „Rechtmäßigkeit der Verarbeitung" Seite 23.

**bb. Transparenz**

Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Sie sollte wissen, dass Daten über sie verarbeitet werden und in welchem Umfang dies erfolgt. Die Transparenz sollte sich u.a. auf die Zwecke der Datenverarbeitung und die Rechte der betroffenen Person beziehen. Die eindeutige Festlegung der Zwecke dient der Information der betroffenen Person. So verpflichten Art. 13 Abs. 1 lit. c) und Art. 14 Abs. 1 lit. c) DS-GVO zur Information über die Zwecke, für die die personenbezogenen Daten verarbeitet werden. Zudem kann die betroffene Person nach Art. 15 Abs. 1 lit. a) Auskunft über die Verarbeitungszwecke verlangen.

Alle Informationen müssen leicht zugänglich, verständlich und in klarer und einfacher Sprache abgefasst sein.[4] Aus Erwägungsgrund 58 ergibt sich, dass diese Informationen auch in elektronischer Form bereitgestellt werden können. Die Art. 12 bis 15 DS-GVO konkretisieren diese Transparenzanforderungen.

Für weitere Ausführungen zu den Art. 12 ff. DS-GVO siehe „Informationspflichten des Verantwortlichen" Seite 109.

**cc. Zweckbindung**

Personenbezogene Daten dürfen nach Art. 5 Abs. 1 lit. b) DS-GVO nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Die eindeutige Festlegung der Zwecke dient der Information der betroffenen Person. Legitim sind die Zwecke dann, wenn sie in Einklang mit der Rechtsordnung stehen.[5] So müssen die Zwecke

[4] Erwägungsgrund 39 DS-GVO.

[5] Kühling/Buchner/*Herbst,* DS-GVO, Art. 5 Rn. 37.

nicht nur dem Datenschutzrecht entsprechen, sondern z. B. auch den Anforderungen des Arbeitsrechts genügen. Sollen Daten für andere Zwecke verarbeitet werden, so sind die Vorgaben von Art. 6 Abs. 4 DS-GVO sowie § 24 BDSG zu beachten.

Für weitere Ausführungen zu Art. 6 DS-GVO siehe „Rechtmäßigkeit der Verarbeitung“ Seite 23.

**PRAXISTIPP**
Die Zwecke müssen bereits zum Zeitpunkt der Datenerhebung festgelegt sein.[6] Die Grundverordnung gibt keine bestimmte Form für die Zweckfestlegung vor. Nachdem der Verantwortliche die Einhaltung des Zweckbindungsgrundsatzes nachweisen können muss, sollten die Zwecke so dokumentiert werden, dass sie auch für einen Dritten nachzuvollziehen sind, so z. B. in Textform. Das ergibt sich auch daraus, dass nach Art. 30 Abs. 1 lit. b) DS-GVO die Zwecke der Verarbeitung in das Verzeichnis der Verarbeitungstätigkeiten aufgenommen werden müssen.

### dd. Datenminimierung

Personenbezogene Daten müssen nach dem Grundsatz der „Datenminimierung“ in Art. 5 Abs. 1 lit. c) DS-GVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Eine im Grundsatz vergleichbare Regelung ist aus § 3a BDSG a. F. bekannt. Unternehmen dürfen nur so viele personenbezogene Daten verarbeiten, wie es nach dem jeweiligen Zweck erforderlich ist. Ist es möglich, denselben Zweck ohne eine Verarbeitung personenbezogener Maßnahmen zu erreichen, so sollte dieser Weg eingeschlagen werden. Bei der Verarbeitung personenbezogener Daten ist deshalb insbesondere zu bedenken, ob der Verarbeitungszweck auch dann erreicht werden kann, wenn die Daten anonymisiert sind.

Der Grundsatz der Datenminimierung wird an verschiedenen Stellen der Datenschutz-Grundverordnung konkretisiert, wie z. B. im Gebot der Speicherbegrenzung in Art. 5 Abs. 1 lit. e) DS-GVO und den Vorschriften über den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in Art. 25 DS-GVO.

---

[6] Erwägungsgrund 39 DS-GVO.

**PRAXISTIPP**
Die Verarbeitung personenbezogener Daten sollte mit regelmäßigen Terminen für die Kontrolle einhergehen, ob die gespeicherten Daten für die Erreichung des Zwecks tatsächlich noch benötigt werden. Sie sind zu löschen oder ihre Verarbeitung ist einzuschränken, wenn dies nicht mehr der Fall ist. Dabei sind jedoch die arbeitsrechtlichen Besonderheiten z. B. im Prozessrecht zur Darlegungs- und Beweislast bei der Abmahnung zu beachten.

Für weitere Ausführungen zum Thema „Löschung" siehe „Recht auf Löschung" Seite 119.

**ee. Richtigkeit**

Art. 5 Abs. 1 lit. d) DS-GVO sieht vor, dass die personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein müssen. Der Verantwortliche muss angemessene Maßnahmen treffen, damit personenbezogene Daten, die im Hinblick auf die Verarbeitungszwecke unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Die „Richtigkeit" der Datenverarbeitung richtet sich nach dem Verarbeitungszweck. Art. 16 DS-GVO führt das Recht auf Berichtigung näher aus. Danach kann ggf. auch eine ergänzende Erklärung genügen. Ist die Richtigkeit bestritten, kann die betroffene Person gemäß Art. 18 Abs. 1 lit. a) DS-GVO die Einschränkung der Verarbeitung verlangen. Eine Verpflichtung zur Löschung kann sich aus Art. 17 Abs. 1 lit. d) DS-GVO ergeben.

Ob personenbezogene Daten immer auf dem neuesten Stand sein müssen, bestimmt sich nach den Zwecken der Verarbeitung und den damit verbundenen konkreten Umständen[7], wie sich aus dem Begriff „erforderlichenfalls" ergibt.

[7] Ehrmann/Selmayr/*Heberlein*, DS-GVO, Art. 5 Rn. 24.

**BEISPIEL**
Wurden in der Vergangenheit z. B. im Rahmen eines Betrieblichen Eingliederungsmanagements personenbezogene Gesundheitsdaten bei der betroffenen Person erhoben, beziehen sie sich auf diesen Zeitpunkt und müssen nicht auf den neuesten Stand gebracht werden. Anders kann dies aussehen, wenn es z. B. um die private Anschrift, den Personenstand oder Zutrittsrechte eines Beschäftigten geht.

### ff. Speicherbegrenzung

Nach Art. 5 Abs. 1 lit. e) DS-GVO darf bei einer Speicherung personenbezogener Daten die Identifizierung der betroffenen Person nur so lange möglich sein, wie es für den Verarbeitungszweck erforderlich ist. Damit wird der Grundsatz der Datenminimierung um eine zeitliche Beschränkung der Speicherung ergänzt.[8]

Aus Erwägungsgrund 39 DS-GVO ergibt sich, dass der Verantwortliche Fristen für die Löschung oder regelmäßige Überprüfung vorsehen sollte. Die festzulegende Speicherfrist muss auf das unbedingt erforderliche Mindestmaß beschränkt werden.

**HINWEIS**
Dieser Grundsatz steht im engen Zusammenhang mit dem der Datenminimierung. Deshalb sollte auch nach diesen Vorgaben der Verantwortliche Prozesse und/oder Fristen vorsehen, um personenbezogene Daten regelmäßig zu überprüfen und ggf. zu löschen. Die Beschäftigten sind ggf. über die Dauer der Speicherung zu informieren und ggf. muss hierüber Auskunft erteilt werden, Art. 13 Abs. 2 lit. a), Art. 14 Abs. 2 lit. a), Art. 15 Abs. 1 lit. d) DS-GVO. Ist die Angabe eines Kalenderdatums für die Speicherdauer nicht möglich, genügt es, die Kriterien für die Speicherdauer – wie die Abhängigkeit von einem nicht feststehenden Ereignis wie z. B. der Beendigung eines Arbeitsvertrags – darzulegen.

Für weitere Ausführungen zu Art. 12 ff. DS-GVO siehe „Informationspflichten des Verantwortlichen“ Seite 109.

[8] *Schulz*, ZESAR 2017, 270.

**gg. Integrität und Vertraulichkeit**

Der Grundsatz der Integrität und Vertraulichkeit in Art. 5 Abs. 1 lit. f) DS-GVO zielt darauf ab, dass personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen in einer solchen Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Konkret werden der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung beispielhaft genannt. Welche Anforderungen in diesem Zusammenhang gestellt werden, konkretisiert Art. 32 DS-GVO, wobei diese Aufzählung nicht abschließend ist. Diese Vorgaben ersetzen die bisherigen Regelungen zu technischen und organisatorischen Maßnahmen in § 9 BDSG a. F. sowie die Anlage zu § 9 BDSG a. F.

**hh. Rechenschaftspflicht**

Nach diesem in Art. 5 Abs. 2 DS-GVO normierten Grundsatz ist der Verantwortliche nicht nur für die Einhaltung der in Art. 5 Abs. 1 DS-GVO genannten Grundsätze verantwortlich, sondern er muss deren Einhaltung auch nachweisen können. Diese Nachweispflicht ist eine wesentliche Veränderung der bisherigen Rechtslage. Bei einer Überprüfung durch Aufsichtsbehörden muss danach der Verantwortliche Informationen bereitstellen können, die die Einhaltung der Grundsätze von Art. 5 Abs. 1 DS-GVO untermauern.

**HINWEIS**
Diese Vorgaben führen dazu, dass in den Unternehmen ein besonderes Augenmerk auf die Dokumentation gelegt werden muss. Sie sollte bei der Anpassung von Prozessen an die Vorgaben der Datenschutz-Grundverordnung mit eingeplant werden. Eine mögliche Form des Nachweises ist das in Art. 30 DS-GVO genannte Verzeichnis von Verarbeitungstätigkeiten. Unternehmen mit weniger als 250 Mitarbeitern, die unter bestimmten Umständen von der Verpflichtung, ein solches Verarbeitungsverzeichnis zu führen, befreit sind, sollten zumindest eine schriftliche Dokumentation zum Nachweis der Einhaltung der Grundsätze vorhalten. Eine solche Befreiung dürfte jedoch im Beschäftigungsverhältnis kaum eintreten. Geeignete technische und organisatorische Maßnahmen gemäß Art. 24 und Art. 25 DS-GVO sind weitere Beispiele, wie man der Nachweispflicht genügen kann.

Für weitere Ausführungen siehe „Verzeichnis von Verarbeitungstätigkeiten“ Seite 36 und „Datenschutz durch Technikgestaltung“ Seite 30.

## e. Rechtmäßigkeit der Verarbeitung – Art. 6 DS-GVO

Gemäß Art. 6 Abs. 1 DS-GVO ist eine Verarbeitung personenbezogener Daten nur dann rechtmäßig, wenn sie durch die Einwilligung der betroffenen Person oder aufgrund einer anderen zulässigen Rechtsgrundlage erfolgt. Die sechs nachfolgend aufgeführten Rechtsgrundlagen sind exklusiver bzw. abschließender Natur.[9]

[9] EuGH, 24.11.2011 (C-468/10 und C-469/10 ASNEF und FECEMD) Rn. 30 in ZD 2012, 33 ff.; Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, S. 69.

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben.
b) Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgt.
c) Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.
d) Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.
e) Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.
f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Die Mitgliedstaaten können bzw. müssen die Rechtsgrundlagen der Art. 6 Abs. 1 lit. c) und e) DS-GVO teilweise spezifischer ausgestalten. Das bedeutet, dass die Mitgliedstaaten beispielsweise konkret festlegen müssen, wann eine Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung oder eines öffentlichen Interesses erforderlich ist.

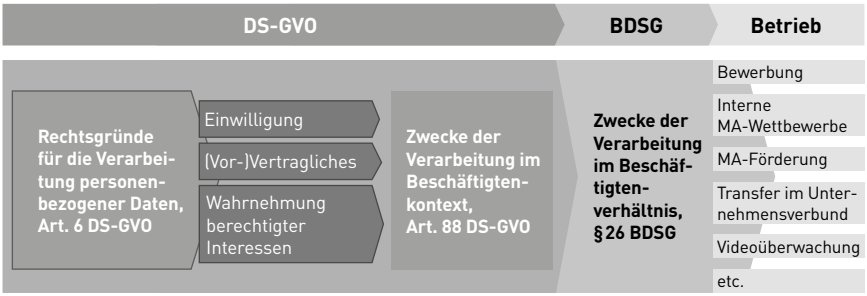
Darüber hinaus können die Mitgliedstaaten gemäß Art. 88 Abs. 1 DS-GVO bezüglich der Verarbeitung personenbezogener Daten im Beschäftigtenkontext „spezifischere Vorschriften" zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorsehen. Diese spezifischeren Vorschriften können sowohl in Kollektivvereinbarungen – so der Wortlaut von Art. 88 Abs. 1 DS-GVO – als auch in Betriebsvereinbarungen – so der ergänzende Erwägungsgrund 155 DS-GVO – enthalten sein.

Deutschland hat von der Möglichkeit einer mitgliedstaatlichen Regelung für die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses mit Erlass von § 26 BDSG (2018) in dem Datenschutz-Anpassungs und -Umsetzungsgesetz EU (DSAnpUG-EU)[10] Gebrauch gemacht.

[10] Gesetz vom 30.06.2017, BGBl 2017 Teil I Nr. 44.

**§ 26 Abs. 1 BDSG [Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses] lautet:**
(1) Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Das Zusammenspiel der verschiedenen Vorschriften von DS-GVO und BDSG bis hin zu den betrieblichen Verarbeitungen veranschaulicht die nachfolgende Grafik.



- Die Rechtsgründe für die Verarbeitung personenbezogener Daten sind in Art. 6 Abs. 1 DS-GVO – mit Ausnahme der erwähnten nationalen Ausgestaltung von lit. c) und e) – exklusiv bzw. abschließend aufgeführt. Das ist praktisch und rechtssicher, weil damit künftig alle Rechtsgrundlagen an einer Stelle im Gesetz zu finden sind.
- Für welche Zwecke Verarbeitungen von personenbezogenen Daten im Beschäftigtenkontext durchgeführt werden können, beschreiben sowohl Art. 88 DS-GVO als auch § 26 BDSG n.F.
- Wichtig für die Praxis ist, dass die konkreten Ausgestaltungen der unterschiedlichsten betrieblichen Anwendungsfälle der Verarbeitung von Beschäftigtendaten in Betriebsvereinbarungen erfolgen können.

Dabei ist allerdings darauf zu achten, dass vorhandene besondere Anforderungen eines Rechtsgrunds, wie beispielsweise der Hinweis auf das Widerspruchsrecht gemäß Art. 21 DS-GVO bei der Wahrnehmung berechtigter Interessen nach Art. 6 Abs. 1 lit. f) DS-GVO, beachtet werden.

**aa. Verarbeitungen von personenbezogenen Daten im Beschäftigtenkontext**

In der betrieblichen Praxis fokussieren sich Verarbeitungen von personenbezogenen Daten von – künftigen, aktuellen und ehemaligen – Beschäftigten im Wesentlichen auf einen der folgenden drei Rechtsgründe:

- Erfüllung des Vertrags mit der betroffenen Person bzw. einer vorvertraglichen Verpflichtung (Art. 6 Abs. 1 lit. b) DS-GVO).
- Wahrnehmung berechtigter Interessen (Art. 6 Abs. 1 lit. f) DS-GVO).
- Einwilligung (Art. 6 Abs. 1 lit. a) DS-GVO),

**(1) Die Erfüllung des (Arbeits-)Vertrags mit der betroffenen Person bzw. einer vorvertraglichen Verpflichtung – Art. 6 Abs. 1 lit. b) DS-GVO**

Verarbeitungen personenbezogener Daten von Beschäftigten, die zur Erfüllung und Ausgestaltung der Pflichten des Arbeitsvertrags erforderlich sind, lassen sich mit diesem Rechtsgrund legitimieren. Die hierunter möglicherweise fallenden Konstellationen können sehr vielschichtig sein. Deshalb hat der europäische Gesetzgeber in Art. 88 Abs. 1 DS-GVO und der deutsche Gesetzgeber in § 26 Abs. 1 BDSG Zwecke aufgelistet, für die eine Verarbeitung im Beschäftigungsverhältnis zulässig sind. Der Begriff des Beschäftigungsverhältnisses ist begrifflich weiter gefasst als der der Vertragserfüllung. Hierdurch wird klar, dass der Gesetzgeber Verarbeitungen im Beschäftigungsverhältnis nicht auf solche der reinen Vertragserfüllung beschränken wollte.

### (2) Der Rechtsgrund der Wahrnehmung berechtigter Interessen – Art. 6 Abs. 1 lit. f) DS-GVO

#### (a) Anwendbarkeit des Rechtsgrunds im Beschäftigungskontext

Folglich kommt der Rechtsgrund der Wahrnehmung der berechtigten Interessen auch nach Auffassung der europäischen Datenschutzbehörden im Kontext eines Beschäftigungsverhältnisses zur Anwendung[11]. Überlegungen, Art. 88 DS-GVO bzw. § 26 BSDG n.F. als eine abschließende Norm für die Verarbeitungen von personenbezogenen Daten im Beschäftigungskontext anzusehen und deshalb die Anwendung des Rechtsgrunds der berechtigten Interessen auszuschließen, sind mit dem Sinn und Zweck der DS-GVO nicht vereinbar. Zum einen sind sie keine die Verarbeitung legitimierenden Rechtsgründe. Zum anderen ließe sich die Existenz von Erwägungsgrund 48 DS-GVO, der den Rechtsgrund der berechtigten Interessen u. a. anhand eines Beispiels aus dem Beschäftigtendatenkontext erläutert, nicht erklären.

#### (b) Die Abwägung der berechtigten Interessen von Arbeitgeber und betroffenen Arbeitnehmern

Was unter berechtigten Interessen zu verstehen ist, wie sie festzustellen sind und wie sie gegen die berechtigten Interessen der betroffenen Person abzuwägen sind, regelt Art. 6 Abs. 1 lit. f) DS-GVO nicht. Erwägungsgrund 47 DS-GVO, der den Rechtsgrund erläutert, spricht lediglich davon, dass die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen sind. Aus der englischsprachigen Masterfassung der DS-GVO ergibt sich, dass diese Formulierung nicht ganz zutreffend ins Deutsche übersetzt worden ist, denn es geht nicht um die Erwartungen einer einzelnen Person, sondern vielmehr um die Erwartungen von allgemein der betroffenen Personen in der gegebenen Situation.

Die europäischen Datenschutzbehörden haben in ihrer Stellungnahme zur Interpretation des Begriffs der berechtigten Interessen[12] beschrieben, wie sie den Rechtsgrund der berechtigten Interessen verstehen und welche Kriterien bzw. Aspekte in die Abwägung der Interessen einfließen bzw. welche unberücksichtigt

---

11 Opinion 2/2017 on data protection at work (WP 249).

12 Stellungnahme 06/2014 zum Begriff des berechtigen Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, angenommen am 09.04.2014, (WP 217).

bleiben müssen. Insbesondere die dort aufgeführten Schlüsselfaktoren für die Ausgewogenheit der Interessensprüfung geben eine hilfreiche und empfehlenswerte Richtschnur für die Praxis.[13]

**(c) Besondere Dokumentations- und Hinweispflichten**

Im Falle der Verarbeitung personenbezogener Daten auf der Grundlage von Art. 6 Abs. 1 lit. f) DS-GVO hat der Verantwortliche spezielle Dokumentations- und Hinweispflichten zu erfüllen. Daher haben Arbeitgeber im Falle der Berufung auf Art. 6 Abs. 1 lit. f) DS-GVO betroffenen Beschäftigten die berechtigten Interessen darzulegen, Art. 13 Abs. 1 lit. d) bzw. Art. 14 Abs. 2 lit. b) DS-GVO. Des Weiteren hat er sie auf ihr Widerspruchsrecht gemäß Art. 21 Abs. 1 DS-GVO hinzuweisen. Ein erhobener Widerspruch ist allerdings unbeachtlich, sofern der Verantwortliche zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann.

**(3) Einwilligung der betroffenen Person – Art. 6 Abs. 1 lit. a) DS-GVO**

Die Datenschutz-Grundverordnung sieht vor, dass personenbezogene Daten auf der Grundlage einer Einwilligung verarbeitet werden können. Eine solche Einwilligung muss den in Art. 7 DS-GVO aufgestellten Regelungen genügen. Da die Freiwilligkeit der Einwilligung im Beschäftigungsverhältnis oftmals fraglich ist, hat der deutsche Gesetzgeber in § 26 Abs. 2 BDSG n.F. Kriterien genannt, bei deren Vorliegen in der Regel hieran nicht gezweifelt werden braucht..

Für weitere Ausführungen zum Thema „Einwilligung“ siehe „Datenverarbeitung auf der Grundlage einer Einwilligung“ Seite 69.

**(4) Weiterverarbeitung nach einer Zweckänderung[14]**

Die Weiterverarbeitung nach einer Zweckänderung ist in Art. 6 Abs. 4 DS-GVO geregelt. Danach ist die Verarbeitung personenbezogener Daten zulässig, wenn sie auf der Einwilligung der betroffenen Person beruht oder auf einer Rechtsvorschrift, die den dort genannten Anforderungen genügt. Sofern diese beiden Möglichkeiten nicht zur Anwendung kommen, ist eine Weiterverarbeitung nur zulässig, wenn der Zweck der Weiterverarbeitung mit dem ursprünglichen Zweck der Datenverarbeitung kompatibel ist.

---

13 Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gem. Art. 7 der RL 95/46/EG, angenommen am 09.04.2014, WP 217, S. 43 ff.

14 *Monreal*, ZD 2016, 507 ff.

**(a) Die Kompatibilitätsprüfung**
Hierzu ist eine sog. Kompatibilitätsprüfung durchzuführen, bei der zumindest die in Art. 6 Abs. 4 DS-GVO genannten Kriterien zu berücksichtigen sind. Dies sind

- Die Verbindung zwischen den unterschiedlichen Zwecken,
- der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden,
- die Art der personenbezogenen Daten,
- die möglichen Folgen der beabsichtigten Weiterverarbeitung
- das Vorhandensein geeigneter Garantien.

Angemerkt sei, dass die bei einer Kompatibilitätsprüfung zu berücksichtigen Kriterien[15] weitestgehend mit denen übereinstimmen, die die europäischen Aufsichtsbehörden im Rahmen der Feststellung von berechtigen Interessen in Sinne von Art. 6 Abs. 1 lit. f) DS-GVO heranziehen.

**(b) Kein eigener Rechtsgrund**
Art. 6 Abs. 4 DS-GVO stellt selbst kein Rechtsgrund für eine Verarbeitung dar. Die Verarbeitung der vorhandenen personenbezogenen Daten wird vielmehr auf der Grundlage des ursprünglichen Rechtsgrunds mit einem – neuen – kompatiblen Zweck weitergeführt. Dies stellen die beiden ersten Sätze von Erwägungsgrund 50 DS-GVO klar.

**(c) Informationspflichten**
Soll eine Verarbeitung mit einem neuen, kompatiblen Zweck fortgeführt werden, hat der Verantwortliche die betroffenen Personen hierüber gemäß den allgemeinen Regeln der Art. 12 ff. DS-GVO zu informieren. Diese Pflicht entfällt, wenn der Betroffene bereits über die geforderten Informationen verfügt, Art. 13 Abs. 4 und Art. 14 Abs. 5 lit. a) DS-GVO bzw. falls sich die Zurverfügungstellung der Informationen als unverhältnismäßig – im Falle des Art. 14 DS-GVO – darstellt.

## f. Besondere Kategorien personenbezogener Daten – Art. 9 DS-GVO

Die Datenschutz-Grundverordnung sieht Schutzvorschriften für alle Arten von personenbezogenen Daten vor. Bestimmte Bereiche dieser personenbezogenen Daten werden aber als so sensibel angesehen, dass sie hierfür einen besonderen Schutz vorschreibt. In Art. 9 Abs. 1 DS-GVO wird festgelegt, dass es untersagt ist, diese „besonderen Kategorien personenbezogener Daten" zu verarbeiten. Aus-

[15] Monreal, ZD 2016, 510 f. m. w. H.

nahmen von diesem Grundsatz werden in Art. 9 Abs. 2 DS-GVO festgeschrieben. Im Bereich des Beschäftigtendatenschutzes schafft § 26 Abs. 3 BDSG eine konkrete Ausnahmeregelung.

Für weitere Ausführungen zu Art. 9 DS-GVO siehe „Umgang mit besonderen Kategorien personenbezogener Daten“ Seite 93.

## g. Rechte der betroffenen Person – Art. 12 ff. DS-GVO

Kapitel III der Datenschutz-Grundverordnung befasst sich sowohl mit den Informationspflichten des Verantwortlichen gegenüber der betroffenen Person als auch mit verschiedenen Rechten, die der betroffenen Person gegenüber dem Verantwortlichen zustehen. Darunter fällt z. B. das Auskunftsrecht gemäß Art. 15 DS-GVO, das Recht darauf, bestimmte Daten löschen zu lassen, Art. 17 DS-GVO und das Recht auf Datenübertragbarkeit in Fällen automatisierter Datenverarbeitung auf Grundlage einer Einwilligung, Art. 20 DS-GVO.

Für weitere Ausführungen zu den Art. 12 ff. DS-GVO siehe „Informationspflichten des Verantwortlichen“ Seite 109 und zu den Art. 15 ff. DS-GVO „Wichtige Betroffenenrechte“ Seite 116.

## h. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen – Art. 25 DS-GVO

Eine Reihe von Vorgaben der Datenschutz-Grundverordnung zielen darauf ab, die Technik in den Dienst des Datenschutzes zu stellen. Hierzu gehört insbesondere Art. 24 DS-GVO, der den Verantwortlichen verpflichtet, technisch-organisatorische Maßnahmen umzusetzen, damit die Datenverarbeitung nach den Vorgaben der Datenschutz-Grundverordnung erfolgt. In Art. 25 Abs. 1 DS-GVO wird diese Regelung dahingehend konkretisiert, dass bereits zu einem frühen Zeitpunkt – nämlich bei der Festlegung der Mittel der Verarbeitung – der Verantwortliche die Grundsätze der Datenschutz-Grundverordnung bedenken muss. Gleichzeitig wird in Art. 25 Abs. 2 DS-GVO der Verantwortliche aufgefordert, durch Maßnahmen den Grundsatz der Datenminimierung praktisch umzusetzen. Art. 32 DS-GVO konkretisiert, welche technisch-organisatorischen Maßnahmen eingesetzt werden können, um ein angemessenes Schutzniveau zu gewährleisten.

**HINWEIS**
Art. 25 DS-GVO zielt auf den Verantwortlichen ab, nicht etwa auf die Hersteller oder Produzenten von IT-Systemen. Sie werden in Erwägungsgrund 78 lediglich ermutigt, datenschutzfreundliche Produkte anzubieten. Wer künftig am Markt bestehen will, wird jedoch Produkte entwickeln, die die Vorgaben der Datenschutz-Grundverordnung aufgreifen. Es dürfte nur eine Frage der Zeit sein, bis zertifizierte Produkte auf den Markt kommen werden. Werden Programme zugekauft, sollten die datenschutzrechtlichen Aspekte besonders berücksichtigt werden. Auch Auftragsverarbeiter werden nicht unmittelbar angesprochen. Werden z. B. Cloud-Dienste im Wege der Auftragsverarbeitung genutzt, muss der Verantwortliche darauf achten, dass er nur solche Auftragsverarbeiter auswählt, die auch den Vorgaben von Art. 25 DS-GVO genügen.

Der Verantwortliche wird aufgefordert interne Strategien festzulegen und Maßnahmen zu ergreifen, um die in Art. 25 DS-GVO aufgeführten Grundsätze des Datenschutzes durch Technik (privacy by design) und datenschutzfreundliche Voreinstellungen (privacy by default) sicherzustellen.[16]

**BEISPIEL**
Welche Maßnahmen hierunter fallen können wird beispielhaft in der Datenschutz-Grundverordnung aufgeführt. Art. 25 Abs. 1 DS-GVO nennt z. B. die Pseudonymisierung als eine mögliche Maßnahme, um den Anforderungen der Verordnung zu genügen. In Erwägungsgrund 78 DS-GVO werden weitere Punkte aufgeführt. Dazu gehört, die Verarbeitung personenbezogener Daten zu minimieren, Transparenz herzustellen, die Kontrolle durch die betroffene Person zu ermöglichen und die Möglichkeit des Verantwortlichen, Sicherheitsfunktionen zu schaffen und zu verbessern. Art. 32 DS-GVO nennt darüber hinaus weitere Maßnahmen: hierzu zählt die Verschlüsselung personenbezogener Daten, die Fähigkeit, dauerhaft Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Systemen und Diensten sicherzustellen, die rasche Wiederherstellung von Verfügbarkeit personenbezogener Daten bei einem Zwischenfall sowie ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der Maßnahmen.

[16] Erwägungsgrund 78 DS-GVO.

**HINWEIS**
Es ist zu empfehlen, dass Verantwortliche sich an bereits vorhandenen Vorgaben orientieren. Die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik[17] können Orientierung bieten.[18] Auch die technischen und organisatorischen Anforderungen an die Datensicherheit, die sich aus der Anlage zu § 9 Satz 1 BDSG a. F. ergeben, können als Orientierungsmaßstab herangezogen werden. Dabei ist zu beachten, dass die Pseudonymisierung zusätzlich als Maßnahme in Art. 32 DS-GVO genannt wird, die Verfügbarkeitskontrolle auf die rasche Wiederherstellung der Daten abzielt und eine regelmäßige Überprüfung der Wirksamkeit in Art. 32 Abs. 1 lit. d) DS-GVO gefordert wird. Nicht übernommen wurden die Eingabekontrolle und das Trennungsgebot aus der Anlage zu § 9 BDSG a. F. Die Auftragskontrolle findet sich im Zusammenhang mit der Auftragsverarbeitung wieder. Hilfestellung kann zudem § 64 BDSG bieten. Auch wenn diese Regelung nicht im Rahmen der Datenschutz-Grundverordnung anzuwenden ist, sondern der Umsetzung der europäischen Richtlinie 2016/680 dient, gibt sie doch gleichwohl Hinweise, welche konkreten Anforderungen an die Sicherheit der Datenverarbeitung gestellt werden.

## i. Gemeinsam für die Verarbeitung Verantwortliche – Art. 26 DS-GVO

In Erwägungsgrund 79 DS-GVO wird festgeschrieben, dass es zum Schutz der Rechte und Freiheiten der betroffenen Person einer klaren Zuteilung der Verantwortlichkeiten bedarf. Dem trägt Art. 26 DS-GVO für den Fall Rechnung, in dem zwei oder mehrere Verantwortliche gemeinsam die Zwecke und Mittel der Verarbeitung festlegen und als gemeinsam Verantwortliche angesehen werden. Hierdurch soll sichergestellt werden, dass die Betroffenen in der Lage sind, ihre Rechte nach der DS-GVO durchzusetzen und die Aufsichtsbehörden durch die klare Zuteilung der Verantwortlichkeiten ihre Überwachungsaufgaben besser ausüben können.

Insbesondere für Konzernstrukturen und andere Unternehmensverbünde ist eine gemeinsame Datenverarbeitung von besonderer Bedeutung. Aber auch darüber hinaus gibt es Konstellationen, in denen mehrere Verantwortliche gemeinsam

17 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html;jsessionid=0E9D6A4AA2BF572C9D20079E305984F6.1_cid369.

18 Ehrmann/Selmayr/*Baumgartner*, DS-GVO, Art. 25 Rn. 10.

Zwecke und Mittel zur Verarbeitung festlegen. Dabei ist die Abgrenzung zur Auftragsverarbeitung wichtig, bei der die personenbezogenen Daten lediglich im Auftrag des Verantwortlichen verarbeitet werden und keine Entscheidungsbefugnis über Zwecke und Mittel der Verarbeitung gegeben ist. Anders als im deutschen Recht kennt die europäische Datenschutzrichtlinie bereits die Konstellation eines gemeinsamen Verantwortlichen.[19] Die Artikel-29-Datenschutzgruppe hat hierzu Ausführungen[20] gemacht, die aufgrund der in der Datenschutzrichtlinie und der Datenschutz-Grundverordnung gleichlautenden Definition des „Verantwortlichen" übertragbar sind. Kernpunkt ist dabei die Frage, ob mehr als eine Partei über die Zwecke und Mittel der Datenverarbeitung entscheidet. Eine gemeinsame Kontrolle ist danach gegeben, wenn verschiedene Parteien im Zusammenhang mit spezifischen Verarbeitungen über den Zweck und über wesentliche Elemente der Mittel entscheiden, die einen für die Verarbeitung Verantwortlichen kennzeichnen. Im Rahmen der gemeinsamen Kontrolle kann die Beteiligung der Parteien an den gemeinsamen Entscheidungen jedoch verschiedene Formen aufweisen und muss nicht gleichmäßig verteilt sein.[21]

In dem Arbeitspapier der Artikel-29-Datenschutzgruppe werden Beispiele aufgeführt, wann wesentliche Entscheidungen über Zweck und Mittel einer Datenverarbeitung – gemeinsam – festgelegt werden.

19 Art. 2 lit. d) Richtlinie 95/46/EG.

20 Artikel-29-Datenschutzgruppe, WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf.

21 Artikel-29-Datenschutzgruppe, WP 169, Seite 23.

**BEISPIEL FÜR GEMEINSAM VERANTWORTLICHE**

Das Unternehmen Headhunterz Ltd. unterstützt das Unternehmen Enterprize Inc. bei der Einstellung neuer Mitarbeiter. Im Vertrag ist klar festgelegt: „Headhunterz Ltd. handelt im Auftrag von Enterprize und handelt bei der Verarbeitung personenbezogener Daten als Auftragsverarbeiter. Enterprize ist der alleinige für die Verarbeitung Verantwortliche." Das Unternehmen Headhunterz Ltd. befindet sich jedoch in einer unklaren Position: Einerseits erfüllt es gegenüber den Arbeitssuchenden die Rolle eines für die Verarbeitung Verantwortlichen, andererseits handelt es als Auftragsverarbeiter im Auftrag von für die Verarbeitung Verantwortlichen, wie z. B. Enterprize Inc. und anderen Unternehmen, die seine Dienste als Personalvermittler in Anspruch nehmen. Darüber hinaus sucht Headhunterz – mit seinem berühmten Mehrwertdienst „Globale Vermittlung" – geeignete Bewerber sowohl unter den Bewerbungen, die direkt bei Enterprize eingehen, als auch unter den Bewerbungen, die bereits in seiner eigenen umfangreichen Datenbank vorhanden sind. Dadurch verbessert das Unternehmen Headhunterz, das vertragsgemäß nur für abgeschlossene Arbeitsverträge bezahlt wird, den Abgleich zwischen offenen Stellen und Arbeitssuchenden und steigert so seine Einnahmen. Aus dem Sachverhalt lässt sich schließen, dass Headhunterz Ltd. trotz der vertraglichen Abmachung als ein für die Verarbeitung Verantwortlicher angesehen werden muss, der zumindest die Vorgangsreihen im Zusammenhang mit der Personalvermittlung für Enterprize Inc. gemeinsam mit Enterprize kontrolliert.[22]

**BEISPIEL FÜR GETRENNT VERANTWORTLICHE**

Das Unternehmen XYZ erhebt und verarbeitet personenbezogene Daten seiner Mitarbeiter zum Zwecke der Verwaltung von Gehältern, Dienstreisen, Krankenversicherung usw. Das Unternehmen ist jedoch auch gesetzlich dazu verpflichtet, alle Daten im Zusammenhang mit Gehältern an die Steuerbehörden zu übermitteln, um die Steueraufsicht zu unterstützen. In diesem Fall verarbeiten das Unternehmen XYZ und die Steuerbehörden zwar dieselben Daten über Gehälter, doch werden die beiden Organisationen aufgrund der nicht gemeinsamen Zwecke und Mittel der Datenverarbeitung als zwei getrennt für die Verarbeitung Verantwortliche eingestuft.[23]

22 Artikel-29-Datenschutzgruppe, WP 169, Beispiel 6.

23 Artikel-29-Datenschutzgruppe, WP 169, Beispiel 9.

Liegt eine Verarbeitung durch mehrere Verantwortliche vor, benötigt jeder einzelne Verantwortliche eine eigene Rechtsgrundlage für die Verarbeitung im Sinne von Art. 6 Abs. 1 DS-GVO.[24] Art. 26 DS-GVO selbst stellt keine Rechtsgrundlage für die Datenverarbeitung dar, sondern geht auf die Zuordnung von Verantwortlichkeiten unter den gemeinsam Verantwortlichen ein. In einer Vereinbarung muss in transparenter Form geregelt werden, wer welche Verpflichtungen der Datenschutz-Grundverordnung übernimmt. Das gilt insbesondere für die Betroffenenrechte und Informationspflichten. Das Wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt. Eine bestimmte Form hierfür ist nicht vorgesehen.[25]

**HINWEIS**
Die betroffene Person kann gemäß Art. 26 Abs. 3 DS-GVO ihre Rechte gegenüber jedem der Verantwortlichen geltend machen, wodurch das Haftungsrisiko jedes Verantwortlichen sich erhöht. Deshalb ist es wichtig, dass vor der Verarbeitung die jeweiligen Rollen klar festgelegt werden.

## j. Auftragsverarbeiter – Art. 28, 29 DS-GVO

Art. 28 DS-GVO regelt die Vorgaben und Verantwortlichkeiten, wenn personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet werden. Zudem werden Vorgaben für den Fall gemacht, dass der Auftragsverarbeiter einen weiteren Auftragsverarbeiter in Anspruch nehmen will. In Art. 29 DS-GVO wird festgeschrieben, dass Personen, die dem Auftragsverarbeiter unterstellt sind und Zugang zu personenbezogenen Daten haben, diese Daten grundsätzlich nur auf Weisung des Verantwortlichen verarbeiten dürfen.

Für weitere Ausführungen zu den Art. 28, 29 DS-GVO siehe „Verarbeitung von Beschäftigtendaten durch Auftragsverarbeiter“ Seite 126.

[24] Ehmann/Selmayr/*Bertermann*, DS-GVO, Art. 26 Rn. 9.

[25] Bitkom hat einen Leitfaden mit näheren Ausführungen zu diesem Thema veröffentlicht, abrufbar unter: https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-Joint-Controllership-online.pdf.

## k. Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO

Nach Art. 30 DS-GVO sind sowohl der für die Verarbeitung Verantwortliche als auch der Auftragsverarbeiter sowie gegebenenfalls deren Vertreter verpflichtet, ein Verzeichnis aller Verarbeitungstätigkeiten zu erstellen. Anders als nach der bisherigen Rechtslage ist der betriebliche Datenschutzbeauftragte nicht mehr dafür zuständig, das Verfahrensverzeichnis gemäß § 4g Abs. 2 BDSG a. F. verfügbar zu machen. Das Verzeichnis kann entweder schriftlich oder in elektronischer Form geführt werden und muss der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden. In Art. 30 Abs. 1 DS-GVO beziehungsweise Abs. 2 DS-GVO ist geregelt, welche Angaben in das Verzeichnis aufgenommen werden müssen. Dazu gehört u. a. eine – wenn möglich – allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach § 32 Abs. 1 DS-GVO. Unklar ist, wie detailliert diese Beschreibung sein muss. Die Datenschutzkonferenz als Zusammenschluss der Datenschutzbehörden des Bundes und der Länder weist darauf hin, dass diese Beschreibung so konkret erfolgen muss, dass die Aufsichtsbehörden eine erste Rechtmäßigkeitsüberprüfung vornehmen können.[26] Sie hat angekündigt, eine Muster-Vorlage für ein Verzeichnis von Verarbeitungstätigkeiten vorlegen zu wollen.

Dem Verzeichnis der Verarbeitungstätigkeiten kommt eine wichtige Stellung zu, um der in Art. 5 Abs. 2 und Art. 24 DS-GVO vorgesehenen Pflicht nachzukommen, nachweisen zu können, dass die Vorgaben der Grundverordnung eingehalten werden. Es enthält alle Informationen, die die Aufsichtsbehörde benötigt, um sich einen Eindruck darüber zu verschaffen, ob Unternehmen ihren Pflichten nach der Datenschutz-Grundverordnung nachkommen. Es kann deshalb von den Aufsichtsbehörden als Einstieg in Kontrollmaßnahmen genutzt werden. Dementsprechend sollten die Unternehmen ein besonderes Augenmerk auf die Erstellung und Pflege dieses Verzeichnisses legen.

Nach Art. 30 Abs. 5 DS-GVO sind Unternehmen und Einrichtungen mit weniger als 250 Mitarbeitern teilweise von der Pflicht befreit, ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Das gilt dann, wenn die Verarbeitung mit keinem Risiko für die Rechte und Freiheiten der betroffenen Person verbunden ist oder die Verarbeitung nur gelegentlich erfolgt. Von der Verarbeitung dürfen keine besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DS-GVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten

[26] DSK, Kurzpapier Nr.1 zu „Verzeichnis von Verarbeitungstätigkeiten", abzurufen unter: https://www.lda.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf

gemäß Art. 10 DS-GVO umfasst sein. Jedes Risiko für die Rechte und Freiheiten der betroffenen Person sind somit ausreichend, um die Pflicht, ein Verarbeitungsverzeichnis zu führen, auszulösen.

**HINWEIS**
Mit der Ausnahmeregelung in Art. 30 Abs. 5 DS-GVO wird das ursprünglich angestrebte Ziel, kleine und mittlere Unternehmen zu entlasten, nicht erreicht. Bereits durch die Vorgabe, dass die Ausnahme nur dann greift, wenn die Verarbeitung gelegentlich erfolgt, werden vielfältige Verarbeitungstätigkeiten wie die Personalaktenführung und die Buchhaltung ausgenommen. Zudem verarbeiten Arbeitgeber regelmäßig besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DS-GVO, z. B. zu religiösen Überzeugungen, so dass auch aus diesem Grund die Ausnahmeregelung nicht einschlägig ist. Zudem bestehen die grundlegenden Verpflichtungen der Datenschutz-Grundverordnung fort, wie z. B. einen Nachweis darüber führen zu können, dass die Verarbeitung unter Einhaltung der Vorgaben der Verordnung erfolgt.

## I. Meldung von Verletzungen des Schutzes personenbezogener Daten – Art. 33, 34 DS-GVO

Die Art. 33 und 34 DS-GVO sehen Meldepflichten gegenüber der Aufsichtsbehörde beziehungsweise Benachrichtigungspflichten gegenüber der betroffenen Person vor, wenn der Schutz personenbezogener Daten verletzt wurde. Wann eine solche Verletzung des Schutzes personenbezogener Daten gegeben ist, wird in Art. 4 Abs. 12 DS-GVO definiert. Danach liegt sie vor, wenn „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden".

**BEISPIEL**
Darunter fallen z. B. Datenpannen und Datenlecks, Hacking und Datendiebstahl.[27] Das Bayerische Landesamt für Datenschutzaufsicht hat konkrete Anwendungen aufgeführt, die hierunter fallen können: ein verloren gegangener USB-Stick, ein Einbruch in einen schlecht gesicherten Serverraum, der mit einem Verlust der Backup-Platten einhergeht, eine Webanwendung, die eine bislang unbekannte SQL-Injection-Lücke aufweist.[28]

Der Verantwortliche muss die Datenschutzverletzung unverzüglich und möglichst innerhalb von 72 Stunden, nachdem sie ihm bekannt wurde, an die zuständige Aufsichtsbehörde melden. Eine Ausnahme hiervon gibt es, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

**HINWEIS**
Liegt eine Datenschutzverletzung vor, muss man in jedem Fall abschätzen, ob sich hierdurch ein Risiko für die betroffene Person ergibt. Wann ein solches Risiko vorliegen kann, beschreibt Erwägungsgrund 75 DS-GVO. Danach fallen z. B. eine Diskriminierung, ein Identitätsdiebstahl oder -betrug, ein finanzieller Verlust und eine Rufschädigung hierunter.

Adressat der Meldepflicht ist der Verantwortliche. Ein Auftragsverarbeiter muss hingegen dem Verantwortlichen eine Verletzung unverzüglich melden, wenn sie ihm bekannt wird.

Welche Informationen die Meldung umfassen muss, ist in Art. 33 Abs. 3 DS-GVO aufgeführt. Danach muss insbesondere die Verletzung beschrieben und ausgeführt werden, welche Folgen sie wahrscheinlich haben wird. Außerdem muss z. B. über die Maßnahmen informiert werden, die der Verantwortliche zur Behebung der Verletzung bereits ergriffen hat oder hierzu vorschlägt.

---

27 Ehmann/Selmayr/*Hladjk*, DS-GVO, Art. 33 Rn. 5.

28 Siehe Bayerisches Landesamt für Datenschutzaufsicht, EU-Datenschutz-Grundverordnung, Umgang mit Datenpannen, abzurufen unter: https://www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf.

Eine ausführliche Dokumentationspflicht ergibt sich für den Verantwortlichen aus Art. 33 Abs. 5 DS-GVO. Dabei ist eine offene Frage, ob hiervon auch die Risikoprognose umfasst ist. Nachdem die Dokumentation es der Aufsichtsbehörde ermöglichen muss zu überprüfen, ob die Bestimmungen des Art. 33 DS-GVO eingehalten werden, spricht einiges dafür, dass auch die Risikoprognose hiervon betroffen ist.

Ist die Verletzung mit einem hohen Risiko für die Betroffenen verbunden, muss die betroffene Person zusätzlich zur Meldung gegenüber der Aufsichtsbehörde gemäß Art. 34 DS-GVO unverzüglich vom Verantwortlichen hierüber benachrichtigt werden. Dabei müssen in klarer und einfacher Sprache die Art der Verletzung beschrieben und die in Art. 33 Abs. 3 lit. b), c) und d) DS-GVO aufgeführten Informationen weitergegeben werden. Art. 34 Abs. 3 DS-GVO sieht Ausnahmen von der Benachrichtigungspflicht vor. Danach ist eine Benachrichtigung der betroffenen Person z. B. dann nicht erforderlich, wenn der Verantwortliche durch nachfolgende Maßnahmen sicherstellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Person aller Wahrscheinlichkeit nicht mehr besteht.

**PRAXISTIPP**
Nicht zuletzt aufgrund der kurzen Meldefristen sollte im Unternehmen ein Prozess eingeführt werden, mit dem sichergestellt wird, dass Mitarbeiter bei einem möglichen Datenschutzverstoß ihren Verdacht unverzüglich an eine festgelegte Person melden. Diese Person sollte die Risikoprognose vornehmen und darüber urteilen können, ob die Aufsichtsbehörden und die betroffene Person informiert werden müssen.

## m. Datenschutz-Folgenabschätzung – Art. 35 DS-GVO

Die in Art. 35 DS-GVO geregelte Datenschutz-Folgenabschätzung dient dazu, Risiken und deren eventuelle Folgen für die persönlichen Rechte und Freiheiten der Betroffenen zu bewerten. Führt die Verarbeitung voraussichtlich zu einem hohen Risiko für den Betroffenen, ist vor der Datenverarbeitung abzuschätzen, welche Folgen mit der Verarbeitung für den Schutz personenbezogener Daten verbunden sind. Das gilt insbesondere bei der Verwendung neuer Technologien.

**BEISPIEL**
Erwägungsgrund 75 erläutert, was unter „Risiken für die Rechte und Freiheiten" natürlicher Personen zu verstehen ist. Hierunter fallen insbesondere:
- Diskriminierung
- Identitätsdiebstahl oder -betrug
- finanzieller Verlust
- Rufschädigung
- unbefugte Aufhebung Pseudonymisierung
- Hinderung der Kontrolle über eigene Daten
- Profilbildung z. B. bzgl. Arbeitsleistung.

Wann eine Datenschutz-Folgenabschätzung tatsächlich erforderlich ist, wird in Art. 35 Abs. 3 DS-GVO beispielhaft ausgeführt und im Erwägungsgrund 91 DS-GVO näher erläutert. Es ist in jedem Fall eine dokumentierte Analyse durchzuführen, ob eine Datenschutz-Folgenabschätzung durchzuführen ist. Die Aufsichtsbehörden werden aufgefordert, eine Liste mit Verarbeitungsvorgängen vorzulegen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist. Die Artikel-29-Datenschutzgruppe, die sich insbesondere aus Vertretern der jeweiligen nationalen Aufsichtsbehörden zusammensetzt, hat im April 2017 Leitlinien hierzu vorgelegt.[29] Als ein Beispiel, bei dem eine Datenschutz-Folgenabschätzung durchzuführen ist, wird die Überwachung der Aktivitäten von Beschäftigten genannt, einschließlich des Arbeitsplatzes und der Internetaktivitäten.

**HINWEIS**
Führt die Prüfung zum Ergebnis, dass keine Datenschutz-Folgenabschätzung durchzuführen ist, muss diese Entscheidung ebenso wie die Entscheidung über die Durchführung mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang schriftlich dokumentiert werden.[30]

Wie eine Folgenabschätzung abläuft, gibt Art. 35 Abs. 7 DS-GVO vor. Danach muss die Folgenabschätzung zumindest eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Verarbeitungszwecke umfassen, die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung sowie die Risiken für die Rechte und Freiheiten der Betroffenen bewerten und beschreiben, welche Maßnahmen

29 Artikel-29-Datenschutzgruppe, WP 248.

30 DSK, Kurzpapier Nr. 5 zu „Datenschutz-Folgenabschätzung", abzurufen unter: https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf.

und Sicherheitsvorkehrungen getroffen wurden, um den Schutz der personenbezogenen Daten und die Einhaltung der Bestimmungen der Datenschutz-Grundverordnung sicherzustellen.

**HINWEIS**
Die Datenschutzkonferenz hat eine Übersicht über die Hauptprozessschritte bei einer Datenschutz-Folgenabschätzung herausgegeben, an der man sich orientieren kann.[31]

Die Datenschutzkonferenz weist darauf hin, dass es unter bestimmten Umständen notwendig sein kann, die Datenschutz-Folgenabschätzung zu überprüfen. Das kann z. B. der Fall sein, wenn sich neue Risiken ergeben haben, sich die Bewertung eines Risikos verändert oder es wesentliche Änderungen im Verfahren vorliegen.

In Art. 35 Abs. 9 DS-GVO wird festgeschrieben, dass ggf. der Standpunkt der betroffenen Person oder ihrer Vertreter zu der beabsichtigten Verarbeitung eingeholt wird. Als „Vertreter" könnte man hier an den Betriebsrat denken, wenn es um eine nach § 87 Abs. 1 Nr. 6 BetrVG mitbestimmungspflichtige Verarbeitung von Arbeitnehmerdaten geht. Diese Vorgabe führt aber nicht zu einer Erweiterung der betriebsverfassungsrechtlichen Mitbestimmungsrechte des Betriebsrats.[32]

Kommt der Verantwortliche zum Ergebnis, dass die Verarbeitung ein hohes Risiko zur Folge hätte und kann er das hohe Risiko nicht eindämmen, muss er gemäß Art. 36 DS-GVO die zuständige Aufsichtsbehörde konsultieren. Art. 36 Abs. 2 DS-GVO beschreibt das Verfahren, das durchgeführt wird, falls die Aufsichtsbehörde zum Ergebnis kommt, dass die geplante Verarbeitung nicht mit der Datenschutz-Grundverordnung im Einklang steht.

In Art. 36 Abs. 3 DS-GVO werden die Informationen und Unterlagen aufgelistet, die der Verantwortliche der Aufsichtsbehörde im Rahmen seines Konsultationsersuchens zur Verfügung stellen muss.

---

31 DSK, Kurzpapier Nr. 5 zu „Datenschutz-Folgenabschätzung", abzurufen unter: https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf.

32 Ehmann/Selmayr/*Baumgartner*, DS-GVO, Art. 35 Rn. 47.

## n. Datenverarbeitung im Beschäftigungskontext – Art. 88 DS-GVO

Ziel der Datenschutz-Grundverordnung ist es insbesondere, ein gleichmäßiges Datenschutzniveau für natürliche Personen zu gewährleisten.[33] Gleichzeitig enthält sie aber auch Öffnungsklauseln, die es den Mitgliedstaaten der EU erlauben, für besondere Verarbeitungssituationen spezifischere Regelungen zu treffen. Hierzu zählt Art. 88 DS-GVO, der auf die Datenverarbeitung im Beschäftigungskontext eingeht.

### aa. Mitgliedstaatliche Regelungen zum Beschäftigtendatenschutz

Art. 88 Abs. 1 DS-GVO erlaubt es den Mitgliedstaaten, durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext zu erlassen. Art. 88 DS-GVO ist damit die zentrale Regelung in der Datenschutz-Grundverordnung zum Beschäftigtendatenschutz.

**HINWEIS**
Die Öffnungsklausel für mitgliedstaatliche Vorgaben zum Beschäftigtendatenschutz wird dazu führen, dass wie bisher die EU-Mitgliedstaaten eigenständige Regelungen zum Beschäftigtendatenschutz vorsehen können. Eine Verpflichtung hierzu besteht nicht. Deshalb muss bei grenzüberschreitenden Fällen innerhalb der EU die jeweilige nationale Rechtslage zum Beschäftigtendatenschutz beachtet werden.

Gleichzeitig stellt Art. 88 Abs. 1 DS-GVO klar, dass die Möglichkeit besteht, die Verarbeitung personenbezogener Daten in einer Kollektivvereinbarung ausgestalten zu können. Hierunter fallen auch Betriebsvereinbarungen, wie Erwägungsgrund 155 DS-GVO klarstellt. Eine Definition des Begriffs „Kollektivvereinbarung" findet sich für das deutsche Recht in § 26 Abs. 1 Satz 1 BDSG.

33 Erwägungsgrund 10 DS-GVO.

**Als Beispiele, welche Zwecke in den EU-Mitgliedstaaten geregelt werden können, zählt Art. 88 Abs. 1 DS-GVO folgende Aspekte auf:**

- Einstellung
- Erfüllung des Arbeitsvertrags, einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten
- Management
- Planung und Organisation der Arbeit
- Gleichheit und Diversität am Arbeitsplatz
- Gesundheit und Sicherheit am Arbeitsplatz
- Schutz des Eigentums der Arbeitsgeber oder Kunden
- Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen
- Beendigung des Beschäftigungsverhältnisses.

In Deutschland macht bislang § 32 BDSG a. F. Vorgaben zum Beschäftigtendatenschutz. Bei der Anpassung des BDSG a. F. an die Vorgaben der Datenschutz-Grundverordnung hat der deutsche Gesetzgeber von der Öffnungsklausel in Art. 88 Abs. 1 DS-GVO Gebrauch gemacht und mit § 26 BDSG die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses geregelt. § 26 BDSG wird am 25. Mai 2018 in Kraft treten und dann § 32 BDSG a. F. ersetzen. Der Gesetzgeber hat sich inhaltlich bei § 26 BDSG ersichtlich an § 32 BDSG a. F. orientiert, aber auch Neuerungen vorgenommen.

**HINWEIS**
Werden Beschäftigtendaten außerhalb des Beschäftigtenkontextes verarbeitet, richtet sich die Frage der rechtmäßigen Verarbeitung allein nach Art. 6 DS-GVO. Beispiele hierfür sind die Übermittlung von Beschäftigtendaten im Rahmen einer „Due-Diligence-Prüfung" beim Kauf von Betrieben oder Unternehmen und die Ansprache von Mitarbeitern zu Werbezwecken, die nichts mit dem Beschäftigungsverhältnis zu tun hat.[34]

### bb. Inhaltliche Ausgestaltung

In Art. 88 Abs. 2 DS-GVO gibt der europäische Gesetzgeber vor, wie die inhaltliche Ausgestaltung der Vorschriften im Sinne von Art. 88 Abs. 1 DS-GVO erfolgen muss. Danach müssen diese Vorschriften „angemessene und besondere Maßnah-

[34] Simitis/*Seifert,* BDSG, § 32 Rn. 122 f.

men zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person" umfassen. Durch den Hinweis in § 26 Abs. 4 BDSG wird klarstellt, dass hiervon nicht nur die Mitgliedstaaten angesprochen werden, sondern auch die Verhandlungspartner einer Kollektivvereinbarung.

Der Begriff der „Angemessenheit" kann so verstanden werden, dass auch im Beschäftigtendatenschutz eine Abwägung derjenigen Belange notwendig ist, die für oder gegen eine Datenverarbeitung sprechen.[35] Der Begriff „besondere Maßnahmen" wird in der englischen Sprachfassung als „specific measures" bezeichnet, so dass hiermit präzisierende Maßnahmen angesprochen sein dürften. Dass bei der Datenverarbeitung die menschliche Würde und die Grundrechte der betroffenen Person zu wahren sind, beinhaltet keine Neuerungen, da sich dies bereits aus den allgemeinen Grundrechtsvorgaben ergibt.

Art. 88 Abs. 2 DS-GVO konkretisiert im Weiteren diese allgemeinen Voraussetzungen. Danach umfassen die Vorschriften Maßnahmen „insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz". Der Schwerpunkt dieser Ausführungen dürfte auf den Maßnahmen zur Herstellung von Transparenz liegen. Diese Transparenzvorgabe sollte bei der Abfassung von Kollektivvereinbarungen besonders beachtet werden. Es ist wichtig, dass die von ihnen erfassten Beschäftigten über die geltenden Informationspflichten bei der Erhebung von personenbezogenen Daten und die ihnen nach der DS-GVO zustehenden Betroffenenrechte aufgeklärt werden.

Für weitere Ausführungen zum Thema „Betriebsvereinbarungen" siehe „Regelung der Datenverarbeitung durch Kollektivvereinbarungen" Seite 63 sowie die Mustertexte in der Anlage.

[35] Kühling/Buchner/*Maschmann*, DS-GVO, Art. 88 Rn. 43.

## o. Verhängung von Geldbußen – Art. 83 DS-GVO

Die Aufsichtsbehörden sollen sicherstellen, dass die Geldbußen für Verstöße gegen die Verordnung „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“[36] sind. Die Wirksamkeit und abschreckende Wirkung der Geldbußen wird durch ihre Höhe erreicht.

Die Aufsichtsbehörden können bei Festlegung der Höhe einer Geldbuße verschiedene Aspekte einbeziehen. Art. 83 Abs. 2 DS-GVO gibt Kriterien vor, die die Aufsichtsbehörden gebührend zu berücksichtigen haben. Ein genaues Studium dieser Aspekte ist sinnvoll, um bei Fehlern auf ein möglichst geringes Bußgeld hinzuwirken. Wie sich aus Art. 83 Abs. 2 lit. k) DS-GVO ergibt, ist dieser Katalog nicht abschließend. Nach Art. 70 Abs. 1 lit. k) DS-GVO gehört es zu den Aufgaben des Europäischen Datenschutzausschusses, Leitlinien für die Festsetzung von Geldbußen zu erarbeiten.

In Art. 83 Abs. 4 und 5 DS-GVO werden Verpflichtungen aufgezählt, deren Verletzung mit einer Geldbuße geahndet werden. Dabei werden die möglichen Verstöße in zwei Bereiche aufgeteilt.

Bei Verstößen, die in Art. 83 Abs. 4 DS-GVO aufgeführt sind, werden Geldbußen von bis zu 10 Mio. Euro oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher Betrag höher ist. Dabei handelt es sich um eher **formale Verstöße**. So fallen u.a. die Verpflichtungen hierunter, die die Verordnung dem Verantwortlichen und Auftragsverarbeiter in den Art. 25 bis 39 DS-GVO auferlegt, also z. B. die Verpflichtung, Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen zu erreichen, ein Verzeichnis von Verarbeitungstätigkeiten zu führen, eine Datenschutz-Folgenabschätzung durchzuführen sowie die Vorgaben zur Auftragsverarbeitung einzuhalten. Auch der Verstoß gegen die Pflicht zur Ergreifung geeigneter und angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten fällt nun neuerdings hierunter.

Bei eher **materiellen Verstößen**, die in Art. 83 Abs. 5 DS-GVO aufgezählt werden, werden Geldbußen von bis zu 20 Mio. Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher Betrag höher ist. Hierunter fallen gemäß Art. 83 Abs. 5 lit. d) DS-GVO auch Verstöße gegen alle Pflichten ge-

[36] Art. 83 Abs. 1 DS-GVO.

mäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden. Damit sind auch Verstöße gegen die Vorgaben zum Beschäftigtendatenschutz hiervon erfasst, die der deutsche Gesetzgeber im Rahmen der Umsetzung von Art. 88 DS-GVO bei der Anpassung des BDSG erlassen hat. Geldbußen in gleicher Höhe werden auch dann verhängt, wenn eine Anweisung der Aufsichtsbehörde, die sie gemäß Art. 58 Abs. 2 DS-GVO erlassen hat, nicht befolgt wurde.

Bei der Frage, was unter dem Begriff „Unternehmen" zu verstehen ist, muss man zunächst auf Art. 4 Nr. 18 DS-GVO abstellen. Danach ist ein Unternehmen eine „natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen". Weiterhin muss Erwägungsgrund 150 DS-GVO beachtet werden. Nach Satz 3 dieses Erwägungsgrundes soll der Begriff des „Unternehmens" im Sinne von Art. 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) verstanden werden. Im Wettbewerbsrecht wird auf den funktionalen Unternehmensbegriff abgestellt, wonach ein Unternehmen eine wirtschaftliche Tätigkeit ausübende Einheit ist, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung.[37] Unklar ist, ob dieser Verweis, der lediglich in einem Erwägungsgrund erfolgt, dazu führen kann, dass die Muttergesellschaft ggf. für das Fehlverhalten ihrer Tochtergesellschaften haftet. Diese Frage ist umstritten. Gute Gründe sprechen dafür, Geldbußen gegen Unternehmen auf der Grundlage des Umsatzes des einzelnen Unternehmens selbst und nicht des Umsatzes der Unternehmensgruppe festzusetzen.[38] Die Datenschutzkonferenz, die sich aus den Datenschutzbehörden des Bundes und der Länder zusammensetzt, vertritt gleichwohl die Auffassung, dass Mutter- und Tochtergesellschaften als wirtschaftliche Einheit betrachtet werden müssen, so dass bei der Bemessung des Bußgeldes der Gesamtumsatz der Unternehmensgruppe zu Grunde zu legen ist.[39]

Nach § 41 Abs. 1 BDSG gelten grundsätzlich die Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG) sinngemäß. Damit müssen auch in diesem Zusammenhang § 30 Abs. 1, § 130 Abs. 1 OWiG Anwendung finden. Das ist für die Frage relevant, wann Verstöße bestimmter Personen gegen die Datenschutz-Grundverordnung dem Unternehmen zugerechnet werden. Nach § 30 Abs. 1 OWiG werden nur Handlungen vertretungsberechtigter Organe einer juristischen Person oder

37 St. Rspr. seit EuGH C-41/90 (Höfner und Elser), Slg. 1991, I-1979, Rn. 21.

38 Faust/Spittka/Wybitul, ZD 2016, 120; a. A. Ehmann/Selmayr/*Nemitz*, DS-GVO, Art. 83 Rn. 42.

39 DSK, Kurzpapier Nr.2 zu „Aufsichtsbefugnisse/Sanktionen", abzurufen unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/07/DSK_KPNr_2_Sanktionen.pdf.

Mitglieder eines solchen Organs sowie andere Leitungspersonen dem Unternehmen zugerechnet. Nach § 130 Abs. 1 OWiG gilt dies, wenn die Aufsichtspflicht über die Mitarbeiter verletzt und hierdurch die Ordnungswidrigkeit ermöglicht wurde. Die Datenschutzkonferenz führt aus, dass es nach dem Wortlaut der DS-GVO für die Zurechnung eines Verstoßes zu einem Unternehmen ausreichen soll, dass ein Beschäftigter des Unternehmens oder ein für das Unternehmen agierender externer Beauftragter gehandelt hat.[40]

[40] DSK, Kurzpapier Nr.2 zu „Aufsichtsbefugnisse/Sanktionen", abzurufen unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/07/DSK_KPNr_2_Sanktionen.pdf.

# 3. GRUNDLAGEN DES BESCHÄFTIGTENDATENSCHUTZES AB MAI 2018

## a. Geltungsbereich des Beschäftigtendatenschutzes

### aa. Beschäftigtenbegriff – § 26 Abs. 8 BDSG

**§ 26 Abs. 8 BDSG:**
Beschäftigte im Sinne dieses Gesetzes sind:

1. Arbeitnehmerinnen und Arbeitnehmer, **einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,**
2. zu ihrer Berufsbildung Beschäftigte,
3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz **oder dem Bundesfreiwilligendienstgesetz** leisten,
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
7. Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

[2] Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte.

Für die Frage, auf welche Personengruppen im Betrieb die spezifischeren deutschen gesetzlichen Regelungen zum Beschäftigtendatenschutz in § 26 BDSG anzuwenden sind, ist entscheidend, wer als Beschäftigter im Sinne dieses Gesetzes zu verstehen ist. Der deutsche Gesetzgeber hat bis auf zwei Anpassungen die bisherige Begriffsdefinition übernommen. Die Datenschutzgrundverordnung selbst enthält keine Begriffsbestimmung.

Aufgrund der Übertragung der bisherigen Regelung in § 3 Abs. 11 BDSG a. F. kann weitestgehend auf die bislang geltenden Begriffsbestimmungen zurückgegriffen werden. Für die betriebliche Praxis sind das besonders folgende Personengruppen:

- **Arbeitnehmer**
  hierfür kann erstmals die gesetzliche niedergelegte Definition in § 611a BGB genutzt werden
- **Leiharbeitnehmer**
  ausdrücklich genannt werden nun auch die Leiharbeitnehmer
- **Auszubildende, Umschüler und Studenten im dualen Studium**
  der Gesetzestext spricht nicht nur von Berufsausbildung, sondern generell von Berufsbildung, d. h. dass nicht nur Auszubildende in IHK-Berufen nach dem BBiG darunter fallen, sondern alle Personen, die von § 1 Abs. 1 BBiG erfasst werden
- **Bewerber**
- **ehemalige Mitarbeiter**
- in **Heimarbeit** Beschäftigte
- **arbeitnehmerähnliche Personen**
  § 12a TVG enthält eine Definition dieses Begriffes. Nach der Rechtsprechung des BAG unterscheidet sich diese Gruppe von den Arbeitnehmern durch den Grad der persönlichen Abhängigkeit, wobei vor allem die Eigenart der jeweiligen Tätigkeit zu berücksichtigen ist. Arbeitnehmerähnliche Personen sind wegen ihrer fehlenden Eingliederung in eine betriebliche Organisation und im Wesentlichen freier Zeitbestimmung nicht im gleichen Maß persönlich abhängig wie Arbeitnehmer; an die Stelle der persönlichen Abhängigkeit und Weisungsgebundenheit tritt das Merkmal der wirtschaftlichen Unselbständigkeit. Jedoch muss der wirtschaftlich Abhängige auch seiner gesamten sozialen Stellung nach einem Arbeitnehmer vergleichbar sozial schutzbedürftig sein[41] (z. B. Einfirmen-Handelsvertreter, Buchhalter, Frachtführer, Franchisenehmer, Testfahrer, nebenamtliche Dozenten, Reporter, Künstler[42]). Eine arbeitnehmerähnliche Person kann auch für mehrere Auftraggeber tätig sein; jedoch ist für sie kennzeichnend, dass die Beschäftigung für einen der Auftraggeber wesentlich ist und die hieraus fließende Vergütung die entscheidende Existenzgrundlage darstellt.[43]

---

41 BAG, 11.04.1997, 5 AZB 33/96, NZA 1998, 499.

42 HWK, 7. Auflage 2016, § 5 BetrVG, Rn. 11; weitere Beispiele: ErfK/*Preis*, § 611 BGB, Rn. 114, 115.

43 BAG, 17.10.1990, 5 AZR 639/89, NZA 1991, 402.

**HINWEIS**
Zwar kommt als spezifizierende Regelung des Art. 6, i. V. m. Art. 88 DS-GVO i. V. m. § 26 Abs. 4 BDSG für die Datenerhebung im Beschäftigtenkontext auch eine Betriebsvereinbarung in Betracht, allerdings gilt diese Betriebsvereinbarung unmittelbar und zwingend nur gegenüber den Personengruppen im Betrieb, für die der Betriebsrat nach § 5 BetrVG zuständig ist. Arbeitnehmerähnliche Personen fallen nicht unter den Anwendungsbereich des BetrVG, so dass eine Betriebsvereinbarung keine Erlaubnisgrundlage für eine Datenverarbeitung ihnen gegenüber sein kann.

Ob Betriebsvereinbarungen auch für Bewerber als eine spezifizierende Ausgestaltung dienen können, ist umstritten.[44] Insbesondere wegen der demokratischen Legitimation durch Betriebsratswahlen sprechen die besseren Argumente gegen eine Regelungsbefugnis der Betriebsparteien für Bewerber.

Fremdpersonal auf dem Betriebsgelände, welches aufgrund von Werk- oder Dienstverträgen mit einem Auftragnehmer-Unternehmer beschäftigt werden (sog. Erfüllungsgehilfen), gehört hingegen ebenso wenig zu den Beschäftigten im Sinn des BDSG wie Soloselbstständige/freie Mitarbeiter, bei denen keine wirtschaftliche Abhängigkeit zum Auftraggeber besteht.

**bb. Datenverarbeitung ohne Dateisystem – § 26 Abs. 7 BDSG**

Die Möglichkeiten der Datenverarbeitung sind vielfältig. Für private Unternehmen findet die DS-GVO gem. Art. 2 Abs. 1 DS-GVO Anwendung,

soweit personenbezogene Daten ganz oder teilweise automatisiert verarbeitet werden (z. B. durch Personalinformationssysteme wie SAP oder PAISY, Zeiterfassungssysteme oder innerhalb der elektronischen Personalakte)

sowie

für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

[44] Dagegen: *Bausewein*, ZD 2014, 443; dafür: *Kort*, NZA-Beilage 2016, 62.

Darauf aufbauend wird durch § 26 Abs. 7 BDSG der Anwendungsbereich der DS-GVO wesentlich erweitert, sofern es sich um die Verarbeitung von Beschäftigtendaten handelt. Danach gelten die Vorgaben des § 26 Abs. 1 bis Abs. 6 BDSG auch, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Damit wird die alte Rechtslage nach § 32 Abs. 2 BDSG a. F. inhaltsgleich fortgeführt.

Diese Ausweitung gilt allerdings nicht für andere Regelungsbereiche außerhalb des § 26 BDSG. Bei § 26 Abs. 7 BDSG handelt es sich systematisch weiterhin um eine materielles Datenschutzrecht in Bezug nehmende Ausnahmevorschrift. Eine generelle Anwendung der Regelung, insbesondere auf die Betroffenenrechte der §§ 32 bis 36 BDSG, ergibt sich auch nach der neuen Rechtslage nicht.[45] Das heißt, der erweiterte Anwendungsbereich auf sämtliche Datenverarbeitungen gilt nur im Zusammenhang mit § 26 BDSG.

Werden Beschäftigtendaten für Zwecke außerhalb des Beschäftigungsverhältnisses verarbeitet, ist das BDSG nur anwendbar, wenn die Voraussetzungen des Art. 2 Abs. 1 DS-GVO erfüllt sind.

**BEISPIEL**
Eine Verwendung von Mitarbeiteradressen zu dem Zweck, die eigenen Unternehmensprodukte zu bewerben, ist nicht für die Durchführung der arbeitsvertraglichen Beziehungen erforderlich und hat somit keinen Bezug zum eigentlichen Beschäftigungsverhältnis.

**HINWEIS**
Die Regelung in § 26 Abs. 7 BDSG führt im Ergebnis dazu, dass jede Form der Verarbeitung von Arbeitnehmerdaten zum Zwecke des Beschäftigungsverhältnisses vom Geltungsbereich des § 26 BDSG erfasst wird. Hierzu zählt bspw. die handschriftliche Notiz der Führungskraft in einem Mitarbeitergespräch.

[45] BAG, 16.11.2010, 9 AZR 573/09.

## b. Die Verarbeitung personenbezogener Daten von Beschäftigten

### aa. Verarbeitung von Beschäftigtendaten – § 26 Abs. 1 BDSG

#### (1) Der in Art. 88 DS-GVO gesetzte Rahmen für spezifischere nationale Regelungen

Die nationale Regelung zur Verarbeitung personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses (besondere Verarbeitungssituation) findet sich in § 26 BDSG. Dieser Paragraph unterscheidet sich auf den ersten Blick aufgrund seines Umfangs deutlich von der bisherigen Regelung in § 32 BDSG a. F. In nunmehr acht Absätzen statt bisher in drei hat der deutsche Gesetzgeber die Möglichkeit wahrgenommen, gemäß Art. 88 Abs. 1 der DS-GVO für die Datenverarbeitung im Beschäftigungskontext spezifischere Vorschriften einzuführen.

Ziel dieser Vorschriften darf nach dem Wortlaut des Art. 88 Abs. 1 DS-GVO nur die Gewährleistung des Schutzes der Rechte und Freiheiten der Beschäftigten hinsichtlich der personenbezogenen Beschäftigtendaten im Beschäftigungskontext sein. Art. 88 Abs. 1 DS-GVO nennt hier, nicht abschließend, die Zwecke

1. Einstellung in ein Beschäftigungsverhältnis,
2. Erfüllung des Arbeitsvertrags einschließlich
   - der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten,
   - des Managements, der Planung und der Organisation der Arbeit,
   - der Gleichheit und Diversität am Arbeitsplatz,
   - der Gesundheit und Sicherheit am Arbeitsplatz,
   - des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie
   - der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und
3. Beendigung des Beschäftigungsverhältnisses.

Diese Vorschriften müssen nach Art. 88 Abs. 2 DS-GVO angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz umfassen.

**(2) Zulässige Verarbeitungszwecke**

In Absatz 1 des § 26 BDSG ist der Inhalt des bisherigen § 32 Abs. 1 BDSG a. F. annähernd wortgleich übernommen worden.

Danach dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies erforderlich ist

1. für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder
2. für dessen Durchführung,
3. für dessen Beendigung oder
4. zur Ausübung oder Erfüllung der sich aus einem Gesetz oder aus einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten.

**Beispiele** für Zwecke der Verarbeitung von Personendaten in den einzelnen Phasen des Beschäftigungsverhältnisses:

In der **Bewerbungsphase** ist die Verarbeitung der Daten daran auszurichten, was für die Entscheidung über den Abschluss eines Vertrages erforderlich ist. Mögliche Daten können sein:

- Ausgefüllter Bewerbungsbogen, Lebenslauf, (ggf. handschriftlich), Anschreiben, Foto, Zeugnisse, Arbeitszeugnisse, Empfehlungsschreiben, Stammdaten, Kontaktdaten, Staatsangehörigkeit, Arbeitserlaubnis, Leistungsbeurteilungen
- Zugangsdaten zu einem elektronischen Bewerbungssystem
- Daten, die sich aus öffentlich zugänglichen sozialen Netzwerken mit beruflichem Schwerpunkt entnehmen lassen
- Daten aus Bewerbungsgesprächen wie Selbsteinschätzung, Gehaltsvorstellungen, Reisebereitschaft, fachliche Kenntnisse, Sprachkenntnisse
- ggf. auch Bild- und Tondaten aus Bewerbungsvideos oder Videointerviews
- Kontodaten im Falle der Erstattung von Reisekosten
- Gesundheitsdaten, zum Beispiel Schwerbehinderteneigenschaft

Die Bewerbungsdaten sollten solange aufbewahrt werden, wie eine Geltendmachung von Ansprüchen nach dem Allgemeinen Gleichstellungsgesetz (AGG) möglich ist.[46]

Sofern die Bewerbung für die Entscheidung der Besetzung einer anderen Stelle als der, auf die sich die betroffene Person konkret beworben hat, genutzt werden soll, ist die Einwilligung der betroffenen Person einzuholen.

Im Rahmen der **Einstellung** werden weitere Daten beim Betroffenen erhoben, insbesondere Sozialversicherungs- und Steuerdaten. In Ausnahmefällen kann nach der Einstellungsentscheidung für bestimmte Funktionen die Vorlage eines polizeilichen Führungszeugnisses verlangt werden, so beispielsweise im Banken- und Versicherungsbereich, im Bewachungsgewerbe oder in der Jugendarbeit.

Während der **Laufzeit eines Beschäftigungsverhältnisses** kommen je nach Art der Tätigkeit vielfältige Verarbeitungszwecke in Frage:

- Personaladministration, ggf. einschließlich des konzerninternen Datenaustausches
- Meldung und Beitragsabführung zur Sozialversicherung (Rente, Arbeitslosigkeit, Krankheit, Pflege)
- Planung der Arbeitszeit (Schichtplanung)
- Erfassung der Arbeitszeit
- Gehaltsberechnung (ggf. mit variablen Anteilen und Zulagen), Gehaltsbesteuerung, Gehaltszahlung und (elektronische) Versendung von Einkommensnachweisen
- Mitarbeiterscreening gegen Sanktionslisten der EU
- Arbeitsorganisation
- Ausstattung mit Arbeitsmitteln wie Kommunikationstechnik, Arbeitskleidung, Büroausstattung

[46] Von Aufsichtsbehörden wird hier für eine kurze Aufbewahrungsfrist von zwei Monaten nach Zugang der Ablehnung argumentiert, wogegen eine Aufbewahrung analog der allgemeinen Verjährungsfristen nach BGB praktikabler erscheint.

- Betriebsinterne Kommunikation, auch in betrieblichen sozialen Netzwerken
- Kommunikation mit Kunden und Dienstleistern
- Kontrolle von ausdrücklichen umfassenden Verboten der privaten Nutzung von Betriebsmitteln, einschließlich der Kommunikationstechnik[47]
- Sicherung der betrieblichen Infrastruktur des Arbeitgebers einschließlich der Informationstechnologie (Mitarbeiterausweise, Zugangsdaten zu Gebäuden und technischer Infrastruktur, Videoüberwachung sicherheitsrelevanter Betriebsbereiche)
- Betriebssteuerung und Produktion, insbesondere mittels IT-Systemen
- Schutz des Eigentums des Arbeitgebers, der Kunden und der Beschäftigten
- Arbeits- und Gesundheitsschutz
- Urlaubsgewährung und Urlaubsabgeltung
- Leistungsbeurteilung
- Fortbildung und berufliche Entwicklung
- Reisebuchung, Reisesicherheit, Reisekostenabrechnung
- Auszeichnungen und betriebliches Vorschlagswesen
- Mitarbeiterbefragungen
- Teilhabe (Diversity)
- Mutterschutz
- Eltern- und Pflegezeit
- Interne Bewerbungsverfahren
- Entgelt-Transparenz
- Betriebliche Altersversorgung
- Firmenwagen, einschließlich Nutzungsdaten
- Kreditkarten, Tankkarten
- Rabattkarten
- Wahrung der betrieblichen Mitbestimmung
- Wahrung der Schwerbehindertenrechte
- Betriebsärztliche Dienste
- Beendigung des Beschäftigungsverhältnisses

[47] Vgl. zur Nutzung von Webmail-Dienst EGMR, 05.09.2017, Az. 61496/08.

Nach der **Beendigung des Beschäftigungsverhältnisses** kann die Datenverarbeitung aufgrund nachwirkender vertraglicher Pflichten, zum Beispiel der Berechnung variablen Entgelts, sowie gesetzlicher Vorgaben zur Aufbewahrung, zum Beispiel nach der Abgabenordnung, erforderlich und zulässig sein.

Im Vergleich zu § 32 BDSG a. F. wurde in § 26 Abs. 1 Satz 1 BDSG ausdrücklich aufgenommen, dass Verarbeitungen von Beschäftigtendaten durch Mitarbeitervertretungen gestattet sind, wenn sie zur Ausübung oder Erfüllung von Rechten und Pflichten der Interessenvertretung erforderlich sind. Diese Rechte und Pflichten müssen sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung ergeben. Die zur Ausübung oder Erfüllung der Rechte und Pflichten erforderliche Datenverarbeitung bedarf folglich immer einer Rechtsgrundlage.

Nach § 26 Abs. 1 Satz 1 BDSG ist eine Erforderlichkeitsprüfung auch dann vorzunehmen, wenn personenbezogene Daten durch Mitarbeitervertretungen verarbeitet werden. Werden Daten von ihr eigenständig verarbeitet, muss deshalb insbesondere darauf geachtet werden, ob ein Aufgabenbezug besteht und die Verarbeitung der Zweckbestimmung entspricht. Es ist zu prüfen, ob tatsächlich ein Personenbezug notwendig oder anonymisierte Daten zur Aufgabenerfüllung ausreichend sind. Zudem ist ein schonender Interessenausgleich zwischen den Interessen der Mitarbeitervertretung und den Interessen der Beschäftigten herbeizuführen. Eine Verarbeitung von Beschäftigtendaten durch die Mitarbeitervertretung kommt nur so lange in Betracht, wie sie im Rahmen seiner kollektivrechtlich begründeten Rechte und Pflichten tatsächlich notwendig ist.

Die Interessenvertretung der Beschäftigten erhält u. a. durch das Betriebsverfassungsrecht zahlreiche Rechte und auch Pflichten, deren Ausübung und Erfüllung von der Verarbeitung von Beschäftigtendaten abhängen.

**BEISPIELE**

- Mitbestimmungsrecht des Betriebsrates bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen, § 87 Abs.1 Nr. 6 Betriebsverfassungsgesetz; in der Regel werden hierzu Betriebsvereinbarungen geschlossen, die dem Betriebsrat Kontrollrechte einräumen. Diese dürfen eine Nutzung personenbezogener Daten jedoch nur im für die Ausübung dieser Rechte erforderlichen Maße und somit keine weitreichenden Dauerzugriffsrechte auf IT-Systeme für Betriebsräte beinhalten.
- Zustimmung bei Einstellungen, § 99 BetrVG und Anhörung bei Kündigungen, § 102 BetrVG

Danach hat der Arbeitgeber dem Betriebsrat die erforderlichen Bewerbungsunterlagen vorzulegen und Angaben über die Person der Beteiligten bzw. den Arbeitnehmer zu machen. Bei Einstellungen und Versetzungen hat der Arbeitgeber insbesondere die vorgesehene zukünftige Stelle und Eingruppierung mitzuteilen. Die Mitglieder des Betriebsrats sind verpflichtet, die ihnen hierbei bekanntwerdenden persönlichen Verhältnisse und Angelegenheiten der Arbeitnehmer vertraulich zu behandeln.

Nach Satz 2 des § 26 Abs. 1 BDSG ist es weiterhin möglich, zur Aufdeckung von Straftaten personenbezogene Daten von Beschäftigten zu verarbeiten, wenn durch tatsächliche Anhaltspunkte der Verdacht besteht, dass die beschäftigte Person im Beschäftigungsverhältnis eine Straftat begangen hat. Der Verdacht muss schriftlich dokumentiert werden und die Verarbeitung der Daten muss zur Aufdeckung erforderlich sein.

Zusätzlich ist zu prüfen, ob die beschäftigte Person ein schutzwürdiges Interesse hat, welches die Verarbeitung der Daten zu diesem Zweck ausschließt. So dürfen Art und Ausmaß der Datenverarbeitung im Hinblick auf den Anlass nicht unverhältnismäßig sein.

Ebenso grundsätzlich zulässig ist, obwohl nicht ausdrücklich erwähnt, die Verarbeitung von personenbezogenen Daten im Zusammenhang mit Pflichtverletzungen unterhalb der Strafbarkeitsschwelle.[48] Dies ergibt sich direkt aus den arbeitsvertraglichen und arbeitsrechtlichen Regelungen.

[48] *Wybitul,* NZA 2017, S. 413.

Beispiele für nicht strafbare Pflichtverletzungen im Beschäftigungsverhältnis sind solche, die Ermahnungen, Abmahnungen oder Kündigungen begründen können.[49]

### (3) Der Verarbeitungsbegriff

Der Verordnung angepasst wurde die Begrifflichkeit der „Verarbeitung". Statt von „Erhebung, Verarbeitung und Nutzung" wie im BDSG a. F. wird nun zusammenfassend von „Verarbeitung" gesprochen.

**Verarbeitung:**
Darunter ist nach Art. 4 Ziffer 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie 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, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung zu verstehen.

### (4) Erforderlichkeit als Prüfungsmaßstab

§ 26 BDSG schreibt vor, dass die Datenverarbeitung erforderlich sein muss. Der Verantwortliche hat deshalb bei jedem einzelnen Verarbeitungsverfahren im Anschluss an die Festlegung der Zwecke und Rechtsgrundlagen die zu verarbeitenden personenbezogenen Daten und die zugehörigen Prozesse einer Erforderlichkeitsprüfung zu unterziehen. Dies setzt voraus, dass die Daten und die Modalitäten ihrer Verarbeitung überhaupt geeignet sind, die zulässigen Zwecke zu erreichen, und gleichzeitig das mildeste aller gleich geeigneten Mittel darstellen. Die Grundrechte des Verantwortlichen und die der betroffenen Beschäftigten sind sodann gegeneinander abzuwägen und die gegensätzlichen Interessen an der Verarbeitung und an einem größtmöglichen Schutz des Persönlichkeitsrechtes soweit als möglich in Einklang zu bringen.[50]

[49] Vgl. zur Nutzung von Webmail-Dienst EGMR, 05.09.2017, 61496/08.

[50] Herstellung praktischer Konkordanz gemäß BT DRS 18/11325, 97.

#### (5) Verhältnis des § 26 BDSG zu anderen bundesrechtlichen Regelungen zum Datenschutz

Die spezifischeren Regelungen des BDSG und anderer nationaler Gesetze kommen dort zur Anwendung, wo die DS-GVO Öffnungsklauseln enthält. Das BDSG a. F. galt gemäß § 1 Abs. 3 Satz 1 nur dort, wo das deutsche Recht nicht die Anwendung anderer Rechtsvorschriften auf personenbezogene Daten und deren Veröffentlichung vorsah. Seine Vorschriften waren Auffangregelungen und subsidiär. Nach § 1 Abs. 2 BDSG gehen andere Rechtsvorschriften des Bundes über den Datenschutz den Vorschriften des BDSG vor. Regeln sie allerdings einen Sachverhalt, für den das BDSG gilt, nicht abschließend, finden die Vorschriften des BDSG Anwendung. Daraus ergibt sich, dass alle bundesrechtlichen Regelungen zum Beschäftigtendatenschutz nunmehr gleichrangig sein können, unabhängig davon, in welchem Gesetz sie enthalten sind. Dies hat zur Folge, dass auch Bestimmungen aus dem kollektiven Arbeitsrecht, deren Umsetzung Datenverarbeitungen nach sich ziehen, nicht mehr generell als vorrangig betrachtet werden dürfen. Für die Zwecke der Mitbestimmung ist dies ein neuer Ansatz, der dazu beiträgt, dass die datenschutzrechtlich notwendigen Rechtsgrundlagen für die Verarbeitung von Beschäftigtendaten durch Betriebsratsgremien nun größere Bedeutung erlangen werden und die Erforderlichkeitsprüfung (siehe vorstehend unter (4)) auch hier durchzuführen ist.[51]

### bb. Videoüberwachung von Mitarbeitern

Unternehmen können erhebliche Schäden durch Straftaten oder andere schwere Verfehlungen ihrer Mitarbeiter sowie durch Eigentumsdelikte von Kunden entstehen. Um dem zu begegnen und ein solches Verhalten zu verfolgen, können insbesondere Videoüberwachungsanlagen eingesetzt werden. Je nach Einzelfall ist es sinnvoll, solche Anlagen offen oder verdeckt zu installieren. Hiervon können Arbeitsplätze betroffen sein, die entweder in öffentlich zugänglichen Räumen liegen oder bei denen die Öffentlichkeit keinen Zugang hat.

#### (1) Offene Videoüberwachung öffentlich zugänglicher Räume

Offene Videoüberwachungsanlagen werden häufig eingesetzt, um das Eigentum des Arbeitgebers vor Diebstahl durch Kunden zu schützen. Ist die Kamera in einem öffentlich zugänglichen Raum angebracht, können hiervon auch Arbeitsplätze betroffen sein.

---

[51] So im Ergebnis auch *Wybitul*, NZA 2017, S. 413.

**BEISPIEL**
Öffentlich zugängliche Arbeitsplätze sind Bereiche, die dem öffentlichen Verkehr gewidmet sind oder nach dem Willen des Berechtigten von jedermann betreten werden können. Erfasst werden hiervon z. B. für Besucher zugängliche Bereiche öffentlicher Gebäude und für das allgemeine Publikum geöffnete Bereiche von Geschäftsräumen[52], so z. B. in Bankfilialen, Kaufhäusern, Tankstellen, Restaurants, Bahnhöfen.

In diesen Fällen macht § 4 BDSG Ausführungen zur Videoüberwachung öffentlicher Räume. Die Datenschutzkonferenz betont jedoch, dass im jeweiligen konkreten Einzelfall entschieden werden muss, ob § 4 BDSG aufgrund des Anwendungsvorrangs der DS-GVO angewendet werden kann.[53]

**HINWEIS**
Zur Stärkung des Sicherheitsniveaus hat der deutsche Gesetzgeber das „Videoüberwachungsverbesserungsgesetz" verabschiedet, mit dem § 6b BDSG a. F. abgeändert wird. Dieses Gesetz ist am 5. Mai 2017 in Kraft getreten. Es nimmt in vielen Fällen die Änderungen vorweg, die ab dem 25. Mai 2018 im Rahmen von § 4 BDSG, der dann die Videoüberwachung öffentlich zugänglicher Räume regeln wird, gelten werden.

Eine Videoüberwachung öffentlich zugänglicher Räume im Sinne von § 4 BDSG ist nur dann zulässig, wenn einer der in § 4 Abs. 1 Satz 1 BDSG aufgezählten Zulässigkeitstatbestände vorliegt. Für die Unternehmenspraxis sind die Wahrnehmung des Hausrechts (Nr. 2) sowie die Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (Nr. 3) relevant. Es ist in jedem Fall eine Abwägungsentscheidung zu treffen, bei der die neu in § 4 BDSG aufgenommenen Belange ein besonderes Gewicht haben.

---

52 Plath/Becker, BDSG, § 6b Rn. 9.

53 Die Datenschutzkonferenz stellt im Rahmen der DS-GVO auf Art. 6 Abs. 1 lit. f) für die Prüfung der Rechtmäßigkeit der Datenverarbeitung ab. Sie führt aus, dass im Rahmen der Interessenabwägung insbesondere im Arbeitsverhältnis ein strengerer Maßstab anzulegen sein wird, als wenn der Betroffene als Kunde, Gast oder Passant von einer Videoüberwachung erfasst würde. Siehe hierzu: DSK, Kurzpapier Nr. 15 zu „Videoüberwachung nach der Datenschutz-Grundverordnung", abzurufen unter: https://www.lda.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf.

In **§ 4 Abs. 1 Satz 2 BDSG** wird folgende Neuerung eingefügt:
Bei der Videoüberwachung von
1. öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder
2. Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs

gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse.

Will der Betreiber einer öffentlich zugänglichen großflächigen Anlage eine Videoüberwachung vornehmen, um hierdurch Leben, Gesundheit oder Freiheit von Personen, die sich dort aufhalten, zu schützen, so ist dies ein besonders wichtiges Interesse. Eine Abwägungsentscheidung wird deshalb regelmäßig zugunsten des Einsatzes der Videoüberwachung ausfallen. Diese Abwägung ist für jede Teilanlage der öffentlich zugänglichen großflächigen Anlage gesondert vorzunehmen.[54]

**HINWEIS**
Unternehmen, die eine Videoüberwachung öffentlich zugänglicher Räume anstreben, müssen vorab eine Datenschutz-Folgenabschätzung durchführen: Nach Art. 35 Abs. 3 lit. c) DS-GVO muss bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche eine Datenschutz-Folgenabschätzung durchgeführt werden. Erwägungsgrund 91 DS-GVO konkretisiert diese Vorgabe auf „optoelektronische Vorrichtungen", worunter auch die Videoüberwachung zu verstehen ist.

### (2) Offene Videoüberwachung nicht öffentlich zugänglicher Räume

Für die offene Videoüberwachung in nicht öffentlich zugänglichen Räumen wie z. B. in einer Lager- oder Werkshalle kommt nach bisheriger Rechtslage § 32 Abs. 1 Satz 1, 2 BDSG a. F. in Betracht. Danach muss die Datenverarbeitung insbesondere zur Durchführung des Beschäftigungsverhältnisses oder zur Aufdeckung einer strafbaren Handlung oder einer anderen schweren Verfehlung erforderlich sein. Nachdem der Gesetzgeber bei der Anpassung des deutschen Rechts an die DS-GVO diese Vorgaben unverändert in § 26 Abs. 1 Satz 1, 2 BDSG übernommen hat, ergibt sich hier keine Veränderung zur bisherigen Rechtslage.

[54] Vgl. Gesetzesbegründung zum Videoüberwachungsverbesserungsgesetz.

**BEISPIEL**
In einem Unternehmen werden kurzzeitig per Video die Arbeitsschritte aufgezeichnet, die im Rahmen der Montage von Maschinen anfallen. Die Aufzeichnungen werden zur Optimierung von Arbeitsabläufen genutzt, um einen Produktivitätsfortschritt zu erzielen.

Gleichwohl muss darauf geachtet werden, dass hierbei die allgemeinen Vorgaben der DS-GVO wie Informationspflichten, Dokumentationspflichten oder ggf. eine Datenschutz-Folgenabschätzung eingehalten werden.

**(3) Verdeckte Videoüberwachung öffentlich zugänglicher Räume**

In Ausnahmefällen kann nach der bisherigen Rechtsprechung des BAG[55] auch eine verdeckte Videoüberwachung öffentlich zugänglicher Räume zur Kontrolle von Beschäftigten zulässig sein. Das BAG hat argumentiert, dass aus der Pflicht zur Kenntlichmachung der Beobachtung in § 6b Abs. 2 BDSG a. F. kein absolutes Verbot der verdeckten Videoüberwachung resultiert. Hintergrund ist, dass bei einem absoluten Verbot der Videoüberwachung die notwendige Interessenabwägung immer zu Ungunsten des Arbeitgebers ausfallen würde, was nicht den Grundsätzen einer Interessenabwägung entsprechen kann.

Ob auch mit Geltung der DS-GVO verdeckte Mitarbeiterkontrollen weiterhin zulässig sind, ist in der Literatur umstritten. Einer verdeckten Mitarbeiterkontrolle könnte der Transparenzgrundsatz in Art. 5 Abs. 1 lit. a) DS-GVO entgegenstehen, der auch im Beschäftigungsverhältnis zu beachten ist. Gleiches gilt für die in Art. 13 DS-GVO vorgesehene Informationspflicht des Verantwortlichen, der bereits bei Erhebung der Daten nachgekommen werden muss.[56] Gegen Stimmen[57] in der Literatur, die hieraus ein grundsätzliches Verbot verdeckter Überwachungsmaßnahmen im Arbeitsverhältnis ableiten, spricht jedoch die oben aufgezeigte Argumentation des BAG, wenn sie auf die neue Rechtlage übertragen wird. Denn auch mit der Geltung der DS-GVO und des neugefassten BDSG ist eine Abwägung der Interessen von Arbeitgeber und Betroffenem erforderlich. Würde man

55 BAG, 21.06.2012, 2 AZR 153/11.

56 Die DSK betont diese europäischen Vorgaben und führt - ohne konkret auf das Arbeitsverhältnis einzugehen - aus, dass eine intransparente Videoüberwachung nicht im Einklang mit der DS-GVO stehe. Siehe hierzu: DSK, Kurzpapier Nr. 15 zu "Videoüberwachung nach der Datenschutz-Grundverordnung", abzurufen unter: https://www.lda.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf

57 Kühling/Buchner/*Maschmann*, DS-GVO, Art. 88 Rn. 47.

wegen des Transparenzgrundsatzes und der Informationspflicht eine verdeckte Videoüberwachung ausschließen, fiele diese Abwägung immer zu Ungunsten des Arbeitgeberinteresses aus und würde damit den Grundsätzen einer Interessenabwägung widersprechen. Seine z. B. durch Art. 14 Abs. 1 Grundgesetz geschützte Rechtsposition ließe sich nicht wirkungsvoll schützen.[58] Das Eigentum unterliegt auch europarechtlich einem besonderen Schutz, wie durch Art. 17 der Charta der Grundrechte der Europäischen Union deutlich wird. Zudem benennt Art. 88 Abs. 1 DS-GVO den Schutz des Eigentums des Arbeitgebers als wichtigen Aspekt im Bereich des Beschäftigtendatenschutzes. Deshalb lässt sich argumentieren, dass auch in Zukunft eine verdeckte Videoüberwachung öffentlich zugänglicher Räume zulässig sein muss.[59]

**(4) Verdeckte Videoüberwachung nicht öffentlich zugänglicher Räume**

Nach heutiger Rechtslage richtet sich die verdeckte Videoüberwachung nicht öffentlich zugänglicher Räume, soweit Arbeitnehmer betroffen sind, nach § 32 Abs. 1 Satz 2 BDSG a. F.[60] Die dort geregelten Voraussetzungen sind unverändert in § 26 BDSG übertragen worden, so dass sich diesbezüglich keine Veränderung zur bisherigen Rechtslage ergibt.

Ebenso wie bei der verdeckten Videoüberwachung öffentlich zugänglicher Räume stellt sich aber vor dem Hintergrund des Transparenzgrundsatzes und der Informationspflicht der DS-GVO auch bei einer verdeckten Überwachung nicht öffentlich zugänglicher Räume die Frage nach der generellen Zulässigkeit eines solchen Vorgehens. Auf der Grundlage der unter Punkt (3) gemachten Ausführungen lässt sich auch in dieser Konstellation argumentieren, dass eine verdeckte Videoüberwachung öffentlich nicht zugänglicher Räume auch unter Geltung der DS-GVO zulässig sein muss.[61]

## c. Regelung der Datenverarbeitung durch Kollektivvereinbarungen

Mit Art. 88 DS-GVO und § 26 BDSG sind erstmals Regelungen in den Wortlaut der Gesetze aufgenommen worden, wonach die Rechtmäßigkeit einer Datenverarbeitung auf eine Kollektivvereinbarung gestützt werden kann.

---

58 *Byers,* NZA 2017, S. 1086.

59 So im Ergebnis auch *Lachenmann*, ZD 2017, S. 407.

60 Gola/Schomerus, BDSG, § 32 Rn. 19.

61 *Byers*, NZA 2017, S. 1086.

Nach Art. 88 DS-GVO können Kollektivverträge – einschließlich Betriebsvereinbarungen aufgrund der expliziten Erwähnung in Erwägungsgrund 155 DS-GVO - „spezifischere Vorschriften" für die Verarbeitung personenbezogener Daten im Beschäftigungskontext vorsehen. Eine nähere Erläuterung wie der Begriff „spezifischere Vorschriften" ausgelegt werden kann, sieht die DS-GVO nicht vor, sodass die Auslegung dieses Begriffes sehr umstritten ist.[62] Es spricht mehr dafür, dass den Mitgliedstaaten im Rahmen des Art. 88 DS-GVO nur eine Konkretisierungs-, aber keine Abweichungskompetenz zukommt. Sollte man dem nationalen Gesetzgeber einen weiten Regelungsspielraum und auch eine Abweichungskompetenz zugestehen, so müsste sowohl das Datenschutzniveau der DS-GVO überschritten als auch unterschritten werden dürfen.[63] Dies bedeutet in Bezug auf Betriebsvereinbarungen, dass diese – wie früher – konkretisieren können und den Betriebsparteien ein weiter Beurteilungsspielraum verbleibt, soweit das Schutzniveau in Art. 88 Abs. 2 DS-GVO beachtet wird. So wird überwiegend davon ausgegangen, dass sich durch die DS-GVO und § 26 BDSG keine großen Veränderungen im Vergleich zu den bisherigen Anforderungen an Betriebsvereinbarungen, die durch die Rechtsprechung aufgestellt wurden, ergeben. Auf der Grundlage von Art. 6 Abs. 1 lit. b) i. V. m. Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 4 BDSG können Betriebsvereinbarungen weiterhin genutzt werden, um praxisnah die Verarbeitung von personenbezogenen Daten zu gestalten. Nach der Gesetzesbegründung stellt § 26 Abs. 4 BDSG klar, dass Tarifverträge, Betriebsvereinbarungen oder Dienstvereinbarung weiterhin die Rechtsgrundlage für Regelungen zum Beschäftigtendatenschutz bilden können. Sie sollen den Handlungsparteien der Kollektivvereinbarungen die Ausgestaltung eines auf die betrieblichen Bedürfnisse zugeschnittenen Beschäftigtendatenschutzes ermöglichen. Dabei steht ihnen ein Ermessensspielraum im Rahmen des geltenden Rechts zur Verfügung, wobei Art. 88 Abs. 2 der DSG-Verordnung zu beachten ist.[64]

Nach der bisherigen Rechtslage konnten Betriebsvereinbarungen Grundlage für die Datenverarbeitung sein, da sie nach der Rechtsprechung des BAG eine andere Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG a. F. darstellten.[65] Bereits auf dieser Grundlage und wegen des Mitbestimmungsrechts des Betriebsrates nach § 87

---

62 Hierzu *Traut*, RDV 2016, S. 312; *Maschmann*, DB 2016, S. 2480; *Körner*, NZA 2016, S. 1383; *Düwell/Brink*, NZA 2016, S. 665; *Gola/Pötters/Thüsing*, RDV 2016, S. 58; *Taeger/Rose*, BB 2016, S. 819, 830; *Wybitul/Sörup/Pötters*, ZD 2015, S. 559; *Klösel/Mahnhold*, NZA 2017, S. 1428; *Haußmann/Brauneisen*, BB 2017, S. 3065; *Wybital*, NZA 2017, S. 1488.

63 In diesem Sinne Beck-OK Datenschutzrecht – *Riesenhuber,* Art 88 Rn. 67; wohl auch *Düwell/Brink* NZA 2017, S. 1081 f.

64 BT-Drs. 2017, S. 101.

65 BAG, 20.12.1995 – 7 ABR 8/95; BAG, 09.07.2013, 1 ABR 2/13; BAG, 17.11.2016, 2 AZR 730/15.

Abs. 1 Nr. 6 BetrVG bei der Einführung von technischen Einrichtungen, wurden bereits in der Vergangenheit Rahmenbetriebsvereinbarungen zum Schutz vor Beschäftigtendaten aufgesetzt.[66] So hat das BAG es als zulässig angesehen, mittels Betriebsvereinbarung einen Busfahrer zu verpflichten – zumindest unter Einsatz eines anonymisierten Schlüssels – an einem sogenannten RIBAS-Systems (System zur Sprit-Spar-Technik) teilzunehmen.[67] Nach der ständigen Rechtsprechung des BAG sind Betriebsvereinbarungen jedoch unwirksam, wenn sie gegen § 75 Abs. 2 Satz 1 BetrVG i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG verstoßen, da sie dem allgemeinen Persönlichkeitsrecht der Arbeitnehmer nicht in angemessenem Umfang Rechnung tragen. Das BAG hat daher zuletzt eine Betriebsvereinbarung zur „Belastungsstatistik", die durch eine technische Überwachungseinrichtung i. S. d. § 87 Abs. 1 Nr. 6 BetrVG dauerhaft die Erfassung, Speicherung und Auswertung einzelner Arbeitsschritte und damit des wesentlichen Arbeitsverhaltens der Arbeitnehmer anhand quantitativer Kriterien während ihrer gesamten Arbeitszeit vorsah, für unwirksam erklärt. Der dadurch gegebene ständige Überwachungs-, Anpassungs- und Leistungsdruck sei nicht durch überwiegende schutzwürdige Belange des Arbeitgebers gerechtfertigt.[68]

Um künftig eine wirksame Grundlage für die Datenverarbeitung von Beschäftigtendaten darstellen zu können, müssen Betriebsvereinbarungen die Grenzen der DS-GVO beachten. In der Literatur wird deshalb häufig darauf hingewiesen, dass die bestehenden Betriebsvereinbarungen überprüft und angepasst werden müssen. Danach sollten Betriebsvereinbarungen künftig

- deutlich machen, dass ein datenschutzrechtlicher Ausnahmetatbestand geschaffen werden soll
- eine genaue und transparente Beschreibung der Datenverarbeitung enthalten,
- geeignete Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und Grundrechte betroffener Personen beinhalten
- die Rechte der Betroffenen sowie die Pflichten des für die Verarbeitung Verantwortlichen (Arbeitgeber/Auftragsdatenverarbeitung) benennen
- mögliche Zweckänderung der erhobenen Daten voraussehen und in der Betriebsvereinbarung selbst bilden.[69]

---

66 Zum systematischen Aufbau von Betriebsvereinbarung siehe *Beckschulze/Fackeldey,* RDV 2013, 109; Wybitul, NZA 2014, S. 225; Baker McKenzie (Hrsg.), Koops, Arbeitsrecht 4.0, 2017, S. 111; *Kramer-Raif,* IT-Arbeitsrecht 2017, C Rn. 158 ff., 183 ff.

67 BAG, 17.11.2016, 2 AZR 730/15, NZA 2017, S. 394.

68 BAG, 25.04.2017, 1 ABR 46/15, BB 2017, S. 2428.

69 *Olberts,* NWB 2016, S. 2118; *Jacobi/Hoffmann-Remy,* ArbRB 2016, S. 129; *Wybitul/Sörup/Pötters, ZD* 2015, S. 559, 564.

Diese Ausführungen gehen aber zu weit. Betriebsvereinbarungen haben sich zwar am Grundsatz des Art. 88 Abs. 2 DS-GVO auszurichten. So wiederholt Art. 88 Abs. 2 DS-GVO im Wesentlichen die allgemeine Abwägungsformel des Art. 6 Abs. 1 lit. f) DS-GVO[70]. Die Ausführungen darin beschreiben jedoch die Grundsätze der Verhältnismäßigkeit und die Wahrung des Persönlichkeitsrechts, wie es bereits jetzt in § 75 BetrVG vorgesehen ist. Die Betriebsvereinbarung stellt nach Art. 6 Abs. 1 lit. b) i. V. m. Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 4 BDSG einen Erlaubnistatbestand unabhängig davon dar, ob die Betriebsvereinbarung dies noch einmal deklaratorisch ausführt oder nicht. Ferner bestehen die Transparenzpflichten nach Art. 12 DS-GVO ebenfalls, unabhängig davon, ob dies in der Betriebsvereinbarung ausgeführt ist oder nicht. Allein die Beschreibung der Datenverarbeitung in der Betriebsvereinbarung ist insoweit ausreichend, da die Betriebsvereinbarung Rechtsnormcharakter hat (§ 77 BetrVG) und sie insoweit aushangpflichtig ist. Durch die Veröffentlichung der entsprechenden BV ist daher dem Transparenzgedanken Rechnung getragen worden. Es ist insofern nicht erforderlich die entsprechenden Vorschriften der DS-GVO nochmals abzuschreiben. Der Arbeitgeber bleibt aber nach Art. 13, 14 DS-GVO verpflichtet, dem Beschäftigten dann anderweitig Informationen zur Verfügung zu stellen, was z. B. durch ein Formblatt ohne Mitwirkung des Betriebsrats geschehen kann (vgl. Anhang 2). Um bis zu einer endgültigen Klärung der Rechtslage sicherzugehen, ist in der in der Anlage abgedruckten Rahmenbetriebsvereinbarung zur Einführung und Nutzung von Datenverarbeitungsmethoden in den Schlussvorschriften die hier angesprochene Problematik noch einmal kurz aufgenommen worden. Sollten bestehende, alte Betriebsvereinbarungen diesen Hinweis aber nicht enthalten, so sind diese weiterhin wirksam. Art. 88 Abs. 1 DS-GVO schließt bereits existierende Rechtsvorschriften – und damit auch Betriebsvereinbarungen – mit ein, so dass sie weiter fortgelten.[71]

Ob sich aus Gründen der Praktikabilität eine Betriebsvereinbarung auch auf die Verarbeitung von Beschäftigtendaten von Leiharbeitnehmern beziehen soll, muss im Einzelfall erwogen werden. Nach § 26 Abs. 8 BDSG sind auch Leiharbeitnehmer im Verhältnis zum Entleiher als Beschäftigte anzusehen. Dies gilt unabhängig von der Einsatzdauer, sodass im BDSG ein anderer Beschäftigtenbegriff als im BetrVG vorherrscht.

---

70 Ebenso *Maschmann,* DB 2016, S. 2480, 2484.

71 *Franzen,* EuZA 2017, S. 313, 348.

**HINWEIS**
Unternehmen, die im Unternehmen die Umsetzung und die Anforderungen der DS-GVO verdeutlichen und den Betriebsrat über seine Mitbestimmungsrechte hinaus miteinbinden möchten, können die umfassende **Rahmenvereinbarung zur Umsetzung der DS-GVO** (Anhang 3) als freiwillige Betriebsvereinbarung i. S. d. § 88 BetrVG abschließen oder die Kurzfassung (Anhang 4) wählen. Mit diesen Regelungen werden aber keine Vereinbarungen zur Einführung von IT-Systemen geschlossen. Die Kurzfassung verdeutlicht nur, dass die bestehenden Betriebsvereinbarungen im Zweifelsfall i. S. d neuen Datenschutzvorschriften ausgelegt werden sollen.

**HINWEIS FÜR NEUE BETRIEBSVEREINBARUNGEN**
Besteht im Unternehmen noch keine Betriebsvereinbarung zur Einführung von IT-Systemen bzw. sollen neue Betriebsvereinbarungen abgeschlossen werden, so ist generell der Abschluss einer **Rahmenbetriebsvereinbarung zur Einführung und Nutzung von Datenverarbeitungsmethoden (DVM)** zu empfehlen, die der Vereinfachung und Standardisierung der Datenverarbeitungsverfahren dienen. Als **Musterbeispiel** sind eine Rahmenbetriebsvereinbarung (Anhang 7) sowie eine darauf aufbauende Einzelbetriebsvereinbarung (Anhang 8) aufgeführt.

Sinn und Zweck dieser Rahmenbetriebsvereinbarung ist es, wie der Name schon sagt, für alle einzuführenden Datenverarbeitungsmethoden (technische Einrichtungen und deren Anwendungen) eine einheitliche Herangehensweise und Standardisierung des Verfahrens aufzunehmen. Es soll damit ein Rahmen geschaffen werden, wonach immer wiederkehrende Fragen einmalig geklärt werden. Dies dient der Zeitersparnis, auch wenn notfalls bei fehlender Übereinstimmung zwischen den Betriebsparteien die Einigungsstelle angerufen werden müsste (§ 87 Abs. 2 BetrVG). Beim Abschluss von neuen Betriebsvereinbarungen können daher die oben beschriebenen deklaratorischen Hinweise zur DS-GVO in der Präambel oder den Schlussvorschriften mitaufgenommen werden.

Neben dem Vorteil der Betriebsvereinbarung gegenüber der Einwilligung eine kollektive Rechtfertigung der Datenverarbeitung zu ermöglichen, ist der Abschluss einer Betriebsvereinbarung in der Regel schon wegen des Mitbestimmungsrechts nach **§ 87 Abs. 1 Nr. 6 BetrVG** bei der Einführung eines IT-Systems erforderlich.[72]

[72] *Wisskirchen/Schiller/Schwindling*, BB 2017, S. 2105; *Haußmann/Brauneisen*, BB 2017, S. 3065.

So stellt § 26 Abs. 6 BDSG (§ 32 Abs. 3 BDSG a. F.) klar, dass die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt bleiben. Dies bedeutet, dass das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG durch eine Betriebsvereinbarung ausgeübt werden muss. Dabei ist zu beachten, dass die Rechtsprechung das Mitbestimmungsrecht des § 87 Abs. 1 Nr. 6 BetrVG sehr weit auslegt. Während das BAG in der Entscheidung zu Google Maps[73] noch zutreffend ausführt, dass die Überwachung durch die technische Einrichtung selbst bewirkt werden muss, kommt es nach der Facebook[74] Entscheidung des BAG nicht darauf an, ob die technische Einrichtung selbst erhebt oder verarbeitet. Ausreichend sei die Speichermöglichkeit und die anschließende Zugriffsmöglichkeit durch den Arbeitgeber. Eine Missachtung des Mitbestimmungsrechts allein führt nach dem BAG bislang jedoch nicht zu einem Beweisverwertungsverbot. Das BAG hat die ohne Mitbestimmung des Betriebsrats aufgrund einer Videoüberwachung gewonnenen Erkenntnisse (auch Zufallsfunde) nach einer umfassenden Verhältnismäßigkeitsprüfung für ein Kündigungsschutzverfahren berücksichtigt und ein Beweisverwertungsverbot abgelehnt.[75] Durch den schon bislang vom BAG angelegten strengen Prüfungsmaßstab an die Rechtmäßigkeit von Eingriffen in das allgemeine Persönlichkeitsrecht des Arbeitnehmers durch technische Überwachungseinrichtungen aufgrund von Betriebsvereinbarungen, wonach kein ständiger Überwachungs- sowie Anpassungs- und Leistungsdruck in allen Arbeitsbereichen vorliegen darf, wenn keine überwiegende schutzwürdige Belange des Arbeitgebers vorliegen, ist den Anforderungen an Art. 88 Abs. 2 DS-GVO bereits Rechnung getragen worden.[76]

Diskussionspunkt ist bei den Verhandlungen mit den Betriebsräten und Gewerkschaften in diesem Zusammenhang immer der Ausschluss der Leistungskontrolle. Die Arbeitgeberseite wird aber regelmäßig ein Interesse daran haben, Missbrauchsfälle aufdecken zu können, sodass in der Rahmenbetriebsvereinbarung über die Einführung und Nutzung von DVM (vgl. Anhang 7) auch eine entsprechende Regelung unter Ziffer 6 aufgenommen wurde. Nach § 87 Abs. 1 Nr. 6 BetrVG ist ein Mitbestimmungsrecht des Betriebsrats für die Fragen der Leistungskontrolle grundsätzlich gegeben. Ein solches entfällt jedoch, wenn zwingende gesetzliche Regelungen entgegenstehen, wie sie in §§ 13 StGB und 31 OWiG zu sehen sind. Diese Regelungen verpflichten die gesetzlichen Vertreter von Gesellschaften, Ordnungswidrigkeiten bzw. Straftaten durch geeignete Organisationsmaßnahmen

---

73 BAG, 10.12.2013, 1 ABR 43/12, NZA 2014, S. 439.

74 BAG, 13.12.2016, 1 ABR 7/15, NZA 2017, S. 657.

75 BAG, 20.10.2016, 2 AZR 395/15 , NZA 2017, S. 443; *Fuhlrott/Schröder*, NZA 2017, S. 278.

76 BAG, 25.04.2017, 1 ABR 46/15, BB 2017, S. 2428 zur BV über eine Belastungsstatistik.

zu verhindern. Da diese Vorschriften zwingend und nicht dispositiv sind, können Betriebsvereinbarungen diese Rechte nicht einschränken und ein Ausschluss der Leistungskontrolle wäre insoweit auch unwirksam.[77]

## d. Datenverarbeitung auf der Grundlage einer Einwilligung – Art. 7 DS-GVO, § 26 Abs. 2 BDSG

### aa. Zulässigkeit

§ 26 Abs. 2 BDSG stellt im Einklang mit dem politischen Willen der DS-GVO[78] klar, dass die Einwilligung im Beschäftigtenkontext grundsätzlich zulässig ist. Dies entspricht auch der bisherigen höchstrichterlichen Rechtsprechung.[79]

Die Einwilligung ist vom Wortverständnis eine vorherige Einverständniserklärung des Beschäftigten (vgl. § 183 Satz 2 BGB).

Die DS-GVO beschreibt die Einwilligung in **Art. 4 Nr. 11** wie folgt:

"Einwilligung" der betroffenen Person [ist] jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

**HINWEIS**
Die Einwilligung muss **vor der Datenverarbeitung** eingeholt werden.[80]

77 Ebenso Baker McKenzie (Hrsg.), *Koops*, Arbeitsrecht 4.0, 2017, S. 113.

78 Erwägungsgrund 155 der DS-GVO.

79 BAG, 19.02.2015, 8 AZR 1011/13, ZD 2015, S. 380; BFH 19.06.2012, VII R 43/11.

80 Gola/*Schomerus*, BDSG, 11. Auflage 2012, § 4a, Rn. 2, 32; OLG Köln, 12.06.1992, 19 U 154/91, NJW 1993, S. 793.

Die Einwilligung ist explizit auch für die Erhebung von besonderen Kategorien personenbezogener Daten zulässig (Art. 6 i. V. m. Art. 9 Abs. 2 lit. b) i. V. m. Art. 88 DS-GVO i. V. m. § 26 Abs. 2 Satz 2 BDSG). Die Einwilligung muss sich dabei ausdrücklich auf diese besonderen Daten beziehen.

Diese gesetzliche Klarstellung ist insbesondere im Hinblick auf die Datenschutzerklärung im Zusammenhang mit dem betrieblichen Eingliederungsmanagement (§ 167 SGB IX bzw. § 84 Abs. 2 SGB IX a. F.) für die betriebliche Praxis wichtig (vgl. auswählte Praxisbeispiele unter ii) (1)).

**HINWEIS**
Die Einwilligung ist zwar im Beschäftigungskontext möglich, aufgrund der richtungsgebenden Regelbeispiele im neugefassten § 26 Abs. 2 BDSG und dem Widerrufsrecht des Beschäftigten sollte sie jedoch nur in eng begrenzten Fällen eingesetzt werden. Dieser zurückhaltende Einsatz empfiehlt sich auch vor dem Hintergrund der von der sog. Artikel-29-Datenschutzgruppe geäußerten grundsätzlichen Bedenken gegen eine Einwilligung im Beschäftigungskontext.[81]

Zuvor ist immer eine Prüfung eines allgemeinen Erlaubnistatbestandes (insbesondere Art. 6 i. V. m. Art. 88 DS-GVO i. V. m. § 26 Abs. 1 BDSG) zu empfehlen.

**bb. Freiwilligkeit**

Gleichlaufend mit dem bisherigen § 4a BDSG und dem Art. 7 der DS-GVO verlangt § 26 Abs. 2 Satz 1 BDSG, dass die Einwilligung freiwillig erfolgt.

Die Freiwilligkeit setzt die **Geschäftsfähigkeit** des Betroffenen voraus.[82] Das bedeutet, dass bei minderjährigen Beschäftigten oder minderjährigen Auszubildenden die Einwilligung des gesetzlichen Vertreters eingeholt werden sollte. Die zwei naheliegenden Ausnahmen greifen im Beschäftigtendatenschutz nicht.

- Zum einen macht die DS-GVO eine ausdrückliche Ausnahme in Art. 8. Danach kann bereits ein Minderjähriger, welcher das 16. Lebensjahr vollendet hat, eine datenschutzrechtlich wirksame Einwilligung erteilen, wenn es sich um das „Angebot von Diensten der Informationsgesellschaft" handelt. Nach der

81 Stellungnahme der Artikel-29-Datenschutzgruppe 2/2017 vom 08.06.2017.

82 BAG, 11.12.2014, 8 AZR 1010/13, NZA 2015, S. 604.

Definition muss es sich um den Austausch von Dienstleistungen im Fernabsatzverkehr handeln.[83]

Das bedeutet z. B., dass die Suche nach Auszubildenden über einen Fragebogen im Onlineportal des Unternehmens nicht unter diese Ausnahmeregelung fällt und eine Einwilligung der Eltern notwendig ist.

- Zum anderen bedarf es nach § 113 BGB nicht der Einwilligung des gesetzlichen Vertreters, wenn diese Willenserklärung des Minderjährigen im Rahmen eines Arbeitsverhältnisses abgegeben werden, zu dem der gesetzliche Vertreter den Minderjährigen ermächtigt hat.

  Das bedeutet für das Datenschutzrecht, dass wegen der besonderen Schutzanforderungen sowie des ernstzunehmenden Willens des Minderjährigen eine doppelte Einwilligung – die der gesetzlichen Vertreter **und** des Kindes – z. B. für die Veröffentlichung eines Fotos im Internet gefordert wird.[84] Eine Einwilligung zur Veröffentlichung des Fotos im Firmenportal gegen den Willen des minderjährigen Auszubildenden soll so ausgeschlossen werden.

Die Freiwilligkeit ist grundsätzlich anzunehmen, wenn die Willensbildung des Betroffenen nicht in unangemessener Weise beeinflusst wurde.[85]

Bei der Beurteilung der Freiwilligkeit sind aufgrund des Gesetzeswortlautes auch die im Beschäftigungsverhältnis bestehende Abhängigkeit und die Umstände, unter denen sie erteilt wurde, zu berücksichtigen. Das bedeutet:

- Dem Beschäftigten darf kein Nachteil in Aussicht gestellt werden, der mit dem verfolgten Zweck der Datenverarbeitung gar nichts zu tun hat.[86]

> **HINWEIS**
> Ausgenommen sind solche Nachteile, die durch die mangels Einwilligung untersagte Datenverarbeitung entstehen[87] (z. B. keine private Nutzung des Internets).

---

83 Art. 4 Nr. 25 DS-GVO i. V. m. Art. 1 Abs. 1b Richtlinie (EU) 2015/1535.

84 *Ehmann,* jurisPR-ArbR 14/2013, Anm. 2.

85 Däubler, Gläserne Belegschaften, § 4 Rn. 160

86 Gola, BDSG, § 4a, Rn. 21.

87 Gola/Pötters/Wronka, Handbuch Arbeitnehmerdatenschutz, 7. Auflage 2016, Rn. 428.

- Der Beschäftigte sollte bei der Erteilung der Einwilligung nicht unter Druck – besonders nicht unter zeitlichen Druck – gesetzt werden.

> **HINWEIS**
> Eine dokumentierte Frist zum Überlegen und Entscheiden ist empfehlenswert.

- Auch sollten übermäßige Anreize für die Einwilligung vermieden werden.[88]

Generell gilt nichts anderes für die Einwilligung vor Beginn des Beschäftigungsverhältnisses oder in der Wartezeit des § 1 KSchG. Allerdings sollte hier die Einwilligung insofern besonders genau geprüft werden, da ggf. im Einzelfall die Frage der Probezeit wegen der Gesetzesformulierung („Umstände der Erteilung") der Freiwilligkeit entgegengehalten wird.[89]

### cc. Regelbeispiele des § 26 Abs. 2 BDSG

Der Gesetzestext enthält Regelbeispiele, bei denen nach Ansicht des Gesetzgebers von einer Freiwilligkeit ausgegangen werden kann:

- Erreichen eines rechtlichen oder wirtschaftlichen Vorteils für den Beschäftigten
  z. B. Einführung eines betrieblichen Gesundheitsmanagements, Privatnutzung der betrieblichen IT-Systeme[90]
- Gleichgelagerte Interessen von Arbeitgeber und Beschäftigtem
  z. B. Aufnahme des Namens und des Geburtsdatums in eine Geburtstagsliste, Nutzung von Fotos für das Intranet[91]

> **HINWEIS**
> Das Kunsturhebergesetz verlangt bei einer Verbreitung oder Veröffentlichung von Fotos ebenfalls die Einwilligung des Betroffenen, § 22 KunstUrhG.[92]

---

88 BGH, 16.07.2008, VIII ZR 348/06, DB 2008, S. 2188.

89 Gesetzesbegründung, BT-Drs. 18/11325, S. 97; *Kort*, NZA-Beilage 2016, S. 62.

90 Gesetzesbegründung, BT-Drs. 18/11325, S. 97.

91 Gesetzesbegründung, BT-Drs. 18/11325, S. 97.

92 BAG, 11.12.2014, 8 AZR 1010/13; BAG, 19.02.2015, 8 AZR 1011/13.

Durch die Verwendung des Wortes „insbesondere" in § 26 Abs. 2 Satz 2 BDSG wird deutlich, dass die Aufzählung nur Beispiele enthält und nicht abschließend ist.[93] Diese Beispiele erleichtern die Anwendung in der betrieblichen Praxis, schließen aber andere Konstellationen nicht aus.

Wegen des Beispielcharakters ist die Ansicht abzulehnen, dass die Einwilligung im Umkehrschluss jedenfalls dann unzulässig ist, wenn die Datenverarbeitung für den Betroffenen insgesamt als nachteilig zu werten ist.[94] Besonders bei der Überprüfung eines Sachverhaltes wegen einer Vertragsverletzung (§ 26 Abs. 1 Satz 2 BDSG greift nicht unmittelbar), kann die Erhebung von Sachverhaltsdaten auch mit Einwilligung des Betroffenen erfolgen, obwohl ihm gegebenenfalls eine verhaltensbedingte Kündigung droht.[95]

**dd. Inhalt – Informierte Einwilligung**

Besonders der Erwägungsgrund 32 der DS-GVO formuliert deutlich die Anforderungen an die Inhalte einer Einwilligungserklärung:

> Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, **für den konkreten Fall, in informierter Weise** und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, .... **Die Einwilligung sollte sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge beziehen. Wenn die Verarbeitung mehreren Zwecken dient, sollte für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden.** ...

Diese Voraussetzung war bereits nach geltendem Recht zu erfüllen.

---

93 *Wybitul*, NZA 2017, S. 413.

94 *Wybitul*, NZA 2017, S. 413.

95 BAG, 20.06.2013, 2 AZR 546/12.

**HINWEIS**
Das bedeutet für die betriebliche Praxis insbesondere, dass generelle Einwilligungsklauseln im Arbeitsvertrag oder in einer separaten Erklärung unwirksam sind, da sie vor allem die Zweckbindung der Einwilligung in der Regel nicht erfüllen.

Für eine wirksame Einwilligungserklärung sollten folgende Punkte beachtet werden:[96]

1. verantwortliche Stelle angeben
2. Zweck der Datenverarbeitung benennen und Zweckbindung verdeutlichen (bei mehreren Zwecken separate Einwilligung im Dokument ermöglichen)
3. Art der Daten beschreiben
4. Separater Hinweis bei besonderer Kategorien personenbezogener Daten aufnehmen (Art. 6 i. V. m. Art. 9 Abs. 2 i. V. m. Art. 88 DS-GVO i. V. m. § 26 Abs. 3 Satz 2 und 3 BDSG)
5. bei Übermittlung an Dritte Kategorien von Empfängern formulieren (ggf. Hinweis auf adäquates Schutzniveau)
6. nachweisbare Dokumentation der Einwilligungserklärung sicherstellen
7. verständliche und nachvollziehbare Formulierung (Transparenz) wählen
8. Hinweis auf Widerrufsrecht nicht vergessen

**HINWEIS**
Wird die Einwilligung im Rahmen von vorformulierten Erklärungen vom Arbeitgeber eingeholt, so sind zudem die Vorgaben der Inhaltskontrolle gemäß §§ 307 bis 309 BGB zu beachten.[97] Werden mit der Einwilligung die Regelbeispiele des § 26 Abs. 2 Satz 2 BDSG erfüllt, so wird die Regelung als angemessen anzusehen sein.

[96] Vgl. auch Hinweise des sog. Düsseldorfer Kreises vom März 2016.

[97] BGH, 16.07.2008, VIII ZR 348/06, NJW 2008, S. 355; BGH, 11.11.2009, VIII ZR 12/08, DB 2010, S. 107.

**Formulierungshilfe Einwilligung – Beispiel Bewerberdaten nach Abschluss des Bewerbungsverfahrens**

**Einwilligungserklärung zur Speicherung von Bewerberdaten[98]**

*Der Arbeitgeber [.....]*
*beabsichtigt, für zukünftige offene Stellen die Bewerberdaten in einer Bewerberdatenbank zu speichern.*

*Der Bewerber erklärt:*
*Ich willige ein – soweit die Datenverarbeitung nicht durch andere Rechtsgrundlage geregelt ist, dass der Arbeitgeber meine personenbezogenen Daten, die ich im Rahmen des gesamten Bewerbungsverfahrens mitgeteilt habe (z. B. in Anschreiben, Lebenslauf, Zeugnissen, Bewerber-Fragebögen, Bewerber-Interviews), über das Ende des konkreten Bewerbungsverfahrens hinaus speichert.*

*Ich willige ein, dass der Arbeitgeber diese Daten nutzt, um mich ggf. später zu kontaktieren und das Bewerbungsverfahren fortzusetzen, falls ich für eine andere Stelle in Betracht kommen sollte.*

*Sofern ich in meinem Bewerbungsschreiben oder anderen von mir im Bewerbungsverfahren eingereichten Unterlagen selbst „besondere Kategorien personenbezogener Daten" mitgeteilt habe, bezieht sich meine Einwilligung auch auf diese Daten.*

*Diese Einwilligung gilt zudem für Daten über meine Qualifikationen und Tätigkeiten aus allgemein zugänglichen Datenquellen (insbesondere berufliche soziale Netzwerke), die der Arbeitgeber im Rahmen des Bewerbungsverfahrens zulässig erhoben hat.*

*Ich erkläre, dass ich diese Einwilligung freiwillig erteile. Ich kann sie ohne Angabe von Gründen verweigern, ohne dass ich deswegen Nachteile zu befürchten hätte. Ich kann meine Einwilligung zudem jederzeit in Textform widerrufen; in diesem Fall werden meine Daten dann gelöscht, soweit keine Ansprüche mehr aus dem Bewerbungsverfahren zu erwarten sind.*

**98** Angelehnt an Koreng/Lachenmann/*Bergt*, Formularhandbuch Datenschutzrecht, 1. Auflage 2015, Einwilligung durch Beschäftigte.

**HINWEIS**
Wegen des subjektiven Fristbeginns der AGG-Ansprüche verbietet sich eine sofortige oder starre Löschfristangabe in dieser Einwilligungserklärung.[99]

Bei Mitarbeiterfotos ist häufig zusätzlich § 22 des Kunsturhebergesetzes (KunstUrhG) zu beachten. Danach bedarf es der Einwilligung des Betroffenen, wenn das Foto verbreitet oder veröffentlicht werden soll.[100] Eine Verbreitung oder Veröffentlichung liegt in der Praxis dann vor, wenn das Foto im Intranet, in Broschüren oder im Internet verwendet werden soll.

Anders verhält es sich, wenn das Foto zur Identifikation auf dem Firmenausweis verwendet wird, um ein Sicherheitskonzept des Unternehmens umzusetzen. In diesen Fällen wird das Foto z. B. zum Abgleich durch den kontrollierenden Pförtner weder verbreitet noch veröffentlicht. Hier dürfte sich die datenschutzrechtliche Zulässigkeit allein aus Art. 6 i. V. m. Art. 88 DS-GVO i. V. m. § 26 Abs. 1 Satz 1 BDSG ergeben. Die Datenverarbeitung ist erforderlich, um das Sicherheitskonzept des Unternehmens umzusetzen.

**ee. Form der Einwilligung**

In § 26 Abs. 2 Satz 3 BDSG wird grundsätzlich die Schriftform wie im bisherigen § 4a BDSG a. F. verlangt. Art. 7 DS-GVO verlangt hingegen nur eine nachweisbare Einwilligung.

Im **Erwägungsgrund 32** heißt es:
Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung.

[99] BAG, 15.03.2012, 8 AZR 37/11, DB 2012, S. 1873.

[100] BAG, 11.12.2014, 8 AZR 1010/13, BAG, 19.02.2015, 8 AZR 1011/13.

**HINWEIS**
Schriftform bedeutet die eigenhändige Unterschrift des Beschäftigten auf einem Dokument (§ 126 BGB). E-Mail, Fax, eingescannte Unterschrift oder Kurznachrichten per SMS oder andere Nachrichtendienste sind nicht ausreichend.

### (1) Regelungsbefugnis des deutschen Gesetzgebers

Es gibt gute Argumente, dass der deutsche Gesetzgeber trotz der Öffnungsklausel in Art. 88 DS-GVO nicht befugt ist, die strenge Form der Schriftform im Beschäftigungsverhältnis vorzugeben.[101] Es gibt jedoch bereits Stimmen in der Literatur, die diese Formvorgabe in § 26 Abs. 2 Satz 3 BDSG als zulässig ansehen.[102]

**HINWEIS**
Solange dieser Streit über die Regelungsbefugnis des deutschen Gesetzgebers nicht höchstrichterlich geklärt ist, sollte möglichst die Schriftform bei der Einwilligungserklärung eingehalten werden. Ein Verstoß gegen das Schriftformerfordernis führt zur Unwirksamkeit der Einwilligungserklärung (§§ 125, 126 BGB), so dass die darauf basierende Datenverarbeitung unzulässig wäre.[103]

Die elektronische Form des § 126a BGB ist in der Praxis untauglich, da die Beschäftigten und meist auch der Arbeitgeber keine Signatur nach dem Signaturgesetz besitzen.

101 *Krohm*, ZD 2016, S. 368.
102 *Kort*, ZD 2017, S. 319 m. w. N.
103 BAG, 11.12.2014, 8 AZR 1010/13, BB 2015, S. 1276.

**HINWEIS**
Für die Verbreitung und Veröffentlichung von Mitarbeiterfotos gilt § 22 KunstUrhG als Sondervorschrift (sog. lex specialis). Auch wenn § 22 KunstUrhG im Gegensatz zu § 26 BDSG /§ 4a BDSG a. F. explizit keine Schriftform verlangt, so hat das BAG auf Grundlage der bisherigen Rechtslage wegen der besonderen Umstände des Arbeitsverhältnisses gleichwohl die Schriftform verlangt.[104]

**(2) Ausnahme von der Schriftform**

Wie schon die bisherige Gesetzesfassung in § 4a BDSG a. F. kann von der Schriftform dann abgesehen werden, „soweit nicht wegen besonderer Umstände eine andere Form angemessen ist." Eine andere Form in diesem Sinne kann grundsätzlich nur die Erklärung in Textform (Email, Fax u.a.) oder eine ausdrücklich (nachweisbare) mündliche sein. Eine stillschweigende Hinnahme durch den Beschäftigten reicht hingegen nicht aus.[105]

Diese Ausnahme wurde bislang sehr restriktiv gehandhabt. Beispielhaft werden in der Literatur in allgemeinen Konstellationen auf eine besondere Eilbedürftigkeit oder auf ein langjähriges Vertragsverhältnis abgestellt.[106] Speziell im Zusammenhang mit dem Beschäftigungsverhältnis wird beispielsweise auf eine mögliche technisch-basierte Einwilligung (z. B. Anklicken eines besonderen Hinweiskästchens) zur Kontrollmöglichkeit bei erlaubter privater Nutzung der IT-Anlagen des Arbeitgebers abgestellt.[107] Ein sog. opt-out des Beschäftigten reicht wegen der gesteigerten Anforderungen an eine Einwilligung in Art. 4 Nr. 11 DS-GVO („unmissverständlich abgegebene Willensbekundung") nicht aus.[108] Das heißt z. B., dass die betriebliche Handhabung in dem Sinne, dass sich die Beschäftigten melden müssen, wenn sie nicht in einer hausinternen Geburtstagsliste stehen möchten, datenschutzrechtlich unzulässig ist.

---

104 BAG, 11.12.2014, 8 AZR 1010/13.

105 Gola/Pötters/Wronka, Handbuch Arbeitnehmerdatenschutz, Rn. 437; Simitis, BDSG, § 4a, Rn. 44.

106 Simitis, BDSG, § 4a, Rn. 45, 46.

107 Gola/Pötters/Wronka, Handbuch Arbeitnehmerdatenschutz, Rn. 437.

108 *Franzen*, EuZA 2017, S. 313.

**HINWEIS**
Angesichts des Risikos einer unwirksamen Einwilligung und damit einer unzulässigen Datenerhebung sollte von der Ausnahme des § 26 Abs. 2 BDSG nur in bestimmten begründeten Einzelfällen Gebrauch gemacht werden oder zuvor mit der Aufsichtsbehörde (ggf. anonym über den Arbeitgeberverband) die Vorgehensweise abgestimmt werden.

Bei der Gestaltung der Einwilligung ist zudem das Transparenzgebot zu beachten. Eine Einwilligungserklärung auf einem separaten Schriftstück erfüllt diese Anforderung. Soll die Einwilligung im Zusammenhang mit einer anderen vertraglichen Vereinbarung eingeholt werden, so ist diese deutlich vom Vertragstext abzusetzen und eine separate Unterschriftenzeile dafür vorzusehen.[109]

### ff. Widerrufsrecht

Aus Art. 7 Abs. 3 DS-GVO folgt die Pflicht des Arbeitgebers, den Beschäftigten (in Textform) über den jederzeitigen Widerruf und dessen Folgen zu informieren.

**HINWEIS**
Da die Einwilligungserklärung inklusive dem Widerrufshinweis in der Regel im Beschäftigtenkontext über vorformulierte Erklärungen erfolgt, gelten die Regelungen zur Inhaltskontrolle nach §§ 307 ff. BGB.[110] Deshalb ist die Neufassung von § 309 Nr. 13 zu beachten. Für den Widerruf durch den Beschäftigten darf keine strengere Form als die Textform verlangt werden.

Es ist davon auszugehen, dass der Widerruf durch die Geltung der DS-GVO keines sachlichen Grundes auf Beschäftigtenseite bedarf. Das BAG[111] hatte zwar zur geltenden Rechtslage entschieden, dass die gegenseitige Rücksichtnahmepflicht im Arbeitsverhältnis es gebietet, dass der Arbeitnehmer einen plausiblen Grund für seinen Widerruf anführen muss. Die DS-GVO geht jedoch von einem (sachgrundlosen) jederzeitigen Widerrufsrecht des Betroffenen aus (Art. 7 Abs. 3 Satz 1 DS-GVO).

---

109 BGH, 16.07.2008, VIII ZR 348/06; BB 2008, S. 2426.

110 Wybitul/*Fladung/Pötters* in, Handbuch EU-Datenschutzgrundverordnung, S. 261.

111 BAG, 19.02.2015, 8 AZR 1011/13.

In Art. 7 Abs. 3 Satz 2 wird klargestellt, dass die bis zum Widerruf erfolgte Datenverarbeitung zulässig bleibt.[112]

**HINWEIS**
Die Einwilligung sollte nur in eng begrenzten Fällen eingesetzt werden. Zuvor ist immer eine Prüfung eines allgemeinen Erlaubnistatbestandes (insbesondere Art. 6 i. V. m. Art. 88 DS-GVO i. V. m. § 26 Abs. 1 BDSG) zu empfehlen. Außerdem sollte die Einwilligung vorbehaltlich anderer Erlaubnisgrundlagen formuliert sein („Soweit nichts anderes im Bundesdatenschutzgesetz oder in der Datenschutzgrundverordnung geregelt, willigt der Beschäftigte .... ein"). Andernfalls könnte im Zusammenhang mit einem möglichen Widerruf der Eindruck erweckt werden, dass die Datenverarbeitung gänzlich auf dem Willen des Beschäftigten beruht.

**Formulierungshilfe Widerrufsrecht**
*Der Arbeitgeber weist den Beschäftigten darauf hin, dass er jederzeit die hiermit erteilte Einwilligung zur Datenverarbeitung widerrufen kann. Der Widerruf kann in Textform erfolgen.*

*Die Datenverarbeitung bleibt bis zum Eingang des Widerrufs beim Arbeitgeber zulässig.*

*Das gleiche gilt für die Datenverarbeitung auf der Grundlage anderer Erlaubnistatbestände nach dem Eingang des Widerrufs*

### gg. Verhältnis zum Fragerecht des Arbeitgebers

Die gesetzlich normierte Zulässigkeit der Einwilligung als Erlaubnisgrundlage zur Datenerhebung führt nicht zur Erweiterung des Fragerechts des Arbeitgebers.[113] Fragen beispielsweise nach einer Schwangerschaft im Bewerbungsverfahren oder anlasslos nach der Gewerkschaftszugehörigkeit sind auch weiterhin unzulässig.[114] Die Frage nach der Schwerbehinderteneigenschaft ist nach Erwerb des

[112] *Franzen*, EuZA 2017, S. 313.

[113] Gola/Pötter/Wronka, Handbuch Arbeitnehmerdatenschutz, Rn. 430; Simitis, BDSG, § 4a, Rn. 19.

[114] Weitere Beispiele: *Kort*, NZA-Beilage 2016, 62; *Asgari*, DB 2017, S. 1325.

Behindertenschutzes gemäß §§ 85 ff. SGB IX jedoch zulässig.[115] Nach der Ergänzung des § 95 Abs. 2 Satz 3 SGB IX auch schon vor Ablauf dieser sechs Monate eine Frage nach der Schwerbehinderteneigenschaft zulässig, wenn eine Kündigung erwogen wird.[116] Denn danach ist jede arbeitgeberseitige Kündigung – auch während der sechsmonatigen Wartezeit – ohne Beteiligung der Schwerbehindertenvertretung unheilbar unwirksam.

**hh. Schicksal bereits vor dem 25. Mai 2018 erteilter Einwilligungen**

Im Erwägungsgrund 171 der DS-GVO wird ausdrücklich festgestellt, dass es nicht erforderlich ist, dass die betroffene Person erneut ihre Einwilligung mit Inkrafttreten des DS-GVO erteilt. Voraussetzung ist jedoch, dass die Art der bereits erteilten Einwilligung den Bedingungen der DS-GVO entspricht. Dann kann der Verantwortliche die Datenvereinbarung auf Grundlage dieser früheren Einwilligung fortsetzen.

In diesem Sinne ist auch die Verlautbarung des sog. Düsseldorfer Kreises in einem Beschluss[117] zu verstehen, dass bisher wirksame Einwilligungserklärungen auch nach dem 25. Mai 2018 wirksam bleiben.

**HINWEIS**
Es empfiehlt sich daher, alle bisher erteilten Einwilligungen der Beschäftigten auf die neue Rechtslage hin zu überprüfen, z. B. hinsichtlich des Hinweises auf das Widerrufsrecht. Die DS-GVO kennt nur einen beschränkten Bestandsschutz für Einwilligungserklärungen vor ihrem Inkrafttreten.

Wenn es Zweifel an den Umständen der Freiwilligkeit gab, so sollte die Einwilligung nochmals eingeholt werden. Sollten eher verpflichtende Hinweise (z. B. zur Art der Daten oder über das Widerrufsrecht) fehlen (vgl. Checkliste unter d. dd)), so können diese – falls die Einholung einer erneuten Einwilligung einen zu großen betrieblichen Aufwand bedeutet – ohne erneute Einwilligungserklärung einseitig vom Arbeitgeber nachgeholt werden.

115 BAG, 16.02.2012, 6 AZR 553/10, DB 2012, S. 1042.

116 *Benkert*, NJW-Spezial 2017, S. 370; *Richter*, ArbRAktuell 2017, 84; *Fuhlrott*, ArbRAktuell 2017, S. 453 f.; krit. *Schmitt*, BB 2017, S. 2293, 2296.

117 Düsseldorfer Kreis, Beschluss v. 13./14.09.2016.

### ii. Ausgewählte Praxisfragen

#### (1) Betriebliches Eingliederungsmanagement – BEM

Einerseits sieht § 167 Abs. 2 Satz 1 SGB IX (§ 84 Abs. 2 Satz 1 SGB IX a.F.) vor, dass ein BEM nur mit Zustimmung des betroffenen Beschäftigten durchgeführt werden kann. Andererseits verlangt § 167 Abs. 2 Satz 3 SGB IX (§ 84 Abs. 2 Satz 3 SGB IX a.F.) ausdrücklich, dass der Beschäftigte auf Art und Umfang der erhobenen und verwendeten Daten hinzuweisen ist.[118] Aus diesem systematischen Zusammenhang lässt sich der folgende Schluss ziehen: Die datenschutzrechtliche Einwilligung im Rahmen eines BEM ist grundsätzlich möglich und zulässig.

Aber: In der Zustimmung zum BEM durch den betroffenen Beschäftigten liegt nicht zugleich die datenschutzrechtliche Einwilligungserklärung zur Datenverarbeitung.[119]

Bei gesundheitsbezogenen Daten handelt es sich um besondere Kategorien personenbezogener Daten gem. § 26 Abs. 3 BDSG. Soweit solche besonderen Arten personenbezogener Daten erhoben, verarbeitet oder genutzt werden sollen, muss sich die Einwilligung des Beschäftigten ausdrücklich auf diese Daten beziehen (Art. 6 i. V. m. Art. 9 Abs. 2 b) i. V. m. Art. 88 DS-GVO i. V. m. § 26 Abs. 3 Satz 2 BDSG).

**HINWEIS**
Es ist deshalb dringend zu empfehlen, eine separate Einwilligungserklärung zum Datenschutz dem Anschreiben an den Beschäftigten mit dem entsprechenden Hinweis im Text als Anlage beizufügen.

[118] BAG, 13.05.2015, 2 AZR 565/14; BAG, 20.11.2014, 2 AZR 755/13.

[119] *Vossen*, DB 2016, S. 1814.

**Formulierungshilfe – Hinweis zu den zu erhebenden Daten**[120]
*Im Rahmen des BEM werden insbesondere folgende Informationen erhoben und verwendet:*

***Personal- und Sozialdaten:*** *Name, Geburtsdatum, Beschäftigungsdauer, Schwerbehinderung/Gleichstellung, etc.*

***Daten zu Fehlzeiten:*** *Anzahl und Verteilung der Arbeitsunfähigkeitstage in den letzten zwölf Monaten und in vorangegangenen Zeiträumen, Arbeitsunfälle etc.*

***Gesundheitsdaten (sensible Daten i. S. v. § 3 Abs. 9 BDSG):*** *medizinisch-diagnostische Daten, bestehende Leistungspotenziale, gesundheits- oder schwerbehinderungsbedingte Leistungseinschränkungen, Gesundheitsstand, Kuren, Heilbehandlungen, Krankheitsursachen, ärztliche Atteste etc.*

***Tätigkeitsdaten:*** *ausgeübte Tätigkeit, Arbeitsplatz- und Tätigkeitsanalysen, Gefährdungsbeurteilungen, Arbeitsschutzdaten, berufliche Qualifizierung etc.*

***Verfahrensdaten:*** *Verläufe und Ergebnisse von BEM-Verfahren (Maßnahmen und Verantwortlichkeiten), von Arbeitsversuchen und von Maßnahmen zur stufenweisen Wiedereingliederung sowie sonstiger arbeitsplatzbezogener Maßnahmen, innerbetriebliche Umsetzung, Anpassungen des Arbeitsplatzes oder der Arbeitsbedingungen etc.*

Es ist davon auszugehen, dass sich die im BEM-Verfahren erteilte Einwilligung des betroffenen Beschäftigten zur Verarbeitung seiner gesundheitsbezogenen Daten nur auf das BEM-Verfahren bezieht. Will der Arbeitgeber die hierbei gewonnen Daten auch für eine krankheitsbedingte Kündigung heranziehen, müsste sich die Einwilligung des Betroffenen ausdrücklich hierauf beziehen. Dies dürfte wegen der Restriktionen in § 26 Abs. 2 BDSG zur Freiwilligkeit nicht möglich sein.

Prozessual ist der Arbeitgeber dadurch jedoch nicht schlechter gestellt als ohne das BEM: Der Arbeitgeber kommt seiner Darlegungs- und Beweislast hinreichend nach, wenn er die Durchführung des BEM sowie dessen (ggf. fruchtloses) Ergebnis vor Gericht darlegt. Das Ergebnis des BEM stellt kein Gesundheitsdatum dar, und kann in den Prozess eingeführt werden. Möchte der Beschäftigte den Vortrag des Arbeitgebers entkräften, so ist es an ihm, seine Gesundheitsdaten vorzutragen.

120 Angelehnt an *Vossen*, DB 2016, S. 1814.

Die im Rahmen des BEM erhobenen Daten sind streng zweckgebunden. Diese Zweckbindung hat praktische Auswirkungen auf organisatorische Vorkehrungen bei der Speicherung und Verarbeitung dieser Daten. Die im Rahmen des BEM gewonnenen Daten dürfen daher nicht mit sonstigen Daten aus der Personalakte zusammengeführt werden.

**HINWEIS**
Der für die bei Durchführung des BEM gewonnenen Daten erforderliche besondere Geheimnisschutz kann dadurch gewährleistet werden, dass diese Daten in einer besonderen Akte oder in einem verschlossenen Umschlag mit eingeschränkten Zugangsrechten enthalten sind.[121]

**(2) Arbeitsschutzrechtliche Untersuchungen**

Entgegen landläufiger Vorstellungen werfen arbeitsschutzrechtliche Untersuchungen häufig keine Fragen zur datenschutzrechtlichen Einwilligung auf. Für den betrieblichen Umgang im Übrigen muss zwischen der sog. arbeitsmedizinischen Vorsorge und der Eignungsuntersuchung differenziert werden.

**(a) Arbeitsmedizinische Vorsorge**
Nach § 11 ArbSchG muss der Arbeitgeber seinen Beschäftigten ermöglichen, sich abhängig von der Gefährdungslage ihrer Tätigkeit regelmäßig arbeitsmedizinisch untersuchen zu lassen. Diese allgemeine arbeitsschutzrechtliche Pflicht wird durch die Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV) konkretisiert. Die ArbMedVV unterscheidet zwischen drei Vorsorgearten:

- **Pflichtvorsorge,** die bei bestimmten besonders gefährdenden Tätigkeiten vom Arbeitgeber veranlasst werden muss (§ 4 ArbMedVV).
- **Angebotsvorsorge,** die bei bestimmten gefährdenden Tätigkeiten angeboten werden muss (§ 5 ArbMedVV).
- **Wunschvorsorge,** die nur auf Wunsch des oder der Beschäftigten ermöglicht werden muss (§ 5a ArbMedVV).

Der Arbeitgeber erhält bei allen Vorsorgemaßnahmen nur (noch) die bloße Mitteilung, dass der Vorsorgetermin stattgefunden hat. Der Arbeitgeber erhält keine Bescheinigung mehr, ob gesundheitliche Bedenken gegen die weitere Ausübung der Tätigkeit bestehen. Die reine Termininformation des Arztes kann datenschutzrechtlich für den Arbeitgeber auf Art. 6 i. V. m. Art. 88 DS-GVO i. V. m. § 26 Abs. 1 Satz 1 BDSG gestützt werden.

[121] BAG, 12.09.2006, 9 AZR 271/06.

**HINWEIS**
Dies gilt auch bei einem negativen Untersuchungsergebnis, also auch dann, wenn gesundheitliche Bedenken gegen die weitere Ausübung der Tätigkeit bestehen. Ergeben sich allerdings Anhaltspunkte dafür, dass vorhandene Maßnahmen des Arbeitsschutzes nicht ausreichen, so hat der Arzt dies dem Arbeitgeber mitzuteilen und Maßnahmen des Arbeitsschutzes vorzuschlagen (§ 6 Abs. 4 Satz 2 ArbMedVV). Hält der Arzt aus medizinischen Gründen, die ausschließlich in der Person des Beschäftigten liegen, einen Tätigkeitswechsel für erforderlich, so bedarf diese Mitteilung an den Arbeitgeber der Entbindung von der Schweigepflicht durch den Beschäftigten (§ 6 Abs. 4 Satz 3 ArbMedVV).

**(b) Eignungsuntersuchungen**
Eignungsuntersuchungen zielen darauf ab, ob der Arbeitnehmer für eine bestimmte Tätigkeit gesundheitlich geeignet ist. Anders als die arbeitsmedizinische Vorsorge sind Eignungsuntersuchungen nur in wenigen Fällen ausdrücklich gesetzlich geregelt. Deren Zulässigkeit und Grenzen richten sich daher im Wesentlichen nach den Grundsätzen des allgemeinen Arbeitsrechts.

**HINWEIS**
Auch die sog. G-Grundsätze sind keine ausreichende Rechtsgrundlage für die wirksame Anordnung einer Eignungsuntersuchung. Die G-Grundsätze sind ausschließlich Leitlinien für Betriebsärzte.

Grundsätzlich gilt: Der Arbeitnehmer muss bei Vorliegen eines berechtigten Interesses des Arbeitgebers eine ärztliche Untersuchung seines Gesundheitszustandes dulden.[122] Bei der Frage nach einer wirksamen arbeitsrechtlichen Rechtsgrundlage muss zwischen der sog. anlassbezogenen und der turnusmäßigen Eignungsuntersuchung differenziert werden:

- **Anlassbezogene Untersuchung**
  Von der Rechtsprechung anerkannte Anlässe für eine Eignungsuntersuchung sind insbesondere konkrete Zweifel des Arbeitgebers an der fortdauernden Eignung des Beschäftigten für seine Tätigkeit, z. B. konkrete Ausfallerscheinung oder Hinweise von Kollegen und Vorgesetzten zu körperlichen

[122] BAG, 12.08.1999, 2 AZR 55/99.

Einschränkungen des Mitarbeiters. Auch ein Wechsel der Tätigkeit oder des Arbeitsplatzes kann einen konkreten Anlass für die Durchführung einer Eignungsuntersuchung begründen.

Liegt einer der beiden Anlässe vor, kann der Arbeitgeber kraft seines Direktionsrechts eine Eignungsuntersuchung anordnen. Der Arbeitnehmer ist aufgrund seiner arbeitsvertraglichen Nebenpflichten (§ 241 Abs. 2 BGB) verpflichtet, in die Untersuchung einzuwilligen und den beauftragten Arzt in Bezug auf das Ergebnis der Untersuchung von seiner Schweigepflicht freizustellen.

**HINWEIS**
Einer datenschutzrechtlichen Einwilligung für die Erhebung des Ergebnisses einer solchen Eignungsuntersuchung bedarf es in diesen Fällen nicht, da diese Daten für die Durchführung des Beschäftigungsverhältnisses nach Art. 6 i. V. m. Art. 88 DS-GVO i. V. m. § 26 Abs. 1 Satz 1 BDSG erforderlich sind.

- **Turnusmäßige Eignungsuntersuchung**
  Bei turnusmäßigen („anlasslosen") Eignungsuntersuchungen möchte der Arbeitgeber sicherstellen, dass die Arbeitsplätze mit gesundheitlich geeigneten Mitarbeitern besetzt werden, um Arbeitsunfälle und damit die Gefährdung von Kollegen, außenstehenden Dritten oder dem Eigentum des Arbeitgebers zu vermeiden (sog. Drittschutz).

  Die Anordnung regelmäßiger Eignungsuntersuchungen bedarf einer gesonderten Rechtsgrundlage.[123] Durch die Rechtsprechung des Bundesarbeitsgerichts ist anerkannt, dass turnusmäßige Untersuchungen in „gewissen Abständen" auch außerhalb von gesetzlichen Sondervorschriften tarifvertraglich, arbeitsvertraglich oder in einer Betriebsvereinbarung verpflichtend angeordnet werden können.[124]

[123] Spezialgesetzliche Grundlagen sind selten und nur für besonders exponierte Berufsgruppen vorhanden, etwa Piloten, Busfahrer, Mitarbeiter im Röntgen oder in Atomanlagen.

[124] BAG, 12.08.1999, 2 AZR 55/99; *Behrens*, NZA 2014, 401; *Beckschulze*, BB 2014, S. 1013 und 1077; *Kleinebrink*, DB 2014, S. 776.

**HINWEIS**
Dabei ist selbstverständlich, dass der Arbeitnehmer auch bei wirksamer Pflichtbegründung nicht zur Untersuchung „gezwungen" werden kann. Eine unberechtigte Verweigerung der Untersuchung ist allerdings eine Pflichtverletzung, die arbeitsrechtliche Konsequenzen nach sich ziehen kann.[125]

Ein berechtigtes Interesse des Arbeitgebers an einer regelmäßigen Eignungsuntersuchung wird insbesondere bei besonders gefährlichen Arbeiten zu bejahen sein, bei deren Ausübung besondere Gefährdungen von Kollegen oder der Allgemeinheit bestehen, z. B. Höhen- und Kletterarbeiten, Arbeiten mit Atemschutz, Kälte- und Hitzearbeiten, Tätigkeit als Kranführer, relevante Fahr- und Steuerungstätigkeiten, Arbeiten unter Hochspannung, Tätigkeit in der Werksfeuerwehr. Bei der Bewertung der Tätigkeit sollten stets die Ergebnisse der Gefährdungsbeurteilung herangezogen werden.

**HINWEIS**
In diesen Fällen folgt u. E. aus der arbeitsrechtlichen Notwendigkeit die nach Art. 6 i. V. m. Art. 88 DS-GVO i. V. m. § 26 Abs. 1 Satz 1 BDSG geforderte „Erforderlichkeit" der Datenverarbeitung.

In den Fällen, in denen eine Flankierung dieser turnusgemäßen Untersuchungen fehlen sollte, empfiehlt es sich gleichwohl in der Praxis, die arbeitsvertragliche Pflicht zur Teilnahme an solchen Untersuchungen mit der datenschutzrechtlichen Einwilligung zu verbinden, allerdings mit einer transparenten – textlich abgesetzten – Gestaltung der Einwilligungserklärung.

125 BAG, 27.09.2012, 2 AZR 811/11.

**Formulierungshilfe – Arbeitsvertragliche Verpflichtung Eignungsuntersuchung**

**1. Vorbehalt Einstellungsuntersuchung**
*Der Arbeitsvertrag wird unter dem Vorbehalt geschlossen, dass, soweit die Erfüllung bestimmter gesundheitlicher Vorausaussetzungen wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung eine wesentliche und entscheidende berufliche Anforderung darstellt, die gesundheitliche Eignung dafür ärztlich festgestellt wird.*

*Der Beschäftigte ist verpflichtet, sich einer solchen ärztlichen Untersuchung zu unterziehen und den Arbeitgeber bis zum … über die Ergebnisse der Untersuchung durch Vorlage der ärztlichen Bescheinigung über seine Eignung zu unterrichten oder den behandelnden Arzt von der Schweigepflicht zu entbinden, soweit sie die Eignung des Beschäftigten für die ihm obliegende Tätigkeiten betreffen.*

*Der Arbeitgeber trägt die Kosten der Untersuchung, wenn diese nicht von einem Dritten übernommen werden.*

*Der Arbeitgeber ist berechtigt, die Untersuchung durch einen Arbeitsmediziner zu verlangen.*

**2. Rechtsgrundlage im laufenden Arbeitsverhältnis**
*Der Beschäftigte ist verpflichtet, sich auf Verlangen des Arbeitgebers einer ärztlichen Untersuchung zu unterziehen, soweit die Erfüllung bestimmter gesundheitlicher Voraussetzungen wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung eine wesentliche und entscheidende berufliche Anforderung darstellt und tatsächliche Anhaltspunkte bestehen, die Zweifel an der fortdauernden gesundheitlichen Eignung des Beschäftigten begründen.*

*Der Beschäftigte ist verpflichtet, den Arbeitgeber über die Ergebnisse der Untersuchung durch Vorlage der ärztlichen Bescheinigung über seine Eignung zu unterrichten oder den behandelnden Arzt von der Schweigepflicht zu entbinden, soweit sie die Frage der gesundheitlichen Eignung des Beschäftigten für die ihm obliegende Tätigkeiten betreffen.*

*Das gleiche gilt, wenn ein Wechsel der Tätigkeit oder des Arbeitsplatzes eine solche Untersuchung erforderlich macht.*

*Der Arbeitgeber trägt die Kosten dieser Untersuchung, wenn diese nicht von einem Dritten übernommen werden.*

*Der Arbeitgeber ist berechtigt, die Untersuchung durch einen Arbeitsmediziner zu verlangen.*

**(3) Private Internet- und E-Mailnutzung**

Datenschutzrechtliche Fragen entstehen in der betrieblichen Praxis dann, wenn den Beschäftigten die „auch private" Nutzung des Internets oder des E-Mail-Kontos erlaubt wird.

Denn durch die private Nutzung kann der Arbeitgeber an personenbezogene Daten gelangen, die dem Schutzbereich der DS-GVO i. V. m. BDSG unterliegen, da der Arbeitergeber im Regelfall die Internetnutzung (stichprobenartig) überwachen möchte oder Zugriff auch auf das E-Mail-Konto des Beschäftigten haben möchte. Für diesen Fall ist die Einwilligung des Beschäftigten ein probates Mittel, wie ausdrücklich durch die Gesetzesbegründung[126] bestätigt wird.

Das bedeutet, dass der Arbeitgeber beispielsweise auf das Postfach zugreifen kann, wenn der Mitarbeiter im Urlaub ist oder erkrankt ist. Ebenso kann hiermit die Internetnutzung und die E-Mail-Nutzung stichprobenartiger anlassloser Kontrollen ermöglicht werden.

[126] Gesetzesbegründung BT-Drs. 18/11325, S. 97.

**HINWEIS**
Die anlassbezogenen oder stichprobenartigen Kontrollen sollten ausdrücklich in den Text der Einwilligung aufgenommen werden.

Liegt hingegen ein Verdacht einer Straftat vor, so können bei einem zu dokumentierenden Verdacht auch ohne Einwilligung des Beschäftigten entsprechende Kontrollen durchgeführt werden (Art. 6 i. V. m. Art. 88 DS-GVO i. V. m. § 26 Abs. 1 Satz 2 BDSG). Da § 26 Abs. 1 Satz 2 BDSG nur für Straftaten eine solche Kontrolle zulässt, ist zu empfehlen, die datenschutzrechtliche Erlaubnis im Einwilligungstext auch auf schwere Vertragsverletzungen zu beziehen. Das BAG geht für § 32 Abs. 1 Satz 1 BDSG a. F. davon aus, dass von diesem Erlaubnistatbestand auch „schwere Verfehlungen" erfasst sind.[127]

**Formulierungshilfe – private Nutzung IT**

***Einwilligungserklärung im Zusammenhang mit der privaten Internet-Nutzung mit flankierender Betriebsvereinbarung***[128]
*Ich möchte von dem Angebot Gebrauch machen, den betrieblichen Internetzugang in geringfügigem Umfang [konkret bestimmen] auch für private Zwecke zu nutzen.*

1. *Ich habe die Gelegenheit gehabt, die Betriebsvereinbarung über die Nutzung von Internet und E-Mail zur Kenntnis zu nehmen und bin mir über die folgenden, mit der Privatnutzung des Internets verbundenen Nutzungsbedingungen bewusst:*

- *Die private Nutzung ist nur in geringfügigem Umfang [konkret bestimmen] gestattet und nur sofern und soweit dadurch die geschäftliche Aufgabenerfüllung und die Verfügbarkeit der IT-Systeme für geschäftliche Zwecke nicht beeinträchtigt werden.*
- *Zum Schutz der IT-Systeme vor Viren, Trojanern und ähnlichen Bedrohungen sind der Download von Programmen aus dem Internet, sowie entsprechende Downloads von Dateianhängen im Rahmen der privaten Nutzung nicht gestattet.*

127 BAG, 20.10.2016, 2 AZR 395/15.; BAG 29.06.2017, 2 AZR 597/16.

128 Mustertext aus der Orientierungshilfe des sog. Düsseldorfer Kreises zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, Januar 2016.

- *Eine vorsätzliche Nutzung, welche geeignet ist, den Interessen der Arbeitgeberin oder deren Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Rechtsvorschriften verstößt, insbesondere*
- *der Abruf für den Arbeitgeber kostenpflichtiger Internetseiten,*
  - *das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenz- und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,*
  - *Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z. B. Angriffe auf externe Webserver) oder*
  - *Aktivitäten, die sich gegen das Unternehmen richten (z. B. Compliance-Verstöße [konkret benennen])*
  - *[an Regelung in Betriebsvereinbarung anpassen]*

  *unzulässig ist.*
- *Die A-GmbH ist berechtigt, den Aufruf bestimmter Internet-Seiten durch den Einsatz geeigneter Filter-Programme zu verhindern. Es besteht kein Rechtsanspruch auf einen Zugriff auf gefilterte Internet-Inhalte.*

2. *Ich willige ein, dass auch meine privaten – also nicht nur die betrieblichen – Internetzugriffe im Rahmen der Betriebsvereinbarung vom [Datum einsetzen] verarbeitet und unter den Voraussetzungen der Ziffern … der Betriebsvereinbarung protokolliert sowie personenbezogen ausgewertet werden.*

*Mir ist bewusst, dass ich hierdurch gegebenenfalls auf den Schutz des Fernmeldegeheimnisses gem. § 88 TKG verzichte.*

*Ich bin mir darüber im Klaren, dass eine missbräuchliche oder unerlaubte Nutzung neben arbeitsrechtlichen Konsequenzen gegebenenfalls auch strafrechtliche Folgen haben kann und dass darüber hinaus ein Verstoß zivilrechtliche Schadensersatzpflichten auslösen kann.*

*Mir ist bewusst, dass ich diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann, mit der Folge, dass ich ab dem Zeitpunkt des Widerrufs das Internet nicht mehr privat nutzen darf.*

Für die Datenverarbeitung und für den Eingriff in das Fernmeldegeheimnis (§ 206 StGB) bedarf der Arbeitgeber der Einwilligung des Beschäftigten.[129]

[129] Gola/*Schomerus*, BDSG, § 4a, Rn. 18; BfDI Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz, www.bfdi.bund.de, Januar 2008.

**HINWEIS**
Das gilt unabhängig von dem juristischen Streit, ob der Arbeitgeber sog. Diensteanbieter im Sinne des TKG oder des TMG ist.[130]

### (4) Bewerbungsgespräche via videobasiertem Internetangebot

Zunehmend wird in der betrieblichen Praxis auch erwogen, Bewerbungsgespräche über Skype oder andere vergleichbare Anbieter zu führen. Da ein solches Gespräch anders als im Bewerbungsgespräch von Angesicht zu Angesicht aufgezeichnet werden kann und anschließend wiederholt abrufbar ist, stellt sich auch hier die Frage nach der datenschutzrechtlichen Zulässigkeit.

Grundsätzlich kann zwar die Einwilligung in Betracht gezogen werden, allerdings ist die besondere Situation für den Bewerber zu berücksichtigen, die gegen die Freiwilligkeit der Einwilligung sprechen kann.[131]

Allenfalls wenn dem Bewerber eine echte (nachteilslose) Wahlmöglichkeit zwischen Video-Bewerbungsgespräch und Vor-Ort-Bewerbungsgespräch eingeräumt wird, kann der Arbeitgeber den Verdacht der mangelnden Freiwilligkeit beseitigen.

---

130 Dafür: Gola/*Schomerus*, BDSG, § 4a, Rn. 18; dagegen: LAG Berlin-Brandenburg, 16.02.2011, 4 Sa 2132/10; LAG Berlin-Brandenburg, 14.01.2016, 5 Sa 657/15; LAG Niedersachsen, 31.05.2010, 2 Sa 875/09.

131 Vgl. Gesetzesbegründung, BT-Drs. 18/11325, S. 97; Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW 2015/2016, S. 52; Jahresbericht Berliner Beauftragte für Datenschutz und Informationsfreiheit 2016, S. 114–118.

**HINWEIS**
Die Einwilligung muss transparent sein hinsichtlich der Ziele und Folgen der gesamten Datenverarbeitung, der technisch-organisatorischen Maßnahmen zum Schutz des Bewerbers. Auch sollte eine enge Beschränkung des Kreises der Beteiligten und Auswerter auf Arbeitgeberseite angegeben werden. Gegebenenfalls können die erhebliche Zeit- und Kostenersparnis als Gründe für das videobasierte Bewerbungsgespräch in den Text der Einwilligung mit aufgenommen werden. Der Hinweis auf das Widerrufsrecht ist zwingend; ein Hinweis auf eine Belehrung, wonach eine nachteilslose Verweigerung der Einwilligung möglich gewesen ist, empfehlenswert.

Auch hinsichtlich der Beschäftigten des Arbeitgebers, die für das Unternehmen die Bewerbungsgespräche führen, sollte eine Erlaubnisgrundlage nicht vergessen werden. Ob das bei solchen videobasierten Angeboten Art. 6 i. V. m. Art. 88 DS-GVO i. V. m. § 26 Abs. 1 Satz 1 BDSG sein kann, ist äußerst fraglich, so dass ebenfalls eine Einwilligung zu empfehlen ist.

## e. Umgang mit besonderen Kategorien personenbezogener Daten

### aa. Begriffsbestimmung

Die Verarbeitung von besonderen Kategorien von personenbezogenen Daten, die allgemein als „sensitive" Daten bezeichnet werden, unterliegt strengeren Anforderungen als die Verarbeitung von anderen personenbezogenen Daten. Dies hängt damit zusammen, dass diesen Daten ein höherer Schutzbedarf zugemessen wird, weil sie die Privat- und Intimsphäre besonderes tangieren.

Der Gesetzgeber zählt zu dieser Kategorie von Daten sämtliche Informationen,

- aus denen die rassische und ethnische Herkunft hervorgeht,
- die politische, religiöse oder weltanschauliche Überzeugungen widerspiegeln
- die Zeugnis von einer Gewerkschaftszugehörigkeit ablegen,
- die Auskunft über den Gesundheits- bzw. Krankheitszustand einer Person geben,
- das Sexualleben bzw. die sexuelle Orientierung betreffen, sowie neuerdings auch
- die genetische oder biometrische Details offenbaren und zur eindeutigen Identifizierung einer natürlichen Person geeignet sind.

Alle anderen personenbezogenen Daten werden nicht als sensitiv eingestuft und unterliegen nicht dem besonderen Schutz, dem diese Datentypen unterliegen. Dies gilt selbst für solche Daten, denen nach der Sozialanschauung ein erhöhter Schutzbedarf zukommt, wie z. B. personenbezogene Daten über strafrechtliche Verurteilungen, laufende oder abgeschlossene Ermittlungsverfahren oder Maßnahmen zur Sicherungsverwahrung. Ihre Verarbeitung unterliegt zwar besonderen Anforderungen (Art. 10 DS-GVO), trotzdem gelten sie nicht als sensitive Daten im Sinne der EU-Datenschutzgrundverordnung. Auch sonstige personenbezogene Daten, die zu Diskriminierungen (z. B. Geschlecht, Alter) führen können, sind ausgenommen.

### bb. Rechtsgrundlage für den Umgang mit besonderen Kategorien personenbezogener Beschäftigtendaten in Deutschland

Die Bedingungen, unter denen sensitive Beschäftigtendaten verarbeitet werden dürfen, sind nach dem neuen europäischen Datenschutzrecht grundsätzlich in Art. 6 DS-GVO i. V. m. Art. 88 DS-GVO i. V. m. § 26 BDSG geregelt, wobei die besonderen Maßgaben des Art. 9 DS-GVO zu berücksichtigen sind. Darüber hinaus haben die EU-Mitgliedstaaten gemäß Art. 88 Abs. 1 DS-GVO die Option, eigene spezifischere Vorschriften zu erlassen, die den Beschäftigtendatenschutz neben Art. 9 DS-GVO national individuell – d. h. anders im Vergleich zu anderen EU-Mitgliedstaaten – regeln.

Die Bundesrepublik Deutschland hat von dieser Option zur nationalen Regelung des Beschäftigtendatenschutzes Gebrauch gemacht und mit § 26 Abs. 3 eine BDSG spezifischere, nationale Vorschrift für den Beschäftigtendatenschutz in Deutschland erlassen, die neben Art. 9 DS-GVO Anwendung finden. Die Neuregelung orientiert sich in weiten Teilen am alten § 32 BDSG a. F.

Es ist davon auszugehen, dass andere EU-Mitgliedstaaten folgen und von der Option Gebrauch machen werden, eigene spezifischere Vorschriften zu erlassen. Bis auf einige Ausnahmen wird der Beschäftigtendatenschutz folglich weiter unterschiedlich in den einzelnen EU-Mitgliedstaaten ausgestaltet sein. Die vom europäischen Gesetzgeber mit der Datenschutz-Grundverordnung angestrebte Harmonisierung des Datenschutzrechts in Europa bleibt folglich in diesem Bereich teilweise aus.

**PRAXISTIPP**
International tätige Unternehmen bzw. Konzerne werden auch weiterhin bei der Klärung das Beschäftigungsverhältnis betreffender datenschutzrechtlicher Fragen Berater in verschiedenen europäischen Ländern konsultieren müssen, um einen Eindruck von der geltenden Rechtslage in den einzelnen EU-Mitgliedstaaten zu erhalten. Unter Umständen wird dies selbst in den EU-Mitgliedstaaten erforderlich sein, die keine eigenen Regelungen zum Beschäftigtendatenschutz treffen und die allgemeinen Regeln der EU-Datenschutz-Grundverordnung (Art. 6, 9 DS-GVO) anwenden. Grund dafür ist, dass bei der Abwägung der Rechtmäßigkeit einer Verarbeitung von sensitiven Daten sämtliche Umstände des Einzelfalls – inklusive nationaler Besonderheiten bei der Gewichtung bestimmter Interessen von Arbeitgeber und Beschäftigten sowie Gewichtung bestimmter Datenkategorien – zu berücksichtigen sind. Im Einzelfall kann dies zu unterschiedlichen Bewertungen desselben Sachverhalts in den EU-Mitgliedstaaten führen.

### cc. Bedingungen für den Umgang mit besonderen Kategorien personenbezogener Beschäftigtendaten

Nach § 26 Abs. 3 BDSG dürfen sensitive Daten prinzipiell nur in bestimmten geregelten Ausnahmefällen verarbeitet werden. Eine Verarbeitung von sensitiven Daten ist damit im Beschäftigungsverhältnis nur eingeschränkt möglich. Dies gilt auch dann, wenn sich Arbeitgeber und Beschäftigte hinsichtlich der Verarbeitung bestimmter sensitiver Daten im Beschäftigungsverhältnis einig sind.

Um Missbrauch vorzubeugen, hat der Gesetzgeber den Korridor der Verarbeitung von sensitiven Daten sehr eng gestaltet. Beschäftigte sollen vor Situationen bewahrt werden, in denen sie ohne tatsächliche Wahlmöglichkeit – etwa aus Opportunitätsdruck oder widerrechtlichem Zwang – zur Preisgabe von sensitiven Daten zwecks anschließender Verarbeitung bewegt werden.

Mit dieser Maßgabe dürfen nach deutschem Beschäftigtendatenschutzrecht sensitive Daten nur dann verarbeitet werden, wenn sie für den Arbeitgeber oder den Beschäftigten zur Ausübung von Rechten erforderlich sind.

**BEISPIELE**
für zulässige Datenverarbeitungen zur Ausübung von Arbeitgeberrechten:

- Nutzung von Daten krankheitsbedingter Ausfallzeiten zur Entgeltfortzahlung und Kontrolle der Arbeitsfähigkeit
- Nutzung von Krankheitsdaten zwecks Ausspruchs einer krankheitsbedingten Kündigung und zur Verteidigung in einem Kündigungsschutzprozess.
- Erhebung von Daten zur Schwerbehinderung von Beschäftigten zwecks Nachweis der Beschäftigungsquote und Meidung einer Ausgleichsabgabe bei Nichterreichung derselben.
- Nutzung von Daten, die die politische, religiöse oder weltanschauliche Überzeugung von Beschäftigten betreffen, zwecks Ausspruchs einer Kündigung und zur Verteidigung im Urteilsverfahren vor Arbeitsgerichten.
- Fingerabdruck für Sicherheitskonzepte auf dem Betriebsgelände (z. B. bekannter Versender).

**BEISPIELE**
für zulässige Datenverarbeitungen zur Ausübung von Beschäftigtenrechten:

- Erlangung besonderen Kündigungsschutzes und Anspruchs auf Sonderurlaub etc. durch Anzeige einer bestimmten Schwerbehinderung.
- Erlangung eines Anspruchs auf bezahlte (z. B. in Hessen) oder unbezahlte (z. B. in Sachsen) Freistellung zur Mitwirkung in der Jugendarbeit durch Offenlegung einer Mitwirkung in einer Vereinigung, die Rückschlüsse auf eine politische, religiöse oder weltanschauliche Überzeugung der Beschäftigten zulässt.
- Antragsgemäße Gewährung von Sonderurlaub von bis zu zwei Monaten innerhalb der letzten zwei Monate vor einem Wahltag bei Offenlegung einer Kandidatur für ein politisches Amt oder Mandat für eine bestimmte Partei.
- Erlangung von Sonderkündigungsschutz durch Anzeige eines kommunalpolitischen Mandats als Abgeordnete/r einer bestimmten Partei im Gemeinde-/Stadtrat (z. B. in Rheinland-Pfalz) bzw. einer Stadtverordnetenversammlung (z. B. in Hessen).
- Erlangung eines Anspruchs auf Entgeltfortzahlung nach dem EfzG bei Anzeige einer krankheitsbedingten Arbeitsunfähigkeit.

Zur Erfüllung des Erlaubnistatbestands muss das zu verarbeitende sensitive Datum in jedem Fall konstitutive, d. h. grundlegende Bedingung für die Rechtsausübung sein. Ohne die Verarbeitung des sensitiven Datums würden Arbeitgeber und Beschäftigte keinen Anspruch haben bzw. eine bessere Rechtsposition erlangen können.

Einen weiteren Ausnahmefall bildet nach § 26 Abs. 3 BDSG der Umstand, dass die Verarbeitung eines sensitiven Datums zur Erfüllung rechtlicher Pflichten aus dem Arbeits- oder Sozialrecht erforderlich ist.

**BEISPIELE**
für zulässige Datenverarbeitungen zur Erfüllung rechtlicher Pflichten des Arbeitgebers:

- Erhebung und Verarbeitung von Gesundheits-/Krankheitsdaten zwecks Durchführung des betrieblichen Eingliederungsmanagements.
- Erhebung von Gesundheitsdaten zur Überprüfung der gesundheitlichen Eignung von Beschäftigten – betrifft minderjährige Beschäftigte gemäß dem Jugendarbeitsschutzgesetz (JArbSchG) ebenso wie Beschäftigte, die der Röntgen- oder Strahlenschutzverordnung (RöV/StrSchutzV), dem Infektionsschutzgesetz (IfSG) und dem Seemannsgesetz (SeemannsG) unterfallen.
- Speicherung von Daten zur Religionszugehörigkeit zu Abrechnungszwecken.
- Weitergabe von Daten zur Schwerbehinderteneigenschaft von Bewerbern und Beschäftigten an den Betriebsrat und die Schwerbehindertenvertretung.
- Weitergabe von Daten krankheitsbedingter Ausfallzeiten an einen Betriebsrat zwecks Durchführung personeller Einzelmaßnahmen und Beteiligung bei Kündigungen.
- Weitergabe von Daten zu einer Schwerbehinderung bei Aufstellung eines Sozialplans.
- Einholung von Auskünften über die sexuelle Orientierung von Beschäftigten, wenn der Betrieb des Arbeitgebers als lebens- oder verteidigungswichtige Einrichtung nach § 3 Abs. Nr. 2 BVerfSchG eingestuft und der Arbeitgeber gesetzlich verpflichtet ist, Sicherheitsüberprüfungen durchzuführen, die entsprechende Informationen voraussetzen.

Neben den dargestellten Ausnahmebedingungen ist für die Rechtmäßigkeit der Verarbeitung sensitiver Daten im Beschäftigungsverhältnis nach § 26 Abs. 3 BDSG stets erforderlich, dass kein schutzwürdiges Interesse der betroffenen Person der Verarbeitung der jeweils betroffenen sensitiven Daten entgegensteht.

Ein schutzwürdiges Interesse, auf das sich Beschäftigte – neben ihren übrigen Grundrechten, wie z. B. dem Recht auf freie Meinungsäußerung und dem Recht auf freie Berufsausübung – im Zweifel immer berufen können, ist das Recht auf Geheimhaltung von Daten über ihre Persönlichkeit. Dieses ergibt sich aus dem grundrechtlich versicherten Recht auf informationelle Selbstbestimmung. Auch wenn dieses im Kontext des Grundgesetzes aufgrund seiner systematischen Stellung als starkes, besonders schutzwürdiges verfassungsmäßig versichertes Recht eingestuft wird, gilt es nicht uneingeschränkt und hat unter entsprechen-

den Umständen gegenüber anderen grundrechtlich geschützten Positionen des Arbeitgebers zurückzutreten. Dazu können das Recht am eingerichteten und ausgeübten Gewerbebetrieb, der Schutz anderer Menschen als Ausprägung der grundgesetzlich verankerten Würde des Menschen und das Recht auf Informationsfreiheit zählen, die auch juristischen Personen wie z. B. einer GmbH oder AG zustehen.

**PRAXISTIPP**
In den oben dargestellten Beispielen ist davon auszugehen, dass die Rechte und Interessen der Arbeitgeber die Rechte der Beschäftigten überwiegen. Ungeachtet dessen kommt es stets auf den Ausgang einer Erforderlichkeitsprüfung in Form einer umfassenden Interessenabwägung an. Hierbei ist zu berücksichtigen, dass ein mögliches entsprechendes überwiegendes Interesse der Beschäftigten am Ausschluss einer Verarbeitung sensitiver Daten regelmäßig dann nicht besteht, wenn die Datenverarbeitung durch den Arbeitgeber der Verfolgung von Zwecken dient, die im Zusammenhang mit der Erbringung der Arbeitsleistung oder Erfüllung arbeitsvertraglicher Pflichten der Beschäftigten oder gesetzlicher Pflichten des Arbeitgebers stehen.

**dd. Einwilligung des Beschäftigten in die Verarbeitung sensitiver Daten**

Sofern keine der oben genannten Ausnahmebedingungen einschlägig sind, kann der Umgang mit sensitiven Daten rechtmäßig sein, wenn Beschäftigte in die Verarbeitung ihrer Daten einwilligen.

Während dies nach bis Mai 2018 gültiger Rechtslage nicht unumstritten war, gibt es an der Möglichkeit der Heranziehung der Einwilligung im Beschäftigungsverhältnis keine grundlegenden Zweifel mehr. Nicht nur § 26 Abs. 3 BDSG, sondern auch Erwägungsgrund 43 DS-GVO belegen dies.

Voraussetzung für eine wirksame Einwilligung ist, dass diese sich ausdrücklich auf die zu verarbeitenden Daten bezieht. Des Weiteren sind an die Freiwilligkeit einer Einwilligung in die Verarbeitung sensitiver Daten strenge Anforderungen zu stellen. So sind etwa bei der Beurteilung, ob eine Einwilligung freiwillig erteilt wurde, insbesondere die im Beschäftigungsverhältnis grundsätzlich bestehende Abhängigkeit der Beschäftigten vom Arbeitgeber und die Umstände des Einzelfalls zu berücksichtigen. Neben der Art der verarbeiteten Daten und der Intensität

des Eingriffs in die Privat- oder Intimsphäre sollen auch der Zeitpunkt der Einwilligungserteilung (günstig vs. ungünstig) und andere prägende Bedingungen in die Bewertung der Freiwilligkeit einbezogen werden.[132]

Es spricht ganz regelmäßig für eine freiwillige Einwilligung, dass Beschäftigte in Folge der Datenverarbeitung einen rechtlichen oder wirtschaftlichen Vorteil erlangen oder Arbeitgeber und Beschäftigter gleichgerichtete Interessen verfolgen. So wird etwa angenommen, dass beispielsweise in der Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung die Gewährung eines Vorteils liegt.[133]

Hingegen spricht gegen eine freiwillige Einwilligung, wenn Beschäftigte nicht eindeutig und transparent auf die Verarbeitung sensitiver Daten hingewiesen werden. Ferner muss die Einwilligung in die Verarbeitung sensitiver Daten von der Einwilligung in die Verarbeitung anderer personenbezogener Daten abgesondert werden.

**PRAXISTIPP**
Arbeitgeber sollten etwa bei der Einholung von Einwilligungen in die Verarbeitung von Mitarbeiterfotos darauf achten, diese auch auf die Verarbeitung von sensitiven Daten zu erstrecken, die sich z. B. aus der Abbildung von Hautfarbe (potentielles Merkmal der rassischen oder ethnischen Herkunft), Kopfbedeckung (z. B. Kopftuch – potentielles Merkmal für eine religiöse oder weltanschauliche Überzeugung), Brille (ggf. Hinweis auf Schwerbehinderung) ergeben können. Zu diesem Zweck ist eine Klarstellung in der Einwilligungserklärung sinnvoll, nach der sich die Einwilligung auch auf die Verarbeitung sensitiver Daten die rassische oder ethnische Herkunft, religiöse oder weltanschauliche Überzeugung und Gesundheit betreffend beziehen.

Neben der freiwilligen Erteilung der Einwilligung setzt § 26 Abs. 2, 3 Satz 2 HS. 1 BDSG als Grundbedingung auch einen schriftlichen Nachweis der Einwilligung voraus, sofern dieser nicht wegen besonderer Umstände entbehrlich ist. Des Weiteren muss der Arbeitgeber beweisen können, dass er den Beschäftigten über den Verarbeitungszweck der sensitiven Daten sowie über sein Widerrufsrecht schriftlich informiert hat, wobei auch eine elektronische Information (z. B. per Email) ausreicht.

---

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

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

Schließlich muss der Arbeitgeber für die Verarbeitung von sensitiven Daten nachweisen können, dass er alle in seiner Macht stehenden Maßnahmen getroffen hat, um die betroffenen Daten zu schützen (§ 26 Abs. 3 Satz 3 i. V. m. § 22 Abs. 2 BDSG). Mit Blick darauf wird vom Arbeitgeber verlangt, dass er geeignete technische und organisatorische Maßnahmen zum Schutz der Daten vor unberechtigtem Zugriff, Verlust, Fälschung, Diebstahl etc. getroffen hat.

Technische Maßnahmen zum Schutz von sensitiven Daten sind sämtliche Sicherheitsvorkehrungen, die direkt mit dem verwendeten Datenverarbeitungssystem zusammenhängen und die eingesetzte Hard- und Software beeinflussen. Damit sind u.a. die Anwendung geeigneter Sicherheitstechniken sowie die Konfiguration von Sicherheitseinstellungen, aber auch die elektronische Kontrolle von Datenverarbeitungsaktivitäten gemeint.

Beispiele für technische Maßnahmen zum Schutz sensitiver Daten sind:
- Beschränkung des Zugriffs auf bestimmte Daten für bestimmte Personengruppen
- Datenverschlüsselung und -entschlüsselung
- Bedarfsgerechte, angemessene Schlüsselverwaltung (Key Management)
- Schutz strukturierter und unstrukturierter Daten
- Schutz von Protokoll- und Konfigurationsdateien
- Schutz der Datenbankausgabe
- Anonymisierung und Pseudonymisierung von Daten
- Datenschutzkonforme Löschung von Dateien und Inhalten
- Permanente Entfernung von sichtbaren Text- und Bildinhalten aus Dokumenten (Redaction)
- Ausblendung von Daten (Data Masking)
- Netzwerküberwachung (Network Monitoring)
- Permanente Kontrollen aller Datenbanken
- (Activity Monitoring), Automatische Detektierung und Meldung von Vorfällen bzw. ungewöhnlichen Vorkommnissen (Alerting, Reporting, Detection)

Organisatorische Maßnahmen betreffen das Umfeld des Systems, insbesondere die Personen die es nutzen, die nach Maßgabe des Gesetzgebers sensibilisiert sein müssen und nur dann Zugriff auf die Daten haben sollen, wenn damit ein legitimer Zweck verfolgt wird. Zudem muss zur Wahrung der Integrität der Daten sichergestellt sein, dass überprüft und festgestellt werden kann, ob und von wem die betreffenden Daten eingegeben, verändert oder entfernt worden sind.

Beispiele für organisatorische Maßnahmen zum Schutz sensitiver Daten sind:
- Schulung von Beschäftigten im angemessenen Umgang mit sensitiven Daten
- Verfahren und Prozesse für die Erteilung und Entziehung von Zugriffsberechtigungen auf Daten bzw. Systeme
- Regelmäßig stattfindende Risiko-Management- und Auditierungsverfahren
- Pläne für den Umgang mit Sicherheits- und Datenschutzverletzungen
- Strukturierte Auftragskontrollen mit Blick auf die Verarbeitung von Daten durch Dienstleister

**PRAXISTIPP**
Je umfassendere Schutzmaßnahmen umgesetzt werden, desto eher wird eine Interessenabwägung im Ergebnis zu Gunsten der Zulässigkeit einer in Aussicht genommenen Datenverarbeitung ausfallen. Es empfiehlt sich deshalb, gerade bei der Verarbeitung von sensitiven Daten sicherzustellen, dass hinreichende Schutzmaßnahmen getroffen werden.

### ee. Verarbeitung von sensitiven Beschäftigtendaten durch Auftragsverarbeiter

In Zeiten der vermehrten Nutzung von Cloud-Diensten und der Globalisierung der Datenverarbeitung sind auch sensitive Daten zunehmend Gegenstand von Auftragsverarbeitungen durch außenstehende Dritte (z. B. Dienstleister). Z. B. kommt es vor, dass sensitive Daten von Auftragsverarbeitern im Rahmen der Nutzung webbasierter HR Informationssysteme, Bewerbermanagementsysteme oder Arbeitssicherheitsdatenbanken/SHE-Systeme[134] verarbeitet werden.

Im Rahmen der Nutzung von Cloud-Diensten kann es auch vorkommen, dass sensitive Daten in Drittländern verarbeitet werden. Grund dafür ist, dass viele – insbesondere große, international agierende – Cloud-Anbieter eine globale Support-Struktur geschaffen haben, die rund um die Uhr an 365 Tagen im Jahr funktioniert und bei der Support – abhängig von der Uhrzeit – von Beschäftigten des Anbieters oder seiner Subunternehmer auf unterschiedlichen Kontinenten erbracht wird. Das heißt, auch wenn der Verantwortliche den Speicherort seiner Daten in Europa gewählt und dies mit dem Cloud-Anbieter vertraglich vereinbart hat, kann es zu einem internationalen Datentransfer in Drittländer kommen, wenn z. B. ein IT-Mitarbeiter des Cloud-Providers Support von Indien oder Australien aus leistet.

[134] SHE = Safety, Health & Environment; zu Deutsch: Sicherheit, Gesundheit und Umwelt.

Weder § 26 Abs. 3 BDSG noch andere Regelungen im Bundesdatenschutzgesetz oder der EU-Datenschutz-Grundverordnung stehen der Verarbeitung von sensitiven Daten durch Auftragsverarbeiter entgegen. Ein generelles Verbot für die Auslagerung von sensitiven Daten zum Zweck der Nutzung von internationalen Cloud-Diensten oder anderen Auftragsverarbeitungen und der Verarbeitung von sensitiven Daten durch Dritte lässt sich dem Gesetzestext nicht entnehmen. Im Gegenteil, manchen Regelungen (z. B. Art. 27 Abs. 2 lit. a) DS-GVO) lässt sich im Umkehrschluss entnehmen, dass diese Art der Datenverarbeitung zulässig ist.

Bevor sensitive Daten vom Arbeitgeber an einen Dienstleister weitergegeben werden können, ist zu überprüfen, ob die Verarbeitung der betroffenen Daten nach Art. 6, 9 DS-GVO i. V. m. Art. 88 DS-GVO i. V. m. § 26 Abs. 3 BDSG zulässig ist und geeignete technische und organisatorische Maßnahmen zum Schutz der Daten vor unberechtigtem Zugriff, Verlust, Fälschung, Diebstahl etc. seitens des Cloud-Anbieters getroffen worden sind (§ 26 Abs. 3, S. 3 i. V. m. § 22 Abs. 2 BDSG). In der Praxis heißt das, dass der Arbeitgeber prüfen und sicherstellen muss, dass geeignete Verschlüsselungs- und Sicherheitstechniken eingesetzt werden bzw. zusätzlich angewendet werden können und eine Pseudonymisierung von Klardaten unter Berücksichtigung des damit einhergehenden Aufwands und der entstehenden Kosten praktikabel ist.

Sofern eine Übermittlung an Dienstleister außerhalb der Europäischen Union in Drittstaaten erfolgt, die über kein der Datenschutz-Grundverordnung entsprechendes, durch die europäische Kommission anerkanntes, angemessenes Datenschutzniveau nach Art. 45 DS-GVO verfügen, müssen Arbeitgeber ferner sicherstellen, dass sie und/oder der Auftragsverarbeiter geeignete Garantien zum Schutz der betroffenen Daten im Sinne des Art. 46 Abs. 2 DS-GVO vorgesehen haben. Solche Garantien können wie bereits unter dem bis Mai 2018 geltenden Recht u. a. in Form von verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules) nach Art. 47 DS-GVO oder der Verwendung von durch die europäische Kommission erlassenen Standarddatenschutzvertragsklauseln[135] gewährleistet werden.

[135] 2010/87/EU.

# 4. RECHTE DER BETROFFENEN PERSON

## a. Grundsätze für die Realisierung der Rechte der betroffenen Personen nach der DS-GVO

Um die Vorschriften des BDSG nachvollziehen zu können, müssen zunächst die für die Rechte der betroffenen Person allgemein geltenden Regelungen und die Systematik der DS-GVO betrachtet werden.

In Art. 12 DS-GVO werden zunächst alle Regelungen vor die Klammer gezogen, die sich auf die Schaffung von Transparenz für die Betroffenen über die Verarbeitung beziehen. Der zugehörige Erwägungsgrund 39 stellt neben der Transparenz auch die anderen Grundsätze des Art. 5 DS-GVO für die Verarbeitung wie Rechtmäßigkeit, Treu und Glauben, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit dar. Jede Verarbeitung soll danach rechtmäßig und nach Treu und Glauben erfolgen. Für natürliche Personen soll Transparenz geschaffen werden über die Tatsache und den Umfang der Verarbeitung. Das setzt voraus, dass alle Informationen und Mitteilungen hierüber leicht zugänglich, verständlich und in klarer und einfacher Sprache abgefasst sind.

Im Einzelnen finden sich in Art. 12 DS-GVO Vorgaben zur Kommunikation mit den Betroffenen und für die Behandlung ihrer auf Art. 15 bis 22 und 34 DS-GVO gestützten Anträge sowie im Hinblick auf die Informationspflichten nach Art. 13, 14 DS-GVO.

### aa. Vorgaben zur Kommunikation mit den Betroffenen

Alle zur Verfügung gestellten Informationen und Mitteilungen müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form und in klarer und einfacher Sprache abgefasst sein. Dies kann schriftlich, mündlich oder elektronisch geschehen. Da die DS-GVO hierzu keine weiteren Ausführungen macht, ist davon auszugehen, dass auch Medienbrüche, zumindest in einem gewissen Umfang und auf Wunsch des Betroffenen, zulässig sind.[136]

[136] Die Datenschutzkonferenz (DSK) ist der Ansicht, dass nicht auf Informationen im Internet verwiesen werden darf, wenn Daten von einer anwesenden Person erhoben werden. Das gelte gleichermaßen für eine schriftliche Korrespondenz auf dem Papierweg; DSK Kurzpapier Nr. 10, abzurufen unter: https://www.lda.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf

Der Arbeitgeber hat geeignete Maßnahmen zu treffen, um den betroffenen Personen die notwendigen Informationen und seine Antworten auf deren Anfragen zu übermitteln. „Übermitteln" ist in diesem Zusammenhang zu verstehen als in einer Weise zur Verfügung stellen, dass von dem Informationsangebot Gebrauch gemacht werden kann. Für die Information sind entsprechende Prozesse aufzusetzen und für die Umsetzung verantwortlichen Stellen im Unternehmen zu kommunizieren. Eine tatsächliche Kenntnisnahme der Information durch den einzelnen Mitarbeiter ist dabei nicht erforderlich und muss im Rahmen der Rechenschaftspflicht auch nicht nachgewiesen werden. Auf Empfangsbestätigungen kann daher in aller Regel verzichtet werden.

Aufgrund des Umfangs der bereitzustellenden Informationen, die richtig und vollständig, aber dennoch für den rechtlichen Laien verständlich sein müssen, ist diese Anforderung in der Praxis nicht einfach zu erfüllen. Daher können ergänzend zu textlicher und/oder mündlicher Information auch standardisierte Bildsymbole, sogenannte Icons verwendet werden. Die EU-Kommission ist befugt, nähere Regelungen zum Inhalt dieser Icons sowie zum Verfahren ihrer Bereitstellung zu machen, Art. 12 Abs. 7 und 8 DS-GVO. Bisher gibt es hierzu jedoch noch keine weiteren Festlegungen.

**PRAXISTIPP**

**Information**
Am einfachsten zu erfüllen wird in diesem Zusammenhang das Kriterium der leichten Zugänglichkeit sein. Aus Gründen der Nachweisbarkeit sollte jedoch eine rein mündliche Information die absolute Ausnahme sein. In der Praxis wird man zu Mischformen gelangen, die nach einer ersten schriftlichen oder elektronischen Information auf weitere persönliche oder schriftliche Informationsmöglichkeiten, ggf. in Form der Verlinkung auf spezielle Unternehmensseiten, verweist. Je nach Branche und Belegschaft ist zu prüfen, welche Abschichtung der Inhalte und welche Art der Informationsbereitstellung die Anforderungen in bestmöglicher Weise erfüllen.

**Mitarbeiterbetreuung**
Nutzt der Arbeitgeber für die Personalverwaltung Service Center, die auch telefonisch erreichbar sind, beispielsweise für Änderungen von Adressdaten, so ist es ausreichend, wenn die Mitarbeiter hierzu bei Einstellung schriftliche Informationen erhalten. Nicht erforderlich oder praktikabel ist es, wenn bei jedem Anruf standardmäßig mündlich Informationen zu den

Details der Datenverarbeitung gegeben werden. Allerdings sind die Mitarbeiter zu schulen, so dass sie bei Bedarf die Inhalte der schriftlichen Information wiedergeben und darüber hinaus gehende Fragen beantworten können.

**Beantwortung von Anfragen**
Für die Beantwortung von Anfragen sollte der gleiche Weg genutzt werden, auf dem die Anfrage gestellt wurde, es sein denn, die betroffene Person hat hierzu entsprechende Wünsche geäußert. Ob der Zugang der Antwort nachweisbar sein soll, beispielsweise durch die Anforderung einer Lesebestätigung für E-Mails oder die Versendung eines Antwortbriefes per Einschreiben, muss im Einzelfall anhand der Kritikalität der Anfrage entschieden werden. Gesetzliche Vorgaben bestehen hierzu nicht.

**bb. Anträge auf Grundlage der Art. 15 bis 22 DS-GVO – Identitätsprüfung**

Vor der Informationserteilung ist zur Umsetzung des Prinzips der Vertraulichkeit vom Verantwortlichen zusätzlich eine Identitätsprüfung vorzunehmen, Art. 12 Abs. 6 DS-GVO. Hat er begründete Zweifel an der Identität und damit an der Berechtigung der Person, die den Antrag gestellt hat, so kann er weitere Informationen anfordern, die als Identitätsnachweis erforderlich sind. Ist der Nachweis erbracht, kann auf Wunsch auch eine mündliche Information erfolgen. Hiervon ist wegen der bestehenden Rechenschaftspflicht des Verantwortlichen bzw. des Verarbeiters jedoch abzuraten.

Allerdings besteht keine Pflicht zur Speicherung personenbezogener Daten, allein um die Identifizierung und damit die Rechtsausübung zu ermöglichen, Art. 11 Abs. 1 DS-GVO. Dies kommt bei der Verarbeitung von Daten zum Tragen, für die eine Identifizierung der betroffenen Person nicht erforderlich ist, wie z. B. bei anonymen Antworten im Rahmen einer Mitarbeiterbefragung. Die Betroffenenrechte nach Art. 15 bis 20 DS-GVO sind hier grundsätzlich nicht anwendbar, Art. 11 Abs. 2 DS-GVO. Der Verantwortliche hat aber gegenüber einer anfragenden Person nachzuweisen, dass er selbst mit zusätzlichen Informationen seitens der Person keine Identifizierung vornehmen kann, Art. 12 Abs. 2 Satz 2 DS-GVO.

### cc. Erleichterung der Rechtsausübung – Art. 12 Abs. 2 Satz 1 DS-GVO

Der Verantwortliche hat der betroffenen Person die Ausübung ihrer Rechte zu erleichtern. Aus Erwägungsgrund 57 lässt sich herauslesen, dass mit „Erleichterung" die Umsetzung von Maßnahmen gemeint ist, die eine digitale Identifizierung und elektronische Kommunikation ermöglichen. In diesem Zusammenhang werden Authentifizierungsverfahren für Online-Dienste erwähnt.

**PRAXISTIPP**
Bei der Umsetzung der Informationspflichten im Beschäftigungsverhältnis wird zu unterscheiden sein, auf welche Daten sich die Geltendmachung der Rechte bezieht (Personaldaten oder operative Daten), welche IT-Systeme diese Daten beinhalten und ob die betroffene Person Zugang zu diesen Systemen hat. In allen IT-Systemen, die eine Datenpflege durch die Betroffenen selbst ermöglichen, sollte geprüft werden, inwieweit Reporting-Funktionalitäten angeboten werden können, die den Auskunftsanspruch decken. Für alle Beschäftigten mit einem personalisierten E-Mail-Account bietet sich eine Antragstellung und Antragsbeantwortung per Mail – unter Einhaltung der Sicherheitsbestimmungen i. S. d. Art. 32 DS-GVO, ggf. mit Passwort geschützten Anhängen – an, da hierüber die Identitätsprüfung ausreichend sicher erfolgen kann. Dies setzt allerdings voraus, dass im Falle eines Auskunftsverlangens die Daten auch elektronisch lesbar oder zumindest als Bilddateien zur Verfügung gestellt werden können. Für alle anderen Mitarbeiter müssen persönliche oder postalische Prozesse für die Kommunikation mit den jeweiligen Verantwortlichen aufgesetzt werden, die Identifizierungsmaßnahmen, zum Beispiel die Beifügung einer Papierkopie des Mitarbeiterausweises, einschließen.

### dd. Frist für die Bearbeitung von Anträgen

Die Frist für eine Reaktion auf die Eingabe einer beschäftigten Person und darin beantragte Maßnahmen beträgt einen Monat ab Eingang des Antrags, Art. 12 Abs. 3 DS-GVO. Eine Verlängerungsoption um zwei weitere Monate ist gegeben, wenn die längere Bearbeitungsfrist aufgrund der Komplexität und der Anzahl der Anträge erforderlich ist. Voraussetzung für die Fristverlängerung ist jedoch eine begründete Zwischennachricht innerhalb des ersten Monats.

Soweit sich der Verantwortliche dazu entscheidet, die beantragte Maßnahme nicht durchzuführen, hat er dies gegenüber der betroffenen Person innerhalb eines Monats nach Eingang des Antrags mit Gründen versehen mitzuteilen und auf das Rechts zur Beschwerde bei der Aufsichtsbehörde oder ggf. auch zur Einlegung eines gerichtlichen Rechtsbehelfs hinzuweisen.

**PRAXISTIPP**
Da in jedem Fall innerhalb eines Monats nach Eingang eines Antrags eine Reaktion gegenüber der betroffenen Person zu erfolgen hat, bietet es sich an, die Anfragen ihrer Art nach zu clustern und bei hoher Komplexität frühzeitig eine Nachricht mit der Begründung für eine Verlängerung der Frist auf die vollen drei Monate zu versenden. Was unter hoher Komplexität zu verstehen ist, wird die Praxis zeigen müssen. Im Falle eines per E-Mail gestellten Antrags bietet die Zwischennachricht per E-Mail einen ausreichenden Nachweis. Von einer automatischen Eingangsbestätigung mit Fristverlängerung auf drei Monate ist dabei dringend abzuraten, da die Voraussetzungen für die Fristverlängerung nicht in jedem Fall gegeben sein werden. Für die postalische Abwicklung empfiehlt sich eine Versendung per Einschreiben, um den Zugang nachweisen zu können.

**ee. Grundsätzliche Kostenfreiheit – Art. 12 Abs. 5 DS-GVO**

Informationen aufgrund Art. 13 und 14 sowie Mitteilungen und Maßnahmen gemäß Art. 15 bis 22 und 34 DS-GVO sind für die Beschäftigten kostenfrei, es sei denn, der Arbeitgeber kann nachweisen, dass die Geltendmachung von Rechten offenkundig unbegründet oder exzessiv ist. Dies kann bei häufigen Wiederholungen, ohne dass sich die Umstände wesentlich geändert haben, und bei ausufernden Anträgen gegeben sein. Man wird hier abzuwägen haben, in welcher Form eine Entgelterhebung überhaupt sinnvoll ist und nach welchen Maßstäben sie erfolgen soll. Neben der Festlegung der entgeltpflichtigen Sachverhalte wären die Höhe des Entgelts anhand der entstehenden Verwaltungskosten sowie die Art der Begleichung des Entgelts zu regeln.

Alternativ zur Erhebung eines angemessenen Entgelts kann sich der Verantwortliche in diesen Fällen weigern, Maßnahmen aufgrund des Antrags zu ergreifen.

Siehe hierzu auch Recht auf Kopie der verarbeiteten Daten gemäß Art. 15 Abs. 3 DS-GVO in Kapitel 5. c. aa.

#### ff. Benachrichtigung von Datenempfängern über getroffene Maßnahmen – Art. 19 DS-GVO

Diese Regelung hätte ebenfalls in Art. 12 DS-GVO vor die Klammer gezogenen werden können, da sie sich auf mehrere Betroffenenrechte bezieht. Gemäß Art. 19 DS-GVO hat der Verantwortliche jede Berichtigung, Löschung oder Einschränkung der Verarbeitung allen Empfängern mitzuteilen, denen gegenüber er personenbezogene Daten offengelegt hat.

Die Pflicht entfällt, sofern dies unmöglich oder mit unverhältnismäßigem Aufwand verbunden ist. Auf Verlangen unterrichtet der Verantwortliche die betroffene Person über die Empfänger dieser Daten.

### b. Informationspflichten des Verantwortlichen

Die Rechte der betroffenen Person sind ein zentraler Punkt der europäischen Harmonisierungsbestrebungen im Bereich des Datenschutzes. Diesen Rechten stehen korrespondierende Pflichten der verantwortlichen Arbeitgeber gegenüber, die den Beschäftigten die Rechtsausübung ermöglichen sollen. Das BDSG enthält hierzu in den §§ 32 bis 37 sechs beschränkende Regelungen. In der DS-GVO im Kapitel III finden sich die zunächst vorrangigen Art. 13 bis 23. Für den Rechtsanwender bedeutet dies eine aufwendige Parallellektüre beider Texte.

Das hat folgenden Grund: Art. 23 DS-GVO ermächtigt die Union und die Mitgliedsstaaten, die Rechte und Pflichten nach den Art. 12 bis 22, aber auch 34 sowie die Grundsätze der Verarbeitung aus Art. 5 durch Gesetzgebungsmaßnahmen zu beschränken. Der deutsche Gesetzgeber hat diese Möglichkeit hinsichtlich der Art. 13, 14, 15, 17, 21 und 22 genutzt.

Siehe hierzu auch Anhang 1 – Muster für ein Informationsblatt.

**Übersicht über die einzelnen Rechte der betroffenen Personen**

| Thema | Grundsätzliche Regel in der DS-GVO | Ergänzende Regel im BDSG |
|---|---|---|
| Information | Art. 13 bzw. 14 | § 32 bzw. 33 |
| Auskunft | Art. 15 | § 34 |
| Berichtigung | Art. 16 | - |
| Löschung und Recht auf Vergessenwerden | Art. 17 | § 35 |
| Einschränkung der Verarbeitung | Art. 18 | § 35 |
| Datenübertragbarkeit | Art. 20 | - |
| Widerspruch | Art. 21 | § 36 |
| Automatisierte Einzelfallentscheidung | Art. 22 | § 37 |

**aa. Informationsinhalte bei der Direkterhebung – Art. 13 DS-GVO**

Um Daten bei der Direkterhebung beim Betroffenen, wie sie im Fall von Bewerbungen und Einstellungen vorliegt, fair und transparent zu verarbeiten, sind den betroffenen Personen spätestens im Zeitpunkt der Datenerhebung folgende Informationen in geeigneter Weise zur Verfügung zu stellen.

- Name und die Kontaktdaten der verantwortlichen Arbeitgebergesellschaft sowie gegebenenfalls ihres Vertreters;
- gegebenenfalls die Kontaktdaten der/des betrieblichen Datenschutzbeauftragten;
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung: Als Zwecke kommen hier alle Sachverhalte in Frage, die sich im Rahmen des sogenannten Mitarbeiter-Lebenszyklusses ergeben. Rechtsgrundlagen werden vornehmlich Verträge, gesetzliche Verpflichtungen, berechtigte Interessen und Einwilligungen des Betroffenen sein.
- ob die Verarbeitung auf Art. 6 Absatz 1 Buchstabe f, den berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden beruht;
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten: nach Ansicht der Datenschutzkonferenz sind aufgrund Art. 4 Ziffer 9 DS-GVO auch die Dienstleister (Auftragsverarbeiter) des Verantwortlichen, weil sie nicht „Dritte" i. S. d. Art. 4 lit. 10 DS-GVO sind, zu nennen.

- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Art. 46, 47 oder 49 Abs. 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.
- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich sein sollte, zumindest, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Auskunft durch den Verantwortlichen über die personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- wenn die Verarbeitung auf Art. 6 Abs. 1 Buchstabe a oder Art. 9 Abs. 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist;
- ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

**PRAXISTIPP**
Betrachtet man diese umfänglichen Informationspflichten, ist zunächst zu unterscheiden, welche Beschäftigtengruppen in welcher Form geeignet informiert werden können.

Es bietet sich an, nach Bewerbern, Neueinstellungen und Leiharbeitnehmern zu unterscheiden, da von diesen Personengruppen nach Art bzw. Umfang unterschiedliche personenbezogene Daten aufgrund unterschiedlicher Rechtsgründe verarbeitet werden. So werden von Leiharbeitnehmern häufig sowohl in der Personalverwaltung als auch im Betrieb weniger Daten verarbeitet als von den eigenen Beschäftigten. Je nach Branche kann sich die Verarbeitung daher auf die Vertragsabwicklung mit dem Verleiher und die Verwaltung der Stundenzettel beschränken.

Zusätzlich sind bis Mai 2018 auch alle Bestandsmitarbeiter zu informieren, da die bisherigen Informationen den neuen Anforderungen nicht ausreichend Rechnung tragen.

Gegenüber allen Zielgruppen, mit Ausnahme der potentiellen Bewerber, bietet es sich an, in mehreren Schritten in der von der DS-GVO geforderten Tiefe zu informieren.

So sollten im ersten Schritt in Form einer generellen Information alle in Art. 13 DS-GVO genannten Inhalte angesprochen werden. Neben den obligatorischen Kontaktdaten ist zu ermitteln und darzustellen, welche möglichen Verarbeitungszwecke und rechtlichen Grundlagen im jeweiligen Unternehmen vorkommen. Die zahlreichen vertraglichen und gesetzlichen Verpflichtungen für eine Verarbeitung, zum Beispiel zur Gehaltszahlung, aus dem Steuerrecht oder im Bereich der Arbeitszeit sind damit in jedem Unternehmen relevant und anzugeben. Gibt es jedoch beispielsweise kein institutionalisiertes betriebliches Vorschlagswesen oder keinerlei Firmenfahrzeuge, so sind diese Punkte auch nicht darzustellen. Ob die konkrete Verarbeitung im Rahmen eines einzelnen Beschäftigungsverhältnisses im Unternehmen tatsächlich zum Tragen kommt, ist für die generelle Information daher unerheblich. Ebenso ist nicht entscheidend, wie und mit welchen technischen Mitteln oder welchem IT-System die Verarbeitung erfolgt. Dies sind Details, die in weiteren Schritten durch zusätzliche Informationsangebote oder zumindest auf Nachfrage mitgeteilt werden müssen. Auf diese weiteren Möglichkeiten ist im Rahmen der generellen Information hinzuweisen.

Um den Informationskontakt möglichst weitreichend zu nutzen, sollte dabei auf alle Punkte, die in den Absätzen 1 und 2 des Art. 13 DS-GVO bzw. Art. 14 (siehe gesonderte Darstellung auf Seite 114) aufgeführt sind, eingegangen werden.

Für weitergehende Informationen kann dann, je nach Mitarbeiterstruktur und technischer Ausstattung, auf das Intranet, Gruppenlaufwerke, Aushänge oder die zuständigen Ansprechpartner, z. B. in den Personalabteilungen, verwiesen werden. Letztere werden bei Informationsersuchen oder der Geltendmachung von Rechten zu entscheiden haben, ob die Anfrage in ihre Verantwortlichkeit fällt, zum Beispiel Recht auf Einsichtnahme in die Personalakte oder Daten aus den Personalverwaltungs- und Zahlungssystemen, oder ob andere Fachabteilungen, operative Bereiche oder Mitbestimmungsgremien betroffen und einzubeziehen sind.

Bewerber im Rahmen eines Online-Bewerbungsverfahrens sollten in einem einzigen Schritt über alle in Frage kommenden Daten und Erhebungswege informiert werden. Die Nutzung von Daten aus Online-Netzwerken mit beruflichem Schwerpunkt kann dabei als Direkterhebung bei der betroffenen Person angesehen werden, da diese die Informationen auch zu diesem Zweck den im Netzwerk agierenden Arbeitgebern zum Abruf zur Verfügung stellt.

Bei klassischen schriftlichen Bewerbungen ist zu unterscheiden, ob es sich um eine Initiativbewerbung handelt oder nicht und wie mit den Unterlagen weiter verfahren wird. Ist eine Einstellung in ein Bewerber-Tool geplant, so sollte dies in jedem Fall im Rahmen der Stellenausschreibung, auf Karriere-Seiten im Internet oder in anderer Weise (notfalls per Post) mitgeteilt und, sofern erforderlich, eine Einwilligung zur Speicherung für die mögliche Besetzung anderer oder zukünftiger offener Stellen eingeholt werden. In Stellenausschreibungen kann auf die Internetseite des Unternehmens verwiesen werden. Dort müssen sich neben den übrigen Datenschutzhinweisen auch Informationen über den Umgang mit Bewerberdaten finden lassen.

Dagegen können Bestandsmitarbeiter auch über interne Medien informiert werden – der Nutzen einer öffentlich zugänglichen Information über die Verarbeitung ihrer Daten im Unternehmen ist daher sehr genau abzuwägen.

**bb. Ausnahmen von der Informationspflicht nach Art. 13 DS-GVO**

Eine Ausnahme von diesen Informationspflichten besteht nach Art. 13 Abs. 4 DS-GVO, wenn die betroffene Person bereits alle in Art. 13 Abs. 1 und 2 DS-GVO geforderten Informationen verfügt. Dies bezieht sich auch auf den Fall der Zweckänderung.

**cc. Informationsinhalte und Frist bei der indirekten Erhebung – Art. 14 DS-GVO**

Im Falle der Dritterhebung teilt der Verantwortliche der betroffenen Person zum einen die gleichen Informationen mit, wie im Falle der Direkterhebung.

Art. 14 DS-GVO zählt die einzelnen Angaben nicht in der gleichen Reihenfolge auf wie Art. 13 DS-GVO.

Zum anderen sind weitere Informationen zu geben, die sich im Falle der Direkterhebung für den Betroffenen unmittelbar ergeben, und zwar die Kategorien personenbezogener Daten, die verarbeitet werden sowie woher die Daten stammen und ob die Quelle öffentlich zugänglich ist.

Der Verantwortliche stellt die Informationen unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats zur Verfügung.

Sollten die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden, sind die Informationen spätestens zum Zeitpunkt der ersten Mitteilung an diese zu erteilen.

Ist die Offenlegung an einen anderen Empfänger beabsichtigt, ist die Information an den Betroffenen spätestens zum Zeitpunkt der ersten Offenlegung zu geben.

**dd. Ausnahmen von der Informationspflicht nach Art.14 Abs. 5 DS-GVO**

**Dies gilt wiederum nicht, wenn**

- die betroffene Person über die Informationen verfügt
- die Informationserteilung unmöglich oder unverhältnismäßig ist (nicht abschließende Beispiele: Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschung, Statistik)
- Erlangung oder Offenlegung durch Unionsrecht oder Recht der Mitgliedsstaaten ausdrücklich geregelt
- Daten einem gesetzlichen Berufsgeheimnis unterliegen.

**ee. Nationale Ausnahmen**

Das BDSG sieht einige zusätzliche Ausnahmen für nicht öffentliche Stellen vor. So nennt § 29 Abs. 1 BDSG als möglichen Grund, dass die Informationen gemäß § 29 Abs. 1 Satz 1 BDSG ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Gleiches soll nach § 33 Abs. 1 lit. 2a) BDSG gelten bei Beeinträchtigung der Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche oder der Verarbeitung von Daten aus zivilrechtlichen Verträgen zur Verhütung von Schäden durch Straftaten, sofern nicht berechtigte Interessen der betroffenen Person an der Informationserteilung überwiegen.

Unterbleibt die Information, hat der Verantwortliche geeignete Maßnahmen zum Schutze der berechtigten Interessen der betroffenen Person zu ergreifen und nach Art. 14 Abs. 1 und 2 DS-GVO die Öffentlichkeit zu informieren.

**ff. Weiterverarbeitung bei Zweckänderung**

**(1) Grundsätzliche Pflicht zur Information über Zweckänderung, Art. 13 Abs. 3 und Art. 14 Abs. 4 DS-GVO**

Beabsichtigt der Arbeitgeber, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er, unabhängig von der Art der Erhebung, der beschäftigten Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen wie hinsichtlich des ursprünglichen Zweckes zur Verfügung.

Die Information muss dabei vor der Zweckänderung gegeben werden. Allerdings ergibt sich nicht, mit welchem Vorlauf diese zu erfolgen hat. In der Regel wird man im Beschäftigungsverhältnis von einer Frist von mindestens 14 Tagen ausgehen können.

Zu den Anforderungen an eine Zweckänderung gemäß Art. 6 Abs. 4 DG-GVO siehe Seite 28.

**(2) Ausnahmen gemäß § 32 BDSG**

§ 32 BDSG regelt Ausnahmen von der Informationspflicht in Fällen der Zweckänderung. Erleichterungen sollen u. a. greifen bei

- der Weiterverarbeitung analog gespeicherter Daten
- der Beeinträchtigung, der Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche

- vorliegender Gefährdung der vertraulichen Übermittlung der Daten an öffentliche Stellen.

Der Verantwortliche hat im Falle, dass eine vorherige Information über die Zweckänderung unterbleibt, der Öffentlichkeit Informationen gemäß Art. 13 Abs. 1 und 2 DS-GVO bereitzustellen und die Gründe hierfür schriftlich zu dokumentieren. Sofern ein vorübergehender Hinderungsgrund für die Vorabinformation vorlag, ist diese spätestens innerhalb von zwei Wochen nach Fortfall nachzuholen.

## c. Wichtige Betroffenenrechte

### aa. Auskunftsrecht – § 34 BDSG, Art. 15 DS-GVO

In Ergänzung zur Informationspflicht des Arbeitgebers (vgl. Kapitel 4 a., b.), räumt Art. 15 DS-GVO dem Arbeitnehmer einen datenschutzrechtlichen Auskunftsanspruch ein. Auf Verlangen des Mitarbeiters – eine bestimmte Form ist nicht vorgeschrieben, wenngleich Schriftform zu begrüßen ist – ist mitzuteilen, ob überhaupt Daten gespeichert sind und falls ja, welche Daten hiervon betroffen sind. Zusätzlich sind folgende Informationen heraus zu geben:

- die Verarbeitungszwecke,
- die Kategorien personenbezogener Daten, die verarbeitet werden **(neu)**,
- die Datenempfänger oder Kategorien von Empfängern,
- falls möglich die geplante Speicherdauer **(neu)**,
- Aufklärung über die Betroffenenrechte (Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht) **(neu)**,
- Aufklärung über Beschwerderecht bei der Aufsichtsbehörde **(neu)**,
- Herkunft der Daten, wenn diese nicht von der betroffenen Person selbst erhoben wurden,
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling inklusive aussagekräftiger Informationen über die verwendete Logik **(neu)**,
- Unterrichtung über die geeigneten Garantien bei Datenübermittlungen in EU-Drittländer **(neu)**.

**PRAXISTIPP**
Die Aufzählung verdeutlicht, dass im Vergleich zum bisherigen Auskunftsanspruch nach § 34 BDSG a. F. der Arbeitgeber deutlich umfangreichere Mitteilungen erarbeiten muss. Zwar kann der Arbeitnehmer in der Praxis nicht im Rahmen des Arbeitsvertrages auf die Geltendmachung seines Auskunftsrechts verzichten. Er darf jedoch dazu angehalten werden, sein Auskunftsverlangen zu konkretisieren, um den Aufwand möglichst gering zu halten.[137] Tut er dies nicht, muss der Arbeitgeber umfassend Auskunft erteilen. Für den Arbeitgeber erscheint es empfehlenswert, dem Auskunftsverlangen in einem „abgestuften Verfahren" nachzukommen (vgl. Kap. 4. b. aa.). Im Beschäftigtenkontext könnte der nunmehr ausdrücklich geregelte Anspruch auf einen Negativbescheid (vgl. Art. 15 Abs. 1 Hs. 1 DS-GVO) vor allem bei abgelehnten Bewerbern[138] oder im Rahmen beendeter Arbeitsverhältnisse von steigender Relevanz sein. In diesem Zusammenhang erlangt die betroffene Person die Bestätigung, ob überhaupt Daten verarbeitet werden oder nicht.

Bestehen begründete Zweifel an der Identität des Antragstellers, so können nach Art. 12 Abs. 6 DS-GVO zusätzliche Informationen zur Bestätigung der Identität angefordert werden. Im Arbeitsverhältnis ist grundsätzlich davon auszugehen, dass die Identität des jeweiligen Beschäftigten bekannt ist.

Die Auskunft selbst kann gem. Art. 12 Abs. 1 Satz 2, 3 DS-GVO je nach Sachverhalt mündlich, elektronisch oder schriftlich erteilt werden. Nach Art. 15 Abs. 3 DS-GVO ist dem Arbeitnehmer auf Antrag eine Kopie zur Verfügung zu stellen. Die erste Kopie ist kostenlos, für alle weiteren können angemessene Verwaltungskosten auferlegt werden. Möglich ist insoweit auch der Fernzugriff des Betroffenen auf ein gesichertes System.

Dem Auskunftsverlangen ist unverzüglich, spätestens jedoch innerhalb eines Monats nach Zugang des Antrags nachzukommen. Die Frist kann um zwei Monate verlängert werden, wenn dies aufgrund der Komplexität und der Gesamtanzahl der Anträge nötig ist.[139]

---

137 Erwägungsgrund 63.

138 Gola, Handbuch Arbeitnehmerdatenschutz, Rn. 1491c.

139 Zu den Einzelheiten vgl. Art. 12 Abs. 3, 4 DS-GVO; Erwägungsgrund 63.

Die Auskunftserteilung kann nach Art. 15 Abs. 4 DS-GVO ausnahmsweise unterbleiben, wenn Geschäftsgeheimnisse oder Rechte anderer Personen entgegenstehen. Hiervon darf allerdings keine allgemeine Verweigerungshaltung abgeleitet werden. Der deutsche Gesetzgeber regelt in § 34 BDSG, vergleichbar mit den bisherigen Ausnahmeregelungen, noch weitere Eingrenzungen des Auskunftsrechts. So kann die Auskunft unterbleiben, wenn die Daten nur aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, die Auskunftserteilung einen unverhältnismäßigen Aufwand mit sich bringt und eine Verarbeitung zu anderen Zwecken durch geeignete Maßnahmen ausgeschlossen ist (z. B. durch Einschränkung der Verarbeitung; vgl. Kapitel 5 c. dd.). Damit der Arbeitnehmer die Auskunftsablehnung nachvollziehen und überprüfen kann, ist diese zu dokumentieren und ihm gegenüber zu begründen.

**PRAXISTIPP**
Arbeitgeber haben zu überprüfen, inwieweit die vorhandenen „Auskunftsbriefe" angepasst und neue Inhalte aufgenommen werden müssen. Etwaige Musterbausteine müssen so gestaltet werden, dass individuelle Erläuterungen möglich sind. Die auskunftsgebenden Personen sollten eine organisatorische oder technische Lösung zur Fristenkontrolle vorhalten können.

**HINWEIS**
Der Auskunftsanspruch aus Art. 15 DS-GVO und das Personalakteneinsichtsrecht des Arbeitnehmers gem. § 83 Abs. 1 BetrVG schließen sich auch nach den Vorgaben der DS-GVO nicht aus.[140] Letzteres reicht teilweise weiter als der datenschutzrechtliche Auskunftsanspruch.

Zum Auskunftsanspruch siehe auch die Prozessbeschreibung im Anhang 6.

**bb. Art. 16 DS-GVO – Recht auf Berichtigung**

Art. 16 DS-GVO räumt dem betroffenen Arbeitnehmer sowohl das Recht auf Berichtigung, als auch das Recht auf Vervollständigung lückenhafter Daten ein. Die Intervention des Arbeitnehmers beruht auf dem zunächst geltend gemachten Auskunftsanspruch. Allerdings ist der Arbeitgeber bereits von sich aus gem. Art. 5

[140] *Franck*, RDV 2016, S. 115.

Abs. 1 lit. d) DS-GVO verpflichtet, unrichtige Daten zu korrigieren und auf dem neusten Stand zu halten, um diese nicht löschen zu müssen. Ausnahmen von der Berichtigungspflicht wurden im Rahmen des Beschäftigtendatenschutzes auch durch das BDSG nicht vorgesehen.

**BEISPIEL**
Der Arbeitnehmer stellt fest, dass der Arbeitgeber seine Sprachkenntnisse falsch oder unvollständig hinterlegt hat. Die Berichtigung ist unabhängig vom Grad der Persönlichkeitsrechtsverletzung vorzunehmen.

Die Berichtigung ist nach Art. 16 DS-GVO unverzüglich durchzuführen. Zur Bestimmung des Begriffes „unverzüglich" kann auf § 121 Abs. 1 BGB zurückgegriffen werden. Die Berichtigung hat je nach Einzelfall „ohne schuldhaftes Zögern" zu erfolgen.[141] Besteht eine offenkundige Unrichtigkeit von Personaldaten, hat die Berichtigung in der Regel sofort zu erfolgen. Ist sich der Arbeitgeber nicht sicher, ob die hinterlegten Daten richtig sind, kann er den Sachverhalt zunächst prüfen. Währenddessen ist die Datenverarbeitung jedoch eingeschränkt (vgl. Art. 18 lit. a)). Das heißt die Daten dürfen zwar gespeichert werden, aber nur noch unter besonders engen Voraussetzungen verwendet werden.

Das Recht auf Gegendarstellung gem. § 83 Abs. 2 BetrVG bleibt vom Anspruch auf Berichtigung unberührt.

Zum Recht auf Berichtigung siehe auch die Prozessbeschreibung in Anhang 6.

### cc. Recht auf Löschung – § 35 BDSG, Art. 17 DS-GVO

#### (1) Neue und alte Löschungsrechte

Neben den personalaktenrechtlichen Löschungs- und Entfernungsansprüchen sind bereits heute die datenschutzrechtlichen Löschungs- und Sperrungsrechte der Arbeitnehmer zu beachten (vgl. § 35 BDSG a. F.). Der Löschungsanspruch von Beschäftigten ist also nicht neu. Ausgehend von der Idee den Betroffenen ein Recht auf „Vergessenwerden" einzuräumen, ist die Pflicht zur Datenlöschung in Art. 17 DS-GVO detailliert geregelt und teilweise modifiziert worden. Die „Löschung" ist Teil der Datenverarbeitung gem. Art. 4 Nr. 2 DS-GVO, wird allerdings nicht mehr explizit definiert. Es ist davon auszugehen, dass unter Löschung wei-

[141] Gola/*Reif*, DS-GVO, Art. 16 Rn. 17.

terhin jede Form des Unkenntlichmachens zu verstehen ist (z. B. durch Überspielen, Überschreiben oder Vernichten eines Datenträgers).[142] Die Vorgaben der DS-GVO können so verstanden werden, dass ein logisches Löschen ausreichend ist. Entscheidend ist, dass die Verbindung zwischen den Daten und der Person gelöst wird, sodass der Personenbezug wegfällt und eine Re-Identifizierung der Person durch ein erneutes Verbinden der Daten technisch-organisatorisch ausgeschlossen wird. Ein physisches Löschen ist oftmals aufgrund der komplexen Backup-Systematiken praktisch unmöglich. Vor diesem Hintergrund erklärt sich auch die Trennung zwischen „Löschen" und physischem „Vernichten" in Art. 4 Nr. 2 DS-GVO.

Die Löschverpflichtung ist nicht nur auf den besonders schützenswerten Online-Bereich, sondern auf alle Datenverarbeitungsvorgänge anzuwenden. Die Pflicht des Verantwortlichen, personenbezogene Daten zu löschen, ist bereits in Art. 5 Abs. 1 lit. e) DS-GVO verankert. Danach ist die Speicherung personenbezogener Daten nur so lange erlaubt, wie sie für den Zweck, für den sie verarbeitet werden, erforderlich sind (Speicherbegrenzung). Eine längere Speicherung ist nur in Ausnahmefällen erlaubt. Erwägungsgrund 39 stellt klar, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt werden muss. Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen (vgl. Art. 30 Abs. 1 lit. f) DS-GVO).

Art. 17 Abs. 1 DS-GVO zählt sechs Anlässe auf, die einen Anspruch des Beschäftigten und eine Verpflichtung des Verantwortlichen zur Löschung begründen:

- Der Zweck für die Datenverarbeitung ist weggefallen **(hohe Priorität)**,[143]
- Die betroffene Person widerruft ihre Einwilligung **(hohe Priorität)**,
- Die betroffene Person legt Widerspruch ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor,
- Die Daten wurden unrechtmäßig verarbeitet **(hohe Priorität)**,
- Die Löschung ist eine gesetzliche Pflicht **(hohe Priorität)**,
- Datenerhebungen in Bezug auf angebotene Dienste der Informationsgesellschaft bei Minderjährigen.

142 Gola/*Nolte/Werkmeister*, DS-GVO, Art. 17 Rn. 8.

143 Bedeutung im Rahmen des Beschäftigtendatenschutzes.

**BEISPIEL**
Es kann davon ausgegangen werden, dass die Legitimationsbefugnis gem. § 26 BDSG regelmäßig nach Beendigung des Beschäftigungsverhältnisses entfällt. Ob die Daten nach dem Ausscheiden noch gespeichert werden dürfen, hängt davon ab, inwieweit spezielle Aufbewahrungsvorschriften hierzu berechtigen oder ggf. sogar verpflichten. Auch die Zweckbestimmung des nachwirkenden Arbeitsverhältnisses kann eine weitere Aufbewahrung gestatten.

**HINWEIS**
Für das Arbeitsverhältnis ist die Regelung in Art. 17 Abs. 1 lit. b) DS-GVO von besonderer Bedeutung. Danach muss eine Löschung nicht vorgenommen werden, wenn der Beschäftigte zwar seine erteilte Einwilligung widerruft, der Verantwortliche sich aber auf eine anderweitige Rechtsgrundlage für die Verarbeitung stützen kann. Dies ist zu begrüßen, da in der Praxis oftmals, aufgrund bestehender Rechtunsicherheiten hinsichtlich der gesetzlichen Erlaubnistatbestände, umfassende Einwilligungserklärungen eingeholt werden.

Zur Datenlöschung siehe auch die Prozessbeschreibung in Anhang 6.

**(2) Weiterentwicklung des Rechts auf „Vergessenwerden"**

Neu ist, dass der Arbeitgeber nicht nur zur Datenlöschung verpflichtet ist, sondern gem. Art. 17 Abs. 2 DS-GVO bei Veröffentlichung der Daten, auch Dritte (andere Verantwortliche) vom Verlangen des Betroffenen informieren muss. Sofern also der Arbeitgeber personenbezogene Daten von Beschäftigten z. B. in das Internet einstellt, muss er im Rahmen der zur Verfügung stehenden Technologien die dazu angemessenen organisatorischen und technischen Maßnahmen ergreifen, damit alle Links zu diesen Daten oder Kopien oder Replikationen gelöscht werden können.[144] Dies gilt auch für Datenübermittlungen innerhalb des Konzernverbunds.

[144] Vgl. Erwägungsgrund 66.

### (3) Keine Regel ohne Ausnahme

Art. 17 Abs. 3 DS-GVO legt fest, inwieweit die Pflicht zur Datenlöschung unterbleiben kann. Voraussetzung ist, dass der Erhalt von Daten für bestimmte Zwecke weiterhin notwendig ist. Im Beschäftigtenkontext ist insbesondere zu prüfen, ob die Datenverarbeitung zur Erfüllung einer Rechtspflicht (Art. 17 Abs. 3 lit. b) DS-GVO) oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 17 Abs. 3 lit. e) DS-GVO) erforderlich ist.

Bei der Erfüllung einer Rechtspflicht sind vor allem die bestehenden gesetzlichen arbeits-, sozial-, steuer- und gesellschaftsrechtlichen Speicherfristen zu beachten. Entscheidend ist, nach welchem Zeitraum bestimmte Rechte oder Pflichten aus dem Arbeitsverhältnis nicht mehr belegt werden müssen. Andernfalls wäre es dem Arbeitgeber nicht möglich, Ansprüche im Zusammenhang mit dem Arbeitsverhältnis abzuwehren oder bestimmten Bußgeldtatbeständen zu entgehen.

**BEISPIEL**
Zu den wichtigsten gesetzlichen Aufbewahrungspflichten im Arbeitsverhältnis zählen insbesondere:

- Arbeitsanweisungen und sonstige Organisationsunterlagen zehn Jahre gem. § 257 Abs. 1 Nr. 1 HGB
- Buchungsbelege zehn Jahre gem. § 257 Abs. 1 Nr. 4 HGB
- steuerliche Aufbewahrungsfristen gem. § 147 AO, § 41 Abs. 1 EStG
- Arbeitszeitnachweise zwei Jahre gem. § 16 Abs. 2 ArbZG
- Mutterschutz-Unterlagen zwei Jahre gem. § 19 Abs. 2 MuSchG
- Arbeitnehmerüberlassung – Geschäftsunterlagen des Verleihers drei Jahre gem. § 7 Abs. 2 AÜG
- Jugendarbeitsschutz-Unterlagen zwei Jahre gem. § 50 Abs. 2 JArbSchG
- Lohnunterlagen (Sozialversicherung), Beitragsabrechnungen und Beitragsnachweise gem. § 28 f. Abs. 1 SGB IV
- Mindestlohn-Unterlagen zwei Jahre gem. § 17 Abs. 1 MiLoG[145]

[145] Hopfner/Erdmann/*Hohenadl*, Praxishandbuch Arbeitsrecht, S. 235; im Internet finden sich zahlreiche Checklisten zu den einzelnen Aufbewahrungsfristen im Personalbereich.

- Ist eine wirksame Rechtsdurchsetzung ohne eine weitere Datenspeicherung nicht mehr möglich, kann die Verpflichtung zur Datenlöschung unterbleiben. Fraglich ist, ob die Speicherung bereits für mögliche künftige Rechtsstreitigkeiten zulässig ist. Ausreichend ist jedenfalls, wenn Auseinandersetzungen anstehen oder mit hinreichender Wahrscheinlichkeit zu erwarten sind.[146] Entscheidend sind die Umstände des Einzelfalls.

**BEISPIEL**
Es besteht kein genereller Anspruch auf Entfernung bzw. Löschung einer zu Recht erteilten Abmahnung, bloß weil diese ihre Warnfunktion verloren hat. Vielmehr muss die Abmahnung für das Arbeitsverhältnis in jeder Hinsicht rechtlich bedeutungslos geworden sein. Ist die Abmahnung für die Interessenabwägung einer möglichen späteren Kündigung erforderlich, erscheint eine weitere Dokumentation angezeigt. Denn im Zusammenhang mit einem Kündigungsrechtsstreit ist zu prüfen, inwieweit einer Abmahnung noch eine gewisse Beweisfunktion zugesprochen werden kann.[147]

### (4) Umsetzung der Löschungsverpflichtung

In der Praxis besteht oftmals ein großes Vollzugsdefizit hinsichtlich der vorgegebenen Löschvorgaben. Hierfür sind unterschiedliche Ursachen verantwortlich (z. B. Unsicherheit bei Mitarbeitern oder unübersichtliche Datenbestände). Damit alle Datenbestände gleichermaßen korrekt gelöscht werden, bedarf es einer systematischen Vorgehensweise. Diese muss durch das verantwortliche Unternehmen entwickelt und dokumentiert werden. Es stellt sich deshalb oftmals die Frage, wie ein sinnvolles Löschkonzept erarbeitet werden kann.

Wie die Anforderungen des Art. 17 DS-GVO in der Praxis durch die Verantwortlichen umzusetzen sind, lässt sich der DS-GVO nicht ohne Weiteres entnehmen. Die Unternehmen werden künftig darauf angewiesen sein, dass der Europäische Datenschutzausschuss so schnell wie möglich Leitlinien, Empfehlungen oder bewährte Verfahren zu Art. 17 DS-GVO bereitstellt.[148]

---

146 Gola/*Nolte/Werkmeister*, DS-GVO, Art. 17 Rn. 44.

147 BAG, 19.07.2012, 2 AZR 782/11.

148 Vgl. Kurz-Papier LDABayern – Recht auf Löschung „Vergessenwerden" – Art. 17 DSGVO.

**PRAXISTIPP**
Sofern im Unternehmen kein reines technisches Löschkonzept für Personaldaten vorhanden ist, bietet die DIN 66398 – eine „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten" eine Hilfestellung bei der Implementierung eines organisatorischen Löschkonzepts. Die DIN 66398 hat ein Vorgehensmodell entwickelt, um ein Löschkonzept für personenbezogene Daten erfolgreich im Unternehmen etablieren zu können. Die Vergabe der einzelnen Löschfristen für die jeweiligen Datensätze erfolgt dabei unternehmensindividuell. [149]

Die Erarbeitung von Löschkonzepten im Rahmen von Personaldatenbanken ist erforderlich, um den bestehenden datenschutzrechtlichen Anforderungen gerecht werden zu können. Dabei sieht die DS-GVO deutlich höhere Bußgelder als bisher vor. Bei Verstößen gegen die Löschpflicht sind gem. Art. 83 Abs. 5 lit. b) DS-GVO Geldbußen von bis zu 20.000.000 € oder von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes möglich.

**dd. Einschränkung der Datenverarbeitung – § 35 BDSG, Art. 18 DS-GVO**

Die „Einschränkung der Verarbeitung" ist auf Antrag des Beschäftigten vorzunehmen, wenn diese im Vergleich zur Löschung sinnvoller ist. Dabei ist unter „Einschränkung der Verarbeitung" im weitesten Sinne die bisher bekannte „Sperrung" zu verstehen, auch wenn der Begriff des „Sperrens" in der DS-GVO nicht zu finden ist.[150] Der neu bezeichnete Vorgang der „Einschränkung der Verarbeitung" besteht nach Art. 4 Nr. 3 DS-GVO in der „Markierung" gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Im Ergebnis handelt es sich – im Vergleich zur Löschung – um das zunächst mildere Mittel. Art. 18 Abs. 1 DS-GVO erkennt einen Anspruch nur an, wenn

- der Betroffene die Richtigkeit der Daten bestreitet (lit. a)),
- die Verarbeitung unrechtmäßig ist, aber ein Löschungswiderspruch des Betroffenen eingegangen ist (lit. b)),
- der Betroffene die Daten auch nach Zweckerreichung noch zur Rechtsdurchsetzung benötigt (lit. c))
- oder der Betroffene gem. Art. 21 Abs. 1 DS-GVO der Datenverarbeitung widerspricht (lit. d)).

[149] Vgl. *Hammer*, DuD 8/2016; S. 528 ff.

[150] Definiert in § 3 Abs. 4 Satz 2 Nr. 4 BDSG a. F.

**HINWEIS**
Der Ausnahmekatalog des Art. 17 Abs. 3 DS-GVO ist im Vergleich zu § 35 BDSG a. F. eingeschränkt worden. Damit die bisherige Rechtslage weitestgehend fortgeführt werden kann, hat der deutsche Gesetzgeber in § 35 BDSG die in der DS-GVO genannten Ausnahmen zur Löschungsverpflichtung ergänzt. Unter den Voraussetzungen des § 35 BDSG tritt an die Stelle der Löschung die Einschränkung der Verarbeitung gem. Art. 18 DS-GVO.

So ist nach § 35 Abs. 3 BDSG eine Einschränkung der Verarbeitung vorzuziehen, wenn einer endgültigen Löschung u.a. arbeitsvertragliche Aufbewahrungsfristen entgegenstehen. Daneben hat der deutsche Gesetzgeber eine weitere wichtige Ergänzung zur DS-GVO vorgenommen. Nach § 35 Abs. 1 BDSG besteht – wie bisher – die Möglichkeit zur „Einschränkung", wenn ein Löschen wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Die zu treffende Abwägungsendscheidung bemisst sich nach dem jeweiligen Stand der Technik. Entscheidend ist, mit welchem Aufwand Datenspeicher verändert oder gelöscht werden können.

Methoden zur Beschränkung der Datenverarbeitung können sein:
- Übertragung ausgewählter Daten auf ein anderes Verarbeitungssystem
- Sperrung bestimmter personenbezogener Daten für einzelne Nutzer
- vorrübergehende Entfernung veröffentlichter Daten (z. B. auf einer Website)[151]

**ee. Art. 20 DS-GVO – Recht auf Datenübertragbarkeit**

Mit dem Recht auf Datenübertragbarkeit (auch Datenportabilität) wurde ein völlig neues Betroffenenrecht sowie ein spezielles „Auskunftsrecht" installiert. Es geht um die Herausgabe strukturierter und maschinenlesbarer Daten, um diese entweder selbst oder – bei technischer Machbarkeit – durch den Verantwortlichen, an einen Dritten übermitteln zu können. Sinn und Zweck der Regelung ist, dem Betroffenen die Kontrolle über „seine" automatisiert verarbeiteten Daten zu geben.[152] Der Anspruch ist jedoch auf die Fälle beschränkt, in denen eine automatisierte Datenverarbeitung auf einer Einwilligung oder einem Vertrag beruht. Stützt sich die Verarbeitung auf einen anderen Erlaubnistatbestand, z. B. die Erfüllung einer Rechtspflicht, muss dem Verlangen des Betroffenen nicht nachgekommen werden.

[151] Erwägungsgrund 67.
[152] Erwägungsgrund 68.

Ursprünglich war die Vorschrift für den Wechsel von Diensteanbietern im Bereich „Social Media" vorgesehen.[153] Eine derartige Beschränkung ergibt sich jedoch nicht mehr aus dem finalen Wortlaut des Art. 20 DS-GVO. In der Folge kann das Recht auf Datenübertragbarkeit auch im Beschäftigtenkontext zur Anwendung kommen. In der Praxis wird sich zeigen, ob Mitarbeiter hiervon tatsächlich Gebrauch machen. Zumindest bei oder nach Beendigung des Arbeitsverhältnisses erscheint ein entsprechendes Begehren nicht ausgeschlossen.

**BEISPIEL**
Der Arbeitnehmer verlangt, im Zuge eines Arbeitgeberwechsels die von ihm automatisiert gespeicherten Daten an den neuen Arbeitgeber zu übermitteln. Von Interesse können dabei nicht nur die Personalstammdaten sondern auch spezielle Karriere- oder Skill-Daten sein.

## 5. VERARBEITUNG VON BESCHÄFTIGTENDATEN DURCH AUFTRAGSVERARBEITER

Die arbeitsteilige Verarbeitung personenbezogener Daten ist für die deutsche Wirtschaft von großer Bedeutung. Insofern kommt den Regelungen zur „Auftragsverarbeitung", so die Terminologie der DS-GVO, eine enorme praktische Relevanz zu. Die meisten Anforderungen an das Verhältnis zwischen Verantwortlichen und IT-Service Provider (Auftragsverarbeiter) sowie die Ausgestaltung ihrer vertraglichen Beziehung finden sich in Art. 28 DS-GVO. Sie werden durch Vorgaben für Verantwortliche und Auftragsverarbeiter im Kontext der Auftragsverarbeitung in zahlreichen anderen Vorschriften ergänzt. Die Regeln zur Auftragsverarbeitung kommen uneingeschränkt auch im Beschäftigungskontext zur Anwendung. Konzeption und Ausgestaltung der Auftragsverarbeitung sind im Vergleich zum BDSG etwas „großzügiger", da sie von einer umfassenderen Verantwortung gekennzeichnet sind.

[153] *Franck*, RDV 2016, S. 118.

## a. Die europäische Konzeption der Auftragsverarbeitung

- Nach der europäischen Konzeption der Auftragsverarbeitung kann sich ein Verantwortlicher jeden qualifizierten Auftragsverarbeiter auf der ganzen Welt als Dienstleister aussuchen. Dies gilt für jeden Verantwortlichen, gleich in welchem Sektor er tätig ist. Hierzu bedarf es keiner spezialgesetzlichen Gestattung.[154]

- Der Datentransfer an den Dienstleister bedarf keiner speziellen (weiteren) Legitimierung.[155] Dies gilt auch wenn sich der Auftragverarbeiter in einem Land ohne ein anerkanntes EU-vergleichbares Datenschutzniveau befindet. Dann sind gemäß Art. 44 ff. DS-GVO – nur – „geeignete Garantien" für die Übermittlung zu bieten.

- Die Tätigkeit eines Auftragsverarbeiters ist nicht - mehr - auf Hilfstätigkeiten beschränkt. Auftragsverarbeiter können Entscheidungen über das „Wie" der Verarbeitung, also z. B. welche Hard- und Software zur Anwendung kommt, eigenverantwortlich treffen. Es ist ausreichend, wenn der Verantwortliche hierüber „nur" informiert wird.[156] Dies sollte allerdings vertraglich niedergelegt sein.

- Die bisherigen Beschränkungen bei der beauftragten Verarbeitung von besonderen Kategorien personenbezogener Daten (siehe § 28 Abs. 6 BDSG a. F.)[157] außerhalb eines Vertragsstaats des Europäischen Wirtschaftsraums gibt es nicht mehr.[158]

## b. Auswahl eines qualifizierten Auftragsverarbeiters

Der Verantwortliche darf nur hinreichend qualifizierte Auftragsverarbeiter mit der Durchführung der Auftragsverarbeitung beauftragen, Art. 28 Abs. 1 DS-GVO. Die Qualifikation bezieht sich auf das technische und rechtliche Fachwissen sowie auf technische und organisatorische Sicherungsmaßnahmen, Erwägungsgrund 81 DS-GVO.

---

154 *Monreal* in PinG 2017, S. 216 ff.

155 *Schmitz/v. Dall'Armi* in ZD 2016, S. 427; *Drewes/Monreal* in PinG 2014, S. 143.

156 Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", WP 169 S. 31, *Monreal* in PinG 2017, S. 216 ff.

157 Erd in DuD 2011, 275 ff. zum Fall des "sicheren Drittlands"(Schweiz).

158 Erd in DuD 2011, 275 ff.; *Monreal* in PinG 2017, S. 216 ff, *Schmidt/Freund*, ZD 2017, S. 14.

## c. Vertrag als Grundlage der Auftragsverarbeitung

Der Vertrag für die Auftragsverarbeitung ist essentiell. Hierin sind alle geforderten Anforderungen zu regeln, und zwar so, dass kein Streit über Verantwortlichkeiten entsteht.

### Die Anforderungen an einen Vertrag zur Auftragsverarbeitung

Verantwortlicher und Auftragsverarbeiter müssen einen den Anforderungen des Art. 28 Abs. 3 DS-GVO entsprechenden Vertrag schließen. Die nachfolgende Tabelle führt die Aspekte auf, zu denen der Vertrag Aussagen enthalten muss. Bei ihr hat sich der europäische Gesetzgeber an den Kriterien von § 11 BDSG a. F. orientiert.

| Zu regelnde Anforderung | Quelle |
|---|---|
| 1. Gegenstand der Verarbeitung | Art. 28 Abs. 3 Satz 1 DS-GVO |
| 2. Dauer der Verarbeitung | Art. 28 Abs. 3 Satz 1 DS-GVO |
| 3. Art und Zweck der Verarbeitung | Art. 28 Abs. 3 Satz 1 DS-GVO |
| 4. Art der personenbezogenen Daten | Art. 28 Abs. 3 Satz 1 DS-GVO |
| 5. Kategorien betroffener Personen | Art. 28 Abs. 3 Satz 1 DS-GVO |
| 6. Dokumentierte Weisung | Art. 28 Abs. 3 lit. a) DS-GVO |
| 7. Vertraulichkeitsverpflichtung | Art. 28 Abs. 3 lit. b) DS-GVO |
| 8. Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO | Art. 28 Abs. 3 lit. c) DS-GVO |
| 9. Unterstützung bei der Wahrnehmung von Betroffenenrechten | Art. 28 Abs. 3 lit. e) DS-GVO |
| 10. Unterstützung bei der Einhaltung der Pflichten aus den Art. 32 bis 36 DS-GVO | Art. 28 Abs. 3 lit. f) DS-GVO |
| 11. Datenrückgabe bzw. -löschung nach Abschluss der Verarbeitungen | Art. 28 Abs. 3 lit. g) DS-GVO |
| 12. Zurverfügungstellung von Informationen zum Nachweis der Pflichten aus Art. 28 | Art. 28 Abs. 3 lit. h) DS-GVO |
| 13. Ermöglichung von Überprüfungen | Art. 28 Abs. 3 lit. h) DS-GVO |
| 14. Schriftlichkeit | Art. 28 Abs. 9 DS-GVO |

Der Verantwortliche kann den Vertrag über die Beauftragung individuell formulieren oder sich eines Mustervertrags („Standardvertragsklauseln" genannt) bedienen.

**PRAXISTIPP**
Die Verwendung von Musterverträgen für die Auftragsverarbeitung von anerkannten Ausgabestellen, wie beispielsweise dem Bitkom[159] oder der Europäischen Kommission[160] (bisher nur für außerhalb der EU) hat mehrere Vorteile. So kann man sicher sein, allen Anforderungen zu entsprechen; vorausgesetzt natürlich, dass die individuell zu machenden Angaben erfolgt sind. Auch kann man sich bei der Verwendung von solchen Musterverträgen wahrscheinlich zeitaufwendige Diskussionen mit Service Providern ersparen.

■ **Schriftlicher Vertrag**

Ein (Unter-)Auftragsverarbeitungsvertrag ist „schriftlich" abzufassen, Art. 28 Abs. 9 DS-GVO, was auch in einem elektronischen Format erfolgen kann. „Schriftlich" bedeutet hier jedoch nicht schriftlich im Sinne des § 126 BGB! Das heißt, dass ein Vertrag nicht (mehr) eigenhändig unterschrieben werden muss. Die Anforderung, den Vertrag schriftlich im Sinne einer dokumentierten Form abzufassen, dient der in Art. 5 Abs. 2 DS-GVO normierten Rechenschaftspflicht. Dennoch ist es sinnvoll den Vertrag zur Auftragsverarbeitung gemeinsam mit dem eigentlichen Servicevertrag – zumindest als Anlage – zu unterschreiben.

■ **„Sicherheitsbehördenklausel"**

Aus Art. 28 Abs. 3 lit. a) 2. HS DS-GVO folgt, das der Auftragsverarbeitungsvertrag eine Aussage dazu enthalten muss,[161] ob der Auftragsverarbeiter nach der für ihn maßgeblichen Rechtsordnung verpflichtet werden kann, personenbezogene Daten des Verantwortlichen an andere (z. B. Sicherheitsbehörden) herauszugeben.

159 https://www.bitkom.org/noindex/Publikationen/2017/Leitfaden/170918-Mustervertragsanlage-ENG-online-final-2.pdf.

160 http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

161 Paal/Pauly/Martini, Datenschutzgrundverordnung, Art. 28 Rn. 40.

## d. Weitere Auftragsverarbeiter – Unterbeauftragung

Die DS-GVO regelt dezidiert, unter welchen Voraussetzungen weitere Auftragsverarbeiter in die Verarbeitung personenbezogener Daten einbezogen werden dürfen. Gemäß Art. 28 Abs. 3 lit. d) DS-GVO ist dies zunächst davon abhängig, dass die Anforderungen der Abs. 2 und 4 von Art. 28 DS-GVO eingehalten werden. Das bedeutet, dass mit dem weiteren (Unter-)Auftragsverarbeiter ein Auftragsverarbeitungsvertrag zu schließen ist, der den gesetzlichen bzw. den ggfs. darüber hinaus individuell ausformulierten Bedingungen des (Haupt-) Auftragsverarbeitervertrags entspricht.

Wie bisher hängt die Involvierung weiterer Auftragverarbeiter von der vorherigen Genehmigung des Verantwortlichen ab. Neu ist, dass die DS-GVO zwischen einer „gesonderten" und einer „allgemeinen" Genehmigung unterscheidet. Erstere bezieht sich auf einzelne, individuell zu benennende weitere Auftragsverarbeiter. Demgegenüber gilt die allgemeine Genehmigung pauschal für alle zuverlässigen und qualifizierten weitere Auftragsverarbeiter, die der (Haupt-)Auftragsverarbeiter auswählt und dem Verantwortlichen vorschlägt. Sofern dieser gegen die von dem Auftragsverarbeiter vorgeschlagenen weiteren Auftragsverarbeiter keinen Einspruch erhebt, gilt die Beauftragung als genehmigt. Der europäische Gesetzgeber hat hiermit die geforderte sog. Widerspruchs- bzw. Einspruchslösung bei der Unterbeauftragung aufgenommen. Wichtig ist, dass der Auftragsverarbeiter dann für Verstöße gegen die datenschutzrechtlichen Pflichten des weiteren Auftragsverarbeiters dem Verantwortlichen haftet, Art. 28 Abs. 4 Satz 2 DS-GVO.

**PRAXISTIPP**
Man sollte als Verantwortlicher abwägen, ob man die „Einspruchslösung" bei der Involvierung von weiteren Auftragsverarbeitern als sinnvoll und wünschenswert erachtet. Dies kann beispielsweise bei großen Cloud-Anwendungen der Fall sein. Wenn dem so ist, ist es ratsam, dezidiert zu regeln, unter welchen Bedingungen, in welchen Fristen und mit welchen Konsequenzen der Verantwortliche Einspruch gegen einen vorgeschlagenen (weiteren) Auftragsverarbeiter erheben kann, ohne die Fortführung der Verarbeitungen zu gefährden.

## e. Teilweise neue weitere Pflichten des Auftragsverarbeiters

Verantwortliche und Auftragsverabeiter haben eine Reihe von weiteren Verpflichtungen, die sie bei der Verarbeitung personenbezogener Daten erfüllen müssen. Hierzu gehört neben der Implementierung der bereits angesprochenen technischen und organisatorischen Sicherheitsmaßnahmen (Art. 32 DS-GVO), die Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33 DS-GVO). Auch Auftragsverarbeiter müssen ggfs. einen Datenschutzbeauftragten benennen, Art. 37 DS-GVO. Von der in Art. 37 Abs. 4 DS-GVO eingeräumten Möglichkeit, diese Verpflichtung durch mitgliedstaatliche Regelungen zu ergänzen, hat Deutschland mit § 38 BDSG Gebrauch gemacht. Neu ist, dass neben dem Verantwortlichen auch ein Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten führen muss, Art. 30 Abs. 2 DS-GVO.

## f. Bußgelder

Der Verantwortliche hat Sorgfalt walten zu lassen, da er sich andernfalls dem Risiko aussetzt mit einem Bußgeld belegt zu werden. Das trifft z. B. auf die Auswahl eines unzuverlässigen Dienstleisters zu und erst recht, wenn kein Vertrag bzw. keiner den Anforderungen genügender Vertrag geschlossen wird.

# 6. ÜBERMITTLUNG VON BESCHÄFTIGTENDATEN IM KONZERN

Die Verarbeitung von personenbezogenen Beschäftigtendaten zwischen rechtlich selbständigen Gesellschaften eines Konzerns ist häufig Normalität. So kann eine Verarbeitung z. B. im Rahmen einer Matrix-Struktur notwendig sein, wonach ein Vorgesetzter bei einer anderen Konzerngesellschaft tätig ist als seine Mitarbeiter, er aber zur Steuerung des Teams personenbezogene Mitarbeiterdaten benötigt. Beschäftigtendaten müssen z. B. auch dann verarbeitet werden, wenn Aufgaben wie die Personalverwaltung im Sinne von „shared services" konzernweit zentralisiert werden.

## a. „Konzern" im Sinne der Datenschutz-Grundverordnung

Der Begriff „Konzern" wird von der Datenschutz-Grundverordnung nicht aufgegriffen. Die Grundverordnung spricht vielmehr von einer „Unternehmensgruppe". Was darunter zu verstehen ist, wird in Art. 4 Nummer 19 DS-GVO definiert: Danach ist eine „Unternehmensgruppe" eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht.

Aus Erwägungsgrund 37 DS-GVO ergibt sich, dass dieser Begriff weit zu verstehen ist. Es genügt, dass das herrschende Unternehmen z. B. aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann. Ein Unternehmen, das die Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, sollte zusammen mit diesem als eine „Unternehmensgruppe" betrachtet werden.

Es ist davon auszugehen, dass sowohl Unterordnungskonzerne im Sinne von § 18 Abs. 1 Aktiengesetz als auch Gleichordnungskonzerne gemäß § 18 Abs. 2 Aktiengesetz unter diesen Begriff fallen. Nach Erwägungsgrund 37 DS-GVO wird eine Konstellation als „Unternehmensgruppe" behandelt, in der ein zentrales Unternehmen, das die Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, zusammen mit diesen eine Einheit bildet.

## b. Konzerninterne Datenübermittlung bei Funktionsübertragung

Um personenbezogene Daten zwischen rechtlich selbständigen Konzerngesellschaften zu übermitteln, sind verschiedene datenschutzrechtliche Gestaltungsmöglichkeiten vorhanden.

Überträgt ein Unternehmen einem anderen Konzernunternehmen bestimmte Funktionen zur eigenständigen und eigenverantwortlichen Erledigung und verwendet der Datenempfänger zur Erfüllung dieser Zwecke die Daten eigenverantwortlich, kann eine sogenannte „Funktionsübertragung" vorliegen.[162] Wird z. B. die Personalverwaltung für den gesamten Konzern an die Konzernmutter ausgelagert und stehen der Konzernmutter Entscheidungsspielräume zu, handelt es sich um einen Fall der Funktionsübertragung.

**HINWEIS**
Bei einer Funktionsübertragung kann das empfangende Unternehmen die Daten zur eigenständigen und eigenverantwortlichen Erledigung von Aufgaben verwenden. Es handelt sich um eine Datenübermittlung ohne Besonderheiten. Hierfür benötigt man einen gesetzlichen Erlaubnistatbestand.

Nach dem bisherigen deutschen Datenschutzrecht gibt es keine Erleichterung für einen solchen Datenaustausch in Konzernstrukturen. Übermittlungen von personenbezogenen Daten zwischen rechtlich selbständigen Konzerngesellschaften werden genauso behandelt, wie die Übermittlung an einen Dritten.

Auch die Datenschutz-Grundverordnung enthält kein echtes Konzernprivileg. Damit benötigt man zur Übermittlung von Beschäftigtendaten zwischen rechtlich selbständigen Konzerngesellschaften im Rahmen der Funktionsübertragung weiterhin eine Rechtsgrundlage wie Art. 6, Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 1 BDSG.

Art. 6 Abs. 1 lit. f) DS-GVO – Wahrung berechtigter Interessen – kommt als Rechtsgrundlage für die Datenübermittlung besondere Bedeutung zu.

**Erwägungsgrund 48:**
„Verantwortliche, die Teil einer Unternehmensgruppe ... sind, ... können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von ... Beschäftigten, zu übermitteln."

[162] Regierungspräsidium Darmstadt, Arbeitsbericht der Arbeitsgruppe „Konzerninterner Datentransfer", S. 2.

Zu dieser Klarstellung hat sich der europäische Gesetzgeber veranlasst gesehen, weil nach der Ausgestaltung und der Interpretation des Rechtsgrunds der Wahrnehmung berechtigter Interessen in den Gesetzen einiger Mitgliedstaaten die in Erwägungsgrund 48 skizzierte Konstellationen nicht als erfasst angesehen wurden.

Erwägungsgrund 48 stellt daher weder eine Neuerung dar, noch enthält er die Ausgestaltung eines irgendwie gearteten Konzernprivilegs. Er führt lediglich ein Beispiel auf, das sich nach Auffassung des europäischen Gesetzgebers auf den Rechtsgrund der Wahrung berechtigter Interessen – Art. 6 Abs. 1 lit. f) DS-GVO – stützen lassen könnte. Neben diesem Beispiel gibt es aber zahlreiche weitere Konstellationen, in denen sich Verarbeitungen auf der Grundlage dieses Rechtsgrunds in einem Konzern legitimieren lassen. Insofern darf der Erwägungsgrund nicht dahin missverstanden werden, dass sich lediglich diese eine Konstellation durch den Rechtsgrund der Wahrung berechtigter Interessen legitimieren lassen könnte.

## c. Auftragsverarbeitung

Eine weitere Möglichkeit, eine Übermittlung von personenbezogenen Daten innerhalb eines Konzerns datenschutzkonform zu gestalten, ist die Auftragsverarbeitung. Die bislang in § 11 BDSG a. F. geregelte Auftragsdatenverarbeitung wird nunmehr von den Art. 28, 29 DS-GVO behandelt.

**HINWEIS**
Bei der Auftragsverarbeitung verbleibt die volle Verantwortung beim Verantwortlichen. Der Auftragsverarbeiter handelt nach Anweisung des Verantwortlichen.

Für weitere Ausführungen zur Auftragsverarbeitung siehe Seite 126.

## d. Gemeinsame Verantwortlichkeit

In Konzernen ist die gemeinsame Datenverarbeitung z. B. bei der Übernahme von Aufgaben durch die Konzernmutter sehr relevant. Art. 26 DS-GVO, der Regelungen für gemeinsam Verantwortliche festlegt, wird deshalb in der Praxis eine wichtige

Rolle spielen. Bereits nach Art. 2 lit. d) der Datenschutzrichtlinie 95/46/EG können mehrere Verantwortliche eine Datenverarbeitung durchführen. Im bisherigen deutschen Recht gibt es keine vergleichbare Regelung.

In Art. 26 DS-GVO wird klargestellt, welche Pflichten bestehen, wenn mehrere Verantwortliche Zwecke und Mittel zur Verarbeitung festlegen und als gemeinsam Verantwortliche anzusehen sind. Nach Art. 26 Abs. 1 DS-GVO muss in einer Vereinbarung das Innenverhältnis der gemeinsam Verantwortlichen festgelegt werden, so z. B. im Hinblick auf Verpflichtungen wie Betroffenenrechte. Art. 26 Abs. 2 DS-GVO geht auf Offenlegungspflichten im Außenverhältnis ein. In Art. 26 Abs. 3 DS-GVO wird geregelt, dass die Betroffenen ihre Rechte grundsätzlich gegenüber jedem einzelnen Verantwortlichen geltend machen können.

Abzugrenzen ist von den „gemeinsam für die Verarbeitung Verantwortlichen" insbesondere die Auftragsverarbeitung. Der Schwerpunkt der Abgrenzung liegt dabei auf der Frage, ob mehr als eine Partei über die Zwecke und Mittel der Verarbeitung entscheidet.[163]

Als Rechtsgrundlage für eine Datenverarbeitung scheidet Art. 26 DS-GVO aus. Als Grundlagen für eine rechtmäßige Datenverarbeitung kommen im Beschäftigungsverhältnis Art. 6, Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 1, 2, 4 BDSG in Betracht.

Siehe hierzu auch „Gemeinsam für die Verarbeitung Verantwortliche" Seite 32.

## e. Konzerndatenschutzbeauftragter

Art. 37 Abs. 2 DS-GVO sieht nunmehr die Möglichkeit für Unternehmensgruppen vor, einen gemeinsamen Datenschutzbeauftragten zu benennen. Eine Verpflichtung hierzu besteht nicht. Voraussetzung der Benennung eines gemeinsamen Datenschutzbeauftragten ist, dass er von jeder Niederlassung aus leicht erreicht werden kann. Die leichte Erreichbarkeit bezieht sich sowohl auf die von der Verarbeitung betroffene Person als auch auf die Aufsichtsbehörden. Sie ist aber auch im Hinblick auf die Unternehmensgruppe insgesamt zu wahren, da es gemäß Art. 39 Abs. 1 lit. a) DS-GVO u.a. zu den Aufgaben des Datenschutzbeauftragten gehört, den Verantwortlichen und die Beschäftigten zu unterrichten und zu bera-

[163] Vgl. zur Abgrenzung Artikel-29-Datenschutzgruppe, WP 169.

ten.[164] Hierzu muss neben der persönlichen oder durch sichere Kommunikationsmittel gewährleisteten Erreichbarkeit auch sichergestellt werden, dass eventuelle Sprachbarrieren überwunden werden.

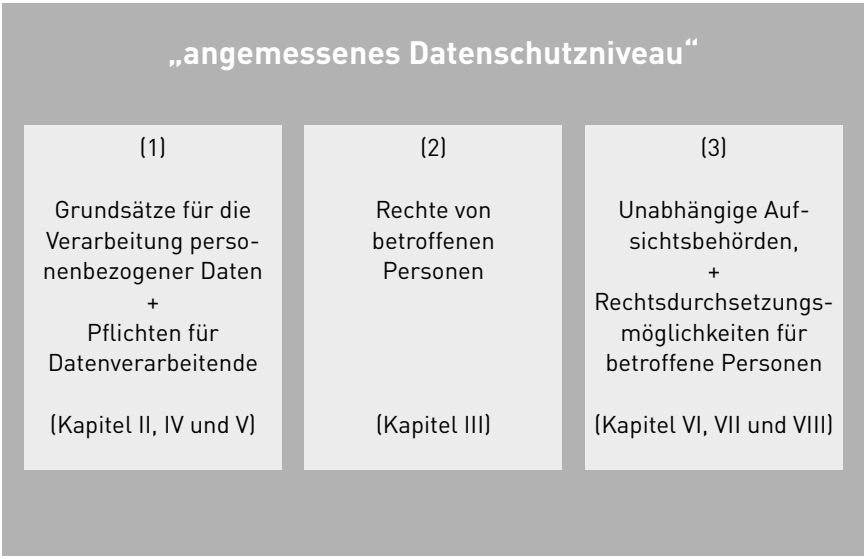
Siehe hierzu auch „Der betriebliche Datenschutzbeauftragte“ Seite 142.

## 7. ÜBERMITTLUNG VON BESCHÄFTIGTENDATEN IN DRITTLÄNDER

Die Übermittlung von Beschäftigtendaten an Empfänger in Drittländern richtet sich nach den Vorschriften von Kapitel V der DS-GVO. Diese haben im Vergleich zu den Regeln der EU-Datenschutzrichtlinie 95/46/EG an Umfang und Detailierungsgrad deutlich zugelegt, inhaltlich sind sie jedoch fast unverändert übernommen worden. In der betrieblichen Praxis können Übermittlungen in Drittländer wie bisher durchgeführt werden. Mit genehmigten Verhaltensregeln gemäß Art. 40 DS-GVO und genehmigten Zertifizierungsmechanismen gemäß Artikel 42 sind weitere Möglichkeiten eröffnet worden, „geeignete Garantien“ für die Durchführung von Drittlandübermittlungen zur Verfügung stellen zu können.

In den Mitgliedstaaten der EU wird durch die DS-GVO ein angemessenes Datenschutzniveau gewährleistet. Es setzt sich im Wesentlichen aus drei Komponenten zusammen: (1) Den Grundsätzen für die Verarbeitung von personenbezogenen Daten und die Pflichten von denjenigen, die Verarbeitungen durchführen, (2) den Rechten der betroffenen Personen und (3) die Existenz von unabhängigen Aufsichtsbehörden sowie die Möglichkeiten deren Entscheidungen und die Rechte betroffener Personen, inklusive der Zahlung von Schadensersatz, durchsetzen.

[164] Vgl. hierzu näher Artikel-29-Datenschutzgruppe, WP 243.




Dieses durch die DS-GVO unionsweit gewährleistete angemessene Datenschutzniveau soll bei der Übermittlung personenbezogener Daten in Drittländer nicht untergraben werden, so Erwägungsgrund 101 DS-GVO. Deshalb dürfen personenbezogene Daten nur dann an Empfänger außerhalb der EU übermittelt werden, wenn das Schutzniveau in dem Land des Empfängers mit dem der EU vergleichbar ist. Anderenfalls muss der Verantwortliche, sofern nicht ein gesetzlicher Ausnahmetatbestand gemäß Art. 49 DS-GVO eingreift, „geeignete Garantien“ hinsichtlich des Schutzes der Privatsphäre, der Grundrechte der betroffenen Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte zur Verfügung stellen, Art. 46 Abs. 1 DS-GVO. Nach Erwägungsgrund 108 DS-GVO sollen sie den in einem Drittland bestehenden Mangel an Datenschutz ausgleichen.

**Praxis-Check für Drittlandübermittlungen**

„Geeignete Garantien“ müssen **nicht** zur Verfügung gestellt werden,

- wenn entweder das Land, in das Sie personenbezogene Daten übermitteln wollen über ein „adäquates Datenschutzniveau“ verfügt oder
- wenn ein gesetzlicher Ausnahmetatbestand zur Anwendung kommt!

## a. Länder mit einem adäquaten Datenschutzniveau – Art. 46 DS-GVO

Ob ein Land über ein der EU vergleichbares angemessenes Datenschutzniveau verfügt, stellt die Europäische Kommission gemäß den Regeln von Art. 45 DS-GVO in einer sog. „Adäquanz-Entscheidung" fest. Neben der Schweiz, Israel und Argentinien verfügen bisher nur wenige Staaten über ein festgestelltes angemessenes Datenschutzniveau. Die Liste der Länder, die über ein angemessenes Datenschutzniveau verfügen, ist auf der Website der Europäischen Kommission abrufbar. [165]

Anzuführen ist an dieser Stelle auch das sog. „Privacy Shield". Das gleichnamige Abkommen[166] zwischen der Europäischen Union und den USA hat das von dem EuGH[167] für rechtswidrig erklärte „Safe Harbor" Abkommen abgelöst. Datenimporteure in den USA können sich bei dem für das „Privacy Shield" verantwortlichen Department of Commerce registrieren und sich verpflichten die europäischen Datenschutzprinzipien einzuhalten. An dort gelistete Empfänger können europäische Datenexporteure personenbezogene Daten in die USA übermitteln.[168]

Die unter der Geltung der Datenschutzrichtlinie 95/46/EG erlassenen Adäquanz-Entscheidungen heißen in der Terminologie der DS-GVO „Angemessenheitsbeschlüsse". Sie gelten solange fort bis die Europäische Kommission sie ändert, ersetzt oder aufhebt, Art. 45 Abs. 9 DS-GVO.

---

165 http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

166 Entscheidung vom 12.07.2016, 2016/1250/EU.

167 EuGH, 06.10.2015, C-362/14.

168 Detaillierte Informationen: https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/EU-US_PrivacyShield_Daten%C3%BCbermittlungenUSA.html))

## b. Übermittlungen auf der Grundlage von „geeigneten Garantien" – Art. 46 DS-GVO

Bei der Übermittlung personenbezogener Daten von Beschäftigten muss man jedoch in der Regel auf andere Rechtsinstrumente zurückgreifen. Von den nachfolgend aufgelisteten Garantien sind (bisher) nur wenige von praktischer Relevanz:

**Art. 46 Abs. 2 DS-GVO:**
(2) Die in Absatz 1 genannten geeigneten Garantien können, ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in
(a) einem rechtlich bindenden und durchsetzbaren Dokument zwischen den Behörden oder öffentlichen Stellen,
(b) verbindlichen internen Datenschutzvorschriften gemäß Art. 47,
(c) Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Art. 93 Abs. 2 erlassen werden,
(d) von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Abs. 2 genehmigt wurden,
(e) genehmigten Verhaltensregeln gemäß Artikel 40 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, oder
(f) einem genehmigten Zertifizierungsmechanismus gemäß Art. 42 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.

- Sehr gut bewährt haben sich die sog. Standardvertragsklauseln der Europäischen Kommission, sei es für Übermittlungen an Auftragsverarbeiter[169] oder Verantwortliche[170] in Drittstaaten – Art. 46 Abs. 2 lit c) DS-GVO. Die DS-GVO erlaubt nationalen Aufsichtsbehörden eigene Standardvertragsklauseln zur Verfügung zu stellen.

[169] Entscheidung vom 05.02.2010, 2010/87/EU.
[170] Entscheidung vom 27.12.2004, 2004/915/EG.

- Verbindliche interne Datenschutzvorschriften, besser unter ihrer englischen Bezeichnung „Binding Corporate Rules" (BCR)[171] bekannt, sind explizit in den Katalog der „geeigneten Garantien" aufgenommen worden – Art. 46 Abs. 2 lit. b) DS-GVO. Ihre Voraussetzungen sowie das Genehmigungsverfahren sind detailliert in Art. 47 DS-GVO aufgeführt. Bisher waren BCR nur internationalen Konzernen vorbehalten. Doch durch die DS-GVO ist der potentielle Nutzerkreis auf Unternehmen, die (nur) eine gemeinsame Wirtschaftstätigkeit ausüben, ausgeweitet worden, Art. 4 Abs. 20 DS-GVO. Bisher galt die Entwicklung von BCR und deren Genehmigungsverfahren als sehr zeitintensiv und damit teuer. Dies dürfte sich künftig ändern, so dass davon ausgegangen werden kann, dass sich die Anwendung von BCR rasch ausweiten wird. Zu beachten ist, dass BCR aber nur geeignete Garantien für Übermittlungen innerhalb des fest definierten Unternehmenskreises sind und, dass es stets einer legitimierten Grundlage für die Übermittlung bedarf.[172]

Neu in den Kreis der geeigneten Garantien sind „genehmigte Verhaltensregeln" aufgenommen worden. Die als Code of Conduct im englischsprachigen Raum bereits bekannten Regeln werden wie die ebenfalls neu aufgenommen „genehmigten Zertifikate" künftig sicher gerne von großen „Datenimporteuren", wie Cloud computing-Anbietern, für die Absicherung von Drittlandverarbeitungen zur Anwendung kommen.

## c. Gesetzliche Ausnahmetatbestände – Art. 49 DS-GVO

Falls weder ein Angemessenheitsbeschluss noch geeignete Garantien bestehen bzw. zur Verfügung gestellt werden können, ist eine Übermittlung nur unter einer der folgenden in Art. 49 Abs. 1 DS-GVO aufgeführten Bedingungen ausnahmsweise zulässig:

> (1) die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde,

[171] Eingehend BITKOM: Verarbeitung personenbezogener Daten in Drittländern (Version 1.2), S. 26, verfügbar unter: https://www.bitkom.org/noindex/Publikationen/2017/Leitfaden/LF-Verarbeitung-personenbezogener-Daten-DE-online-final.pdf.

[172] Dies stellt Satz 2 des Erwägungsgrunds 48 DS-GVO klar.

(2) die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich,
(3) die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich,
(4) die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig,
(5) die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich,
(6) die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,
(7) die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind,
(8) die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat.

In der betrieblichen Praxis spielen insbesondere die Ausnahmetatbestände der Einwilligung (1) und der Erfüllung eines (Arbeits-)Auftrags die größte Rolle.

# 8. DER BETRIEBLICHE DATENSCHUTZBEAUFTRAGTE

Mit Artikel 37 ff. der Datenschutz-Grundverordnung greift die Pflicht zur Ernennung eines betrieblichen Datenschutzbeauftragten erstmals europaweit. Terminologie und Inhalt der Datenschutz-Grundverordnung weicht dabei im Wesentlichen in folgenden Punkten vom Bundesdatenschutzgesetz ab:

- In der Datenschutz-Grundverordnung heißt es Benennung statt Bestellung.
- Die Verpflichtung zur Benennung eines Datenschutzbeauftragten nach der Datenschutz-Grundverordnung besteht dann, wenn die Kerntätigkeit des Unternehmens in systematischer Überwachung oder Verarbeitung besonderer personenbezogener Daten besteht.[173]
- Nach der Datenschutz-Grundverordnung besteht auch die Möglichkeit der Einsetzung eines Konzern-Datenschutzbeauftragten.
- Nach der Datenschutz-Grundverordnung müssen die Kontaktdaten des Datenschutzbeauftragten veröffentlicht und der Aufsichtsbehörde mitgeteilt werden.

Die Öffnungsklausel des Art. 37 Abs. 4 DS-GVO ermöglicht es den Mitgliedstaaten, die Benennungspflicht des Datenschutz-Beauftragten zu konkretisieren. Von diesem Recht hat der deutsche Gesetzgeber mit dem neuen § 38 BDSG Gebrauch gemacht. Der Absatz 1 des § 38 BDSG entspricht weitgehend dem bisherigen § 4f Abs. 1 Satz 4 und 6 BDSG a.F.

## a. Benennungspflicht

Unverändert besteht nach § 38 BDSG die Pflicht zur Benennung eines betrieblichen Datenschutzbeauftragten ab zehn Personen, die ständig mit der automatisierten Datenverarbeitung beschäftigt sind. Der betriebliche Datenschutzbeauftragte unterliegt weiterhin dem besonderen Kündigungsschutz, der Verschwiegenheitspflicht und hat ein Zeugnisverweigerungsrecht. Dies ergibt sich aus den Verweisen in § 38 Abs. 2 BDSG auf § 6 Abs. 4, Abs. 5 Satz 2 und Abs. 6 BDSG.

[173] Nähere Erläuterungen dazu, wann diese Voraussetzungen vorliegen liefert die Artikel-29-Datenschutzgruppe: Guidelines on Data Protection Officers (‚DPO's), adopted on 13 December 2016 as last Revised and Adopted on 5 April 2017, S. 8 ff., http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

Neu ist, dass unabhängig von der Anzahl der mit der Datenverarbeitung beschäftigten Personen auch solche Verantwortliche einen Datenschutzbeauftragten benennen müssen, wenn sie oder der Auftragsverarbeiter Verarbeitungen vornehmen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegen. Die Benennungspflicht besteht auch wenn der Verantwortliche personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet.

Nach Art. 37 Abs. 1 lit. b), c) DS-GVO besteht die Benennungspflicht auch dann, wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO besteht.

Zu den Kerntätigkeiten eines Unternehmens zählen dabei nur solche, die dem wesentlichen Betriebszweck entsprechen. Dieser muss in der spezifischen Datenverarbeitung oder sonstigen benannten Verarbeitungsvorgängen liegen.[174] Entscheidend ist der Hauptgeschäftszweck eines Unternehmens, der sich auf die erhöhten Schutzanforderungen auswirkt.[175] Nach Erwägungsgrund 97 DS-GVO soll es sich nicht um eine Kerntätigkeit des Verantwortlichen handeln, wenn dieser personenbezogene Daten nur als Nebentätigkeit verarbeitet. Beispiele für solche Nebentätigkeiten sind Mitarbeiterverwaltung, Rechnungswesen, Bereitstellung technischer Infrastruktur[176], es sei denn, diese Bereiche stellen gerade den Hauptzweck der Tätigkeit dar, wie z. B. bei Personaldienstleistern, Steuerberatern oder IT-Dienstleistern.[177]

---

174 *Niklas/Faas,* NZA 2017, S. 1091 f.; *Klug*, ZD 2016, S. 315, S. 316; *Dammann*, ZD 2016, S. 307 f.; a. A. *Marschall/Müller*, ZD 2016, S. 414, S. 417, die davon ausgehen, dass auf sämtliche mit der Haupttätigkeit eines Unternehmens verbundenen Aufgaben abzustellen ist.

175 *Jaspers/Reif*, RDV 2016, S. 61 f.; *Franzen*, EuZA 2017, S. 313, 338; *Reinhard,* ArbRB 2017, S. 317, 319.

176 *Franzen*, EuZA 2017, S. 313, 338; Piltz, K&R 2016, S. 709, 717.

177 *Franzen*, EuZA 2017, S. 313, 338.

**PRAXISTIPP**
Aufgrund der Ausweitung der Benennungspflicht sollten auch Unternehmen mit weniger als zehn Mitarbeitern prüfen, ob sie zukünftig verpflichtet sind, einen Datenschutz-Beauftragten zu benennen. Zudem sollte ggf. dokumentiert werden, warum ein Datenschutzbeauftragter nicht bestellt wird und regelmäßig überprüft werden, ob die Voraussetzungen für die Benennung eines Datenschutzbeauftragten entstehen.[178]

Nicht konkretisiert wurde, was unter dem Begriff „Benennung" der Datenschutz-Grundverordnung zu verstehen ist, denn die DS-GVO schreibt keine bestimmte Form für die Benennung vor. Vom Begriffssinn her ist eine Benennung weniger formal als eine Bestellung.

## b. Verantwortliche bei der Einhaltung des Datenschutzes

Liegen die Voraussetzungen für die Benennung eines betrieblichen Datenschutzbeauftragten vor, bleibt es originäre Aufgabe des Verantwortlichen oder Auftragsverarbeiters, die datenschutzrechtlichen Bestimmungen einzuhalten. Beispielsweise nach Auffassung des Bayerischen Landesdatenschutz-Beauftragten[179] sind Datenschutz-Beauftragte im Fall der Nichteinhaltung der Datenschutz-Grundverordnung nicht persönlich verantwortlich. Aus der Datenschutz-Grundverordnung gehe klar hervor, dass es Aufgabe des Verantwortlichen oder des Auftragsverarbeiters ist, sicherzustellen und nachweisen zu können, dass die Verarbeitung gemäß der Verordnung erfolgt. Für die Einhaltung der datenschutzrechtlichen Bestimmungen seien der Verantwortliche oder der Auftragsverarbeiter verantwortlich. Neue Haftungsrisiken bzw. den Bedarf einer Versicherung gegen neue Risiken sieht der Bayerische Landesdatenschutz-Beauftragte daher bei angestellten Datenschutzbeauftragten nicht. Es werden nach der Ansicht des Bayerischen Landesdatenschutzbeauftragten weiterhin für den Datenschutzbeauftragten im Beschäftigungsverhältnis die von der Rechtsprechung aufgestellten Grundsätze der Arbeitnehmer-Haftung gelten. Auch die Artikel-29-Datenschutzgruppe geht

[178] Artikel-29-Datenschutzgruppe: Guidelines on Data Protection Officers (‚DPO's), adopted on 13 December 2016 as last Revised and Adopted on 5 April 2017, S. 5 und 17, http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

[179] https://www.lda.bayern.de/de/datenschutz_eu.html.

davon aus, dass der Datenschutzbeauftragte nicht persönlich verantwortlich für die Einhaltung bzw. Nichteinhaltung der Vorschriften der DS-GVO ist[180], dies soll allein der für die Datenverarbeitung Verantwortliche sein.

**Die Aufgaben des Datenschutz-Beauftragten in Kürze (Art. 39 Abs. 1 DS-GVO):**

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Datenschutz-Pflichten;
- Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO und Überwachung ihrer Durchführung;
- Zusammenarbeit mit der Aufsichtsbehörde;
- Anlaufstelle für die Aufsichtsbehörde;
- Hinzu kommen noch aus Artikel 38 Abs. 4 DS-GVO die Beratung der betroffenen Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß den mit der DS-GVO in Zusammenhang stehenden Fragen.

**HINWEIS**

Die Artikel-29-Datenschutzgruppe hat zur näheren Erläuterung der Artikel 37 bis 39 DS-GVO ein Arbeitspapier erstellt, das unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 abgerufen werden kann.

[180] Guidelines on Data Protection Officers (‚DPO's), adopted on 13 December 2016 as last Revised and Adopted on 5 April 2017, S. 5, http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

## c. Stellung des Datenschutz-Beauftragten – Art. 38 DS-GVO

Sichergestellt werden muss, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle Datenschutzfragen eingebunden wird. Der Datenschutzbeauftragte muss bei Erfüllung seiner Aufgaben mit den erforderlichen Ressourcen, einem Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie zur Erhaltung seines Fachwissens unterstützt werden.

Der Verantwortliche muss die Weisungsfreiheit des Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben sicherstellen. Der Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Er berichtet unmittelbar der höchsten Managementebene des Verantwortlichen. Bei der Erfüllung seiner Aufgaben ist der Datenschutzbeauftragte zur Verschwiegenheit verpflichtet. Der Verantwortliche muss sicherstellen, dass bei einem nebenamtlichen Datenschutzbeauftragten keine Interessenkonflikte auftreten.

## d. Rechtsfolgen bei Verstoß

Verletzungen der Vorschriften zum Datenschutz-Beauftragten aus Artikel 37 bis 39 DS-GVO (die Nichtbenennung eines Datenschutzbeauftragten, unzureichende Unterstützung oder Benachteiligung des Datenschutzbeauftragten usw.) sind nach Artikel 83 Abs. 4a DS-GVO mit Geldbuße bedroht und zwar von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist. Die ordnungsgemäße Beteiligung des Datenschutzbeauftragten sollte daher umfassend dokumentiert werden.

## e. Anforderungen an die Benennung

### aa. Qualifikationen und persönliche Voraussetzungen; Benennung des Datenschutzbeauftragten – Art. 37 DGSVO

Der Datenschutzbeauftragte kann Beschäftigter oder Externer[181] (mit Dienstleistungsvertrag) sein. Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen und der Aufsichtsbehörde mitzuteilen. Zu den Kontaktdaten gehört nicht der Name des Datenschutzbeauftragten (siehe unten unter bb.)

[181] Davon geht auch die Artikel-29-Datenschutzgruppe aus: Guidelines on Data Protection Officers (‚DPO's), adopted on 13 December 2016 as last Revised and Adopted on 5 April 2017, S. 12, http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

Die Benennung erfolgt auf der Grundlage der beruflichen Qualifikation, insbesondere des Fachwissens auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis und der Fähigkeit zur Erfüllung der in Art. 39 DS-GVO genannten Aufgaben. Dies regelt Art. 37 Abs. 5 DS-GVO. Dies entspricht inhaltlich weitgehend dem bisherigen § 4f Abs. 2 Satz 1 BDSG a. F., so dass es bei der Erforderlichkeit rechtlicher, technischer und organisatorischer Kenntnisse bleibt.[182] Erwägungsgrund 97 betont, dass der Grad der Qualifikation des Datenschutzbeauftragten dem Grad der Komplexität der Datenverarbeitungsvorgänge entsprechen muss, eine Voraussetzung, die bisher ebenfalls in § 4f Abs. 2 Satz 1 BDSG a. F. geregelt war.

Wie das BDSG verbietet Art. 36 Abs. 6 Satz 2 der DS-GVO Interessenkonflikte. Hinzu kommt das Erfordernis der persönlichen Integrität, die in der DS-GVO nicht ausdrücklich geregelt wird, sich aber aus der Aufgabenstellung des Datenschutzbeauftragten, Ansprechpartner des Unternehmens und der betroffenen Person, zu sein, ergibt.

**PRAXISTIPP**

Die Datenschutz-Grundverordnung liefert den Anreiz für freiwillige Bestellungen als Datenschutzbeauftragte, dass dieser gemäß Art. 57 Abs. 3 DS-GVO Anspruch auf unentgeltliche Beratung durch die Aufsichtsbehörden hat. Dieser Anspruch steht dem für die Verarbeitung Verantwortlichen nicht zu. Argument für eine Bestellung auch ohne Pflicht kann sein, dass Datenschutzbeauftragte einen zentralen Beitrag zur Gewährleistung von Datenschutzkonformität und damit zur Vermeidung von Unternehmensrisiken darstellen. Für eine freiwillige Bestellung wird auch von der Artikel-29-Datenschutzgruppe geworben.[183] Gemäß § 38 Abs. 2 BDSG genießt der auf freiwilliger Basis eingesetzte Datenschutzbeauftragte keinen besonderen Kündigungsschutz nach § 6 Abs. 4 BDSG.

[182] Zu den Fachkundeanforderungen vgl. Beschluss des Düsseldorfer Kreises vom 24./25. November 2010: Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 BDSG, abrufbar unter: https://www.lda.bayern.de/media/dk_mindestanforderungen_dsb.pdf

[183] Guidelines on Data Protection Officers (‚DPO's), adopted on 13 December 2016 as last Revised and Adopted on 5 April 2017, S. 4, http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

**bb. Form und Dauer der Benennung**

Die Form der Bestellung wird durch die DS-GVO nicht geregelt.

**PRAXISTIPP**
Aufgrund der möglichen Rechtsfolgen einer Benennung empfiehlt es sich aber aus Gründen der Rechtssicherheit immer, eine schriftliche Benennung vorzunehmen. Zumindest die Textform sollte eingehalten werden.

Im Hinblick auf die Dauer der Benennung enthält die DS-GVO keine Vorgaben. Beliebig kurze Befristungen sind allerdings nicht möglich, weil die Unabhängigkeit des Datenschutzbeauftragten (Erwägungsgrund 97) gewährleistet werden muss. Wenn die Fristen so kurz sind, dass sie den Datenschutzbeauftragten hindern, seine Aufgaben wahrzunehmen und gegenüber der Unternehmensleitung und den Fachabteilungen zu vertreten, ist von einer Unwirksamkeit der Befristung auszugehen. Wirksam dürfte eine mindestens zwei Jahre dauernde befristete Benennung sein[184], eine Befristung auf die sechsmonatige Probezeit bei Einstellung dagegen nicht.[185]

Die „Kontaktdaten" des Datenschutzbeauftragten sind gemäß Art. 37 Abs. 7 DS-GVO zu veröffentlichen und der Aufsichtsbehörde mitzuteilen. Da Art. 37 Abs. 7 DS-GVO ausdrücklich nur die „Kontaktdaten" nennt, im Gegensatz zu Art. 13 Abs. 1 lit. a) DS-GVO, wo von „Name und Kontaktdaten" die Rede ist, setzt die Angabe dieser Kontaktdaten, beispielsweise auf der Homepage, nicht voraus, dass der Name des Datenschutzbeauftragten genannt wird. Im Verhältnis zur Aufsichtsbehörde kann die namentliche Nennung des Datenschutzbeauftragten trotzdem sinnvoll sein. (vgl. Art. 30 Abs. 1 lit. a) i. V. m. Abs. 4 DS-GVO).

184 *Reinhard*, NZA 2013, S. 1049.

185 ArbG Dortmund, 20.02.2013, 10 Ca 4800/12, RDV 2013, S. 319.

**HINWEIS**
Die Artikel-29-Datenschutzgruppe empfiehlt die Veröffentlichung einer Postanschrift des Datenschutzbeauftragten nebst Telefonnummer oder E-Mail-Anschrift und gegenüber der Aufsichtsbehörde sowie den Beschäftigten des Unternehmens auch die Mitteilung des Namens des Datenschutzbeauftragten, letzteres beispielsweise im Unternehmens-Intranet.[186]

### cc. Möglichkeit der externen Benennung

Wie bisher gemäß § 4f Abs. 2 BDSG a. F. kann auch nach Art. 37 Abs. 6 DS-GVO ein externer Datenschutzbeauftragter bestellt werden. Für die Entscheidung, ob es für das Unternehmen sinnvoller ist, einen internen oder externen Datenschutzbeauftragten zu bestellen, sollte berücksichtigt werden, ob dem Datenschutzbeauftragten weitere Aufgaben übertragen werden sollen. Aufgrund hoher Bußgelder bei Datenschutzverstößen und der Vergleichbarkeit eines Datenschutz-Management-Systems mit bestehenden Compliance-Management-Systemen kann es sinnvoll sein, Compliance-Funktionen im Unternehmen mit Datenschutzfunktionen zu verknüpfen. Dann muss aber sichergestellt werden, dass der Datenschutz gegenüber sonstigen Compliance-Aufgaben keine untergeordnete Rolle einnimmt, damit keine Interessenskonflikte entstehen.[187]

### dd. Möglichkeit der Benennung eines Konzern-Datenschutzbeauftragten

Art. 37 Abs. 2 DS-GVO sieht die Möglichkeit der Benennung eines gemeinsamen Datenschutzbeauftragten in Unternehmensgruppen vor. Die Möglichkeit der Berufung eines solchen Beauftragten ist mit der Bedingung verbunden, dass dieser von jeder Niederlassung aus leicht erreicht werden kann. Damit besteht die Möglichkeit der Benennung nur eines Konzerndatenschutzbeauftragten nun auch in Deutschland, weil das BDSG keine eigene Regelung trifft.[188] Zum Erfordernis der leichten Erreichbarkeit gehört auch, dass keine Sprachbarrieren bestehen.[189]

---

186 Guidelines on Data Protection Officers (‚DPO's), adopted on 13 December 2016 as last Revised and Adopted on 5 April 2017, S. 13, http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

187 Vgl. *Wybitul/von Gierke*, BB 2017, S. 181, 183

188 *Niklas/Faas*, NZA 2017, S. 1091, 1093.

189 *Franzen*, EuZA 2017, S. 313, 339; *Jaspers/Reif*, RDV 2016, S. 61, 63; Klug, ZD 2016, S. 315, 317.

Die Definition der Unternehmensgruppe ergibt sich aus Art. 4 Nr. 19 DS-GVO: Die Unternehmensgruppe besteht danach aus einem herrschenden und den von diesem abhängigen Unternehmen. Eine einheitliche Leitung wie nach § 18 AktG ist nach dieser Definition nicht erforderlich.[190]

Bereits bisher wurde die Möglichkeit gesehen, Mehrfachbestellungen im Konzern durch die Bestellung eines externen Datenschutzbeauftragten zu vermeiden.[191] Nach der Rechtsprechung des Bundesarbeitsgerichts führt die Absicht der konzernweiten Betreuung des Datenschutzes durch einen externen Beauftragten nicht zu einem wichtigen Grund gemäß § 4f Abs. 3 Satz 4 BDSG a. F. zur Abberufung des bisherigen Datenschutzbeauftragten.[192]

Obwohl das Bundesdatenschutzgesetz hinsichtlich der Benennung auf die verantwortliche Stelle abstellt, muss es bei der gemeinsamen Bestellung für mehrere Verantwortliche genügen, wenn die Leitung der jeweiligen Organisation die Benennung vornimmt.[193] Die DS-GVO gibt nicht vor, welches Organ den gemeinsamen Datenschutzbeauftragten benennen muss.

## f. Stellung des Datenschutzbeauftragten

### aa. Unabhängigkeit

Der Datenschutzbeauftragte muss unabhängig sein. Diese Unabhängigkeit wird als übergeordnete Gewährleistung in Erwägungsgrund 97 der DS-GVO erwähnt. Art. 38 Abs. 3 DS-GVO regelt die unmittelbaren Ausprägungen der Unabhängigkeit, nämlich die Unabhängigkeit von fachlichen Weisungen und die Verpflichtung zur Gewährleistung eines unmittelbaren Berichtswegs des Datenschutzbeauftragten zur höchsten Managementebene. Das ist das Organ, welches das Unternehmen nach außen vertritt, bei einer Aktiengesellschaft also der Vorstand und bei einer Gesellschaft mit beschränkter Haftung der Geschäftsführer.[194] Sinnvoll ist es, den Datenschutzbeauftragten auch organisatorisch unmittelbar der Lei-

190 *Franzen*, EuZA 2017, S. 313, 339.

191 Forgó/Helfrich/Schneider/*Haag*, Betrieblicher Datenschutz, 2014, S. 28.

192 BAG, 23.03.2011, 10 AZR 562/09, NZA 2011, S. 1036.

193 *Franzen*, EuZA 2017, S. 313, 339 und im Ergebnis auch *Jaspers/Reif*, RDV 2016, S. 61, 63; a. A. *Lepperhoff/Müthlein*, Leitfaden zur Datenschutz-Grundverordnung 2017, S. 83.

194 *Franzen*, EuZA 2017, 313, 341.

tung des für die Verarbeitung Verantwortlichen zu unterstellen, damit durch die damit verbundene Sonderstellung diesem bei denjenigen, die personenbezogene Daten verarbeiten, die notwendige Autorität verschafft wird.

**bb. Abberufungsschutz und Benachteiligungsverbot**

Art. 38 Abs. 3 Satz 2 DS-GVO gewährleistet den Abberufungsschutz des Datenschutzbeauftragten sowie ein Benachteiligungsverbot. Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Möglich ist jedoch nach der DS-GVO ein betriebsbedingter Wegfall der Bestellung. Außerdem sieht die DS-GVO keinen arbeitsrechtlichen Schutz der Datenschutzbeauftragten vor.

Dies ändert nichts am Sonderkündigungsschutz für Datenschutzbeauftragte in Deutschland, da der nationale Gesetzgeber die Befugnis zur Regelung des materiellen Arbeitsrechts hat und die Regelungen zum Sonderkündigungsschutz aus § 4f Abs. 3 BDSG a. F. inhaltlich unverändert in § 6 Abs. 4 i. V. m. § 38 Abs. 2 BDSG übernommen wurden. Danach ist die Kündigung des Arbeitsverhältnisses eines Beauftragten für den Datenschutz unzulässig, soweit nicht Tatsachen vorliegen, welche die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach der Abberufung als Beauftragter für den Datenschutz ist die Kündigung innerhalb eines Jahres nach der Beendigung einer Benennung unzulässig, es sei denn, dass die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist. Die Benennung zum Beauftragten für den Datenschutz kann in entsprechender Anwendung von § 626 BGB widerrufen werden.

Im Einzelnen gilt nach der Rechtsprechung des BAG für die Abberufung des Datenschutzgebeauftragten Folgendes[195]:

1. Nach § 4f Abs. 3 Satz 4 a. F. BDSG kann die Bestellung zum Beauftragten für den Datenschutz in entsprechender Anwendung von § 626 BGB, bei nicht-öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden.

[195] BAG, 23.03.2011, 10 AZR 562/09, NZA 2011, S. 1036.

2. Als wichtige Gründe kommen insbesondere solche in Betracht, die mit der Funktion und Tätigkeit des Datenschutzbeauftragten zusammenhängen und eine weitere Ausübung dieser Tätigkeit unmöglich machen oder sie zumindest erheblich gefährden. Beispielsweise ein Geheimnisverrat, eine dauerhafte Verletzung der Kontrollpflichten als Datenschutzbeauftragter oder die wirksame Beendigung des zugrunde liegenden Arbeitsverhältnisses kann ein wichtiger Grund für den Widerruf der Bestellung eines internen Beauftragten für den Datenschutz sein.

3. Eine organisatorische Änderung, nach der der betriebliche Datenschutz zukünftig durch einen externen statt durch einen internen Datenschutzbeauftragten gewährleistet werden soll, rechtfertigt den Widerruf der Bestellung aus wichtigem Grund nicht. Die Zulassung einer jederzeitigen Widerrufsmöglichkeit aufgrund einer organisatorischen Änderung und die generelle Anerkennung einer freien Strukturentscheidung als wichtiger Grund würden dazu führen, den besonderen Abberufungsschutz, der insbesondere der Sicherung der unabhängigen Stellung des Datenschutzbeauftragten dient, zur Disposition der nicht-öffentlichen Stelle zu stellen.

4. Für die Darlegung, dass eine entsprechende Umorganisation aus sonstigen Gründen zwingend geboten war, reichen allein Kostenersparnisgründe und die Schaffung einer „einheitlichen Organisation" im Konzern nicht aus.

5. Ein wichtiger Grund für einen Widerruf der Bestellung folgt nicht aus der Mitgliedschaft im Betriebsrat. Eine generelle Unvereinbarkeit ist nicht anzunehmen. Ein Widerruf der Bestellung kommt erst bei einer unzureichenden Aufgabenwahrnehmung in Betracht.

6. Wird die Bestellung nach § 4f Abs. 3 Satz 4 a. F. BDSG wirksam widerrufen, ist die Tätigkeit des Beauftragten für den Datenschutz nicht mehr Bestandteil der vertraglich geschuldeten Leistung. Es bedarf dann keiner Teilkündigung mehr.[196]

[196] Vgl. BAG, 29.09. 2010, 10 AZR 588/09, NZA 2011, S. 151.

### cc. Unterstützung, Einbindung und Fortbildung

Wie schon bisher das BDSG sieht die DS-GVO zur Unterstützung, Einbindung und Fortbildung des Datenschutzbeauftragten in Artikel 38 Abs. 1 und 2 Folgendes vor:

- die ordnungsgemäße und frühzeitige Einbindung hinsichtlich aller mit dem Schutz personenbezogener Daten zusammenhängender Fragen;
- die Unterstützung des Datenschutzbeauftragten bei seiner Aufgabenerfüllung;
- die nötigen Hilfsmittel zur Wahrnehmung seiner Aufgaben und Erhaltung des Fachwissens;
- den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen.

Zur Wahrnehmung seiner Aufgaben müssen dem Datenschutzbeauftragten die notwendigen zeitlichen Kapazitäten zur Verfügung gestellt werden. Welchen Umfang dies konkret bedeutet, muss im Einzelfall bestimmt werden. Folgende Kriterien können dazu dienen, die ausreichende finanzielle und materielle Ausstattung sowie das notwendige Zeitbudget für die Wahrnehmung der gesetzlichen Aufgaben zu bemessen[197]:

- Unternehmensgröße und Anzahl der Mitarbeiter, sowie Anzahl der Standorte und Betriebsstätten
- die Organisation des Unternehmens, national und international
- die Einbindung in eine Konzernstruktur
- Matrix-Organisation
- die Komplexität der Geschäftsprozesse
- Außendienst- und Vertriebsorganisation
- Einsatz von Home-Office und Telearbeit
- bestehende Delegationsmöglichkeiten auf Rechtsabteilung, Revisionsabteilung, IT-Sicherbeauftragten und externe Berater.
- Outsourcing-Möglichkeiten
- Branchenzugehörigkeit
- Art und Anzahl der zu verwaltenden personenbezogenen Daten von Mitarbeitern, Kunden, Lieferanten, Kontaktpersonen, Dritten usw.
- Art und Sensibilität der zu verarbeitenden personenbezogenen Daten bzw. der verwendeten Verfahren.

[197] Vgl. GDD-Praxishilfe DS-GVO I, November 2016, S. 8, abrufbar unter: http://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo.

### dd. Geheimhaltungspflicht und Vertraulichkeit

Art. 38 Abs. 4 DS-GVO entspricht im Wesentlichen dem bisherigen § 4f Satz 2 BDSG a. F., wonach sich Betroffene jeder Zeit an den Beauftragten für Datenschutz wenden können. Der Datenschutzbeauftragte ist verpflichtet, Datenschutzanliegen und -beschwerden zu prüfen und die betroffenen Personen über das Ergebnis seiner Prüfung zu informieren. Ergibt seine Prüfung eine Verletzung der datenschutzrechtlichen Vorschriften, muss er darauf hinwirken, dass diese beendet werden.

Geheimhaltungs- und Vertraulichkeitsverpflichtungen sind in der DS-GVO nicht ausdrücklich vorgesehen. Sie verweist auf das Unionsrecht bzw. das Recht der Mitgliedstaaten. In Deutschland wird dies geregelt durch § 6 Abs. 5 Satz 2 und Abs. 6 BDSG, der über § 38 Abs. 2 BDSG Anwendung findet, sowie § 203 Abs. 2a StGB. § 203 Abs. 2a StGB regelt die Strafbarkeit der Verletzung von Privatgeheimnissen unter ausdrücklicher Einbeziehung des Beauftragten für den Datenschutz. Gemäß § 6 Abs. 5 Satz 2 BDSG ist der Datenschutzbeauftragte zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

Gemäß § 6 Abs. 6 BDSG i. V. m. § 38 Abs. 2 BDSG steht dem Datenschutzbeauftragten ein Zeugnisverweigerungsrecht zu, wenn er bei seiner Tätigkeit Kenntnis von Daten erhält, für die der Leitung oder einer beim Verantwortlichen beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht zusteht, es sei denn, dass diese Entscheidung nicht in absehbarer Zeit herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht des Datenschutzbeauftragten reicht, unterliegen seine Akten und andere Dokumente einem Beschlagnahmeverbot.

## g. Aufgaben

### aa. Unterrichtung und Beratung

Gemäß Art. 39 Abs. 1lit. a) DS-GVO berät der Datenschutzbeauftragte den Verantwortlichen bzw. Auftragsverarbeiter und die mit der Datenverarbeitung Beschäftigten hinsichtlich ihrer Pflichten nach der DS-GVO sowie nach den sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten. Die Unterrichtung

umfasst allgemeine Informationen über die bestehenden datenschutzrechtlichen Pflichten, Beratung und Unterstützung bei der Lösung konkreter datenschutzrechtlicher Fragestellungen.

Anders als nach § 4g Abs. 1 Nr. 2 BDSG a. F. sieht die DS-GVO keine Pflicht zur Schulung der Mitarbeiter durch den Datenschutzbeauftragten vor. Eine zielgerichtete pädagogische Aufbereitung der für die konkret ausgeübte Tätigkeit relevanten datenschutzrechtlichen Informationen ist hiernach Aufgabe des für die Verarbeitung Verantwortlichen.

**bb. Überwachung der Einhaltung des Datenschutzes**

Hauptaufgabe des Datenschutzbeauftragten neben der Unterrichtung und Beratung ist die Überwachung der Einhaltung des Datenschutzes nach Art. 39 Abs. 1 lit. b) DS-GVO. Zu überwachen ist die Einhaltung der Datenschutz-Grundverordnung und anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder Auftragsverarbeiters für den Schutz personenbezogener Daten. Zu diesen Strategien gehören die Zuweisung von Zuständigkeiten, die Schulung der an Verarbeitungsvorgängen beteiligten Mitarbeiter und deren Überprüfung. Durch die Datenschutz-Grundverordnung kommen die Aufgaben der Kontrolle der Einhaltung der Datenschutz-Strategien des Verantwortlichen bzw. Auftragsverarbeiters zu den bisherigen Pflichten ausdrücklich hinzu. Die Verpflichtung zur Überwachung der Datenschutzkonformität des Unternehmenshandelns war auch bisher schon Bestandteil der Hinwirkungspflicht des Datenschutzbeauftragten nach BDSG. Operative Aufgaben wie die Mitarbeiterschulung, die Vorabkontrolle und die Bereitstellung des Verfahrensverzeichnisses für jedermann sieht die DS-GVO nicht vor.

**cc. Datenschutz-Folgenabschätzung**

Die Durchführung der Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ist nicht Aufgabe des Datenschutzbeauftragten.[198] Zuständig hierfür ist der für die Verarbeitung Verantwortliche und damit in abgeleiteter Verantwortung die jeweilige Fachabteilung. Die Aufgaben des Datenschutzbeauftragten bei der Datenschutz-Folgenabschätzung nach der DS-GVO liegen in der Überwachung, ob diese durchge-

[198] Vgl. Artikel-29-Datenschutzgruppe: Guidelines on Data Protection Officers ('DPO's), adopted on 13 December 2016 as last Revised and Adopted on 5 April 2017, S. 17, http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

führt wird und in der Verpflichtung, auf Anfrage zu deren Durchführung zu beraten (Art. 39 Abs. 1 lit c) DS-GVO). Gemäß Art. 35 Abs. 2 DS-GVO besteht die Verpflichtung der Fachabteilungen den Rat des Datenschutzbeauftragten einzuholen.

**dd. Zusammenarbeit mit der Aufsichtsbehörde**

Die DS-GVO sieht vor, dass der Datenschutzbeauftragte mit der Aufsichtsbehörde zusammenarbeitet. Er ist deren „Anlaufstelle" beim für die Verarbeitung Verantwortlichen. Er berät sich gemäß Art. 39 Abs. 1 lit. d) und e) DS-GVO zu allen sonstigen Fragen mit der Behörde. Anlass zur Konsultation der Behörde kann insbesondere sein, dass sich der Datenschutzbeauftragte über die Auslegung der gesetzlichen Regelungen und die Angemessenheit einzelner Datenschutzmaßnahmen im Unklaren ist.

**ee. Pflicht zur risikoorientierten Tätigkeit**

Gemäß Art. 39 Abs. 2 DS-GVO muss der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben dem Risiko gebührend Rechnung tragen, das mit den Verarbeitungsvorgängen verbunden ist. Hierbei muss er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigen. Zur Gewährleistung der Unabhängigkeit des Datenschutzbeauftragten muss die Bewertung, welche Verarbeitungsvorgänge aufgrund des mit ihm verbundenen Risikos einer vorrangigen Bewertung bedürfen, dem Datenschutzbeauftragten selbst obliegen. An den Datenschutzbeauftragten gerichtete Prüfaufträge dürfen diesen nicht daran hindern, die aus seiner Sicht vordringlichen datenschutzrechtlichen Angelegenheiten zu bearbeiten.

# 9. DIE ROLLE DES BETRIEBSRATS BEI DER DATENVERARBEITUNG

## a. Die datenschutzrechtliche Verantwortung des Betriebsrats

Nach der DS-GVO ist der sog. „Verantwortliche" zur Einhaltung der gesetzlichen Normen bei der Erhebung von Mitarbeiterdaten verpflichtet. „Verantwortlich" ist gem. Art. 4 Abs. 7 DS-GVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die bisherige Begriffsbestimmung in § 3 Abs. 7 BDSG a. F. spricht insoweit von der „verantwortlichen Stelle". Im Arbeitsverhältnis ist dies stets der Arbeitgeber.

Art. 24 DS-GVO fordert im Rahmen eines risikobasierten Ansatzes, dass die „Verantwortlichen" sicherstellen und nachweisen können, dass die Verarbeitung personenbezogener Daten gemäß den Vorgaben der DS-GVO erfolgt.

Eine häufig gestellte Frage in diesem Zusammenhang ist, inwieweit der Betriebsrat eigenverantwortlich für die Einhaltung datenschutzrechtlicher Bestimmungen herangezogen werden kann. Trotz seiner betriebsverfassungsrechtlichen Unabhängigkeit wurde der Betriebsrat von der Rechtsprechung des BAG bisher nicht als „Dritter" gem. § 3 Abs. 4 Nr. 3 BDSG a. F. außerhalb der verantwortlichen Stelle angesehen, sondern ist Teil derselben. Der Personaldatenfluss zwischen Personalabteilung und Betriebsrat ist folgerichtig nicht als Datenübermittlung, sondern als interne Datennutzung zu werten. Vor diesem Hintergrund ist der Betriebsrat selbst Teil der verantwortlichen Stelle. Dies entbindet ihn jedoch nicht aus der Verantwortung, die betrieblichen und gesetzlichen Datenschutzbestimmungen einzuhalten.[199] Vielmehr unterliegt er dem Datengeheimnis und hat eigenständig über Maßnahmen zu beschließen, um den datenschutzrechtlichen Anforderungen Rechnung zu tragen. Daneben hat er für etwaige Datensicherungsmaßnahmen Sorge zu tragen.[200] Konsequenz dieser Rechtsprechung ist, dass dem Arbeitgeber die Datenverarbeitungen des Betriebsrats und damit einhergehendes etwaiges Fehlverhalten zugerechnet werden, obwohl dieser den Betriebsrat nicht kontrollieren kann. So scheidet derzeit wohl auch eine Kontrolle durch den betrieblichen Datenschutzbeauftragten aus. Nach einer nicht unumstrittenen Entscheidung des BAG hat der betriebliche Datenschutzbeauftragte keine Kontrollkompetenz gegenüber dem Betriebsrat.[201] Ansonsten wäre die vom BetrVG vorgeschriebene Unabhängigkeit des Betriebsrates nicht mehr gewährleistet. Inwieweit das BAG an seiner Rechtsprechung festhält, wurde zuletzt offen gelassen.[202] Hiervon unberührt bleibt die Möglichkeit, dass die jeweilige Datenschutzaufsichtsbehörde den rechtmäßigen Datenumgang durch den Betriebsrat überprüft.

Es erscheint äußerst fraglich, ob die höherrangigen Regelungen der DS-GVO eine derartige Interpretation – ausgelöst durch den Schutzgedanken des BetrVG – weiterhin zulassen. Aufgrund der gestiegenen Informations-, Auskunfts-, Löschungs- und Widerspruchsrechte nach der DS-GVO, ist es nicht mehr sachgerecht, wenn Arbeitnehmer ihre Betroffenenrechte nicht direkt gegenüber dem

199 BAG, 07.02.2012, 1 ABR 46/10; BAG, 14.01.2014, 1 ABR 54/12.

200 BAG, 18.07.2012, 7 ABR 23/11.

201 BAG, 11.11.1997, 1 ABR 21/97.

202 BAG, 23.03.2011, 10 AZR 562/09.

Betriebsrat geltend machen können, sondern nur gegenüber dem Arbeitgeber, der wiederum keine eigenen Kontrollmöglichkeiten hat. Eine interne Befriedung datenschutzrechtlicher „Problemfälle" wird somit erheblich erschwert.

**HINWEIS**
Der Betriebsrat hat sich auch zukünftig vor dem Umgang mit Personaldaten zu fragen, ob die gewünschten Verarbeitungszwecke durch die Zulässigkeitstatbestände der DS-GVO, des BDSG und des BetrVG gedeckt sind.[203] Vor dem Hintergrund, dass insbesondere die Betroffenenrechte der vertretenen Arbeitnehmer in der DS-GVO umfassender als bisher geregelt sind (vgl. Kapitel 5.), müssen Betriebsräte künftig näher erläutern, weshalb eine Weitergabe anonymisierter Daten für die verfolgten Zwecke nicht ausreicht. Der Betriebsrat kann jedenfalls die Vorgaben der DS-GVO nicht mit Verweis auf seinen betriebsverfassungsrechtlichen Sonderstatus umgehen.

**PRAXISTIPP**
Die Einhaltung datenschutzrechtlicher Bestimmungen durch den Betriebsrat könnte wie folgt sichergestellt werden:
- Der Betriebsrat unterzieht sich freiwillig der Kontrolle des betrieblichen Datenschutzbeauftragten.
- Es werden entsprechende Regelungen, insbesondere zur Weitergabe von Daten und Datensicherung, im Rahmen einer freiwilligen Betriebsvereinbarung festgehalten.
- Der Betriebsrat installiert umfassende Schutzmechanismen in seiner Geschäftsordnung.
- Der Betriebsrat gibt sich einen eigenen „Datenschutzkoordinator".
- Es findet eine Kontrolle durch die Datenschutzaufsichtsbehörden statt.

## b. Beteiligungsrechte der Interessenvertretung – § 26 Abs. 6 BDSG

Die DS-GVO und das BDSG sehen vor, dass Betriebsvereinbarungen weiterhin „spezifischere Vorschriften" für die Verarbeitung personenbezogener Beschäftigtendaten vorsehen können (vgl. Kapitel 3.c.). Damit wird der Betriebsrat auch

[203] Vgl. TB 2013/2014, Bayerisches Landesamt für Datenschutzaufsicht, S. 110.

künftig als datenschutzrechtlicher Akteur mit unmittelbar wirkender Regelungsbefugnis anerkannt. Der Arbeitgeber hat deshalb beim Umgang mit personenbezogenen Arbeitnehmerdaten die umfassenden Mitbestimmungsrechte des Betriebsrats zu beachten. Diese Wertung spiegelt sich in § 26 Abs. 6 BDSG wieder, wonach die Beteiligungsrechte des Betriebsrats von den Regelungen des § 26 BDSG unberührt bleiben. Der Abs. 6 entspricht dabei wort- und inhaltsgleich dem § 32 Abs. 3 BDSG a. F. Somit muss der Arbeitgeber auch weiterhin vor Einführung neuer datenschutzrelevanter Maßnahmen prüfen, inwieweit ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG besteht.

Von besonderer datenschutzrechtlicher Bedeutung sind die Mitbestimmungsrechte bei Personalfragebögen und Beurteilungsgrundsätzen (§ 94 BetrVG), im Rahmen der betrieblichen Ordnung (§ 87 Abs. 1 Nr. 1 BetrVG) und bei der Verhaltens- oder Leistungskontrolle mittels technischer Einrichtungen (§ 87 Abs. 1 Nr. 6 BetrVG). Zur Bestimmung, wann Mitbestimmungsrechte eingreifen, kann auf die umfangreiche – wenngleich oftmals nicht stringente – Rechtsprechung zurückgegriffen werden.

Von besonderer Relevanz ist die Beteiligung des Betriebsrats im Rahmen von Mitarbeiterkontrollen, die mithilfe technischer Einrichtungen durchgeführt werden. Aufgrund der ausufernden Auslegungspraxis des BAG wird der Anwendungsbereich des § 87 Abs. 1 Nr. 6 BetrVG immer weiter gefasst. So reicht es nach der Rechtsprechung aus, wenn die technische Einrichtung zur Arbeitnehmerüberwachung lediglich objektiv geeignet ist. Auf die konkrete Verwendungsabsicht des Arbeitgebers kommt es nicht an.[204] In der Folge sind Datenverarbeitungsmaßnahmen mitbestimmungspflichtig, die nur theoretisch Rückschlüsse auf Verhalten oder Leistung eines bestimmten Arbeitnehmers ermöglichen.

**BEISPIEL**

Ein Arbeitgeber möchte bestimmte Schulungen (z. B. Compliance, Arbeitssicherheit, Datenschutz) mithilfe von E-Learning-Tools durchführen. Im Vordergrund steht dabei einzig und allein die Weiterbildung der Mitarbeiter. Eine Auswertung oder ein Abgleich der Lernerfolge erfolgt nicht. Erfasst das E-Learning-Tool (bspw. in Form reiner Software-Tools) die Log-in-Daten der Arbeitnehmer, kann festgehalten werden, wer wann welche Schulung benutzt hat. Unabhängig davon, dass die technische Einrichtung die Überwachung der Mitarbeiter nicht zum Ziel hat, ist die Maßnahme mitbestimmungspflichtig.[205]

[204] BAG, 10.12.2013, 1 ABR 43/12.

[205] Hopfner/Erdmann/*Hohenadl,* Praxishandbuch Arbeitsrecht, S. 238.

Die Überwachung bzw. ein Teil des Überwachungsvorgangs muss mittels der technischen Einrichtung erfolgen. Nicht ausreichend ist, wenn die Mitarbeiterkontrolle ausschließlich durch menschliches Handeln ausgelöst wird.[206] Seit der umstrittenen „Facebook-Entscheidung" ist es jedoch nicht erforderlich, dass die Verhaltens- oder Leistungsdaten von Arbeitnehmern von der technischen Einrichtung selbst – „automatisch" – erhoben werden. Die manuelle Eingabe ist ausreichend, wenn die Daten anschließend gespeichert werden und auf sie zugegriffen werden kann.[207]

Darüber hinaus können Kontrollen am Arbeitsplatz und damit verbundene Datenverarbeitungen Fragen der betrieblichen Ordnung oder des Verhaltens der Mitarbeiter gem. § 87 Abs. 1 Nr. 1 BetrVG betreffen. Mitbestimmungspflichtig ist dabei nicht das arbeitsvertraglich individuell geschuldete „Arbeitsverhalten", sondern nur das kollektive „Ordnungsverhalten".[208] So ist die Entscheidung des Arbeitgebers, „ob" die private Nutzung betrieblicher Telekommunikationsmittel zugelassen werden soll, eine Weisung des Arbeitgebers, die sich auf die Erfüllung der arbeitsvertraglichen Pflichten bezieht und daher mitbestimmungsfrei. Etwas anderes gilt jedoch, wenn der Arbeitgeber das „Wie" der erlaubten Privatnutzung regeln will, z. B. zeitliche oder inhaltliche Nutzungsbeschränkungen. In der Praxis erweist sich eine klare Zuordnung zwischen Ordnungs- und Arbeitsverhalten oftmals schwierig.

**PRAXISTIPP**

In diesen Fällen sollten weniger ausufernde systematische Überlegungen angestellt, als vielmehr vergleichbare Einzelentscheidungen in die Bewertung miteinbezogen werden. Kann nicht abschließend geklärt werden, ob ein Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 BetrVG besteht, sollte aufgrund der Unwirksamkeitsfolgen eine Betriebsvereinbarung abgeschlossen werden. Dabei darf nicht der Mindestschutzstandard der DS-GVO und des BDSG unterschritten, wohl aber konkretisiert werden. Soll eine betriebseinheitliche Lösung erreicht werden und besteht kein Mitbestimmungsrecht des Betriebsrats, bietet sich der Abschluss einer freiwilligen Betriebsvereinbarung gem. § 88 BetrVG an. Daneben bilden Betriebsvereinbarungen einen pragmatischen Lösungsansatz, um unklare gesetzliche Vorgaben zu konkretisieren.

206 BAG, 10.12.2013, 1 ABR 43/12.

207 BAG, 13.12.2016, 1 ABR 7/15; *Prinz*, SAE 2017, 91.

208 BAG, 07.02.2012, 1 ABR 63/10.

## c. Datenverarbeitung durch den Betriebsrat

Eine der wesentlichen Aufgaben des Betriebsrats ist, dass die zugunsten des Arbeitnehmers geltenden Gesetze eingehalten werden. Hierzu zählt auch die Durchführung der Bestimmungen der DS-GVO. Damit der Betriebsrat seine Aufgaben und Beteiligungsrechte wahrnehmen kann, ist er auf einen entsprechenden Informationsfluss seitens des Arbeitgebers angewiesen. Vor diesem Hintergrund stellt das BetrVG zahlreiche Auskunftsansprüche (z. B. §§ 80 Abs. 2, 87 Abs. 1, 99 Abs.1, 102 Abs. 1 BetrVG) zur Verfügung.

Dabei muss der Arbeitgeber dem Betriebsrat eine Fülle von personenbezogenen Arbeitnehmerdaten überlassen. Dies ist bisher ohne Probleme möglich. Soweit das BetrVG eine konkrete Regelung bezüglich der personenbezogenen Datenweitergabe vorsieht, stellen die Vorschriften des BetrVG gem. § 1 Abs. 2 einen dem BDSG vorrangigen Erlaubnistatbestand dar. Mit Anwendung der DS-GVO gehen aber die Vorschriften der EU-Verordnung den nationalen Regelungen vor. Fraglich ist deshalb, ob das BetrVG – im Gleichlauf zu § 26 BDSG (vgl. Kapitel 3. b. aa.) – als „spezifischere Vorschrift" i. S. d. Art. 88 Abs. 1 DS-GVO angesehen werden kann und insoweit eine entsprechende Öffnungsklausel bildet. Dagegen spricht, dass die Durchsetzung kollektiver Beteiligungsrechte der Arbeitnehmer im Betrieb eine durchaus andere Zielrichtung verfolgt als § 26 BDSG.[209] Andererseits ist Art. 88 DS-GVO sehr weit gefasst und enthält keinen Anhaltspunkt, dass nur neu konzipierte gesetzliche Regelungen unter den Anwendungsbereich der „spezifischeren Vorschriften" fallen sollen. Die parallele Geltung von Datenschutz und Betriebsverfassungsrecht wird künftig auch durch § 26 Abs. 6 BDSG zum Ausdruck gebracht. In jedem Fall ist neben der Einwilligung als wirksamer Erlaubnistatbestand (vgl. Kapitel 3. d.) die Datenübermittlung an den Betriebsrat zur Erfüllung rechtlicher Verpflichtungen, denen der Arbeitgeber unterliegt, gem. Art. 6 Abs. 1 lit. c) DS-GVO zulässig. In Bezug auf den Beschäftigtendatenschutz handelt es sich hierbei um die Erfüllung betriebsverfassungsrechtlicher Informationspflichten, die eine Datenweitergabe an den Betriebsrat rechtfertigt. Daneben stellt § 26 Abs. 1 Satz 1 BDSG klar, dass personenbezogene Beschäftigtendaten erhoben werden dürfen, wenn dies zur Ausübung gesetzlicher Rechte und Pflichten des Betriebsrats erforderlich ist. Es ist deshalb davon auszugehen, dass die arbeitsgerichtliche Rechtsprechung auch weiterhin ein betriebsverfassungsrechtlich legitimiertes Auskunftsverlangen datenschutzrechtlich für unbedenklich halten wird.

---

**209** *Wybitul*, ZD 2016, S. 203.

**BEISPIELE**

- Einblick des Betriebsrats in die Brutto- und Gehaltslisten[210]
- Mitteilung der Namen der für die Durchführung eines betrieblichen Eingliederungsmanagements in Betracht kommenden Arbeitnehmer[211]
- Vorlage von Zielvereinbarungen und damit einhergehenden Informationen[212]

In der Praxis stellen sich Mitarbeitervertretungen häufig die Frage, wie lange die Speicherung der Beschäftigtendaten ohne Einwilligung der Betroffenen zulässig ist. Aufgrund der geänderten Anforderungen, die die DS-GVO mit sich bringt, wird diese Thematik wohl noch stärker in den Fokus der Datenschutzaufsichtsbehörden rücken. Zwar wird auch künftig den Mitarbeitervertretungen nicht verwehrt werden können, die erlangten Informationen für eine gewisse Zeit aufzubewahren. Allerdings ist in besonderer Weise darauf zu achten, dass die Datenverarbeitung nur solange erfolgt, wie sie zur Aufgabenerfüllung des Betriebsrats erforderlich ist.

**HINWEIS**

Der Betriebsrat handelt nur insoweit datenschutzkonform, als er die Speicherung der Personaldaten auf die Dauer der jeweiligen Betriebsratsaufgabe beschränkt. Eine dauerhafte Speicherung kommt ausnahmsweise nur dann in Betracht, sofern einzelne Beschäftigtendaten für die Erfüllung bestimmter Betriebsratsaufgaben auf Dauer zur Verfügung stehen müssen.[213] Eigene Datensammlungen bzw. -banken ohne entsprechendes Löschkonzept sind zu unterlassen. Hierauf sollte auch der Arbeitgeber zwingend hinwirken.

Das Recht auf informationelle Selbstbestimmung des einzelnen Arbeitnehmers kann einer Datenweitergabe an den Betriebsrat entgegenstehen. Nach § 26 Abs. 1 Satz 1 BDSG ist das Interesse des Betriebsrats an einer Datenweitergabe mit dem Persönlichkeitsrecht des Betroffenen zu einem schonenden Ausgleich zu bringen, der beide Interessen weitgehend berücksichtigt. Dabei ist der Rechtsgedanke der jeweiligen arbeitsrechtlichen Schutznorm in die Abwägung miteinzubeziehen.

---

210 LAG Schleswig-Holstein, 09.02.2016, 1 TaBV 43/15.

211 BAG, 07.02.2012, 1 ABR 46/10.

212 Hessisches LAG, 24.11.2015, 16 TaBV 106/15.

213 Vgl. BVerwG, 04.09.1990, 6 P 28.87; Bayerischer Landesdatenschutzbeauftragter, 25. TB, S. 218 f.

**BEISPIEL**
Aus § 83 Abs. 1 BetrVG lässt sich ableiten, dass der Betriebsrat kein allgemeines Einsichts- oder Vorlagerecht einzelner Personalakten besitzt. Im Zusammenhang mit der elektronischen Personalakte darf der Arbeitgeber keinen vollumfänglichen Online-Lesezugriff einräumen. Dem Betriebsrat steht es nicht zu, die Einsicht in die elektronisch geführten Personalakten selbst durchzusetzen.[214] Vor diesem Hintergrund ist es dem Betriebsrat nicht gestattet, aus den ihm zur Verfügung gestellten Unterlagen eine eigene zweite (automatisierte) Personalakte aufzubauen.

Die betriebsverfassungsrechtlichen Verschwiegenheitspflichten gem. §§ 99 Abs. 1 Satz 3, 102 Abs. 5 Satz 2, 82 Abs. 2 Satz 3, 83 Abs. 1 Satz 3 BetrVG beschränken die mögliche Verarbeitung von Mitarbeiterdaten auf die interne Verwendung. Die Datenweitergabe durch den Betriebsrat an Dritte, wie z. B. Gewerkschaften, kann deshalb nur mit Einwilligung des Betroffenen erfolgen. § 26 Abs. 1 Satz 1 BDSG enthält keine entsprechende Übermittlungsbefugnis. Auch die Veröffentlichung von Betriebsinterna im Internet sowie auf der „Betriebsratshomepage" eines Betriebsratsmitglieds ist unzulässig. Der Betriebsrat hat lediglich das Recht, das Internet als Informationsquelle heranzuziehen, nicht mehr und nicht weniger.[215]

[214] LAG Berlin-Brandenburg, 12.11.2012, 17 TaBV 1318/12, NZA-RR 2013, S. 293.

[215] Hessisches LAG, 15.07.2004, 9 TaBV 190/03.

## 10. ANHANG 1 – SYNOPSE BDSG BIS MAI 2018, BDSG AB MAI 2018, DS-GVO

| Kontext | Text BDSG bis Mai 2018 | Text BDSG ab Mai 2018 | Text DS-GVO |
|---|---|---|---|
| Europäische Öffnungsklausel für mitgliedschaftliche Regelungen zum Beschäftigtendatenschutz | | | **Art. 88 DS-GVO**<br>(1) Die Mitgliedstaaten können durch **Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften** zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen.<br>... |

| Kontext | Text BDSG bis Mai 2018 | Text BDSG ab Mai 2018 | Text DS-GVO |
|---|---|---|---|
| Europäische Öffnungsklausel für mitgliedschaftliche Regelungen zum Beschäftigtendatenschutz | | | **Erwägungsgrund 155 Verarbeitung im Beschäftigungskontext**<br>Im Recht der Mitgliedstaaten oder in Kollektivvereinbarungen (einschließlich 'Betriebsvereinbarungen') können spezifische Vorschriften für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorgesehen werden, und zwar insbesondere Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen, über die Verarbeitung dieser Daten für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses. |

| Kontext | Text BDSG bis Mai 2018 | Text BDSG ab Mai 2018 | Text DS-GVO |
|---|---|---|---|
| Beschäftigtenbegriff | **§ 3 – Begriffsbestimmungen**<br>(11) Beschäftigte sind:<br><br>1. Arbeitnehmerinnen und Arbeitnehmer,<br>2. zu ihrer Berufsbildung Beschäftigte,<br>3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),<br>4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,<br>5. nach dem Jugendfreiwilligendienstegesetz Beschäftigte,<br>6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,<br>7. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,<br>8. Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende. | **§ 26 – Datenverarbeitung Beschäftigungsverhältnis**<br>(8) [1]Beschäftigte im Sinne dieses Gesetzes sind:<br><br>1. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,<br>2. zu ihrer Berufsbildung Beschäftigte,<br>3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),<br>4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,<br>5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten,<br>6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,<br>7. Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.<br>[2]Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte. | |

| Kontext | Text BDSG bis Mai 2018 | Text BDSG ab Mai 2018 | Text DS-GVO |
|---|---|---|---|
| Zentrale Erlaubnisnorm Beschäftigungsverhältnis | **§ 32 Datenverarbeitung Beschäftigungsverhältnis**<br>(1) [1]Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.<br>[2]Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. | **§ 26 Datenverarbeitung Beschäftigungsverhältnis**<br>(1) [1]Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.<br>[2]Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. | |
| Anwendbarkeit – keine automatisierte Datenverarbeitung | **§ 32 Datenverarbeitung Beschäftigungsverhältnis**<br>(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden. | **§ 26 Datenverarbeitung Beschäftigungsverhältnis**<br>(7) Die Absätze 1 bis 6 sind auch anzuwenden, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen. | |
| Beteiligungsrechte Interessenvertretung | **§ 32 Datenverarbeitung Beschäftigungsverhältnis**<br>(3) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt. | **§ 26 Datenverarbeitung Beschäftigungsverhältnis**<br>(6) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt. | |

| Kontext | Text BDSG bis Mai 2018 | Text BDSG ab Mai 2018 | Text DS-GVO |
|---|---|---|---|
| Einwilligung | **§ 4a Einwilligung**<br>(1) [1]Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. [2]Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. [3]Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. [4]Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.<br>....<br>(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen. | **§ 26 Datenverarbeitung Beschäftigungsverhältnis**<br>(2) [1]Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. [2]Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. [3]Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. 4Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären. | **Art. 7 Bedingungen Einwilligung**<br>(1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.<br>(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.<br>(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.<br>(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. |

| Kontext | Text BDSG bis Mai 2018 | Text BDSG ab Mai 2018 | Text DS-GVO |
|---|---|---|---|
| Besondere Kategorien von Daten | | **§ 26 Datenverarbeitung Beschäftigungsverhältnis**<br>(3) [1]Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, 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. [2]Absatz 2 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. [3]§ 22 Absatz 2 gilt entsprechend. | **Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten**<br>(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.<br>(2) Absatz 1 gilt nicht in folgenden Fällen:<br>a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,<br>b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,<br>... |

| Kontext | Text BDSG bis Mai 2018 | Text BDSG ab Mai 2018 | Text DS-GVO |
|---|---|---|---|
| Kollektivvereinbarungen | **§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung**<br>(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. | **§ 26 Datenverarbeitung Beschäftigungsverhältnis**<br>(4) [1]Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von Kollektivvereinbarungen zulässig. [2]Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten. | **Art. 88 Beschäftigungsverhältnis**<br>(2) Diese Vorschriften umfassen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz. |
| Allgemeine Verarbeitungsgrundsätze | **§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung**<br>(3) [1]Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über<br>1. die Identität der verantwortlichen Stelle,<br>2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und<br>3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,<br>zu unterrichten. [2]Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. [3]Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären. | **§ 26 Datenverarbeitung Beschäftigungsverhältnis**<br>(5) Der Verantwortliche muss geeignete Maßnahmen ergreifen, um sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden. | **Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten**<br>(1) Personenbezogene Daten müssen<br>a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden **(„Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);**<br>b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken **(„Zweckbindung“);** |

| Kontext | Text BDSG bis Mai 2018 | Text BDSG ab Mai 2018 | Text DS-GVO |
|---|---|---|---|
| Allgemeine Verarbeitungsgrundsätze | **§ 3a Datenvermeidung und Datensparsamkeit**<br>[1]Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. 2Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert. | | c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);<br>d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden **(„Richtigkeit“);**<br>e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);<br>f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);<br>(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“). |

**BDA** | Bundesvereinigung der
Deutschen Arbeitgeberverbände

Mitglied von BUSINESSEUROPE

**Hausadresse:**
Breite Straße 29 | 10178 Berlin

**Briefadresse:**
11054 Berlin

**T** +49 30 2033-1200
**F** +49 30 2033-1205

arbeitsrecht@arbeitgeber.de
www.arbeitgeber.de

Arbeitgeberverband Gesamtmetall

**Hausadresse:**
Voßstraße 16
10117 Berlin

**Briefadresse:**
Postfach 060249
10052 Berlin

**T** +49 30-55150-0

info@gesamtmetall.de
www.gesamtmetall.de

www.arbeitgeber.de

# VERFAHREN FÜR DEN UMGANG MIT ANFRAGEN VON BESCHÄFTIGTEN. ANFRAGE NACH KOPIE PERSONENBEZOGENER DATEN (SCHRITT 1).

## Beschäftigter

Einleitende Anfrage nach personen-bezogenen Daten

Erhalt von Kopien durch Postzustellung/ E-Mail

## Örtliche Personalabteilung

Beschäftigter fragt an, wenn er eine Kopie der über ihn gespeicherten Daten sowie seiner (elektronischen) Personalakte erhalten möchten.

Hinweis an ihn, dass die Bereitstellung der Daten bis zu einem Monat dauern kann.

Beschäftigter wählt den von ihm bevorzugten Weg der Daten-übermittlung.

- Elektronische Übermittlung an Unternehmens-Emailadresse
- Postalische Übermittlung an die im Unter-nehmen hinter-legte Adresse

Dank für die Anfrage. Hinweis, dass Beschäftigter innerhalb eines Monats eine Kopie seiner personenbezogenen Daten erhält.

## System

Abgleich und Prüfung im Hinblick auf evtl. weitere Datensätze auf der Grundlage verschiedener Personal-nummern und/oder Gruppen IDS

## Personalmanagement

Bereitstellung der Daten und Dokumen-tation

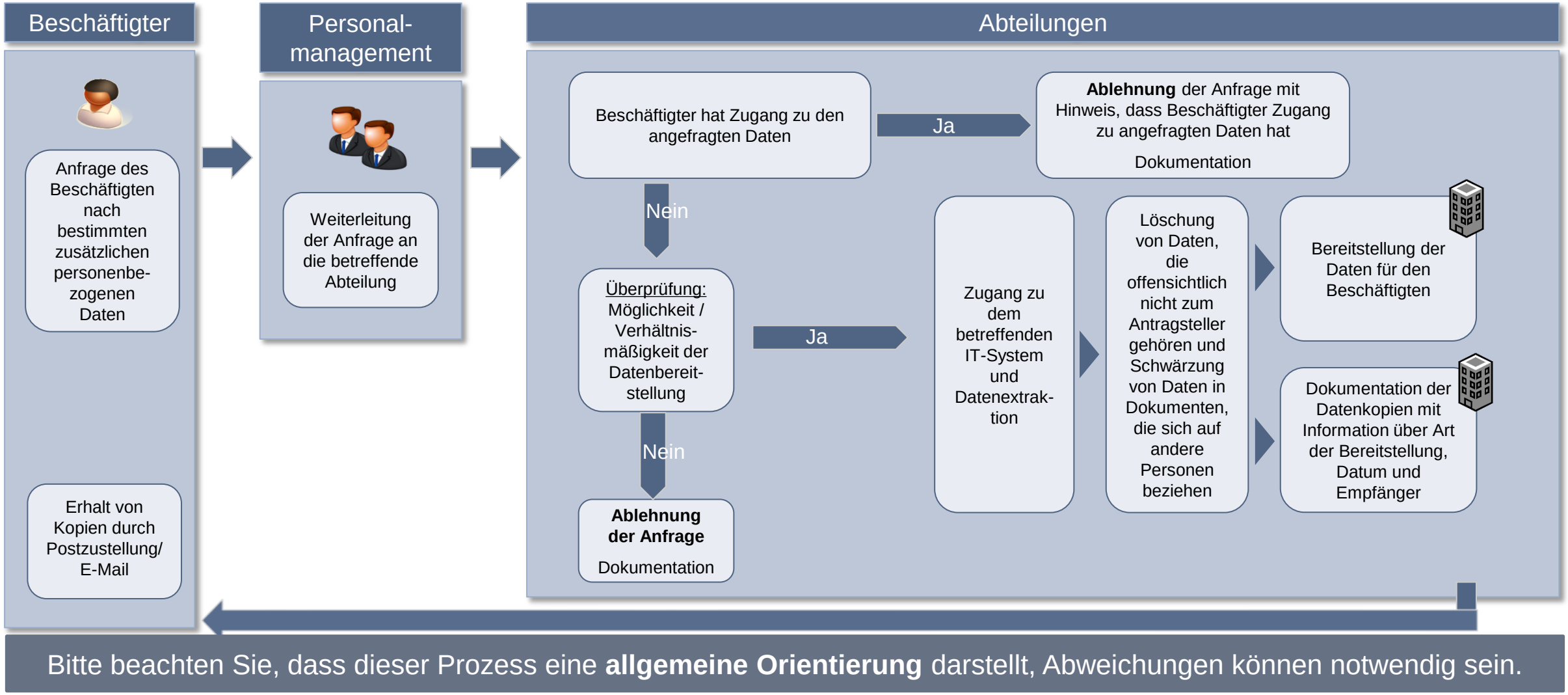
Löschung von Daten, die offensichtlich nicht zum Antragsteller gehören und Schwärzung von Daten in den Dokumenten, die sich auf andere Personen beziehen

Prüfung der Daten

SAP-Bericht und Extraktion der (elektronischen) Personalakte

Bitte beachten Sie, dass dieser Prozess eine **allgemeine Orientierung** darstellt, Abweichungen können notwendig sein.

# VERFAHREN FÜR DEN UMGANG MIT ANFRAGEN VON BESCHÄFTIGTEN. ANFRAGE NACH KOPIE PERSONENBEZOGENER DATEN (SCHRITT 2).




Bitte beachten Sie, dass dieser Prozess eine **allgemeine Orientierung** darstellt, Abweichungen können notwendig sein.

# VERFAHREN FÜR DEN UMGANG MIT ANFRAGEN VON BESCHÄFTIGTEN. ANFRAGE NACH LÖSCHUNG PERSONENBEZOGENER DATEN.

**Beschäftigter**

Anfrage nach Löschung personenbe-zogener Daten (bestimmte Daten oder alle gespeicherten Daten)

**Personaldienstleistung**

Nach Identifikation

Überprüfung,

- ob Daten des Antrag-stellers in HR-Systemen gespeichert sind (z. B. SAP oder andere Systeme)
- ob bestimmte Daten außerhalb üblicher Systeme gespeichert werden; nur, wenn der Antragsteller seine Anfrage konkretisiert
- ob es eine Rechtsgrund-lage für die Speicherung der Daten insgesamt oder teilweise gibt

Rechtsgrundlage für die Speicherung / keine Daten gespeichert

Ja

**Ablehnung** der Löschung mit Hinweis, dass es eine rechtliche Notwendigkeit gibt, die Daten vorzuhalten oder keine Daten vorhanden sind

Dokumentation

Nein

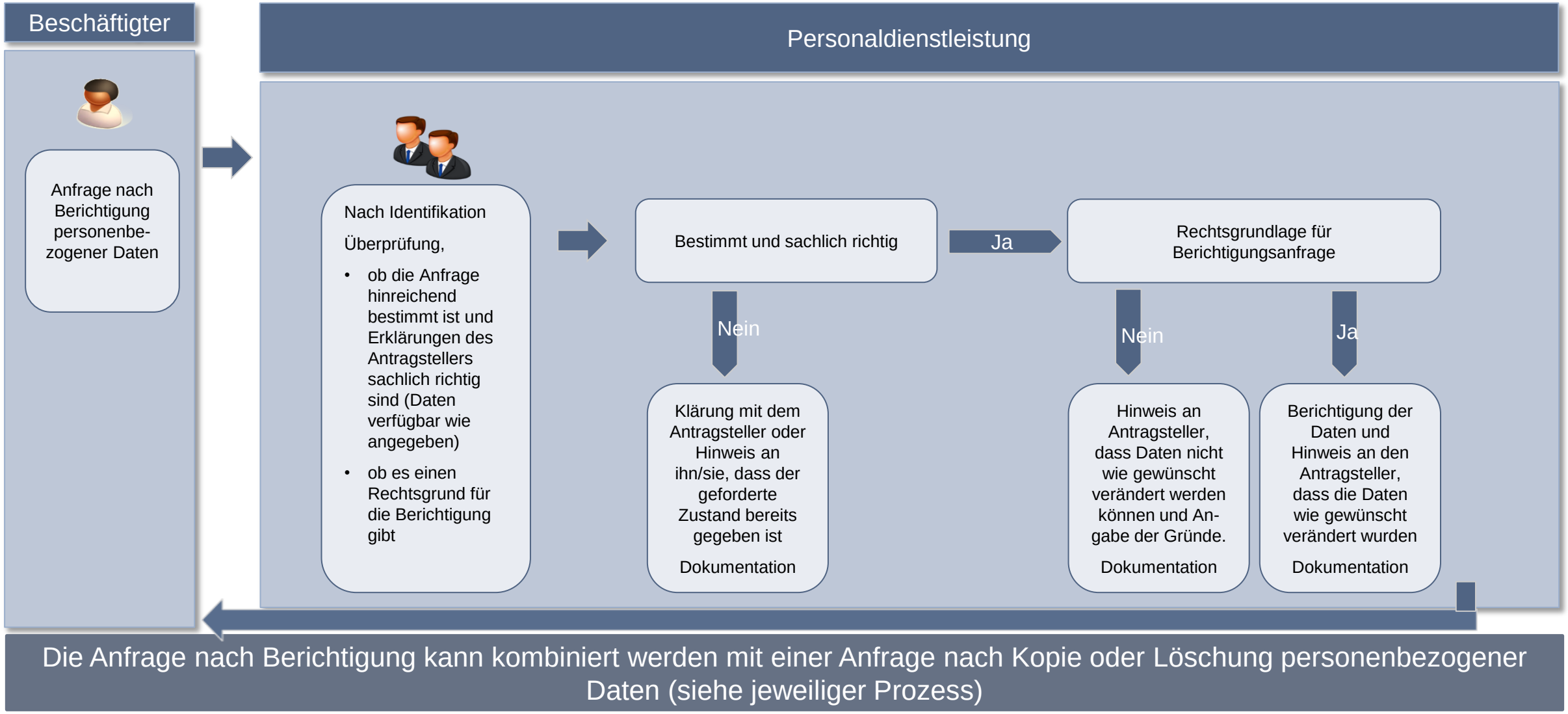
Löschung der betroffenen Daten

Hinweis an den Anfragenden, welche Daten gelöscht wurden und dass es eine rechtliche Grundlage für diejenigen Daten gibt, die weiter vorgehalten werden

Dokumentation

Die Anfrage nach Löschung kann kombiniert werden mit einer Anfrage nach einer Kopie oder einer Berichtigung personenbezogener Daten (siehe jeweiliger Prozess)

# VERFAHREN FÜR DEN UMGANG MIT ANFRAGEN VON BESCHÄFTIGTEN. ANFRAGE NACH BERICHTIGUNG PERSONENBEZOGENER DATEN.




Die Anfrage nach Berichtigung kann kombiniert werden mit einer Anfrage nach Kopie oder Löschung personenbezogener Daten (siehe jeweiliger Prozess)