

## **Referentenentwurf**

### **des Bundesministeriums für Arbeit und Soziales und des Bundesministeriums des Innern und für Heimat**

#### **Entwurf eines Gesetzes zur Stärkung eines fairen Umgangs mit Beschäftigtendaten und für mehr Rechtssicherheit für Arbeitgeber und Beschäftigte in der digitalen Arbeitswelt**

(Beschäftigtendatengesetz – BeschDG)

#### **A. Problem und Ziel**

Die fortschreitende Digitalisierung verändert die Arbeitswelt tiefgreifend. Datenbasierte bzw. -getriebene Geschäftsmodelle gewinnen zunehmend an Bedeutung und haben das Potenzial, ein bedeutsamer Wirtschafts- und damit auch Beschäftigungsfaktor zu werden. Künftig wird es immer mehr Arbeitsplätze geben, die von Künstlicher Intelligenz (KI) betroffen sind. Eine innovative Datennutzung kann Beschäftigte in ihrer täglichen Arbeit unterstützen und sie von Routinetätigkeiten entlasten, Unternehmen können ihre Arbeitsorganisation effizienter gestalten und neue Geschäftsfelder erschließen.

Gleichzeitig führt die Digitalisierung auch zu neuen Herausforderungen im Verhältnis zwischen Beschäftigten und Arbeitgebern. Große Datenmengen und neue Mittel zur Verknüpfung von Daten untereinander ermöglichen eine weitreichende Kontrolle und Überwachung. Ebenso kann eine umfassende Bewertung der Persönlichkeit gerade für Beschäftigte einschneidende Folgen haben. Dies kann bei Beschäftigten zu Verunsicherung und Zurückhaltung gegenüber technologischen Entwicklungen führen. Das gilt insbesondere vor dem Hintergrund, dass die Datenverarbeitung im Beschäftigungsverhältnis durch ein Über-/ Unterordnungsverhältnis zwischen Arbeitgebern und abhängig Beschäftigten geprägt ist.

Die Bundesregierung setzt sich zum Ziel, eine innovative und verantwortungsvolle Datennutzung zu fördern. Für den sensiblen Beschäftigungskontext bedeutet dies, dass ein guter Rechtsrahmen innovative Datennutzung mit einem starken Datenschutz für Beschäftigte verbindet. Dazu gehört, dass Arbeitgeber, Beschäftigte sowie Betriebs- und Personalräte wissen, was erlaubt ist und was nicht.

Mit dem vorliegenden Gesetzentwurf wird die seit Jahrzehnten diskutierte Schaffung eigenständiger Regelungen für den Beschäftigtendatenschutz verwirklicht. Dieser ist derzeit überwiegend lediglich abstrakt in der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) und dem Bundesdatenschutzgesetz (BDSG) geregelt. Die geltende Rechtslage ist stark von der Auslegung durch Gerichte und Aufsichtsbehörden geprägt. Mit einem bundesweit einheitlichen und verbindlichen Regelwerk soll daher nun ein klarer Rechtsrahmen geschaffen werden. Anlass dazu gibt auch das Urteil C-34/21 des Europäischen Gerichtshofs vom 30. März 2023 zu der zu § 26 BDSG parallelen Vorschrift in § 23 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes. Mit einem klaren und passgenauen Beschäftigtendatengesetz wird eine sichere Rechtsgrundlage für die betriebliche Datennutzung geschaffen, die ein angemessenes Schutzniveau gewährleistet. Der vorliegende Entwurf macht insofern von der Öffnungsklausel für den Beschäftigungskontext in Artikel 88 der Verordnung (EU) 2016/679 Gebrauch. So wird Beschäftigten und Arbeitgebern die Rechtskenntnis und -anwendung in der Praxis erleichtert. Ein eigenständiges Beschäftigtendatengesetz stellt einen wichtigen Baustein bei der sozialen Begleitung der digitalen

Transformation dar und trägt dazu bei, dass technologische Innovation zu sozialem Fortschritt wird.

## **B. Lösung**

Mit dem Beschäftigtendatengesetz wird der Rahmen für einen modernen Beschäftigtendatenschutz geschaffen, der eine Balance zwischen den Interessen der Betriebe und der Beschäftigten zum Ziel hat und dabei gleichzeitig den erforderlichen Schutz für die Beschäftigten gewährleistet. Klare, handhabbare Vorschriften für typische Verarbeitungssituationen schaffen Rechtssicherheit für Arbeitgeber und Vertrauen in den Einsatz neuer Technologien bei den Beschäftigten.

Mit klaren Kriterien für die Abwägung der Interessen von Arbeitgebern und Beschäftigten werden die in den Rechtsgrundlagen der Verordnung (EU) 2016/679 und derzeit in § 26 BDSG lediglich abstrakt formulierten Abwägungen konkret konturiert. Dadurch wird Arbeitgebern sowie Beschäftigten und deren Interessenvertretungen eine Hilfestellung gegeben, die die Zulässigkeitsprüfung in komplexen Einzelfällen erleichtert. Für die Bewerbungsphase wird Rechtsklarheit darüber geschaffen, welche Fragen Arbeitgeber stellen dürfen und wann Gesundheitsuntersuchungen oder psychologische Tests erlaubt sind. Der Entwurf trifft differenzierte Regelungen zu unterschiedlichen Formen der Überwachung von Beschäftigten, wie der nicht nur kurzzeitigen und der verdeckten Überwachung sowie der Videoüberwachung und der Ortung von Beschäftigten. Maßnahmen, die stets unverhältnismäßig sind, wie die längerfristige Überwachung zur Leistungskontrolle sowie die Überwachung von Sanitär- und Umkleieräumen, werden ausgeschlossen. Beim Einsatz von Künstlicher Intelligenz am Arbeitsplatz wird durch Kennzeichnungs- und Informationspflichten die Transparenz für die Beschäftigten gestärkt. Für die automatisierte Bewertung von Beschäftigten (Profiling) werden klare Regelungen geschaffen, die eine umfassende Durchleuchtung verhindern. Automatisierte Emotionserkennung von Beschäftigten und die Bewertung der sozialen Beziehungen zwischen Beschäftigten auf Basis von Kommunikationsdaten werden ausgeschlossen.

## **C. Alternativen**

Keine.

## **D. Haushaltsausgaben ohne Erfüllungsaufwand**

Keine.

## **E. Erfüllungsaufwand**

Der Erfüllungsaufwand wurde in Abstimmung mit dem Statistischen Bundesamt ermittelt. Dieser ergibt sich aus einigen Informations- und Dokumentationspflichten des Arbeitgebers sowie aus Auskunftsrechten der betroffenen Beschäftigten. Mit Ausnahme von § 10 Absatz 1 BeschDG, der eine spezifische Auskunftspflicht auf Verlangen für alle Datenverarbeitungen aufgrund eines berechtigten Interesses statuiert, beziehen sich die relevanten Rechte und Pflichten auf konkrete Regelungen aus den Bereichen KI, Profiling und Videoüberwachung. Insbesondere Datenverarbeitungen im Zusammenhang mit KI bzw. Profiling sind häufig mit tiefen Eingriffen in die informationelle Selbstbestimmung verbunden. Hinzu tritt bei diesen neuen Technologien und Methoden, dass ihre Funktionsweise für die Beschäftigten oft eine „Black Box“ ist, die aber, gerade beim Profiling, zu gewichtigen Entscheidungs-

gen führen kann. Daher sind erhöhte Transparenzanforderungen in diesem Bereich unerlässlich, um einen angemessenen Grundrechtsschutz zu gewährleisten. Der Erfüllungsaufwand für einzelne Unternehmen wird häufig sehr gering ausfallen. Dies gilt insbesondere für Kleinstunternehmen sowie kleine und mittlere Unternehmen, in denen eingriffsintensive Verarbeitungsmaßnahmen wie Profiling nur in wenigen Fällen zur Anwendung kommen dürften.

### **E.1 Erfüllungsaufwand für Bürgerinnen und Bürger**

Bei den Bürgerinnen und Bürgern entsteht mit Blick auf die mögliche Wahrnehmung neuer Rechte zusätzlicher jährlicher Erfüllungsaufwand in Höhe von rund 32.451 Stunden.

### **E.2 Erfüllungsaufwand für die Wirtschaft**

Für die Wirtschaft erhöht sich der jährliche Erfüllungsaufwand um rund 3.964.000 Euro. Dabei handelt es sich komplett um Bürokratiekosten aus Informationspflichten. Darüber hinaus entsteht der Wirtschaft einmaliger Aufwand von rund 3.509.000 Euro. Dieser ist komplett der Kategorie „Einmalige Informationspflicht“ zuzuordnen.

### **E.3 Erfüllungsaufwand der Verwaltung**

Für die Verwaltung steigt der jährliche Erfüllungsaufwand um rund 32.000 Euro. Der jährliche Aufwand entfällt komplett auf den Bund.

### **F. Weitere Kosten**

Weitere Kosten, insbesondere Auswirkungen auf Einzelpreise und das Preisniveau, sind nicht zu erwarten.

# **Referentenentwurf des Bundesministeriums für Arbeit und Soziales und des Bundesministeriums des Innern und für Heimat**

## **Entwurf eines Gesetzes zur Stärkung eines fairen Umgangs mit Beschäftigtendaten und für mehr Rechtssicherheit für Arbeitgeber und Beschäftigte in der digitalen Arbeitswelt**

### **(Beschäftigtendatengesetz – BeschDG)**

**Vom ...**

Der Bundestag hat das folgende Gesetz beschlossen:

#### Inhaltsübersicht

- Artikel 1 Gesetz zur Stärkung eines fairen Umgangs mit Beschäftigtendaten und für mehr Rechtssicherheit für Arbeitgeber und Beschäftigte in der digitalen Arbeitswelt (Beschäftigtendatengesetz – BeschDG)
- Artikel 2 Folgeänderungen
- Artikel 3 Inkrafttreten

## **Artikel 1**

### **Gesetz zur Stärkung eines fairen Umgangs mit Beschäftigtendaten und für mehr Rechtssicherheit für Arbeitgeber und Beschäftigte in der digitalen Arbeitswelt**

#### **(Beschäftigtendatengesetz – BeschDG)**

#### Inhaltsübersicht

##### **T e i l 1**

##### **A l l g e m e i n e r T e i l**

##### **Kapitel 1**

##### **Allgemeine Bestimmungen**

- § 1 Anwendungsbereich
- § 2 Begriffsbestimmungen

##### **Kapitel 2**

##### **Grundlagen der Datenverarbeitung**

- § 3 Grundlagen der Datenverarbeitung

- § 4 Prüfung der Erforderlichkeit
- § 5 Einwilligung
- § 6 Besondere Kategorien von Beschäftigtendaten
- § 7 Kollektivvereinbarungen
- § 8 Verarbeitung zu anderen Zwecken
- § 9 Schutzmaßnahmen

### **Kapitel 3**

#### **Betroffenenrechte, Verwertungsverbot und Datenschutzbeauftragte**

- § 10 Spezifische Betroffenenrechte
- § 11 Verwertungsverbot
- § 12 Mitbestimmung bei der Bestellung und Abberufung von Datenschutzbeauftragten

## **T e i l 2**

### **B e s o n d e r e r T e i l**

#### **Kapitel 1**

##### **Datenverarbeitung vor Begründung des Beschäftigungsverhältnisses**

- § 13 Eignungsfeststellung
- § 14 Fragerecht
- § 15 Positive Maßnahmen
- § 16 Untersuchungen und Tests
- § 17 Löschpflichten

#### **Kapitel 2**

##### **Überwachung**

- § 18 Überwachung von Beschäftigten
- § 19 Nicht nur kurzzeitige Überwachungsmaßnahmen
- § 20 Verdeckte Überwachung
- § 21 Videoüberwachung
- § 22 Ortung
- § 23 Weiterverarbeitung zur Leistungskontrolle

#### **Kapitel 3**

##### **Profiling**

- § 24 Profiling
- § 25 Informationspflicht bei Profiling

- § 26 Auskunftsrecht bei Profiling
- § 27 Erklärung und Überprüfung der Entscheidung

#### **Kapitel 4**

##### **Besondere Verarbeitungssituationen**

- § 28 Datenverarbeitung zu Autorisierungs- und Authentifizierungszwecken
- § 29 Betriebliches Eingliederungsmanagement
- § 30 Datenverarbeitung im Konzern

## Teil 1

### Allgemeiner Teil

#### Kapitel 1

##### Allgemeine Bestimmungen

#### § 1

##### **Anwendungsbereich**

(1) Dieses Gesetz gilt für die Verarbeitung von Beschäftigtendaten im Zusammenhang mit ihrem Beschäftigungsverhältnis durch Arbeitgeber, sofern es sich um

1. öffentliche Stellen des Bundes im Sinne von § 2 Absatz 1 und 3 Bundesdatenschutzgesetz oder
2. nichtöffentliche Stellen im Sinne von § 2 Absatz 4 und 5 Bundesdatenschutzgesetz handelt; § 1 Absatz 4 Bundesdatenschutzgesetz gilt entsprechend.

(2) Dieses Gesetz gilt entsprechend für die Verarbeitung von Beschäftigtendaten durch Dritte, wenn sie mit dem Arbeitgeber in gemeinsamer Verantwortlichkeit Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses verarbeiten.

(3) Dieses Gesetz gilt für die nichtautomatisierte sowie für die ganz oder teilweise automatisierte Verarbeitung von Beschäftigtendaten.

(4) Besondere Rechtsvorschriften des Bundes über den Schutz von Beschäftigtendaten gehen den Vorschriften dieses Gesetzes vor. Regeln sie einen Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschließend, finden die Vorschriften dieses Gesetzes insoweit Anwendung. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(5) Die Vorschriften des Bundesdatenschutzgesetzes bleiben unberührt, soweit dieses Gesetz nichts anderes bestimmt.

§ 2

**Begriffsbestimmungen**

(1) Beschäftigtendaten im Sinne des Gesetzes sind personenbezogene Daten von Beschäftigten.

(2) Als Beschäftigte im Sinne dieses Gesetzes gelten

1. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeiterinnen und Leiharbeiter,
2. zu ihrer Berufsbildung Beschäftigte, einschließlich Praktikantinnen und Praktikanten,
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. Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten,
7. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
8. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis und
9. Personen, deren Beschäftigungsverhältnis beendet ist.

(3) Arbeitgeber im Sinne dieses Gesetzes sind öffentliche Stellen des Bundes nach § 1 Absatz 1 Nummer 1 sowie nichtöffentliche Stellen nach § 1 Absatz 1 Nummer 2, die Personen nach Absatz 2 beschäftigen. Als Arbeitgeber im Sinne dieses Gesetzes gelten insbesondere auch

1. der Entleiher im Verhältnis zu den Leiharbeiterinnen und Leihararbeitern im Fall von Absatz 2 Nummer 1,
2. die natürliche oder juristische Person oder die rechtsfähige Personengesellschaft, die Beschäftigte im Fall von Absatz 2 Nummer 2 ausbildet oder für die Praktikanten und Praktikantinnen im Fall von Absatz 2 Nummer 2 tätig sind,
3. die natürliche oder juristische Person oder die rechtsfähige Personengesellschaft, bei der Rehabilitandinnen und Rehabilitanden im Fall von Absatz 2 Nummer 3 tätig sind,
4. der Träger der Werkstatt für behinderte Menschen im Fall von Absatz 2 Nummer 4,
5. die Einrichtung, in der der Freiwilligendienst nach dem Jugendfreiwilligendienstegesetz oder nach dem Bundesfreiwilligendienstgesetz im Fall von Absatz 2 Nummer 5 geleistet wird,
6. der Dienstherr für die Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten im Fall von Absatz 2 Nummer 6,

7. der Auftraggeber oder Zwischenmeister für die arbeitnehmerähnlichen Personen, einschließlich für die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten im Fall von Absatz 2 Nummer 7,
8. der potentielle Arbeitgeber im Verhältnis zu Bewerberinnen und Bewerbern für ein Beschäftigungsverhältnis im Fall von Absatz 2 Nummer 8 und
9. der ehemalige Arbeitgeber im Verhältnis zu Personen, deren Beschäftigungsverhältnis beendet ist, im Fall von Absatz 2 Nummer 9.

(4) Kollektivvereinbarung im Sinne dieses Gesetzes sind Tarifverträge, Betriebs- oder Dienstvereinbarungen oder gleichwertige kollektive Verträge.

(5) KI-Systeme im Sinne dieses Gesetzes sind Systeme der künstlichen Intelligenz im Sinne von Artikel 3 Nr. 1 der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024).

(6) Besondere Kategorien von Beschäftigtendaten im Sinne des Gesetzes sind besonderen Kategorien personenbezogener Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35) von Beschäftigten.

## Kapitel 2

### Grundlagen der Datenverarbeitung

#### § 3

##### **Grundlagen der Datenverarbeitung**

(1) Die Verarbeitung von Beschäftigtendaten ist im Zusammenhang mit einem Beschäftigungsverhältnis zulässig, soweit dies für einen konkreten Zweck

1. zur Entscheidung über die Begründung, zur Durchführung oder zur Beendigung eines Beschäftigungsverhältnisses,
2. zur Erfüllung von durch Rechtsvorschriften festgelegten Pflichten des Arbeitgebers,
3. zur Erfüllung von durch Kollektivvereinbarung festgelegten Pflichten des Arbeitgebers,
4. zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einer Kollektivvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten,
5. zum Schutz lebenswichtiger Interessen der betroffenen Beschäftigten oder einer anderen natürlichen Person,



6. zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Arbeitgeber übertragen wurde, oder
7. zur Wahrung eines berechtigten betrieblichen oder dienstlichen Interesses des Arbeitgebers

erforderlich ist und dabei in den Fällen der Nummern 1 und 7 die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen.

(2) Der Zweck einer Verarbeitung nach Absatz 1 kann sich insbesondere beziehen auf die Planung und Organisation der Arbeit, das Management, die Gleichheit und Diversität am Arbeitsplatz, die Gesundheit und Sicherheit am Arbeitsplatz, den Umwelt- und Klimaschutz, den Schutz des Eigentums der Arbeitgeber, der Beschäftigten oder der Kunden sowie die Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen. Keine zulässigen Zwecke sind insbesondere die Verhinderung oder Einschränkung der Ausübung von gesetzlichen Rechten der Beschäftigten und ihrer Interessenvertretungen. Dies gilt auch für den Zweck der Vorhersage der Ausübung der Koalitionsfreiheit durch Beschäftigte.

(3) Werden Beschäftigtendaten nach diesem Gesetz verarbeitet, muss der Arbeitgeber den Zweck der Verarbeitung so konkret festlegen, dass anhand des Zwecks die Rechtmäßigkeit der Verarbeitung und die Einhaltung der Verarbeitungsgrundsätze und Pflichten nach diesem Gesetz und der Verordnung (EU) 2016/679 bewertet werden können. Der Zweck muss zum Zeitpunkt der Verarbeitung feststehen.

(4) Die Verarbeitung folgender Beschäftigtendaten ist insbesondere für folgende Zwecke zulässig im Sinne des Absatzes 1:

1. für den Zweck der Kontaktaufnahme zu Bewerberinnen und Bewerbern jedenfalls Anrede, Name, Anschrift, Telefonnummer und E-Mail-Adresse,
2. für den Zweck der Kontaktaufnahme im laufenden Beschäftigungsverhältnis zur Zusendung allgemeiner betrieblicher Informationen sowie zur Klärung von Fragen, die das Beschäftigungsverhältnis betreffen, jedenfalls Anrede, Name, Anschrift und E-Mail-Adresse,
3. für den Zweck der Gehaltsauszahlung jedenfalls Name, Personalnummer und, sofern nicht das Entgelt auf andere Weise als durch Banküberweisung gezahlt wird, Bankverbindung.

## § 4

### **Prüfung der Erforderlichkeit**

Bei der Prüfung der Erforderlichkeit einer Verarbeitung von Beschäftigtendaten nach diesem Gesetz ist die im Beschäftigungsverhältnis bestehende Abhängigkeit der Beschäftigten zu berücksichtigen. Bei der im Rahmen der Prüfung der Erforderlichkeit durchzuführenden Abwägung der Interessen des Arbeitgebers an einer Verarbeitung mit den Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung können insbesondere folgende Aspekte zu berücksichtigen sein:

1. unter Berücksichtigung des legitimen Verarbeitungszwecks das Gewicht der mit der Verarbeitung verfolgten Interessen des Arbeitgebers, das insbesondere davon abhängt,

- a) ob in Rechtsvorschriften, in Kollektivvereinbarungen oder vertraglich festgelegte Pflichten erfüllt werden sollen,
  - b) ob und wie stark Grundrechtspositionen des Arbeitgebers betroffen sind,
  - c) ob ein öffentliches Interesse besteht und wie dieses zu gewichten ist,
2. unter Berücksichtigung des mit der Verarbeitung im Beschäftigungskontext verbundenen Grundrechtseingriffs, wie tief die Verarbeitung in die Rechte und Interessen der betroffenen Beschäftigten eingreift, welche möglichen Folgen die Verarbeitung für die betroffenen Beschäftigten haben kann und welches Risiko für die Rechte und Interessen der betroffenen Beschäftigten besteht; dies wird insbesondere beeinflusst durch
- a) die Dauer und Häufigkeit der Verarbeitung, unter Berücksichtigung des Charakters des Beschäftigungsverhältnisses als Dauerschuldverhältnis,
  - b) die Art der verarbeiteten Beschäftigtendaten,
  - c) den Umfang der verarbeiteten Beschäftigtendaten,
  - d) den Umstand, ob die Beschäftigtendaten mit anderen verarbeiteten Beschäftigtendaten abgeglichen oder verknüpft und so verschiedene Informationen und persönliche Aspekte zusammengeführt werden,
  - e) die Mittel und die Art der Verarbeitung, zum Beispiel ob die Verarbeitung analog oder mittels technischer Einrichtungen oder in Echtzeit oder mit Speicherung erfolgt,
  - f) die Anzahl und Funktion der Personen, die an der Verarbeitung beteiligt sind und Zugriff auf die Daten haben, zum Beispiel ob es sich um direkte Vorgesetzte handelt,
  - g) den Umstand, ob eine Datenerhebung bei der betroffenen beschäftigten Person selbst erfolgt,
  - h) die begründeten Erwartungen der Beschäftigten an den Umgang mit ihren Daten durch den Arbeitgeber unter Berücksichtigung der im Beschäftigungsverhältnis bestehenden besonderen Schutz- und Fürsorgepflichten,
  - i) das Risiko, dass aus den verarbeiteten Beschäftigtendaten in zweckwidriger Weise Rückschlüsse auf die Arbeitsleistung gezogen werden, insbesondere wenn sich dies nachteilig auf das berufliche Fortkommen der betroffenen Beschäftigten auswirken kann,
  - j) die Möglichkeiten zur menschlichen Aufsicht und Kontrolle beim Einsatz von KI-Systemen und die Möglichkeiten, den Beschäftigten die Funktionsweise der KI-Systeme in verständlicher Weise zu erläutern,
3. welche technischen und organisatorischen Maßnahmen zur Minimierung des Risikos für die betroffenen Beschäftigten und zur Wahrung ihrer menschlichen Würde, berechtigten Interessen und Grundrechte durch den Arbeitgeber nach § 9 getroffen werden.

## § 5

### **Einwilligung**

(1) Erfolgt die Verarbeitung von Beschäftigtendaten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit von Beschäftigten sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Hierbei sind insbesondere die Art und der Umfang der zu verarbeitenden Beschäftigtendaten sowie der Zeitpunkt der Einwilligungserteilung maßgeblich. Soll die Einwilligung vor Begründung eines Vertragsverhältnisses erteilt werden, ist das verstärkte Machtungleichgewicht besonders zu berücksichtigen.

(2) Freiwilligkeit kann insbesondere vorliegen, wenn für die Beschäftigte oder den Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Dies kann insbesondere bei der Verarbeitung zu folgenden Zwecken der Fall sein:

1. vor Begründung eines Beschäftigungsverhältnisses die Aufnahme in eine Bewerbungsdatenbank, wenn die Einwilligung nach der Beendigung eines erfolglosen Auswahlverfahrens erteilt wird,
2. im laufenden Beschäftigungsverhältnis
  - a) die Nutzung von Fotos für das Intranet,
  - b) die Aufnahme von Name und Geburtsdatum in eine Geburtstagsliste,
  - c) die Teilnahme an Angeboten zur Gesundheitsförderung im Rahmen eines betrieblichen Gesundheitsmanagements,
  - d) die Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen,
  - e) die Nutzung von biometrischen Daten zur erleichterten Identifizierung, sofern es eine gleichwertige Alternative gibt, die keine Nutzung biometrischer Daten erfordert,
3. nach Beendigung des Beschäftigungsverhältnisses
  - a) die Kontaktaufnahme zur Gratulation anlässlich von Geburtstagen, Beschäftigungs- oder Dienstjubiläen oder vergleichbaren besonderen Ereignissen,
  - b) die Kontaktaufnahme zur Einladung zu Betriebs- oder Firmenfeiern oder vergleichbaren besonderen Veranstaltungen,
  - c) die Kontaktaufnahme zur Benachrichtigung über geeignete Stellenangebote oder Weiterbildungsmöglichkeiten.

(3) Keine Freiwilligkeit liegt insbesondere vor, wenn der Abschluss oder die Erfüllung des Vertrages zwischen Arbeitgeber und der oder dem Beschäftigten von einer Einwilligung zu einer Verarbeitung von Beschäftigtendaten abhängig gemacht wird, obwohl diese Einwilligung für den Abschluss oder die Erfüllung des Vertrags nicht erforderlich ist.

(4) Die Einwilligung hat schriftlich oder elektronisch zu erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die Beschäftigte oder den Beschäftigten über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

## § 6

### **Besondere Kategorien von Beschäftigtendaten**

(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien von Beschäftigtendaten zulässig, soweit sie für einen konkreten Zweck zur Ausübung oder Erfüllung von durch Rechtsvorschrift oder Kollektivvereinbarung festgelegten Rechten oder Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen.

(2) Genetische Daten dürfen nur gemäß den §§ 19 bis 22 des Gendiagnostikgesetzes verarbeitet werden.

(3) § 22 des Bundesdatenschutzgesetzes findet keine Anwendung.

(4) § 5 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien von Beschäftigtendaten. Die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen.

## § 7

### **Kollektivvereinbarungen**

(1) Die Verhandlungspartner können spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung von Beschäftigtendaten, einschließlich besonderer Kategorien von Beschäftigtendaten, im Beschäftigungskontext in Kollektivvereinbarungen nach Maßgabe der folgenden Absätze vorsehen.

(2) Kollektivvereinbarungen nach Absatz 1 dürfen nicht zu Lasten des Schutzes der Beschäftigten von diesem Gesetz abweichen. Sie können nicht die Zulässigkeit der Verarbeitung von Beschäftigtendaten festlegen.

(3) Die Verhandlungspartner haben bei Kollektivvereinbarungen nach Absatz 1 die Anforderungen von Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten und die besonderen Belange von Beschäftigten der jeweiligen Branche oder des jeweiligen Betriebs zu berücksichtigen. Kollektivvereinbarungen nach Absatz 1 dürfen nicht zu Lasten des Schutzes der Beschäftigten von der Verordnung (EU) 2016/679 und nicht von den grundlegenden Prinzipien der Verordnung (EU) 2016/679, insbesondere der Artikel 5, 6 und 9, abweichen.

(4) Soweit keine spezifischeren Vereinbarungen getroffen werden, bleiben die Bestimmungen dieses Gesetzes, des Bundesdatenschutzgesetzes und der Verordnung (EU) 2016/679 unberührt.

(5) Die Beteiligungsrechte und sonstigen gesetzlichen Rechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

## § 8

### **Verarbeitung zu anderen Zwecken**

(1) Die Verarbeitung von Beschäftigtendaten zu einem anderen Zweck als demjenigen, zu dem die Beschäftigtendaten ursprünglich erhoben wurden, ist zulässig, wenn sie

1. auf einer Einwilligung der betroffenen Beschäftigten unter den Voraussetzungen des § 5 beruht,
2. auf einer Rechtsvorschrift außerhalb dieses Gesetzes beruht, die eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 Verordnung (EU) 2016/679 genannten Ziele darstellt oder
3. mit dem Zweck, zu dem die Beschäftigtendaten ursprünglich erhoben wurden, vereinbar ist und die Verarbeitung darüber hinaus zu dem anderen Zweck zulässig ist.

(2) Bei Beurteilung der Vereinbarkeit nach Absatz 1 Nummer 3 ist über Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 hinaus zu berücksichtigen, wie sich die im Beschäftigungsverhältnis bestehende Abhängigkeit der Beschäftigten bei der ursprünglichen Erhebung der Beschäftigtendaten und der Verarbeitung zu einem anderen Zweck im Einzelfall auswirkt, insbesondere ob nachteilige Folgen für das berufliche Fortkommen der Beschäftigten möglich sind und ob diese bei der ursprünglichen Datenerhebung für die Beschäftigten absehbar waren.

(3) § 23 Absatz 1 Nummer 6 und § 24 Absatz 1 des Bundesdatenschutzgesetzes sind mit der Maßgabe anwendbar, dass die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen müssen. § 23 Absatz 2 und § 24 Absatz 2 des Bundesdatenschutzgesetzes sind mit der Maßgabe anwendbar, dass statt der Voraussetzungen des § 22 des Bundesdatenschutzgesetzes die Voraussetzungen für die Verarbeitung besonderer Kategorien von Beschäftigtendaten nach diesem Gesetz vorliegen müssen.

## § 9

### **Schutzmaßnahmen**

(1) Der Arbeitgeber muss geeignete und besondere Maßnahmen treffen, um die Einhaltung der Grundprinzipien und Regelungen der Verordnung (EU) 2016/679 und dieses Gesetzes sicherzustellen, sowie die menschliche Würde, die berechtigten Interessen und die Grundrechte der betroffenen Beschäftigten zu wahren. Unter Berücksichtigung der besonderen Belange der Beschäftigten, des Stands der Technik, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten der Beschäftigten können dazu insbesondere gehören:

1. technische und organisatorische Maßnahmen, die dafür sorgen, dass bestimmte Verarbeitungsformen gar nicht bereitgestellt, unterbunden oder eingeschränkt werden,
2. Trennung von Beschäftigtendaten, die zu unterschiedlichen Zwecken verarbeitet werden, insbesondere die gesonderte Verwahrung von Personalakten,
3. Beschränkung des Zugangs zu Beschäftigtendaten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern, beispielsweise durch dokumentierte Zuweisung von Berechtigungen und Rollen anhand von funktionalen Zuständigkeiten,

4. besondere Sicherung etwa durch Verschlüsselung oder sichere Authentifizierungsverfahren, insbesondere von Personalaktendaten,
5. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten und Beschränkung auf Personen, die zur Verschwiegenheit verpflichtet sind,
6. Maßnahmen zur Pseudonymisierung von Beschäftigtendaten,
7. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Beschäftigtendaten eingegeben, verändert oder entfernt wurden,
8. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen,
9. frühzeitige Einbindung der Interessenvertretungen von Beschäftigten, im Rahmen der Gestaltung von Verarbeitungsvorgängen und im Rahmen der Überprüfung von Verarbeitungsvorgängen oder Schutzmaßnahmen,
10. freiwillige Einbindung einer oder eines Datenschutzbeauftragten,
11. beim Einsatz von KI-Systemen zur Verarbeitung von Beschäftigtendaten
  - a) eine regelmäßige Evaluierung, welche personenbezogenen Eingabe- und Ausgabedaten für die Nutzung relevant und erforderlich sind,
  - b) soweit möglich die Anonymisierung der durch die KI-Systeme erzeugten Ergebnisse und Zwischenergebnisse sowie ein Ausschluss von deren zweckwidriger Nutzung,
  - c) soweit es für den Arbeitgeber technisch möglich ist, die regelmäßige Überprüfung des KI-Systems auf diskriminierende und unrichtige Ergebnisse.

(2) Werden besondere Kategorien von Beschäftigtendaten verarbeitet, hat der Arbeitgeber bei der Auswahl und Umsetzung der Maßnahmen nach Absatz 1 zu berücksichtigen, dass besondere Kategorien von Beschäftigtendaten ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel und deshalb besonders schutzbedürftig sind.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 der Verordnung (EU) 2016/679 oder eines genehmigten Zertifizierungsverfahren gemäß Artikel 42 der Verordnung (EU) 2016/679 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der in Absatz 1 genannten Anforderungen nachzuweisen.

## Kapitel 3

### Betroffenenrechte, Verwertungsverbot und Datenschutzbeauftragte

#### § 10

##### **Spezifische Betroffenenrechte**

(1) Beruht die Verarbeitung von Beschäftigtendaten auf diesem Gesetz und wird sie auf ein berechtigtes betriebliches oder dienstliches Interesse gestützt, hat der Arbeitgeber die wesentlichen Erwägungen der Abwägung der Interessen nach § 4 den betroffenen Beschäftigten auf Verlangen in einer für diese verständlichen Weise darzulegen. Über das Bestehen des Auskunftsrechts nach Satz 1 sind die betroffenen Beschäftigten bei der Erfüllung und in Ergänzung der Informationspflichten nach den Artikeln 13 und 14 der Verordnung (EU) 2016/679 zu informieren.

(2) Wird bei der Verarbeitung von Beschäftigtendaten ein KI-System eingesetzt, muss der Arbeitgeber die betroffenen Beschäftigten spätestens mit Beginn der Verarbeitung über den Einsatz und das nach Absatz 3 bestehende Auskunftsrecht informieren.

(3) Wird bei der Verarbeitung von Beschäftigtendaten ein KI-System eingesetzt, haben von der Verarbeitung betroffene Beschäftigte ein Recht auf Auskunft über folgende Informationen:

1. aussagekräftige Informationen über die Funktionsweise des KI-Systems sowie die Funktion der verarbeiteten Beschäftigtendaten innerhalb des KI-Systems;
2. welche Schutzmaßnahmen nach § 9 Absatz 1 Nummer 11 der Arbeitgeber getroffen hat.

#### § 11

##### **Verwertungsverbot**

(1) Wurden Beschäftigtendaten datenschutzrechtswidrig verarbeitet, dürfen diese Daten in einem gerichtlichen Verfahren über die Rechtmäßigkeit einer auf diese Daten gestützten personellen Maßnahme des Arbeitgebers gegen einen Beschäftigten oder eine Beschäftigte nicht verwertet werden. Dies gilt nicht, wenn ein offensichtliches Missverhältnis zwischen dem Eingriff in das allgemeine Persönlichkeitsrecht der betroffenen beschäftigten Person durch die gerichtliche Verwertung und dem grundrechtlich geschützten Interesse des Arbeitgebers an der gerichtlichen Verwertung besteht.

(2) Die Verhandlungspartner können für datenschutzrechtswidrige oder kollektivvereinbarungswidrige Verarbeitungen von Beschäftigtendaten ein Verwertungsverbot in Kollektivvereinbarungen regeln.

## § 12

### **Mitbestimmung bei der Bestellung und Abberufung von Datenschutzbeauftragten**

Der Betriebsrat hat bei der Bestellung und Abberufung der oder des betrieblichen Datenschutzbeauftragten mitzubestimmen. Kommt eine Einigung nicht zustande, so entscheidet die Einigungsstelle nach § 76 des Betriebsverfassungsgesetzes. Der Spruch der Einigungsstelle ersetzt die Einigung zwischen Arbeitgeber und Betriebsrat.

## Teil 2

### Besonderer Teil

#### Kapitel 1

#### Datenverarbeitung vor Begründung des Beschäftigungsverhältnisses

### § 13

#### **Eignungsfeststellung**

(1) Die Verarbeitung von Beschäftigtendaten einschließlich besonderer Kategorien von Beschäftigtendaten, ist vor Begründung eines Beschäftigungsverhältnisses zulässig, soweit sie erforderlich ist,

1. um die Eignung des oder der Beschäftigten für die auszuübende Tätigkeit festzustellen oder
2. zur Erfüllung von durch Rechtsvorschrift festgelegten Pflichten des Arbeitgebers

und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen. Unter den Voraussetzungen von Satz 1 Nummer 1 dürfen insbesondere Beschäftigtendaten über die fachlichen und persönlichen Fähigkeiten, Kenntnisse und Erfahrungen sowie über die Ausbildung und den bisherigen beruflichen Werdegang verarbeitet werden.

(2) Auf die Verarbeitung von Beschäftigtendaten vor Begründung eines Beschäftigungsverhältnisses durch oder aufgrund von Profiling finden §§ 24 bis 27 entsprechende Anwendung.

(3) Ergänzend zu den nach § 9 zu treffenden Schutzmaßnahmen sind nach dieser Vorschrift erhobene Daten besonders gegen Verletzungen ihrer Vertraulichkeit und Integrität, insbesondere durch unbefugten Zugang, zu schützen. Werden die Daten elektronisch verarbeitet, hat der Arbeitgeber die Daten nach dem Stand der Technik in angemessener Weise zu verschlüsseln.



## § 14

### **Fragerecht**

(1) Der Arbeitgeber darf vor Begründung eines Beschäftigungsverhältnisses Auskunft von Beschäftigten oder Dritten über Abstammung, ethnische und sonstige Herkunft, Nationalität, Religion oder Weltanschauung, Behinderung, Alter, politische Meinungen oder Gewerkschaftszugehörigkeit, Geschlecht oder sexuelle Identität, Gesundheit, Vermögensverhältnisse, Vorstrafen und laufende Ermittlungsverfahren nur verlangen,

1. soweit dies zur Eignungsfeststellung erforderlich ist, weil diese Merkmale wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung eine wesentliche und entscheidende berufliche Anforderung darstellen oder
2. soweit die Verarbeitung dieser Beschäftigtendaten zur Erfüllung von durch Rechtsvorschrift festgelegten Pflichten des Arbeitgebers erforderlich ist

und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen. Die Vorschriften des Bundeszentralregistergesetzes bleiben unberührt. § 7 Absatz 2 des Bundesgleichstellungsgesetzes bleibt unberührt.

(2) Der Arbeitgeber darf vor Begründung eines Beschäftigungsverhältnisses keine Auskunft darüber verlangen, ob eine Schwerbehinderung oder Gleichstellung mit einer Schwerbehinderung nach § 2 Absatz 2 und 3 des Neunten Buches Sozialgesetzbuch vorliegt.

(3) Soll eine Beschäftigung bei einer Religionsgemeinschaft, einer ihr zugeordneten Einrichtung oder bei einer Vereinigung erfolgen, die sich die gemeinschaftliche Pflege einer Religion oder Weltanschauung zur Aufgabe gemacht hat, darf der Arbeitgeber unbeschadet des Artikels 91 der Verordnung (EU) 2016/679 auch Auskunft über die religiöse Überzeugung, die Religionszugehörigkeit oder die Weltanschauung von Beschäftigten verlangen, soweit diese Merkmale unter Beachtung des Selbstverständnisses der jeweiligen Religionsgemeinschaft oder Vereinigung im Hinblick auf ihr Selbstbestimmungsrecht oder nach der Art der Tätigkeit eine gerechtfertigte berufliche Anforderung darstellen und die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen.

(4) Eine Auskunft, die gemäß den Absätzen 1 bis 3 nicht verlangt werden darf, darf der Arbeitgeber auch nicht aufgrund von Profiling herleiten. Die Erweiterung der gesetzlichen Verarbeitungsbefugnisse nach dieser Vorschrift aufgrund einer Einwilligung ist unzulässig.

- (5) § 13 Absatz 3 gilt entsprechend.

## § 15

### **Positive Maßnahmen**

(1) Die Verarbeitung von Beschäftigtendaten über ethnische und sonstige Herkunft, Geschlecht, Religion oder Weltanschauung, Behinderung, Alter oder sexuelle Identität, die freiwillig angegeben wurden, ist vor Begründung eines Beschäftigungsverhältnisses zulässig, soweit sie erforderlich ist, um durch geeignete und angemessene Maßnahmen nach § 5 des Allgemeinen Gleichbehandlungsgesetzes bestehende Nachteile zu verhindern oder auszugleichen und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen.

(2) § 13 Absatz 3 gilt entsprechend.

## § 16

### Untersuchungen und Tests

(1) Die Verarbeitung von Beschäftigtendaten, einschließlich besonderer Kategorien von Beschäftigtendaten, im Rahmen von Gesundheitsuntersuchungen vor Begründung eines Beschäftigungsverhältnisses ist nur zulässig,

1. soweit die dabei erlangten Kenntnisse erforderlich sind, um festzustellen, ob der oder die Beschäftigte eine wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung wesentliche und entscheidende berufliche Anforderung erfüllt oder
2. soweit die Feststellung der gesundheitlichen Eignung zur Erfüllung von durch Rechtsvorschrift festgelegten Pflichten des Arbeitgebers erforderlich ist

und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen. Satz 1 gilt auch für Drogen- und Alkoholtests. § 19 des Gendiagnostikgesetzes bleibt unberührt.

(2) Die Verarbeitung von Beschäftigtendaten, einschließlich besonderer Kategorien von Beschäftigtendaten, im Rahmen von psychologischen Eignungstests und -untersuchungen vor Begründung eines Beschäftigungsverhältnisses ist nur zulässig,

1. wenn das angewandte Verfahren, die Art und Weise der Durchführung und die Qualifikation der die Untersuchung durchführenden Person wissenschaftlich anerkannten Standards, etwa den Anforderungen der DIN 33430 in der jeweils aktuellen Fassung entsprechen,
2. soweit die dabei erlangten Kenntnisse erforderlich sind, um festzustellen, ob der oder die Beschäftigte eine wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung wesentliche und entscheidende berufliche Anforderung erfüllt

und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen.

(3) Sind Gesundheitsuntersuchungen und psychologische Eignungstests und -untersuchungen ganz oder teilweise durch Personen durchzuführen, die einer beruflichen Schweigepflicht unterliegen, so darf dem Arbeitgeber insoweit nur mitgeteilt werden, ob der oder die Beschäftigte nach dem Ergebnis des Tests oder der Untersuchung für die auszuübende Tätigkeit geeignet ist. Dem oder der Beschäftigten ist auf Verlangen das vollständige Untersuchungsergebnis mitzuteilen.

(4) Die Verarbeitung von Beschäftigtendaten nach den Absätzen 1 und 2 ohne Information der betroffenen Beschäftigten ist ausgeschlossen.

(5) § 13 Absatz 3 gilt entsprechend.

## § 17

### Löschpflichten

(1) Beschäftigtendaten, die vor der Eingehung eines Beschäftigungsverhältnisses verarbeitet wurden, sind spätestens drei Monate nachdem feststeht, dass ein Beschäftigungsverhältnis nicht zustande kommt, zu löschen. Dies gilt nicht, wenn eine Speicherung über drei Monate hinaus wegen eines bereits anhängigen oder aufgrund zu dokumentierender konkreter Anhaltspunkte wahrscheinlichen Rechtsstreits erforderlich ist. Zieht der oder die Beschäftigte seine oder ihre Bewerbung zurück, sind die Beschäftigtendaten unverzüglich zu löschen.

(2) Arbeitgeber dürfen Beschäftigtendaten, die vor der Eingehung eines Beschäftigungsverhältnisses verarbeitet wurden, abweichend von Absatz 1 zum Zweck des Abgleichs mit offenen Stellen und der Kontaktaufnahme für spätere Auswahlverfahren weiter speichern und verarbeiten, wenn die betroffene Person nach der Beendigung eines Auswahlverfahrens unter Berücksichtigung von § 5 einwilligt.

## Kapitel 2

### Überwachung

## § 18

### Überwachung von Beschäftigten

(1) Die Verarbeitung von Beschäftigtendaten durch Überwachungsmaßnahmen ist nur zulässig, soweit sie für einen konkreten Zweck zur Durchführung des Beschäftigungsverhältnisses, zur Erfüllung von durch Rechtsvorschrift oder Kollektivvereinbarung festgelegten Pflichten des Arbeitgebers oder zur Wahrung wichtiger betrieblicher oder dienstlicher Interessen erforderlich ist und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen. Die Verarbeitung nach Satz 1 darf nur kurzzeitig und entweder anlassbezogen oder stichprobenhaft erfolgen.

(2) Der Zweck einer Verarbeitung nach Absatz 1 kann sich insbesondere auf den Schutz von Gesundheit und Sicherheit von Beschäftigten sowie die Verhütung und Aufdeckung von Straftaten und Pflichtverletzungen beziehen.

(3) Überwachungsmaßnahmen im Sinne von Absatz 1 Satz 1 sind alle Maßnahmen zur zielgerichteten Beobachtung von Personen oder Objekten durch Personen oder technische Einrichtungen. Dies gilt nur, wenn Beschäftigtendaten ganz oder teilweise automatisiert verarbeitet werden, sowie wenn nichtautomatisiert verarbeitete Beschäftigtendaten in einem Dateisystem gespeichert werden oder gespeichert werden sollen.

(4) Bei der Abwägung der Interessen nach Absatz 1 sind über § 4 hinaus insbesondere folgende Aspekte zu berücksichtigen:

1. Art und Umfang der Überwachungsmaßnahme, insbesondere:

- a) wie viele Parameter oder Merkmale in Bezug auf die betroffenen Beschäftigten durch die Maßnahme erfasst werden,

- b) ob durch die Maßnahme über die erstrebte Information hinaus weitere Beschäftigtendaten verarbeitet werden können, insbesondere Daten aus dem Bereich der privaten Lebensgestaltung,
  - c) ob die Maßnahme während der Arbeitszeit durchgeführt wird,
2. zu erwartende Folgen der Überwachungsmaßnahme für die Beschäftigten, insbesondere welche Nachteile den betroffenen Beschäftigten aus der Maßnahme drohen, oder von ihnen nicht ohne Grund befürchtet werden,
3. bei anlassbezogenen Überwachungsmaßnahmen zur Aufdeckung von Straftaten und Pflichtverletzungen, der Anlass der Maßnahme, insbesondere
- a) die Stärke des Verdachts,
  - b) die Schwere der festgestellten oder vermuteten Rechtsguts- oder Rechtsverletzung,
  - c) die Höhe des eingetretenen Schadens,
4. bei anlassbezogenen Überwachungsmaßnahmen zur Verhütung von Straftaten und Pflichtverletzungen die Gefahrenlage, insbesondere
- a) wie konkret die Gefahrenlage ist, die die Maßnahme rechtfertigt,
  - b) das Gewicht der durch die Gefahrenlage bedrohten Rechtsgüter und Interessen.

(5) Die Verarbeitung von Beschäftigtendaten, die den Kernbereich privater Lebensgestaltung betreffen, ist unzulässig. Die Verarbeitung von Beschäftigtendaten durch eine Überwachung von Bereichen, die auch als kollektive und kommunikative Rückzugsräume sowie der privaten Lebensgestaltung dienen, ist unzulässig.

(6) Die Verarbeitung besonderer Kategorien von Beschäftigtendaten durch Überwachungsmaßnahmen ist zulässig, wenn die Voraussetzungen dieser Vorschrift und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 6 vorliegen.

## § 19

### **Nicht nur kurzzeitige Überwachungsmaßnahmen**

(1) Die abweichend von § 18 Absatz 1 Satz 2 nicht nur kurzzeitige Verarbeitung von Beschäftigtendaten durch Überwachungsmaßnahmen ist nur zulässig, soweit sie für einen konkreten Zweck zum Schutz von Leib oder Leben von Beschäftigten oder von Dritten oder zur Wahrung besonders wichtiger betrieblicher oder dienstlicher Interessen erforderlich ist und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung erheblich überwiegen. § 18 Absatz 4 und 5 findet auch auf eine Datenverarbeitung nach Satz 1 Anwendung.

(2) Der Zweck einer Verarbeitung nach Absatz 1 kann sich insbesondere beziehen auf die Sicherung von Beschäftigten bei Tätigkeiten, bei deren Ausübung sie Gefahren für Leib und Leben ausgesetzt sind, die Sicherung von besonders hochwertigen oder sicherheitsrelevanten Gegenständen oder Anlagen, sowie die Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit informationstechnischer Systeme.

(3) Die Verarbeitung nach Absatz 1 darf nicht zur Leistungskontrolle erfolgen.

(4) Ergänzend zu den nach § 9 zu treffenden Schutzmaßnahmen ist vor der Durchführung einer Maßnahme nach Absatz 1 der oder die Datenschutzbeauftragte im Sinne des Artikel 38 Absatz 1 der Verordnung (EU) 2016/679 ordnungsgemäß und frühzeitig einzubeziehen. Bei der Durchführung mehrerer gleichgelagerter Maßnahmen mit ähnlich hohen Risiken genügt eine einmalige Einbeziehung.

(5) Die Verarbeitung besonderer Kategorien von Beschäftigendaten durch nicht nur kurzzeitige Überwachungsmaßnahmen ist zulässig, wenn die Voraussetzungen dieser Vorschrift und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 6 vorliegen.

## § 20

### **Verdeckte Überwachung**

(1) Abweichend von Artikel 13 und 14 der Verordnung (EU) 2016/679 müssen die betroffenen Beschäftigten über die Verarbeitung von Beschäftigendaten durch Überwachungsmaßnahmen nicht informiert werden, soweit

1. zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass aus einem räumlich und funktional abgrenzbaren Kreis von Beschäftigten heraus eine Straftat oder schwere Pflichtverletzung begangen wurde,
2. die Datenverarbeitung zur Aufdeckung dieser Straftat oder schweren Pflichtverletzung erfolgt und
3. keine andere Möglichkeit besteht, diese Straftat oder schwere Pflichtverletzung aufzudecken.

(2) In den Fällen des Absatzes 1 ist die Information unverzüglich nachzuholen, sobald der Zweck der Überwachungsmaßnahme hierdurch nicht mehr gefährdet wird.

(3) Ergänzend zu den nach § 9 zu treffenden Schutzmaßnahmen ist vor der Durchführung einer Maßnahme nach Absatz 1 der oder die Datenschutzbeauftragte im Sinne des Artikel 38 Absatz 1 der Verordnung (EU) 2016/679 ordnungsgemäß und frühzeitig einzubeziehen.

## § 21

### **Videüberwachung**

(1) Die Verarbeitung von Beschäftigendaten durch Videoüberwachung ist nur zulässig, soweit sie für einen konkreten Zweck zur Durchführung des Beschäftigungsverhältnisses, zur Erfüllung von durch Rechtsvorschrift oder Kollektivvereinbarung festgelegten Pflichten des Arbeitgebers oder zur Wahrung wichtiger betrieblicher oder dienstlicher Interessen erforderlich ist und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen. Die Verarbeitung nach Satz 1 darf nur kurzzeitig und entweder anlassbezogen oder stichprobenhaft erfolgen. § 18 Absatz 4 und 5 findet auch auf eine Datenverarbeitung nach Satz 1 Anwendung.

(2) Der Zweck einer Verarbeitung nach Absatz 1 kann sich insbesondere auf die Verhütung und Aufdeckung von Straftaten und schweren Pflichtverletzungen, sowie auf Zutrittskontrollen und die Sicherung von Anlagen beziehen.

(3) Videoüberwachung im Sinne von Absatz 1 ist die Überwachung mittels optisch-elektronischer Einrichtungen.

(4) Abweichend von Absatz 1 Satz 1 ist die Verarbeitung von Beschäftigtendaten durch Videoüberwachung zur Verhütung von Straftaten und schweren Pflichtverletzungen nur zulässig,

1. wenn zu dokumentierende tatsächliche Anhaltspunkte für eine Gefahrenlage in Bezug auf Straftaten oder schwere Pflichtverletzungen vorliegen,
2. soweit die Datenverarbeitung zu diesem Zweck erforderlich ist

und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen.

(5) Bei der Verarbeitung von Beschäftigtendaten durch Videoüberwachung sind Bereiche oder Personen technisch auszublenden oder unkenntlich zu machen, die für die Zweckerfüllung nicht erforderlich sind. Der Arbeitgeber hat eine Videoüberwachung durch geeignete Maßnahmen für die Beschäftigten erkennbar zu machen. Hierzu gehören insbesondere gut sichtbare Piktogramme und Kurz-Informationen gemäß Artikel 13 Absatz 1 Buchstabe a bis d, Absatz 2 Buchstabe a der Verordnung (EU) 2016/679.

(6) Sofern eine Speicherung von nach Absatz 1 oder 4 erhobenen Beschäftigtendaten erforderlich ist, sind diese regelmäßig spätestens nach 72 Stunden zu löschen. Dauert die Speicherung nach Satz 1 länger als 72 Stunden, hat der Arbeitgeber die Gründe für die weitere Speicherung zu dokumentieren.

(7) Eine abweichend von Absatz 1 Satz 2 nicht nur kurzzeitige Verarbeitung von Beschäftigtendaten durch Videoüberwachung ist nur zulässig, soweit sie für einen konkreten Zweck zum Schutz von Leib oder Leben von Beschäftigten oder von Dritten oder zur Wahrung besonders wichtiger betrieblicher oder dienstlicher Interessen erforderlich ist und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung erheblich überwiegen. § 19 Absatz 2 bis 5 gilt entsprechend. Auf eine verdeckte Videoüberwachung findet § 20 entsprechende Anwendung.

(8) Die Verarbeitung besonderer Kategorien von Beschäftigtendaten durch Videoüberwachung ist zulässig, wenn die Voraussetzungen dieser Vorschrift und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 6 vorliegen.

## § 22

### Ortung

(1) Die Verarbeitung von Beschäftigtendaten durch Ortung ist nur zulässig, soweit sie für einen konkreten Zweck zur Durchführung des Beschäftigungsverhältnisses, zur Erfüllung von durch Rechtsvorschrift oder Kollektivvereinbarung festgelegten Pflichten des Arbeitgebers, oder zur Wahrung wichtiger betrieblicher oder dienstlicher Interessen erforderlich ist und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen. Die Verarbeitung nach Satz 1 darf nur kurzzeitig und entweder anlassbezogen oder stichprobenhaft erfolgen. § 18 Absatz 4 und 5 findet auch auf eine Datenverarbeitung nach Satz 1 Anwendung.

(2) Der Zweck einer Verarbeitung nach Absatz 1 kann sich insbesondere beziehen auf den Schutz von Gesundheit und Sicherheit von Beschäftigten, die Verhütung und Aufdeckung von Straftaten oder Pflichtverletzungen, sowie die Koordinierung des wechselnden Einsatzes von Beschäftigten an verschiedenen Orten.

(3) Ortung im Sinne von Absatz 1 ist die Bestimmung des geografischen Standortes von Beschäftigten mit Hilfe einer technischen Einrichtung.

(4) Der Arbeitgeber hat eine Ortung durch geeignete Maßnahmen für die Beschäftigten erkennbar zu machen.

(5) Ergänzend zu den nach § 9 zu treffenden Schutzmaßnahmen muss der Arbeitgeber, sofern er dem oder der Beschäftigten einen Gegenstand, der mit einer Einrichtung im Sinne des Absatzes 3 ausgestattet ist, auch zur privaten Nutzung überlässt, der oder dem Beschäftigten die Möglichkeit einräumen, bei privater Nutzung die Ortung abzuschalten.

(6) Eine abweichend von Absatz 1 Satz 2 nicht nur kurzzeitige Verarbeitung von Beschäftigtendaten durch Ortung ist nur zulässig, soweit sie für einen konkreten Zweck zum Schutz von Leib oder Leben von Beschäftigten oder von Dritten oder zur Wahrung besonders wichtiger betrieblicher oder dienstlicher Interessen erforderlich ist und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung erheblich überwiegen. Der Zweck einer Verarbeitung nach Satz 1 kann sich über § 19 Absatz 2 hinaus insbesondere auf die Koordinierung des wechselnden Einsatzes von Beschäftigten an verschiedenen Orten sowie auf die Nachverfolgbarkeit von Lieferungen beziehen. § 19 Absatz 2 bis 5 gilt entsprechend. Auf eine verdeckte Ortung findet § 20 entsprechende Anwendung.

## § 23

### **Weiterverarbeitung zur Leistungskontrolle**

Der Arbeitgeber darf Beschäftigtendaten, die nach diesem Abschnitt zu einem anderen Zweck, als zur Leistungskontrolle erhoben wurden, nicht zum Zweck der Leistungskontrolle verarbeiten.

## Kapitel 3

### Profiling

## § 24

### **Profiling**

(1) Die Verarbeitung von Beschäftigtendaten durch oder aufgrund eines Profilings, das nicht bereits nach Artikel 22 der Verordnung (EU) 2016/679 ausgeschlossen ist, ist zulässig, soweit dies für einen konkreten Zweck zur Durchführung des Beschäftigungsverhältnisses, zur Erfüllung von durch Rechtsvorschriften oder Kollektivvereinbarungen festgelegten Pflichten des Arbeitgebers oder zur Wahrung wichtiger betrieblicher oder dienstlicher Interessen erforderlich ist und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung erheblich überwiegen.

(2) Der Zweck einer Verarbeitung nach Absatz 1 kann sich insbesondere auf den Einsatz betrieblicher oder dienstlicher Systeme für Weiterbildungs- und Entwicklungsmöglichkeiten auf der Grundlage automatisierter Vorschläge beziehen. Bei der Festlegung des Zwecks der Verarbeitung nach § 3 Absatz 3 muss der Arbeitgeber konkretisieren, welche persönlichen Aspekte bewertet werden sollen, wofür die Ergebnisse verwendet werden sollen und über welchen Zeitraum sich das Profiling erstrecken soll.

(3) Bei der Abwägung der Interessen nach Absatz 1 sind über § 4 hinaus insbesondere folgende Aspekte zu berücksichtigen:

1. die Art der durch das Profiling bewerteten persönlichen Aspekte,
2. der Umfang der Bewertung persönlicher Aspekte der betroffenen Beschäftigten,
3. die Detailtiefe der Ergebnisse hinsichtlich einzelner persönlicher Aspekte der betroffenen Beschäftigten,
4. die möglichen Folgen des Profilings, insbesondere ob auf dem Profiling eine Entscheidung beruhen soll, die gegenüber den betroffenen Beschäftigten rechtliche Wirkung entfaltet oder sie in ähnlicher Weise beeinträchtigt, oder das Profiling der Vorbereitung einer solchen Entscheidung dienen soll sowie mögliche mit dem Profiling verbundene Vorteile für die betroffenen Beschäftigten,
5. das Risiko einer zweckwidrigen Verarbeitung der durch oder aufgrund von Profiling verarbeiteten Beschäftigtendaten sowie mögliche Folgen einer zweckwidrigen Verarbeitung,
6. die Eignung der mathematischen und statistischen Verfahren zur Bewertung der persönlichen Aspekte,
7. das Risiko diskriminierender Ergebnisse,
8. die Nachvollziehbarkeit und Transparenz der mathematischen und statistischen Verfahren und ihrer Ergebnisse für die Beschäftigten und den Arbeitgeber;
9. die Möglichkeiten zur menschlichen Aufsicht und zur Kontrolle der Ergebnisse des Profilings.

(4) Die Verarbeitung von Beschäftigtendaten durch oder aufgrund eines Profilings ist unzulässig,

1. zur Analyse oder Vorhersage von Emotionen von Beschäftigten oder
2. im Fall der Verarbeitung von Beschäftigtendaten aus Kommunikationsvorgängen zur Bewertung der sozialen Beziehungen zwischen Beschäftigten.

(5) Der Arbeitgeber darf Beschäftigtendaten, die zu einem anderen Zweck erhoben wurden, nicht durch ein Profiling zur Bewertung der Arbeitsleistung verarbeiten. Der Arbeitgeber darf Beschäftigtendaten, die durch oder aufgrund eines Profilings zu einem anderen Zweck verarbeitet wurden, nicht zum Zwecke der Bewertung der Arbeitsleistung verarbeiten.

(6) Liegt in dem Profiling zugleich eine Verarbeitung nach § 18 Absatz 1, ist auch § 18 Absatz 4 bis 6 zu beachten. Liegt in dem Profiling zugleich eine Verarbeitung nach § 19 Absatz 1, ist auch § 19 Absatz 3 und 4 zu beachten. Liegt in dem Profiling zugleich eine Verarbeitung nach § 21 Absatz 1, ist auch § 21 Absatz 3 bis 8 zu beachten. Liegt in



dem Profiling zugleich eine Verarbeitung nach § 22 Absatz 1, ist auch § 22 Absatz 4 bis 6 zu beachten.

(7) Der Arbeitgeber hat bei der Auswahl und Umsetzung der geeigneten und besonderen Maßnahmen zum Schutz der Beschäftigten nach § 9 insbesondere auch die Risiken fehlerhafter Ergebnisse zu berücksichtigen. Ergänzend zu den nach § 9 zu treffenden Schutzmaßnahmen sind, soweit es technisch möglich ist und das Erreichen des Zwecks nicht gefährdet wird, zur Vermeidung von Rückschlüssen auf einzelne Beschäftigte aggregierte Ergebnisse für eine Gruppe von Beschäftigten anzuzeigen. Der Arbeitgeber hat eine geeignete menschliche Aufsicht über das Profiling sicherzustellen, insbesondere durch Maßnahmen, die vor einer durch Profiling vorbereiteten Entscheidung, die gegenüber den Beschäftigten rechtliche Wirkung entfaltet oder sie in ähnlicher Weise beeinträchtigt, eine aktive Freigabe oder Ablehnung des Entscheidungsvorschlags durch eine natürliche Person erfordern sowie eine sorgfältige Prüfung der Entscheidung erleichtern.

(8) Die Verarbeitung besonderer Kategorien von Beschäftigtendaten durch oder aufgrund eines Profilings ist zulässig, wenn die Voraussetzungen dieser Vorschrift und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 6 vorliegen.

## § 25

### Informationspflicht bei Profiling

(1) Werden Beschäftigtendaten durch oder aufgrund eines Profilings verarbeitet, so teilt der Arbeitgeber unbeschadet seiner Informationspflichten nach den Artikeln 13 und 14 der Verordnung (EU) 2016/679 den betroffenen Beschäftigten spätestens mit Beginn des Profilings mit:

1. dass ein Profiling stattfindet, die Zwecke der Verarbeitung gemäß § 24 Absatz 2, sowie die Rechtsgrundlage für die Verarbeitung,
2. welche Kategorien von Eingabedaten verwendet werden,
3. ob ein KI-System eingesetzt wird,
4. aussagekräftige Informationen über die beim Profiling involvierte Logik, insbesondere Informationen über die zentralen Bewertungskriterien und ihre Gewichtung zueinander, einschließlich der Art und Weise, wie die personenbezogenen Eingabedaten oder das Verhalten der betroffenen Beschäftigten das Profiling beeinflussen,
5. wenn auf dem Profiling eine Entscheidung beruhen soll, die gegenüber den betroffenen Beschäftigten rechtliche Wirkung entfaltet oder sie in ähnlicher Weise beeinträchtigt, oder das Profiling der Vorbereitung einer solchen Entscheidung dienen soll, umfasst die Informationspflicht aussagekräftige Informationen über die Tragweite und die angestrebten Auswirkungen der Verarbeitung auf die Beschäftigten oder den Beschäftigten; dazu gehören insbesondere,
  - a) der Gegenstand möglicher Entscheidungen und die möglichen Folgen für die Beschäftigte oder den Beschäftigten,
  - b) die Funktion des Profiling im Entscheidungsprozess,
  - c) ob und in welcher Weise eine menschliche Aufsicht gewährleistet werden soll und ein menschliches Eingreifen in den Entscheidungsprozess vorgesehen ist.

6. das Bestehen spezieller Auskunftsrechte nach § 26 sowie der Rechte auf Erklärung und Überprüfung der Entscheidung nach § 27 dieses Gesetzes.

(2) Von den Informationspflichten nach dieser Vorschrift und nach den Artikeln 13 und 14 der Verordnung (EU) 2016/679 kann bei der Verarbeitung von Beschäftigtendaten durch oder aufgrund eines Profilings nicht unter den Voraussetzungen des § 20 Absatz 1 abgewichen werden.

## § 26

### **Auskunftsrecht bei Profiling**

Unbeschadet des Artikel 15 der Verordnung (EU) 2016/679 haben von der Verarbeitung von Beschäftigtendaten durch oder aufgrund eines Profiling betroffene Beschäftigte ein Recht auf Auskunft über folgende Informationen:

1. auf Grundlage welcher personenbezogener Eingabedaten der beschäftigten Person das Profiling durchgeführt wird und die Ergebnisse des Profiling bezüglich persönlicher Aspekte der Beschäftigten;
2. aussagekräftige Informationen über die beim Profiling involvierte Logik, insbesondere über die zentralen Bewertungskriterien und ihre Gewichtung zueinander, einschließlich der Art und Weise, wie die personenbezogenen Eingabedaten oder das Verhalten der betroffenen Beschäftigten das Profiling beeinflussen;
3. wenn auf dem Profiling eine Entscheidung beruhen soll, die gegenüber den betroffenen Beschäftigten rechtliche Wirkung entfaltet oder sie in ähnlicher Weise beeinträchtigt oder das Profiling der Vorbereitung einer solchen Entscheidung dienen soll, aussagekräftige Informationen über die Tragweite und die angestrebten Auswirkungen der Verarbeitung auf die betroffenen Beschäftigten dazu gehören insbesondere,
  - a) der Gegenstand möglicher Entscheidungen und die möglichen Folgen für die betroffenen Beschäftigten
  - b) die Funktion des Profilings im Entscheidungsprozess;
  - c) ob und in welcher Weise eine menschliche Aufsicht gewährleistet werden soll und ein menschliches Eingreifen in den Entscheidungsprozess vorgesehen ist.
4. wenn ein KI-System eingesetzt wird, welche Schutzmaßnahmen nach § 9 Absatz 1 Nummer 11 der Arbeitgeber getroffen hat.

## § 27

### **Erklärung und Überprüfung der Entscheidung**

(1) Hat der Arbeitgeber eine Entscheidung getroffen, die gegenüber den betroffenen Beschäftigten rechtliche Wirkung entfaltet oder sie in ähnlicher Weise beeinträchtigt und beruht die Entscheidung auf einem Profiling oder wurde durch ein Profiling vorbereitet, haben die von der Entscheidung betroffenen Beschäftigten ein Recht auf Erklärung der Entscheidung im Einzelfall. Die Erklärung umfasst insbesondere,

1. wie die personenbezogenen Eingabedaten oder das Verhalten der betroffenen Beschäftigten das Profiling im Einzelfall beeinflusst haben,

2. welche konkrete Funktion das Profiling im Entscheidungsprozess hatte, insbesondere ob und in welcher Form eine menschliche Überprüfung der Entscheidung stattgefunden hat,
3. welche Folgen die Entscheidung für die betroffenen Beschäftigten hat.

(2) Die betroffenen Beschäftigten haben das Recht zum Ergebnis des Profilings und der durch das Profiling vorbereiteten oder auf dem Profiling beruhenden Entscheidung Stellung zu nehmen und vom Arbeitgeber eine Überprüfung der Entscheidung zu verlangen. Der Arbeitgeber muss den Beschäftigten innerhalb von vier Wochen eine begründete Antwort übermitteln. Die Beschäftigten können nach ihrer Wahl anstelle der begründeten Antwort des Arbeitgebers auch eine mündliche Erörterung verlangen.

(3) Auf Verlangen der Beschäftigten hat der Arbeitgeber auch der Interessenvertretung der Beschäftigten die Informationen nach Absatz 1 zu übermitteln. Die Interessenvertretung kann mit Zustimmung der beschäftigten Person nach Absatz 2 Stellung nehmen sowie an der mündlichen Erörterung zwischen dem Arbeitgeber und beschäftigten Person teilnehmen.

## Kapitel 4

### Besondere Verarbeitungssituationen

#### § 28

##### **Datenverarbeitung zu Autorisierungs- und Authentifizierungszwecken**

(1) Die Verarbeitung biometrischer Beschäftigtendaten ist nur zulässig, wenn sie zu Autorisierungs- und Authentifizierungszwecken in besonders sicherheitsrelevanten Bereichen erforderlich ist und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung erheblich überwiegen.

(2) Der Arbeitgeber darf biometrische Beschäftigtendaten, die nach Absatz 1 erhoben wurden, nicht zu anderen Zwecken verarbeiten.

(3) Die Verarbeitung biometrischer Beschäftigtendaten nach Absatz 1 ohne Information der betroffenen Beschäftigten gemäß Artikel 13 Absatz 1 bis 3, 14 Absatz 1 bis 4 der Verordnung (EU) 2016/679 ist ausgeschlossen.

(4) Ergänzend zu den nach § 9 zu treffenden Schutzmaßnahmen sind Verarbeitungsverfahren zu nutzen, die Rückschlüsse auf über die Zugangs- oder Verfügungsberechtigung hinausgehende Informationen, etwa zum Gesundheitszustand, technisch ausschließen. Biometrische Daten sind dezentral und nicht beim Arbeitgeber zu speichern. Die biometrischen Daten haben der alleinigen Zugangs- und Verfügungsberechtigung der beschäftigten Person zu unterliegen; das Speichermedium hat der alleinigen Verfügungsgewalt der beschäftigten Person zu unterliegen. Ist eine dezentrale Speicherung nicht möglich, müssen die Daten, etwa durch Verschlüsselung oder sichere Authentifizierungsverfahren, gegen unbefugten Zugang besonders gesichert werden.

## § 29

### **Betriebliches Eingliederungsmanagement**

(1) Die Verarbeitung von Beschäftigtendaten, einschließlich besonderer Kategorien von Beschäftigtendaten, im Rahmen eines betrieblichen Eingliederungsmanagements gemäß § 167 Absatz 2 des Neunten Buches Sozialgesetzbuch ist nur zulässig, soweit sie

1. zur Prüfung, ob ein betriebliches Eingliederungsmanagement angeboten werden muss,
2. sofern der oder die Beschäftigte im Sinne des § 167 Absatz 2 Satz 1 des Neunten Buches Sozialgesetzbuch zugestimmt hat und dies zur Durchführung eines zielführenden, der Gesundheit und Gesunderhaltung der beschäftigten Person dienenden betrieblichen Eingliederungsmanagements oder
3. zur Erfüllung von durch Kollektivvereinbarung festgelegten Pflichten des Arbeitgebers

erforderlich ist und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen.

(2) Die Verarbeitung von Beschäftigtendaten, deren Verarbeitung nicht nach Absatz 1 erforderlich ist, ist zur Durchführung eines betrieblichen Eingliederungsmanagements nur zulässig, sofern der oder die Beschäftigte gemäß § 5 in die Datenverarbeitung einwilligt. Die Einwilligung hat schriftlich oder elektronisch zu erfolgen. Die Information gemäß § 5 Absatz 4 Satz 2 muss mindestens 24 Stunden vor Abgabe der Einwilligungserklärung erfolgen.

(3) Der Arbeitgeber darf Beschäftigtendaten, die nach den Absätzen 1 und 2 erhoben wurden, nicht zu anderen Zwecken verarbeiten. Satz 1 gilt nicht für das Ergebnis eines betrieblichen Eingliederungsmanagements.

(4) Ergänzend zu den nach § 9 zu treffenden Schutzmaßnahmen dürfen eine Mitwirkung am betrieblichen Eingliederungsmanagement sowie ein Zugriff auf die Akte zum betrieblichen Eingliederungsmanagement nur durch Personen erfolgen, die zur Verschwiegenheit verpflichtet sind. Die Akte zum betrieblichen Eingliederungsmanagement ist getrennt von der Personalakte zu führen; insbesondere dürfen die nach den Absätzen 1 und 2 erhobene Gesundheitsdaten nicht in die Personalakte aufgenommen werden.

## § 30

### **Datenverarbeitung im Konzern**

(1) Die Offenlegung von Beschäftigtendaten durch einen Arbeitgeber, der Teil einer Unternehmensgruppe nach Artikel 4 Nummer 19 der Verordnung (EU) 2016/679 ist, gegenüber einem anderen Unternehmen innerhalb dieser Unternehmensgruppe, zu dem die Beschäftigungsverhältnisse nicht bestehen (Konzernunternehmen) ist zulässig, soweit sie für einen konkreten Zweck zur Durchführung des Beschäftigungsverhältnisses, zur Erfüllung von durch Rechtsvorschrift oder Kollektivvereinbarung festgelegten Pflichten des Arbeitgebers oder zur Wahrung der berechtigten betrieblichen Interessen des Arbeitgebers oder des Konzernunternehmens erforderlich ist und dabei die Interessen des Arbeitgebers oder im zuletzt genannten Fall des Konzernunternehmens an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen.

(2) Der Zweck einer Verarbeitung nach Absatz 1 kann sich insbesondere beziehen auf

1. den unternehmensübergreifenden Einsatz von Beschäftigten, wenn der Konzern in einem Mehrliniensystem organisiert ist, in dem das gegenüber den betroffenen Beschäftigten bestehende fachliche Weisungsrecht durch eine oder einen Beschäftigten des Konzernunternehmens ausgeübt oder diesem übertragen wird,
2. eine durch ein Konzernunternehmen zentralisiert wahrgenommene konzerninterne Verwaltungsaufgabe oder
3. Verwaltungsvorgänge, die konzernweit einheitlich gestaltet werden sollen.

(3) Für die Verarbeitung von im Sinne von Absatz 1 offengelegten Beschäftigtendaten durch ein Konzernunternehmen, das im Sinne des Artikel 4 Nummer 7, erster Halbsatz der Verordnung (EU) 2016/679 für die Datenverarbeitung verantwortlich ist, gelten die Vorschriften dieses Gesetzes, mit Ausnahme von Absatz 1 dieser Vorschrift, entsprechend.

(4) Die Offenlegung besonderer Kategorien von Beschäftigtendaten gegenüber einem anderen Konzernunternehmen ist zulässig, wenn die Voraussetzungen von Absatz 1 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 6 vorliegen.

## Artikel 2

### Folgeänderungen

(1) Das Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 10 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858; 2022 I 1045) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu „§ 26“ wie folgt gefasst:  
„§ 26 (weggefallen)“
2. „§ 26“ wird aufgehoben.

(2) In § 2 Absatz 2 des THW-Gesetzes vom 22. Januar 1990 (BGBl. I S. 118), das zuletzt durch Artikel 2 Absatz 8 des Gesetzes vom 30. März 2021 (BGBl. I S. 402) geändert worden ist, wird die Angabe „§ 26 des Bundesdatenschutzgesetzes“ durch die Angabe „das Beschäftigtendatengesetz“ ersetzt.

(3) In „§ 9 Absatz 3 Satz 3“ des Hinweisgeberschutzgesetzes vom 31. Mai 2023 (BGBl. 2023 I Nr. 140) wird die Angabe „§ 26 Absatz 2 des Bundesdatenschutzgesetzes“ durch die Angabe „§ 5 des Beschäftigtendatengesetzes“ ersetzt.

(4) § 1g Absatz 4 Satz 2 des Straßenverkehrsgesetzes in der Fassung der Bekanntmachung vom 5. März 2003 (BGBl. I S. 310, 919), das zuletzt durch Artikel 16 des Gesetzes vom 2. März 2023 (BGBl. 2023 I Nr. 56) geändert worden ist wird wie folgt geändert:

1. Im ersten Halbsatz wird „§ 26 des Bundesdatenschutzgesetzes“ durch „§ 2 Absatz 2 des Beschäftigtendatengesetzes“ ersetzt.
2. Im zweiten Halbsatz wird „§ 26 des Bundesdatenschutzgesetzes“ durch „das Beschäftigtendatengesetz“ ersetzt.

## **Artikel 3**

### **Inkrafttreten**

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

## **Begründung**

### **A. Allgemeiner Teil**

#### **I. Zielsetzung und Notwendigkeit der Regelungen**

Der Entwurf schafft mehr Rechtsklarheit für Arbeitgeber und Beschäftigte. Regelungen zum Beschäftigtendatenschutz sind derzeit in verschiedenen europäischen und nationalen Regelwerken enthalten und für Beschäftigte und Arbeitgeber weder leicht auffindbar noch leicht zu verstehen. Die zentralen Normen in der Datenschutz-Grundverordnung und im BDSG sind sehr abstrakt formuliert, etwa im Hinblick auf die erforderliche Abwägung der Interessen von Arbeitgebern und Beschäftigten. Konkretisiert und konturiert wurden die Vorschriften bisher im Wesentlichen durch die Rechtsprechung. Mit einem bundesweit einheitlichen und verbindlichen Regelwerk soll daher nun ein klarer Rechtsrahmen geschaffen werden. Anlass dazu gibt auch das Urteil C-34/21 des Europäischen Gerichtshofs vom 30.03.2023 zu der zu § 26 BDSG parallelen Vorschrift in § 23 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes.

Die Schaffung eines eigenständigen Beschäftigtendatengesetzes trägt auch der wachsenden Bedeutung des Schutzes der Privatsphäre im Beschäftigungskontext angesichts der fortschreitenden Digitalisierung Rechnung. Datenbasierte bzw. -getriebene Geschäftsmodelle haben das Potenzial, ein bedeutsamer Wirtschafts- und damit auch Beschäftigungsfaktor zu werden. Eine innovative Datennutzung kann Beschäftigte in ihrer täglichen Arbeit unterstützen und sie von Routinetätigkeiten entlasten, Unternehmen können ihre Arbeitsorganisation effizienter gestalten und neue Geschäftsfelder erschließen. Gleichzeitig führt die Digitalisierung auch zu neuen Herausforderungen im Verhältnis zwischen Beschäftigten und Arbeitgebern. Durch eine vermehrte Nutzung von Beschäftigtendaten entstehen neuartige und umfassendere Möglichkeiten zur Überwachung, die bei Beschäftigten zu Verunsicherung und Zurückhaltung gegenüber technologischen Entwicklungen führen können.

Ein eigenständiges, klar strukturiertes Gesetz ist handhabungsfreundlich und kann Innovation fördern. Gesetzlich klar geregelte Rahmenbedingungen führen zu mehr Rechtssicherheit. Arbeitgebern und Betriebsräten kann die Planung neuer Prozesse sowie die Prüfung und Auswahl neuer Software erleichtert werden und für Beschäftigte werden diese Prozesse besser nachvollziehbar. So werden durch das Gesetz die Vorteile neuer Technologien sowie deren positive Wahrnehmung gefördert und innovationshemmende Rechtsunsicherheit sowie Misstrauen in technologische Entwicklung verhindert bzw. abgebaut.

Der Entwurf für ein Beschäftigtendatengesetz macht von der Öffnungsklausel in Artikel 88 Verordnung 2016/679 Gebrauch, die es den Mitgliedstaaten ermöglicht, „spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext“ vorzusehen. Die Vorschriften umfassen „geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person“ im Sinne von Artikel 88 Absatz 2 Verordnung (EU) 2016/679 und bewegen sich innerhalb der Vorgaben des Europäischen Gerichtshof zum mitgliedstaatlichen Regelungsspielraum im Rahmen von Öffnungsklauseln in der Verordnung (EU) 2016/679. Insbesondere bezwecken die Vorschriften den Schutz der Rechte und Freiheiten der Beschäftigten. Der Entwurf regelt die Zulässigkeit von Eingriffen in Artikel 8 der Charta der Grundrechte der Europäischen Union sowie in das Grundrecht auf informationelle Selbstbestimmung als Ausfluss des Allgemeinen Persönlichkeitsrechts nach Artikel 1 Absatz 1 i.V.m. Artikel 2 Absatz 1 des Grundgesetzes. Dabei werden die verfassungsrechtlichen Schranken beachtet,

insbesondere der allgemeine Grundsatz der Verhältnismäßigkeit von Grundrechtseingriffen.

## II. Wesentlicher Inhalt des Entwurfs

Mit dem Gesetz werden insbesondere die Empfehlungen des vom Bundesministerium für Arbeit und Soziales in der 19. Legislaturperiode eingesetzten interdisziplinären Beirats zum Beschäftigtendatenschutz berücksichtigt, der sich in seinem Abschlussbericht für die Schaffung entsprechender Vorschriften ausgesprochen hat. Der Entwurf kodifiziert zudem in Teilen die geltende Rechtsprechung. Weiterhin werden Vorschriften geschaffen, die den durch die zunehmende Digitalisierung geänderten Arbeitsbedingungen und neuartigen Datenverarbeitungsmöglichkeiten, etwa mittels Künstlicher Intelligenz, Rechnung tragen.

Um flexibel für künftige technische Innovationen zu bleiben, verfolgt das Beschäftigtendatengesetz grundsätzlich einen technologieneutralen Ansatz. Gleichzeitig werden für einzelne Technologien, die speziellen Anforderungen unterliegen oder eine besondere Praxisrelevanz aufweisen (wie z.B. die Videoüberwachung am Arbeitsplatz), spezifische Regelungen geschaffen.

Das Gesetz umfasst im Wesentlichen folgende Regelungen:

- Anwendungsbereich: der persönliche Anwendungsbereich wird, weitestgehend entsprechend der derzeitigen Regelung in § 26 Absatz 8 BDSG, grundsätzlich weit gefasst. Abwägung der Interessen: anhand eines beispielhaften Kriterienkatalogs wird Arbeitgebern eine Hilfestellung für die Durchführung der Interessenabwägung bei Datenverarbeitungen gegeben. Die erstmals ausdrücklich gesetzlich aufgeführten Kriterien erleichtern die bereits jetzt durchzuführende, derzeit lediglich abstrakt formulierte Interessenabwägung.
- Einwilligung: es werden Regelbeispiele dazu eingeführt, wann eine Einwilligung im Beschäftigungskontext freiwillig erfolgen und somit wirksam eingeholt werden kann, etwa bei der Veröffentlichung von Fotos im Intranet.
- Kollektivvereinbarungen: der Entwurf schafft Rechtsklarheit hinsichtlich der Anforderungen an beschäftigtendatenschutzrechtliche Vorschriften in Kollektivvereinbarungen. Diese dürfen insbesondere nicht zu Lasten des Schutzes von Beschäftigten von der Verordnung (EU) 2016/679 oder dem Beschäftigtendatengesetz abweichen.
- Transparenzpflichten beim Einsatz Künstlicher Intelligenz: es werden spezifische Betroffenenrechte für den Einsatz von KI-Systemen durch den Arbeitgeber geschaffen, insbesondere ein Auskunftsrecht über die Funktionsweise des Systems.
- Verwertungsverbot: es wird ein grundsätzliches Verbot der Verwertung datenschutzrechtswidrig verarbeiteter Beschäftigtendaten in Gerichtsverfahren über personelle Maßnahmen geschaffen.
- Datenverarbeitung in der Bewerbungsphase: der Entwurf kodifiziert die ständige Rechtsprechung zum Fragerecht des Arbeitgebers in der Bewerbungsphase und regelt das Auskunftsverlangen nach sensiblen Merkmalen in Anlehnung an § 8 des Allgemeinen Gleichbehandlungsgesetzes. Zudem wird erstmals ausdrücklich geregelt, unter welchen Voraussetzungen der Arbeitgeber Bewerberdaten im Rahmen von Gesundheitsuntersuchungen sowie psychologischen Tests und Untersuchungen verarbeiten darf.



- Überwachungsmaßnahmen: durch differenzierte Regelungen zu Überwachungsmaßnahmen werden Rechtssicherheit und -klarheit geschaffen. Der Entwurf enthält eigene Vorschriften für die besonders eingriffsintensive nicht nur kurzfristige bzw. verdeckte Überwachung sowie für die sehr praxisrelevante Videoüberwachung oder Ortung von Beschäftigten. Durch spezifische Schutzmaßnahmen und insbesondere ein Verbot der Weiterverarbeitung zur Leistungskontrolle wird ein angemessenes Schutzniveau gewährleistet.
- Profiling: es werden konkrete Vorgaben geschaffen, wann ein Profiling im Sinne von Artikel 4 Nummer 4 der Verordnung (EU) 2016/679 in Bezug auf Beschäftigte zulässig ist. Neben einer Auflistung von Abwägungskriterien wird insbesondere ein Verbot des Profilings zur Vorhersage oder Analyse von Emotionen sowie zur Bewertung der sozialen Beziehungen von Beschäftigten anhand von Kommunikationsvorgängen geschaffen.
- Besondere Verarbeitungssituationen: für in der betrieblichen Praxis besonders relevante Situationen, bei denen zudem große Rechtsunsicherheit hinsichtlich der datenschutzrechtlichen Anforderungen herrscht, werden spezifische Vorschriften geschaffen, um die Rechtsanwendung zu erleichtern. Das betrifft die Verarbeitung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken, die Datenverarbeitung im betrieblichen Eingliederungsmanagement, sowie die Konzerndatenverarbeitung.

### **III. Alternativen**

Keine.

### **IV. Gesetzgebungskompetenz**

Die Gesetzgebungskompetenz des Bundes folgt für datenschutzrechtliche Regelungen als Annex aus den jeweiligen Sachkompetenzen der Artikel 73 bis 74 des Grundgesetzes (GG). Die Gesetzgebungskompetenz des Bundes im Bereich des Beschäftigtendatenschutzes beruht vorwiegend auf Artikel 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft) und Artikel 74 Absatz 1 Nummer 12 GG (Arbeitsrecht), sowie auf Artikel 73 Absatz 1 Nummer 8 GG (im Dienste des Bundes stehende Personen). Die Kompetenz für die Änderung des Bundesdatenschutzgesetzes folgt aus Artikel 74 Absatz 1 Nummer 11 und 12 GG in Verbindung mit Artikel 72 Absatz 2 GG. Die Gesetzgebungskompetenz des Bundes für die Änderung des THW-Gesetzes ergibt sich aus Artikel 73 Absatz 1 Nummer 1 GG (auswärtige Angelegenheiten, Schutz der Zivilbevölkerung) und aus Artikel 74 Absatz 1 Nummer 12 GG in Verbindung mit Artikel 72 Absatz 2 GG. Die Gesetzgebungskompetenz für die Änderung des Hinweisgeberschutzgesetzes ergibt sich aus Artikel 74 Absatz 1 Nummer 1 (Strafrecht, gerichtliches Verfahren), Nummer 11 GG und Artikel 74 Absatz 1 Nummer 12 GG in Verbindung mit Artikel 72 Absatz 2 GG. Die Gesetzgebungskompetenz für die Änderung des Straßenverkehrsgesetzes folgt aus Artikel 74 Absatz 1 Nummer 22 (Straßenverkehr) in Verbindung mit Artikel 72 Absatz 2 GG. Soweit der Gesetzentwurf Regelungen betreffend das Recht der Wirtschaft, das Arbeitsrecht, den Straßenverkehr sowie das Strafrecht enthält, ist eine bundesgesetzliche Regelung im Sinne von Artikel 72 Absatz 2 GG zur Wahrung der Rechts- und Wirtschaftseinheit erforderlich, um Unsicherheiten für Arbeitgeber, die in verschiedenen Ländern tätig sind, sowie unzumutbare Behinderungen für den länderübergreifenden Rechtsverkehr zu vermeiden.

## **V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen**

Der Gesetzentwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen vereinbar.

Das Beschäftigtendatengesetz macht, unter Berücksichtigung der übrigen Vorgaben der Verordnung (EU) 2016/679 und insbesondere von deren Artikel 88 Absatz 2, von der Öffnungsklausel in Artikel 88 Absatz 1 der Verordnung (EU) 2016/679 Gebrauch.

## **VI. Gesetzesfolgen**

### **1. Rechts- und Verwaltungsvereinfachung**

Der Gesetzentwurf schafft rechtsklare, konkretere Vorschriften und erleichtert so insbesondere Unternehmen und Behörden die Rechtsanwendung.

### **2. Nachhaltigkeitsaspekte**

Die Wirkungen des Vorhabens entsprechen einer nachhaltigen Entwicklung. Das Vorhaben wirkt sich positiv auf das Nachhaltigkeitsziel "Menschenwürdige Arbeit und Wirtschaftswachstum" aus und berücksichtigt das Prinzip, nachhaltige Entwicklung als Leitprinzip konsequent in allen Bereichen und bei allen Entscheidungen anzuwenden.

Mit dem Beschäftigtendatengesetz wird der Rahmen für einen modernen Beschäftigtendatenschutz geschaffen, der eine Balance zwischen den Interessen der Betriebe und der Beschäftigten zum Ziel hat, indem er die Digitalisierung in den Unternehmen fördert und dabei gleichzeitig den erforderlichen Schutz für die Beschäftigten gewährleistet. Klare, handhabbare Vorschriften für typische Verarbeitungssituationen schaffen Rechtssicherheit für Arbeitgeber und Vertrauen in den Einsatz neuer Technologien bei den Beschäftigten. Ein eigenständiges Beschäftigtendatengesetz stellt einen wichtigen Baustein bei der sozialen Begleitung der digitalen Transformation dar und trägt dazu bei, dass technologische Innovation zu sozialem Fortschritt wird.

### **3. Haushaltsausgaben ohne Erfüllungsaufwand**

Keine.

### **4. Erfüllungsaufwand**

Der Erfüllungsaufwand wurde in Abstimmung mit dem Statistischen Bundesamt ermittelt. Dieser ergibt sich aus einigen Informations- und Dokumentationspflichten des Arbeitgebers sowie aus Auskunftsrechten der betroffenen Beschäftigten. Mit Ausnahme von § 10 Absatz 1 BeschDG, der eine spezifische Auskunftspflicht auf Verlangen für alle Datenverarbeitungen aufgrund eines berechtigten Interesses statuiert, beziehen sich die relevanten Rechte und Pflichten auf KI, Profiling und Videoüberwachung. Insbesondere Datenverarbeitungen im Zusammenhang mit KI bzw. Profiling sind häufig mit tiefen Eingriffen in die informationelle Selbstbestimmung verbunden. Hinzu tritt bei diesen recht neuen Technologien und Methoden, dass ihre Funktionsweise für die Beschäftigten oft eine „Black Box“ ist, die aber, gerade beim Profiling, zu gewichtigen Entscheidungen führen kann. Daher sind erhöhte Transparenzanforderungen in diesem Bereich unerlässlich, um einen angemessenen Grundrechtsschutz zu gewährleisten. Der Erfüllungsaufwand für einzelne Unternehmen wird häufig sehr gering ausfallen. Dies gilt insbesondere für Kleinunternehmen sowie kleine und mittlere Unternehmen, in denen eingriffsintensive Verarbeitungsmaßnahmen wie Profiling nur in wenigen Fällen zur Anwendung kommen dürften.

Erfüllungsaufwand für Bürgerinnen und Bürger

Veränderung des jährlichen Zeitaufwands (in Stunden):	<b>32.451</b>
Veränderung des jährlichen Sachaufwands (in Tsd. Euro):	<b>0</b>
Einmaliger Zeitaufwand (in Stunden):	<b>0</b>
Einmaliger Sachaufwand (in Tsd. Euro):	<b>0</b>

Bei den Bürgerinnen und Bürgern entsteht mit Blick auf die mögliche Wahrnehmung neuer Rechte zusätzlicher jährlicher Erfüllungsaufwand in Höhe von rund 32.451 Stunden. Fast die Hälfte davon mit etwa 16 Tsd. Stunden entfällt dabei auf § 10 Absatz 3 BeschDG (Auskunftsrecht der Beschäftigten über weitere Informationen zum Einsatz von künstlicher Intelligenz). Dies ist bedingt durch die hohe Fallzahl der betroffenen Beschäftigten. Weitere 9 Tsd. Stunden entstehen durch § 27 Absatz 2 (Stellungnahme über eine auf Profiling beruhende Entscheidung und Beantragung von deren Überprüfung). Hier ist neben der Fallzahl der vergleichsweise hohe Zeitaufwand je Fall von 35 Minuten entscheidend. Den drittgrößten Effekt auf den Erfüllungsaufwand der Bürgerinnen und Bürger hat § 26 mit etwa 5 Tsd. Stunden zusätzlich je Jahr, ebenfalls aufgrund der hohen Anzahl der Betroffenen.

Erfüllungsaufwand für Wirtschaft

Veränderung des jährlichen Erfüllungsaufwands (in Tsd. Euro)	<b>3.964</b>
davon Bürokratiekosten aus Informationspflichten (in Tsd. Euro):	<b>3.964</b>
Einmaliger Erfüllungsaufwands (in Tsd. Euro)	<b>3.509</b>
davon Einmalige Informationspflicht (in Tsd. Euro):	<b>3.509</b>

Für die Wirtschaft erhöht sich der jährliche Erfüllungsaufwand um rund 3.964 Euro. Dabei handelt es sich komplett um Bürokratiekosten aus Informationspflichten. Darüber hinaus entsteht der Wirtschaft einmaliger Aufwand von rund 3.509 Euro. Dieser ist komplett der Kategorie „Einmalige Informationspflicht“ zuzuordnen. Ein erheblicher Teil der Änderung beim jährlichen Erfüllungsaufwand mit 1,3 Mio. Euro sowie des einmaligen Erfüllungsaufwands mit 1,9 Mio. sind dabei auf § 10 Absatz 1 des vorliegenden Gesetzentwurfes zurückzuführen. Dabei geht es um die Auskunftspflicht des Arbeitgebers auf Verlangen des betroffenen Beschäftigten über Erwägungen bezüglich der Verarbeitung von Beschäftigten-daten in Fällen des berechtigten Interesses. Der Erfüllungsaufwand wird hier vor allem durch die hohe Fallzahl determiniert. Diese wird bestimmt durch die Anzahl der Arbeitgeber und die Anzahl der Tatbestände der Beschäftigten-datenverarbeitung je Arbeitgeber.

Des Weiteren ändert sich der jährliche Erfüllungsaufwand der Wirtschaft um zusätzliche jeweils etwa 0,4 bis 0,9 Mio. Euro durch § 25 Absatz 1 (Informationspflicht des Arbeitgebers zum Profiling), § 27 Absatz 1 (Recht der Beschäftigten auf Erklärung der Entscheidung aus dem Profiling durch den Arbeitgeber im Einzelfall) und § 27 Absatz 2 (Recht auf erneute Überprüfung einer auf Profiling beruhenden Entscheidung). Ursächlich sind hier jeweils ebenfalls die hohen Fallzahlen bzw. teilweise auch Zeitaufwände je Fall. § 25 Absatz 1 und § 21 Absatz 4 führen fallzahlbedingt auch zu hohem einmaligem Erfüllungsaufwand von jeweils ca. 0,8 Mio. Euro.

Erfüllungsaufwand für Verwaltung

Veränderung des jährlichen Erfüllungsaufwands (in Tsd. Euro):	<b>32</b>
davon auf Bundesebene (in Tsd. Euro):	<b>32</b>
davon auf Landesebene (in Tsd. Euro):	<b>0</b>
Einmaliger Erfüllungsaufwand (in Tsd. Euro):	<b>0</b>

davon auf Bundesebene (in Tsd. Euro):	0
davon auf Landesebene (in Tsd. Euro):	0

Für die Verwaltung steigt der jährliche Erfüllungsaufwand um rund 32 Tsd.Euro. Der jährliche Aufwand entfällt komplett auf den Bund.

Auch die Bundesverwaltung fungiert als Arbeitgeber, die Fallzahl (Anzahl der Behörden und Sozialversicherungen) ist hier aber deutlich geringer als bei der Wirtschaft. Am bedeutendsten in der Relation ist hier § 27 Absatz 1 (Recht der Beschäftigten auf Erklärung der Entscheidung aus dem Profiling durch den Arbeitgeber im Einzelfall) mit etwa 19 Tsd. Euro zusätzlichem jährlichen Erfüllungsaufwand. Dies liegt an der Kombination aus vergleichsweise hoher Fallzahl und hohem Zeitaufwand je Fall von rund 30 Minuten.

### 5. Weitere Kosten

Weitere Kosten, insbesondere Auswirkungen auf Einzelpreise und das Preisniveau, sind nicht zu erwarten.

### 6. Weitere Gesetzesfolgen

Auswirkungen für Verbraucherinnen und Verbraucher und Auswirkungen von gleichstellungspolitischer oder demografischer Bedeutung sind nicht zu erwarten. Der Gesetzentwurf fördert gleichwertige Lebensverhältnisse, indem durch klare, bundesrechtliche Regelungen einer unterschiedlichen Auslegung und Rechtsanwendung in den Ländern in Bezug auf gleiche Lebenssachverhalte entgegengewirkt wird.

## VII. Befristung; Evaluierung

Eine Befristung der in dem Entwurf vorgesehenen Rechtsänderungen kommt nicht in Betracht. Die Regelungen sind darauf angelegt, den angemessenen Schutz der Persönlichkeitsrechte von Beschäftigten auf Dauer zu gewährleisten.

Das Gesetz wird nach 5 Jahren nach Inkrafttreten evaluiert. Dabei soll überprüft werden, ob und inwieweit das Gesetz die Ziele, mehr Rechtssichersicherheit für Arbeitgeber und Beschäftigte sowie Stärkung der Persönlichkeitsrechte von Beschäftigten, erreicht. Als Indikator für die Zielerreichung dient die Wahrnehmung in diesen Punkten (vorher vs. nachher) auf Seiten aller Betroffenen, namentlich der Beschäftigten, der Arbeitgeber, der Beschäftigtenvertretungen und der Datenschutzaufsichtsbehörden. Die Datengrundlage bilden noch zu erhebende Befragungsdaten zu dieser Thematik in den Betroffenengruppen.

## B. Besonderer Teil

### Zu Artikel 1 (Gesetz zur Stärkung eines fairen Umgangs mit Beschäftigtendaten und für mehr Rechtssicherheit für Arbeitgeber und Beschäftigte in der digitalen Arbeitswelt)

#### Zu Teil 1 (Allgemeiner Teil)

#### Zu Kapitel 1 (Allgemeine Bestimmungen)

Dieses Gesetz schafft ein grundlegendes und weitestgehend umfassendes Regelwerk für die Verarbeitung von personenbezogenen Daten von Beschäftigten durch den Arbeitgeber

im Beschäftigungskontext. Durch klare Regelungen soll ein angemessener Ausgleich zwischen den berechtigten Interessen der Beschäftigten am Schutz ihres Persönlichkeitsrechts und dem Informationsbedürfnis des Arbeitgebers hergestellt werden.

Es handelt sich um spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung von Beschäftigtendaten im Beschäftigungskontext im Sinne von Artikel 88 der Verordnung (EU) 2016/679. Das Gesetz sieht geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Beschäftigten im Sinne von Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 vor. Insbesondere sind im Rahmen der Verarbeitung von Beschäftigtendaten nach diesem Gesetz grundsätzlich besondere Schutzmaßnahmen nach § 9 vorzusehen und bei der Abwägung der Interessen stets die in § 4 vorgesehenen Abwägungskriterien zu berücksichtigen.

## **Zu § 1 (Anwendungsbereich)**

### **Zu Absatz 1**

Die Vorschrift bestimmt den Anwendungsbereich des Gesetzes. Es gilt für Verarbeitungen von Beschäftigtendaten, das heißt personenbezogener Daten von Beschäftigten, und enthält spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung von Beschäftigtendaten im Beschäftigungskontext im Sinne von Artikel 88 der Verordnung (EU) 2016/679. Es gelten die Begriffsbestimmungen der Verordnung (EU) 2016/679, soweit dieses Gesetz keine eigenen Begriffsbestimmungen vorsieht. Nach Artikel 4 Nummer 1 und 2 der Verordnung (EU) 2016/679 bezeichnet der Ausdruck „personenbezogene Daten“ „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“; und der Ausdruck „Verarbeitung“ „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten 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, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“.

Für die Eröffnung des sachlichen Anwendungsbereiches dieses Gesetzes ist ein funktionaler Zusammenhang mit dem Beschäftigungsverhältnis entscheidend. Dies trägt der Besonderheit des Beschäftigungsverhältnisses als Über-/Unterordnungsverhältnis und der daraus resultierenden Abhängigkeit und Schutzbedürftigkeit der Beschäftigten Rechnung. Der im Gesetz verwendete Begriff des Beschäftigungsverhältnisses bezeichnet das Rechtsverhältnis zu den in § 2 Absatz 2 legal definierten Beschäftigten und ist nicht identisch mit dem im Sozialversicherungsrecht verwendeten Begriff des Beschäftigungsverhältnisses. Erfasst werden Verarbeitungen von Beschäftigtendaten zu sämtlichen Zwecken, die im Zusammenhang mit dem Beschäftigungskontext stehen. Die in Artikel 88 Absatz 1 der Verordnung (EU) 2016/679 aufgezählten Verarbeitungszwecke sind lediglich beispielhaft zu verstehen (vgl. EuGH, Urteil vom 30.03.2023, C-34/21 Rn. 63). Der Anwendungsbereich ist auch eröffnet, wenn eine Verarbeitung im Zusammenhang mit einem potentiellen Beschäftigungsverhältnis oder einem bereits beendeten Beschäftigungsverhältnis erfolgt. Das Gesetz ist anwendbar auf Verarbeitungen durch den Arbeitgeber. Der Begriff des Arbeitgebers ist für dieses Gesetz in § 2 Absatz 3 bestimmt. Entscheidend für die Anwendung des Gesetzes ist, dass der Arbeitgeber Verantwortlicher im Sinne von Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 für die Verarbeitung von Beschäftigtendaten ist. Das Gesetz erfasst daher

zum Beispiel auch die Verarbeitung von Beschäftigtendaten durch interne Betriebsärztinnen und Betriebsärzte oder nach § 79a Satz 2 Betriebsverfassungsgesetz durch den Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben. Ebenso ist dieses Gesetz im Fall einer Auftragsverarbeitung nach Artikel 28 der Verordnung (EU) 2016/679 anwendbar, wenn eine Verarbeitung nach Absatz 1 im Auftrag des Arbeitgebers als Verantwortlichen erfolgt.

Der zweite Halbsatz legt die Anwendbarkeit des Gesetzes auf öffentliche Stellen des Bundes sowie nichtöffentliche Stellen fest. Das Gesetz findet Anwendung auf öffentliche Stellen des Bundes im Sinne von § 2 Absatz 1 und 3 Bundesdatenschutzgesetz. Danach sind öffentliche Stellen des Bundes die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, der Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nichtöffentlicher Stellen als öffentliche Stellen des Bundes, wenn sie über den Bereich eines Landes hinaus tätig werden oder dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht. In diesen Fällen gilt der Dienstherr als Arbeitgeber im Sinne dieses Gesetzes. Zum Anwendungsbereich können auch gemeinsame Einrichtungen nach § 44b des Zweiten Buches Sozialgesetzbuch im Verhältnis zu den Beamtinnen und Beamten sowie Arbeitnehmerinnen und Arbeitnehmern der Bundesagentur für Arbeit, denen gemäß § 44b Absatz 1 Satz 4 SGB II Tätigkeiten in den gemeinsamen Einrichtungen zugewiesen worden sind, gehören.

Das Gesetz findet auf sämtliche nichtöffentliche Stellen im Sinne von § 2 Absatz 4 und 5 Bundesdatenschutzgesetz Anwendung. Dies umfasst grundsätzlich natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts. Der räumliche Anwendungsbereich bei der Verarbeitung durch nichtöffentliche Arbeitgeber ergibt sich nach Nummer 2 aus der Regelung des § 1 Absatz 4 Bundesdatenschutzgesetz. Danach sind die Regelungen anwendbar, wenn die Datenverarbeitung einen Inlandsbezug aufweist, zum Beispiel wenn der Arbeitgeber oder Auftragsverarbeiter personenbezogene Beschäftigtendaten im Inland verarbeitet oder die Verarbeitung im Rahmen der Tätigkeiten einer inländischen Niederlassung des Arbeitgebers oder Auftragsverarbeiters erfolgt.

Die als Körperschaften des öffentlichen Rechts organisierten Kirchen fallen nicht unter den Anwendungsbereich des Gesetzes. Die Geltung von Artikel 91 der Verordnung (EU) 2016/679 wird durch dieses Gesetz nicht beschränkt. Kircheneigene Datenschutzvorschriften, die im Einklang mit Artikel 91 der Verordnung (EU) 2016/679 stehen, bleiben innerhalb der Grenzen des verfassungsrechtlich verbürgten Selbstbestimmungsrechts der Religionsgemeinschaften anwendbar.

### **Zu Absatz 2**

Die Vorschrift legt fest, dass das Gesetz entsprechend anzuwenden ist, wenn Dritte in gemeinsamer Verantwortlichkeit im Sinne von Artikel 26 der Verordnung (EU) 2016/679 Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses verarbeiten. Auch in diesem Fall bestehen ein funktionaler Zusammenhang mit dem Beschäftigungsverhältnis und ein gesteigertes Schutzbedürfnis der Beschäftigten.

### **Zu Absatz 3**

Absatz 3 legt fest, dass das Gesetz für die ganz oder teilweise automatisierte Verarbeitung von Beschäftigtendaten sowie für die nichtautomatisierte Verarbeitung von Beschäftigtendaten gilt. Damit findet das Gesetz auch dann Anwendung, wenn Beschäftigtendaten, einschließlich besonderer Kategorien von Beschäftigtendaten, verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Absatz 3 geht dabei von der Beschreibung des Anwendungsbereichs in Artikel 2 Absatz 1 der Verordnung

(EU) 2016/679 aus und führt die auch schon zuvor im nationalen Recht geltende Anwendungsbereichserweiterung für den Beschäftigtendatenschutz in § 26 Absatz 7 BDSG a. F. fort. Die Regelungen des Gesetzes gelten danach für jede Form der Verarbeitung, sei es automatisiert oder nichtautomatisiert, und somit beispielsweise auch für Tor- und Taschenkontrollen oder mündliche Fragen im Bewerbungsgespräch.

#### **Zu Absatz 4**

Absatz 4 bestimmt das Verhältnis dieses Gesetzes zu spezialgesetzlichen Vorschriften über den Schutz von Beschäftigtendaten. Solche Vorschriften gehen den Vorschriften dieses Gesetzes vor und gelten im Rahmen ihrer Zweckbestimmung jeweils als abschließend. Das heißt, dass im Fall spezialgesetzlicher Verarbeitungsgrundlagen die Zulässigkeit einer Datenverarbeitung nicht zusätzlich nach diesem Gesetz geprüft werden muss. Dies betrifft beispielsweise spezialgesetzliche Verarbeitungsgrundlagen im Infektionsschutzgesetz. Wenn die spezialgesetzlichen Regelungen zudem ein umfassendes und abschließendes Regelsystem über den Umgang mit Beschäftigtendaten in einem bestimmten Kontext oder für einen bestimmten Zweck enthalten, findet dieses Gesetz insofern keine Anwendung. Dies gilt etwa für die spezifischen Vorschriften zu Personalaktendaten im Beamtenrecht.

Satz 2 trägt der Möglichkeit Rechnung, dass bereichsspezifische Datenschutzvorschriften unter Umständen nicht abschließend sind und vermeidet so, durch Anwendbarkeit dieses Gesetzes in derlei Fällen, Regelungslücken. Eine nicht abschließende Regelung oder das Schweigen eines Spezialgesetzes führt dazu, dass die Vorschriften dieses Gesetzes anzuwenden sind. Bedeutsam ist dies beispielsweise auch für die nach diesem Gesetz zu treffenden Schutzmaßnahmen oder das Beweisverwertungsverbot.

#### **Zu Absatz 5**

Absatz 5 stellt klar, dass das Bundesdatenschutzgesetz subsidiär anwendbar bleibt, soweit dieses Gesetz nichts anderes bestimmt, indem speziellere Vorschriften geschaffen, oder Vorschriften des Bundesdatenschutzgesetzes ausdrücklich ausgeschlossen oder modifiziert werden. Dies entspricht der lückenfüllenden Auffangfunktion des Bundesdatenschutzgesetzes.

### **Zu § 2 (Begriffsbestimmungen)**

#### **Zu Absatz 1**

Mit Beschäftigtendaten im Sinne des Gesetzes sind ausschließlich personenbezogene Daten (gemäß Artikel 4 Nummer 1 der Verordnung (EU) 2016/679) von Beschäftigten gemeint.

#### **Zu Absatz 2**

Absatz 2 definiert den Kreis der Beschäftigten, auf den die Regelungen dieses Gesetzes Anwendung finden, und übernimmt weitgehend die Begriffsbestimmung von Beschäftigten im Datenschutzrecht aus § 26 Absatz 8 BDSG a.F. Die Regelung stellt entsprechend dem Schutzzweck des Gesetzes klar, dass zum Begriff des Beschäftigten nicht nur Arbeitnehmerinnen und Arbeitnehmer im engeren Sinn gehören. Dem Gesetz liegt ein funktionaler Beschäftigtenbegriff zugrunde. Nicht erfasst sind Beamtinnen und Beamte der Länder und Kommunen. Als Beschäftigte im Sinne dieses Gesetzes gelten auch solche Personen, die mit Blick auf die Verarbeitung ihrer Daten durch Arbeit- oder Auftraggeber, zu denen ein Abhängigkeitsverhältnis besteht, vergleichbar schutzbedürftig wie Arbeitnehmerinnen und Arbeitnehmer im engeren Sinn sind. Dies gilt zum Beispiel, wie auch nach bisheriger Rechtslage, nach Nummer 7 für Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind. Die vergleichbare Schutzbedürftigkeit ergibt sich in diesem Fall aus der wirtschaftlichen Abhängigkeit vom Auftraggeber,

aus der ein besonderes Schutzbedürfnis auch im Hinblick auf die Verarbeitung personenbezogener Daten resultiert. Über § 26 Absatz 8 BDSG a.F. hinaus werden nach Nummer 2 Praktikantinnen und Praktikanten ausdrücklich in den Anwendungsbereich einbezogen. Dies gilt unabhängig davon, ob es sich um Pflichtpraktika oder freiwillige Praktika im Sinne des § 26 Berufsbildungsgesetzes handelt, da mit Blick auf die Verarbeitungssituation in beiden Fällen eine vergleichbare Schutzbedürftigkeit besteht.

### **Zu Absatz 3**

Absatz 33 definiert den Begriff des Arbeitgebers im Sinne dieses Gesetzes. Arbeitgeber sind danach öffentliche und nichtöffentliche Stellen nach § 1 Absatz 1 Nummer 1 und 2, die Personen nach Absatz 1 beschäftigen. In Satz 2 wird für die Einbeziehung der Personen, die nicht zu den Arbeitnehmerinnen und Arbeitnehmern im engeren Sinn gehören, klargestellt, wer im Verhältnis zu den einzelnen Beschäftigten auch als Arbeitgeber im Sinne dieses Gesetzes gilt.

### **Zu Absatz 4**

Kollektivvereinbarungen im Sinne des Gesetzes sind neben Tarifverträgen sowie Betriebs- und Dienstvereinbarungen auch gleichwertige kollektive Verträge.

### **Zu Absatz 5**

Die Definition von KI-Systemen entspricht der der Verordnung (EU) 2024/1689.

### **Zu Absatz 6**

Besondere Kategorien von Beschäftigtendaten werden als besondere Kategorien personenbezogener Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 von Beschäftigten legaldefiniert.

## **Zu Kapitel 2 (Grundlagen der Datenverarbeitung)**

### **Zu § 3 (Grundlagen der Datenverarbeitung )**

Die Regelung stellt eine spezifischere Vorschrift zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung von Beschäftigtendaten im Beschäftigungskontext nach Artikel 88 der Verordnung (EU) 2016/679 dar. Sie sieht mit Blick auf das im Beschäftigungskontext bestehende Abhängigkeitsverhältnis und die daraus resultierende Schutzbedürftigkeit der Beschäftigten abgestufte Anforderungen für die Verarbeitung von Beschäftigtendaten durch den Arbeitgeber zu sämtlichen Zwecken vor und spezifiziert daher, insbesondere in Verbindung mit den besonderen Kriterien zur Prüfung der Erforderlichkeit nach § 4, alle Rechtmäßigkeitstatbestände des Artikel 6 Absatz 1 Unterabsatz 1 der Verordnung (EU) 2016/679 für die Verarbeitungssituation im Beschäftigungskontext. Zudem spezifiziert die Vorschrift in Absatz 3 die Anforderungen an die Festlegung des konkreten Zwecks der Verarbeitung durch den Arbeitgeber für alle Verarbeitungen nach diesem Gesetz und damit für alle Rechtmäßigkeitstatbestände des Artikel 6 Absatz 1 Unterabsatz 1 der Verordnung (EU) 2016/679. Das Gesetz sieht geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Beschäftigten im Sinne von Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 vor. Neben den spezifischen Anforderungen an die Rechtmäßigkeit einer Verarbeitung im Beschäftigungskontext sind insbesondere auch geeignete und besondere Schutzmaßnahmen nach § 9 vorzusehen.



## **Zu Absatz 1**

Absatz 1 regelt, unter welchen Voraussetzungen Beschäftigtendaten vor, im und nach dem Beschäftigungsverhältnis verarbeitet werden dürfen. Die Verarbeitung muss zu einem konkreten Zweck, der unter einen der aufgeführten Tatbestände fällt, erforderlich sein. Das Tatbestandsmerkmal der Erforderlichkeit verlangt die Durchführung einer umfassenden Verhältnismäßigkeitsprüfung. Die konkrete Verarbeitung muss zur Verfolgung des Zwecks geeignet und erforderlich sein, das heißt, es darf kein mildereres, gleich effektives Mittel zur Verfügung stehen, um das vom Arbeitgeber verfolgte Ziel zu erreichen. Zusätzlich muss die Verarbeitung angemessen sein und eine Interessenabwägung vorgenommen werden.

Die Regelung konkretisiert die verschiedenen Rechtmäßigkeitstatbestände des Artikel 6 Absatz 1 Unterabsatz 1 der Verordnung (EU) 2016/679 für die besondere Situation des Beschäftigungsverhältnisses dahingehend, dass sich die Prüfung der Erforderlichkeit bei allen aufgezählten Rechtmäßigkeitstatbeständen nach den Maßstäben dieses Gesetzes richtet und sich die Risikoverteilung bei der im Rahmen der Prüfung der Erforderlichkeit vorzunehmenden umfassenden Abwägung der Interessen differenziert nach dem jeweiligen Rechtmäßigkeitstatbestand bestimmt. Das Tatbestandsmerkmal der Erforderlichkeit beinhaltet eine umfassende Abwägung der Interessen des Arbeitgebers an der Verarbeitung und der Interessen der Beschäftigten an dem Ausschluss der Verarbeitung. Widerstreitende Grundrechtspositionen sind zur Herstellung praktischer Konkordanz abzuwägen und zu einem schonenden Ausgleich zu bringen. In Verbindung mit § 4 wird das Merkmal der Erforderlichkeit durch spezifische Abwägungskriterien weiter konturiert. Darüber hinaus trifft Absatz 1 eine spezifizierende Regelung zur Risikoverteilung bei der Prüfung der Erforderlichkeit einer Verarbeitung von Beschäftigtendaten im Zusammenhang mit dem Beschäftigungsverhältnis und unterscheidet dabei zwischen den jeweiligen Rechtmäßigkeitstatbeständen. Bei der Verarbeitung von Beschäftigtendaten zur Entscheidung über die Begründung, zur Durchführung oder zur Beendigung eines Beschäftigungsverhältnisses (Nummer 1) sowie zur Wahrung eines berechtigten betrieblichen oder dienstlichen Interesses des Arbeitgebers (Nummer 7) muss der Arbeitgeber als positive Voraussetzung der Rechtmäßigkeit einer Verarbeitung im Beschäftigungskontext darlegen, dass die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen. Bei Verarbeitungen nach diesen Tatbeständen wirkt sich die im Beschäftigungsverhältnis bestehende Abhängigkeit der Beschäftigten typischerweise besonders stark aus, weshalb für ein angemessenes Schutzniveau die Risikoverteilung grundsätzlich umgekehrt wird. Bei den übrigen Tatbeständen (Nummern 2 bis 6) gelten die allgemeinen Grundsätze, nach denen bei einer zulässigen Verarbeitung die schutzwürdigen Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung nicht gegenüber den Interessen des Arbeitgebers an der Verarbeitung überwiegen dürfen. Im Rahmen der erforderlichen Abwägung können die spezifischen Abwägungskriterien des § 4 je nach Relevanz für den konkreten Fall herangezogen werden.

Soweit der Arbeitgeber die Rechtsgrundlage einer Verarbeitung anzugeben hat, sollte neben der Vorschrift dieses Gesetzes der in der Verordnung (EU) 2016/679 jeweils einschlägige Tatbestand mitangegeben werden.

Nummer 1 konkretisiert Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe b der Verordnung (EU) 2016/679. Darunter sind alle konkreten Zwecke zu fassen, die sich auf die Erfüllung des Arbeitsvertrages, bzw. des Vertrages, der das Beschäftigungsverhältnis regelt, beziehen. Ebenso fallen darunter Zwecke, die sich auf die Einstellung beziehen, etwa die Kontaktaufnahme zu Personen, die sich beworben haben, um sie zu einem Bewerbungsgespräch einzuladen. Ebenfalls erfasst sind konkrete Zwecke zur Beendigung eines Beschäftigungsverhältnisses, etwa zu dessen Abwicklung.

Die Tatbestände in Nummer 2, 3 und 4 stellen für Verarbeitungen nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe c der Verordnung (EU) 2016/679 klar, dass die spezifischen Anforderungen an die Verarbeitung nach diesem Gesetz - etwa an die Prüfung der Erforderlichkeit, die Zweckfestlegung oder Schutzmaßnahmen - grundsätzlich auch für diesen Rechtmäßigkeitstatbestand gelten. Dass eine rechtliche Pflicht vorliegt und der Arbeitgeber die Daten deshalb grundsätzlich verarbeiten muss, ist im Rahmen der Interessenabwägung nach § 4 Nummer 1 Buchstabe a entsprechend zu berücksichtigen. Die Pflicht zur Durchführung einer Interessenabwägung stellt nicht in Frage, dass sich der Arbeitgeber rechtstreuhaltend verhalten muss und kann. Zu prüfen kann jedoch etwa der Umfang und die Art und Weise der Datenverarbeitung sein, da diese nur insoweit zulässig sein kann, wie die Datenverarbeitung zur Erfüllung der rechtlichen Pflicht erforderlich ist. Ist dies in der jeweiligen Rechtsvorschrift nicht vorgegeben, könnte beispielsweise zu prüfen sein, ob die rechtliche Pflicht in bestimmten Fällen bereits dadurch erfüllt werden kann, dass anonymisierte oder pseudonymisierte Daten verarbeitet werden.

Wenn eine Rechtsvorschrift konkret vorgibt, welche Daten zu welchem Zweck in welcher Weise zu verarbeiten sind (vgl. Artikel 6 Absatz 3 Satz 3 der Verordnung (EU) 2016/679), handelt es sich um eine abschließende speziellere Norm, die nach § 1 Absatz 4 vorrangig anzuwenden ist. Die Prüfung der Zulässigkeit einer davon erfassten Datenverarbeitung ist dann nicht mehr nach § 3 und § 4 dieses Gesetzes zu prüfen.

Nummer 3 und 4 stellen klar, dass auch Kollektivvereinbarungen Regelungen zur Verarbeitung von Beschäftigtendaten enthalten können, etwa wenn es um die Verarbeitung zur Erfüllung einer Verpflichtung aus diesen Vereinbarungen geht. Kollektivvereinbarungen sind als Tarifverträge, Betriebs- oder Dienstvereinbarungen oder gleichwertige kollektive Verträge legaldefiniert. § 7 ist zu beachten. Darüber hinaus können Regelungsinhalte von Kollektivvereinbarungen auch im Rahmen anderer Tatbestände dieser Vorschrift von Bedeutung sein, etwa wenn sie Bestimmungen zur Durchführung von Beschäftigungsverhältnissen näher ausgestalten.

Nummer 5 stellt für Verarbeitungen nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe d der Verordnung (EU) 2016/679 klar, dass die spezifischen Anforderungen an die Verarbeitung nach diesem Gesetz - etwa an die Prüfung der Erforderlichkeit, die Zweckfestlegung oder Schutzmaßnahmen - auch für diesen Rechtmäßigkeitstatbestand gelten. Für eine Verarbeitung zum Schutz von natürlichen Personen kann sich der Anwendungsbereich des Tatbestandes von Nummer 5 mit den Anwendungsbereichen insbesondere der Nummern 1, 2, 6 und 7 teilweise überschneiden. Grundsätzlich ist der Rechtmäßigkeitstatbestand Nummer 5 nachrangig anzuwenden. Insbesondere darf eine Verarbeitung aufgrund eines lebenswichtigen Interesses einer anderen natürlichen Person nur dann auf Nummer 5 in Verbindung mit Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe d der Verordnung (EU) 2016/679 gestützt werden, wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann (vgl. Erwägungsgrund 46 Satz 2 der Verordnung (EU) 2016/679). Der Schutz eines lebenswichtigen Interesses ist im Rahmen der Interessenabwägung nach § 4 Nummer 1 entsprechend hoch zu gewichten.

Nummer 6 stellt für Verarbeitungen von Beschäftigtendaten insbesondere durch öffentliche Stellen nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e für die Verarbeitung klar, dass die spezifischen Anforderungen an die Verarbeitung nach diesem Gesetz - etwa an die Prüfung der Erforderlichkeit, die Zweckfestlegung oder Schutzmaßnahmen - auch für diesen Rechtmäßigkeitstatbestand gelten. Wenn eine gesetzliche Regelung detailliert vorgibt, welche Daten zu welchem Zweck in welcher Weise durch öffentliche Stellen zu verarbeiten sind (vgl. Artikel 6 Absatz 3 Satz 3 der Verordnung (EU) 2016/679), handelt es sich um eine spezialgesetzliche Norm, die nach § 1 Absatz 4 vorrangig anzuwenden ist.

Nummer 7 konkretisiert Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e und f der Verordnung (EU) 2016/679 und stellt klar, dass im Beschäftigungskontext eine Verarbeitung, die nicht bereits zur Vertragsdurchführung nach Nummer 1 erforderlich ist, zu einem konkreten

Zweck zur Wahrung eines berechtigten Interesses erfolgen kann, wenn es sich um ein berechtigtes betriebliches oder dienstliches Interesse handelt und die Interessen des Arbeitgebers überwiegen. Berechtigte betriebliche Interessen können beispielsweise den Verkauf eines Unternehmens oder den Schutz des Eigentums des Arbeitgebers betreffen. Berechtigtes betriebliches Interesse des Arbeitgebers kann auch der Schutz des Eigentums von Kunden des Betriebes sein. Berechtigte dienstliche Interessen im Sinne der Vorschrift sind als äquivalenter Begriff für öffentliche Arbeitgeber zu verstehen und können beispielsweise fiskalische Interessen betreffen, wenn die Datenverarbeitung nicht der Aufgabenerfüllung (Nummer 6) dient.

### **Zu Absatz 2**

Absatz 2 konkretisiert, auf welche exemplarischen Bereiche sich die im Einzelfall unter Beachtung von Absatz 3 konkret festzulegenden Verarbeitungszwecke beziehen können. Der gesetzgeberischen Wertung lässt sich entnehmen, dass die in Satz 1 aufgezählten Ziele grundsätzlich als legitime Interessen für die Verarbeitung von Beschäftigtendaten nach diesem Gesetz anerkannt sind. Die weiteren Voraussetzungen für die Zulässigkeit einer Verarbeitung nach Absatz 1 bleiben unberührt und sind anhand des konkreten Zweckes zu prüfen.

Verarbeitungszwecke können sich zum Beispiel auf Zwecke der Planung und der Organisation der Arbeit, des Managements, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Umwelt- und Klimaschutzes oder des Schutzes des Eigentums der Arbeitgeber, der Beschäftigten oder der Kunden sowie die Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen beziehen. Zu den individuellen und kollektiven Rechten der Beschäftigten gehört insbesondere die Teilnahme an Wahlen der Interessenvertretungen.

Die beispielhafte Aufzählung der abstrakten Oberbegriffe im Gesetz entbindet nicht von der Pflicht nach Absatz 3, die Zwecke konkret festzulegen. Die Aufzählung ist nicht abschließend. Sie soll den Rechtsanwenderinnen und Rechtsanwendern eine Hilfestellung bei der Zweckbestimmung bieten.

Satz 2 stellt klar, dass bestimmte Zwecke für die Verarbeitung von Beschäftigtendaten im Beschäftigungskontext nicht zulässig sind. Eine Verarbeitung zu diesen Zwecken ist stets ausgeschlossen. Dies gilt zum Beispiel für Zwecke der Verhinderung oder Einschränkung der Ausübung von gesetzlichen Rechten der Beschäftigten, insbesondere der Koalitionsfreiheit. Auch Zwecke der Verhinderung oder Einschränkung der Ausübung von gesetzlichen Rechten der Interessenvertretungen der Beschäftigten sind ausgeschlossen. Aufgrund der besonderen Bedeutung im Beschäftigungskontext wird in Satz 3 klarstellend und beispielhaft hervorgehoben, dass auch die Vorhersage der Ausübung bestimmter Rechte per se unzulässig ist. Der Begriff der Vorhersage meint eine zielgerichtete Bewertung von Daten dadurch, dass die Information allein oder in Kombination mit anderen interpretiert wird, um künftiges Verhalten oder Entscheidungen in bestimmten Situationen zu prognostizieren. Nach Satz 3 ist die Bewertung von Daten mit dem Ziel, die Ausübung der Koalitionsfreiheit durch Beschäftigte zu prognostizieren, etwa die Wahrscheinlichkeit zu errechnen, dass eine beschäftigte Person eine Koalition gründet, ihr beitrifft, in ihr verbleibt oder an einer geschützten Koalitionstätigkeit teilnimmt, ausgeschlossen.

### **Zu Absatz 3**

Der Zweck einer Verarbeitung muss so konkret festgelegt werden, dass er Aufschluss darüber gibt, zu welchem bestimmten Zweck welche Verarbeitung erfolgt, und es somit ermöglicht, dass die Einhaltung des Rechts bewertet werden kann. Anhand des konkreten Zweckes ist die Einhaltung dieses Gesetzes und der Verordnung (EU) 2016/679 zu prüfen. Absatz 3 regelt Vorgaben an die Festlegung des Zwecks ohne eine zusätzliche Dokumentati-

onspflicht über die Regelungen der Verordnung (EU) 2016/679 hinaus zu statuieren. Vielmehr können sich die Vorgaben an eine konkrete Zweckfestlegung an unterschiedlichen Stellen auswirken. Der nach Absatz 3 konkret festgelegte Zweck wird zum Maßstab bei der Prüfung der Erforderlichkeit einer Verarbeitung nach diesem Gesetz. Ebenso wirkt sich die Zweckfestlegung auf die Frage aus, ob eine Verarbeitung zu anderen Zwecken vorliegt, für die gemäß § 8 besondere Anforderungen gelten. Wenn nach diesem Gesetz oder der Verordnung (EU) 2016/679 eine Informationspflicht über die Zwecke der Verarbeitung besteht, sind ebenfalls die Anforderungen an die konkrete Festlegung des Zwecks zu beachten. Schließlich richten sich auch die nach § 9 zu ergreifenden Schutzmaßnahmen unter anderem nach dem konkreten Zweck der Verarbeitung. Die Regelung hat teils klarstellenden Charakter und konkretisiert zugleich die Vorgaben der Verordnung (EU) 2016/679, insbesondere den Grundsatz der Zweckbindung in Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679. Die Zwecke dürfen nicht zu pauschal und allgemein festgelegt werden. Daher genügt ein Verweis auf die beispielsweise in den Absätzen 1 und 2 genannten abstrakten Oberbegriffe in der Regel, insbesondere bei eingriffsintensiven Datenverarbeitungen, nicht. Die übrigen Anforderungen an die Zweckbestimmung sowie die Informationspflichten nach der Verordnung (EU) 2016/679 bleiben unberührt.

Soll eine Verarbeitung gleichzeitig zu verschiedenen Zwecken erfolgen, so ist jeder einzelne Zweck gesondert zu definieren, damit die Prüfung der Rechtmäßigkeit der Verarbeitung für jeden einzelnen Zweck gesondert erfolgen kann. Die Vorschrift ist auch anzuwenden, soweit nach anderen Vorschriften dieses Gesetzes als nach § 3 der Zweck einer Verarbeitung festzulegen ist.

#### **Zu Absatz 4**

Für drei konkret benannte Zwecke hat der Gesetzgeber für bestimmte Beschäftigtendaten die Interessenabwägung selbst durchgeführt. In diesen Fällen der Datenverarbeitung muss keine weitere Prüfung der Erforderlichkeit nach Absatz 1 und § 4 erfolgen. Die Regelung soll einen möglichen Prüfaufwand für stets unproblematische, alltägliche Verarbeitungen verringern und die Verarbeitung der entsprechenden Daten im Alltag damit erleichtern. Für den Zweck der Kontaktaufnahme zu Bewerberinnen und Bewerbern dürfen stets jedenfalls Anrede, Name, Anschrift, Telefonnummer und E-Mail-Adresse der Bewerberinnen und Bewerbern verarbeitet werden (Nummer 1). Für den Zweck der Kontaktaufnahme im laufenden Beschäftigungsverhältnis zur Zusendung allgemeiner betrieblicher Informationen sowie zur Klärung von Fragen, die das Beschäftigungsverhältnis betreffen, dürfen stets jedenfalls Anrede, Name, Anschrift und E-Mail-Adresse der Beschäftigten verarbeitet werden (Nummer 2). Für den Zweck der Gehalts- und Besoldungsauszahlung dürfen stets jedenfalls Name und Personalnummer sowie, sofern nicht das Entgelt auf andere Weise als durch Banküberweisung gezahlt wird, die Bankverbindung verarbeitet werden.

Aufgezählt sind jeweils nur die Daten, die stets zu den genannten Zwecken verarbeitet werden dürfen. Die Liste ist jedoch nicht abschließend. Es können weitere Daten zu den genannten Zwecken verarbeitet werden, sofern die Verarbeitung dieser Daten für den Zweck erforderlich ist. In diesen Fällen sind die Voraussetzungen von Absatz 1 zu prüfen.

#### **Zu § 4 (Prüfung der Erforderlichkeit)**

Eine Verarbeitung nach diesem Gesetz ist nur zulässig, wenn sie zu einem konkreten Zweck, der unter einen der Tatbestände nach diesem Gesetz fällt, erforderlich ist. Im Rahmen der Prüfung der Erforderlichkeit ist eine Abwägung der Interessen des Arbeitgebers an der Verarbeitung mit den Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung vorzunehmen. § 4 konkretisiert diese Interessenabwägung im Rahmen der Prüfung der Erforderlichkeit. Stets zu berücksichtigen sind die Abhängigkeit der Beschäftigten von ihrem Arbeitgeber und die daraus resultierende besondere Schutzbedürftigkeit der Beschäftigten. Es handelt sich um eine spezifischere Vorschrift zur Gewährleis-

tung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung von Beschäftigtendaten im Beschäftigungskontext im Sinne von Artikel 88 der Verordnung (EU) 2016/679, die die Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Beschäftigten sicherstellt.

Die Regelung stellt weiterhin einen nicht abschließenden Katalog von Abwägungskriterien auf, die in vielen Verarbeitungssituationen im Zusammenhang mit dem Beschäftigungsverhältnis typischerweise eine Rolle spielen können, aber nicht in jedem Einzelfall eine Rolle spielen müssen. Es handelt sich deshalb um eine beispielhafte Aufzählung von Kriterien, die je nach Relevanz für den konkreten Fall herangezogen werden können. Die Abwägungskriterien sollen die Handhabung der Abwägung im Einzelfall für alle Beteiligten durch klare Orientierungspunkte vereinfachen und zu mehr Rechtsklarheit und -sicherheit führen, dabei aber Flexibilität bei der Prüfung im Einzelfall erhalten. Es ist eine umfassende Abwägung der Interessen des Arbeitgebers auf der einen, und der Interessen des oder der Beschäftigten auf der anderen Seite durchzuführen, in die je nach Einzelfall verschiedene Kriterien mit unterschiedlicher Gewichtung aufzunehmen sind.

Unter Nummer 1 sind verschiedene Faktoren zur Bestimmung des Gewichts der arbeitgeberseitigen Interessen an der Datenverarbeitung aufgeführt. Höher zu gewichten sind die Arbeitgeberinteressen, wenn die Verarbeitung zur Erfüllung von in Rechtsvorschriften festgelegten Pflichten oder von Pflichten, die in zulässiger Weise in Kollektivverträgen oder individualvertraglich festgelegt wurden, erfolgt. Dies betrifft die Fälle von § 3 Absatz 1 Nummer 1 bis 4. Je genauer diese Festlegung geschieht, desto umfangreicher wird auch die „Erforderlichkeit“ einer solchen Verarbeitung vorbestimmt. Erfolgt die Festlegung hingegen in abstrakter Weise, muss die Interessenabwägung im Rahmen der Prüfung dessen, was zur Erfüllung der Verpflichtung erforderlich ist, umfangreicher ausfallen.

Es kann auch zu berücksichtigen sein, ob und wie stark Grundrechtspositionen betroffen sind oder ein öffentliches Interesse besteht.

Unter Nummer 2 sind verschiedene Faktoren zur Bestimmung des Gewichtes der Beschäftigteninteressen und zu deren Beeinträchtigung durch die Verarbeitung aufgeführt. Zu berücksichtigen ist, dass mit der Verarbeitung von Beschäftigtendaten grundsätzlich ein Eingriff in das allgemeine Persönlichkeitsrecht der Beschäftigten verbunden ist, so dass die Interessen der Beschäftigten grundsätzlich hoch zu gewichten sind und nur mit ebenfalls grundrechtlich geschützten Interessen des Arbeitgebers in Ausgleich gebracht werden können.

Die Abwägung hängt weiterhin von der Eingriffstiefe und den möglichen Folgen der Verarbeitung für die Beschäftigten ab, sowie davon, welches Risiko für die Beschäftigten besteht. Für die Beurteilung dieser Faktoren ist auf den Zeitpunkt der Verarbeitung abzustellen.

Es spielt nach Buchstabe a eine Rolle, ob eine Verarbeitung nur einmalig, punktuell oder über längere Zeit erfolgt. Dabei ist die Rechtsnatur des Beschäftigungsverhältnisses als Dauerschuldverhältnis zu berücksichtigen. Dies gilt vor allem dann, wenn es um andauernde oder wiederkehrende Verarbeitungen geht. In Beamtenverhältnissen ist zudem die Rechtsnatur des Beamtenverhältnisses als öffentlich-rechtliches Dienst- und Treuverhältnis zu berücksichtigen.

Entscheidend ist nach Buchstabe b auch, welche Art von Beschäftigtendaten verarbeitet wird, insbesondere wie sensibel diese sind. Als sensibel sind nicht nur die besonderen Datenkategorien im Sinne von Artikel 9 der Verordnung (EU) 2016/679 einzuordnen, eine Sensibilität kann sich auch darüber hinaus ergeben, etwa bei Kommunikationsdaten oder Standortdaten. Dabei sind die Grundsätze der Sphärentheorie zu beachten, aus denen folgt, dass Beschäftigtendaten, die der Privatsphäre von Beschäftigten entstammen, nur in

Ausnahmen und solche aus der Intimsphäre der Beschäftigten im Grundsatz gar nicht verarbeitet werden dürfen.

Zu berücksichtigen ist nach Buchstabe c insbesondere, in welchem Umfang Beschäftigtendaten verarbeitet werden. Der Grundrechtseingriff fällt umso tiefer aus, je größer und umfassender die verarbeiteten Datensätze sind.

Es spielt auch eine Rolle, ob nach Buchstabe d die verarbeiteten Daten mit anderen Beschäftigtendaten abgeglichen oder verknüpft und so verschiedene Informationen und persönliche Aspekte zusammengeführt werden. Zu betrachten sind auch die Mittel der Verarbeitung, etwa ob diese analog, automatisiert oder durch besondere technische Einrichtungen erfolgt. Unterschiedlich zu gewichten ist, ob eine Verarbeitung in Echtzeit erfolgt oder ob und wie lange die Daten auch gespeichert werden (Buchstabe e).

Weiterhin sind die Umstände der Verarbeitung zu beachten, etwa die Anzahl und Funktion der Personen, die an der Verarbeitung beteiligt sind und Zugriff auf die Daten haben (Buchstabe f). Im Beschäftigungskontext kann es schwerer wiegen, wenn die Daten durch direkte Vorgesetzte verarbeitet werden. Ein Risiko kann hingegen abgemildert werden, wenn die Personen besonders sensibilisiert oder zur Verschwiegenheit verpflichtet sind.

Grundsätzlich sind Daten bei den Beschäftigten selbst zu erheben. Eine Datenerhebung aus anderen Quellen stellt einen starken Eingriff in die Persönlichkeitsrechte des oder der Beschäftigten dar, an dessen Rechtfertigung entsprechend höhere Anforderungen zu stellen sind. Dies ist in der Abwägung nach Buchstabe g zu berücksichtigen.

In der Abwägung ist auch zu berücksichtigen, welche begründeten Erwartungen die Beschäftigten an den Umgang mit ihren Daten durch ihren Arbeitgeber haben (Buchstabe h). Hierbei spielt die Stellung des Arbeitgebers als Vertragspartner im Beschäftigungsverhältnis eine entscheidende Rolle. Diesen treffen besondere Schutz- und Fürsorgepflichten, die bestimmte Erwartungen auf eine strengere Vertraulichkeit und Zweckbindung begründen können. Das Beschäftigungsverhältnis ist durch ein strukturelles Machtungleichgewicht der Vertragspartner geprägt.

Auch das Risiko von zweckwidrigen Rückschlüssen auf die Arbeitsleistung kann vor diesem Hintergrund zu beachten sein, insbesondere wenn sich dies nachteilig auf das berufliche Fortkommen der Beschäftigten auswirken kann (Buchstabe i). So kann berücksichtigt werden, wenn der Zweck der Verarbeitung etwa in der Steuerung von Betriebsabläufen liegt, die Vorgesetzten aber ohne Schwierigkeiten missbräuchlich auf Daten einzelner Beschäftigter zugreifen können, anhand derer sie die Arbeitsleistung umfassend bewerten könnten.

Werden bei einem Verarbeitungsvorgang KI-Systeme eingesetzt, ist insbesondere zu berücksichtigen, ob es Möglichkeiten zur Aufsicht und Kontrolle durch Menschen gibt und ob die Funktionsweise in verständlicher Weise erklärt werden kann (Buchstabe h). Damit soll bereits vor der Verarbeitung von Beschäftigtendaten durch oder aufgrund eines KI-Systems geprüft und berücksichtigt werden, in welchem Umfang gegenüber den Beschäftigten Transparenz über den Einsatz des KI-Systems hergestellt werden kann, insbesondere in Erfüllung der spezifischen Informationspflichten nach § 10.

## **Zu § 5 (Einwilligung)**

Die Vorschrift konkretisiert die Anforderungen an Einwilligungen in die Verarbeitung von Beschäftigtendaten nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a und Artikel 7 der Verordnung (EU) 2016/679 für den Beschäftigungskontext. Es handelt sich um eine spezifischere Vorschrift im Sinne von Artikel 88 Absatz 1 der Verordnung (EU) 2016/679, die von der Regelungsmöglichkeit, die in Erwägungsgrund 155 der Verordnung (EU) 2016/679 explizit aufgeführt wird, Gebrauch macht. Die erhöhten Anforderungen berücksichtigen die

Besonderheiten des Beschäftigungsverhältnisses, insbesondere das Abhängigkeitsverhältnis zwischen Beschäftigten und Arbeitgeber und die daraus resultierende, erhöhte Schutzbedürftigkeit der Beschäftigten. Die erhöhten Anforderungen und die Formvorschriften in Absatz 4 tragen zur Wahrung der Interessen und Grundrechte der Beschäftigten, insbesondere auch der menschlichen Würde, bei.

Die Regelung erfolgt unbeschadet der übrigen Voraussetzungen für eine wirksame Einwilligung nach Artikel 4 Nummer 11, Artikel 7 und Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679.

### **Zu Absatz 1**

Absatz 1 Satz 1 führt die Regelung von § 26 Absatz 2 Satz 1 BDSG a.F. fort, nach der die besonderen Umstände der Verarbeitungssituation im Beschäftigungskontext allgemein sowie im Speziellen zu berücksichtigen sind. Um mehr Rechtsklarheit zu erreichen, kodifiziert Satz 2 beispielhaft Aspekte, die bei der Beurteilung der Umstände zu berücksichtigen sind. Mit der Verarbeitung von Beschäftigtendaten ist ein Eingriff in die informationelle Selbstbestimmung verbunden. Für die Eingriffstiefe spielt es unter anderem eine Rolle, welche Arten von Daten in welchem Umfang verarbeitet werden. Zu berücksichtigen ist auch der Zeitpunkt der Einwilligungserteilung. In der Bewerbungssituation vor Abschluss eines (Arbeits-)Vertrages sind Beschäftigte einer größeren Drucksituation ausgesetzt, eine Einwilligung zu erteilen, um die Chancen auf eine erfolgreiche Bewerbung nicht zu gefährden. Daher sind in dieser Situation für die Freiwilligkeit der Erklärung besonders hohe Maßstäbe anzusetzen.

### **Zu Absatz 2**

Absatz 2 Satz 1 führt die Regelung von § 26 Absatz 2 Satz 2 BDSG a.F. fort und benennt als Regelbeispiele Fallgruppen, bei denen Freiwilligkeit vorliegen kann. Grundsätzlich ist dabei zu beachten, dass ein wirtschaftlicher Vorteil nicht in einem erhöhten Arbeitsentgelt liegen kann. Die Erlangung eines wirtschaftlichen Vorteils darf nicht zu einem „Abkaufen“ der Einwilligung führen.

Um mehr Rechtsklarheit zu erreichen, kodifiziert Satz 2 Regelbeispiele, bei denen eine freiwillige Einwilligung insbesondere vorliegen kann. Der Verantwortliche ist dadurch jedoch nicht von der Prüfung der Anforderungen an die Freiwilligkeit im Einzelfall entbunden. Vor Begründung eines Beschäftigungsverhältnisses kann eine Einwilligung in die Aufnahme in eine Bewerbungsdatenbank nach Nummer 1 insbesondere dann freiwillig erfolgen, wenn sie erst nach der Beendigung eines erfolglosen Auswahlverfahrens erteilt wird.

Die Regelbeispiele in Nummer 2 für das laufende Beschäftigungsverhältnis führen die bereits nach § 26 Absatz 2 BDSG a.F. geltenden Maßstäbe weiter aus. Beispiele für die Gewährung eines Vorteils sind etwa die Teilnahme an Angeboten zur Gesundheitsförderung im Rahmen eines betrieblichen Gesundheitsmanagements (Buchstabe c) oder die Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen (Buchstabe d). Beschäftigte und Arbeitgeber können beispielsweise gleichgerichtete Interessen verfolgen, wenn es um die Nutzung von Fotos für das Intranet, das heißt ein nichtöffentliches, geschlossenes organisations- bzw. firmeninternes Computernetzwerk, (Buchstabe a) oder die Aufnahme von Name und Geburtsdatum in eine Geburtstagsliste geht (Buchstabe b). In diesen Fällen wirken Arbeitgeber und Beschäftigte im Sinne eines betrieblichen Miteinanders zusammen.

Nummer 2 Buchstabe e stellt klar, dass die Nutzung von biometrischen Daten zur Identifizierung, die nur mit dem Zweck erfolgt, bestimmte Prozesse, wie etwa die Zugangskontrolle oder Zeiterfassung zu vereinfachen und zu beschleunigen, auf Grundlage einer Einwilligung möglich sein kann. Voraussetzung ist, dass es für die Beschäftigten eine echte Wahlmöglichkeit geben muss, dass also eine gleichwertige Alternative zur Verfügung stehen muss, die die Nutzung biometrischer Daten nicht erfordert und keine Nachteile für die Beschäftigten birgt. Eine Identifizierung könnte beispielsweise auch mit einer Zugangskarte oder der

Eingabe eines Passwortes erfolgen. Wird den Beschäftigten keine echte Wahlmöglichkeit gegeben, etwa wenn sie zur Nutzung von Identifikationssystemen, die biometrische Daten verarbeiten, verpflichtet werden, scheidet die Freiwilligkeit einer Einwilligung in die damit verbundene Datenverarbeitung regelmäßig aus. Ob eine solche Datenverarbeitung zulässig ist, richtet sich ausschließlich nach § 28.

Nach Beendigung des Beschäftigungsverhältnisses kann insbesondere eine Einwilligung in die Kontaktaufnahme zu den unter Nummer 3 aufgeführten Anlässen freiwillig sein, etwa zur Gratulation anlässlich von Geburtstagen, Beschäftigungs- oder Dienstjubiläen oder vergleichbaren besonderen Ereignissen, zur Einladung zu Betriebs- oder Firmenfeiern oder vergleichbaren besonderen Veranstaltungen oder zur Benachrichtigung über geeignete Stellenangebote oder Weiterbildungsmöglichkeiten. In diesen Fällen handelt es sich um die Verfolgung gleichgelagerter Interessen, etwa die Pflege und Aufrechterhaltung von Kontakten und Netzwerken.

### **Zu Absatz 3**

Keine Freiwilligkeit liegt nach Absatz 3 insbesondere dann vor, wenn der Abschluss oder die Erfüllung des Vertrages zwischen Arbeitgeber und Beschäftigten von einer Einwilligung abhängig gemacht wird, obwohl diese für die Erfüllung des Vertrages nicht erforderlich ist. Diese Regelung konkretisiert den Grundsatz des Kopplungsverbots aus Artikel 7 Absatz 4 und dem Erwägungsgrund 43 der Verordnung (EU) 2016/679 für die besondere Verarbeitungssituation im Beschäftigungskontext. Gegenstand einer Einwilligung nach Absatz 3 wären nur solche Daten, die im Beschäftigungskontext nicht schon zu Zwecken der Vertragsdurchführung zum Beispiel aufgrund von Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe b der Verordnung (EU) 2016/679 in Verbindung mit § 3 rechtmäßig verarbeitet werden dürfen. Eine solche Einwilligung dürfte gerade nicht zur Bedingung für den Abschluss eines Beschäftigungsverhältnisses oder die Erbringung der vertraglich geschuldeten Leistungen gemacht werden. Dies würde die Freiwilligkeit der Erteilung ausschließen.

### **Zu Absatz 4**

Absatz 4 Satz 1 und 2 führt die Regelungen von § 26 Absatz 2 Satz 3 und 4 fort und konkretisiert und ergänzt die Nachweispflicht des Arbeitgebers im Sinne von Artikel 7 Absatz 1 der Verordnung (EU) 2016/679.

Auch im Rahmen einer Einwilligung ist der Zweck der Datenverarbeitung konkret festzulegen und § 3 Absatz 3 zu beachten.

### **Zu § 6 (Besondere Kategorien von Beschäftigtendaten)**

#### **Zu Absatz 1**

Die Vorschrift macht von den Öffnungsklauseln in Artikel 88 Absatz 1, Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 Gebrauch und konkretisiert die Voraussetzungen für die Verarbeitung besonderer Kategorien personenbezogener Daten im Beschäftigungskontext. Dabei umfasst die Ausübung von Rechten aus dem Arbeitsrecht auch Zwecke der Arbeitsmedizin und die Beurteilung der Arbeitsfähigkeit von Beschäftigten, soweit der Arbeitgeber hierfür im Sinne von Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 datenschutzrechtlich verantwortlich ist. Die Interessen des Arbeitgebers an der Verarbeitung müssen die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen, wobei die Abwägungskriterien aus § 4 zu beachten sind. Die Anwendbarkeit der übrigen Tatbestände von Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 wird durch die Vorschrift nicht beschränkt.



## **Zu Absatz 2**

Absatz 2 stellt klar, dass genetische Beschäftigendaten nur unter den engen Voraussetzungen der §§ 19 bis 22 des Gendiagnostikgesetzes verarbeitet werden dürfen.

## **Zu Absatz 3**

§ 22 des Bundesdatenschutzgesetzes findet auf eine Verarbeitung besonderer Kategorien von Beschäftigendaten keine Anwendung, da sonst die strengeren Anforderungen des § 6 unterlaufen würden.

## **Zu Absatz 4**

Absatz 4 führt die Regelung von § 26 Absatz 3 Satz 2 BDSG a.F. fort und stellt klar, dass die Vorschriften der Absätze 1 bis 2 auch für die Einwilligung in die Verarbeitung besonderer Kategorien von Beschäftigendaten gelten. Die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. Der Umstand, dass besondere Kategorien personenbezogener Daten, wie etwa Gesundheitsdaten, verarbeitet werden, muss entsprechend berücksichtigt werden. Es sind strenge Anforderungen an die Freiwilligkeit einer solchen Einwilligung zu stellen.

## **Zu § 7 (Kollektivvereinbarungen)**

### **Zu Absatz 1**

Artikel 88 Absatz 1 der Verordnung (EU) 2016/679 eröffnet den Mitgliedsstaaten die Möglichkeit, spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung von Beschäftigendaten im Beschäftigungskontext auch durch Kollektivvereinbarungen zuzulassen. In Absatz 1 macht der Gesetzgeber von dieser Option Gebrauch und lässt zu, dass die Verhandlungspartner in Kollektivvereinbarungen, das heißt nach Legaldefinition in § 2 Absatz 4 Tarifverträgen, Betriebs- und Dienstvereinbarungen sowie gleichwertigen kollektiven Verträgen, Regelungen zum Beschäftigtendatenschutz treffen können. Gleichzeitig setzt die Vorschrift dem Regelungsspielraum in den folgenden Absätzen Grenzen. Die Regelung übernimmt dabei in Einklang mit Erwägungsgrund 8 der Verordnung (EU) 2016/679 Teile des Artikel 88 Absatz 1 der genannten Verordnung, soweit dies erforderlich ist, um die Kohärenz zu wahren und die Vorschrift verständlich zu machen.

### **Zu Absatz 2 und Absatz 3**

Der effektive Schutz der Persönlichkeitsrechte von Beschäftigten, wie er durch dieses Gesetz gewährleistet wird, darf durch abweichende Regelungen in den Kollektivvereinbarungen nicht gefährdet werden. Es bestünde sonst die Gefahr, dass die Regelungen dieses Gesetzes unterlaufen werden. Es darf nicht zu Lasten des Schutzes der Beschäftigten von diesem Gesetz abgewichen werden.

Kollektivvereinbarungen können als branchenbezogenes bzw. betriebsnahes und praxisgerechtes Instrument Regelungen zum Beschäftigtendatenschutz mit Blick auf die jeweiligen branchenbezogenen bzw. betrieblichen Bedürfnisse ausgestalten. Die Verhandlungspartner können zum Beispiel Verfahrensvorgaben schaffen. Satz 2 stellt klar, dass in Kollektivvereinbarungen nicht abschließend die Zulässigkeit einer Verarbeitung von Beschäftigendaten festgelegt werden kann, das heißt die erforderliche Interessenabwägung kann nicht vollständig durch die Verhandlungspartner vorweggenommen und es kann keine eigenständige Verarbeitungsgrundlage geschaffen werden. Der Regelungsspielraum der Verhandlungspartner war diesbezüglich umstritten, sodass die Vorschrift Rechtssicherheit schafft und dem Regelungsspielraum nunmehr einen klaren Rahmen setzt. Neben Verfah-

rensvorgaben bleibt es weiter möglich, dass die Verhandlungspartner die gesetzlichen Voraussetzungen für die Verarbeitung von Beschäftigtendaten konkretisieren. Konkrete Beispiele für spezifische Festlegungen und Konkretisierungen wären etwa die Festlegung der Arten von Daten, die verarbeitet werden, sowie der Personen, die betroffen sind, oder Regelungen dazu, wie lange bestimmte Daten gespeichert werden dürfen, wann sie zu löschen sind oder welche Verarbeitungsvorgänge und -verfahren im Rahmen der Erforderlichkeit angewandt werden dürfen. Auch zusätzliche Bedingungen für die Rechtmäßigkeit von bestimmten Verarbeitungen können festgelegt werden.

Bei der Ausgestaltung eines auf die branchenbezogenen bzw. betrieblichen Bedürfnisse zugeschnittenen Beschäftigtendatenschutzes steht den Verhandlungspartnern ein Ermessensspielraum im Rahmen des geltenden Rechts einschließlich der Verordnung (EU) 2016/679 zu. Absatz 3 stellt klar, dass die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten und die besonderen Belange von Beschäftigten der jeweiligen Branche oder des jeweiligen Betriebs zu berücksichtigen haben. In Bezug auf öffentliche Stellen sind die besonderen Belange von Beschäftigten der jeweiligen Behörden zu berücksichtigen.

Absatz 3 Satz 2 stellt zudem klar, dass die Verhandlungspartner nicht beliebig von der Verordnung (EU) 2016/679 abweichen können. Die nationalen Rechtsvorschriften dürfen nicht gegen den Inhalt und die Ziele der Verordnung (EU) 2016/679 verstoßen (vgl. EuGH, Urteil vom 28. April 2022, Meta Platforms Ireland, C-319/20, Rn. 60). Das Ziel der auf der Grundlage von Artikel 88 der Verordnung (EU) 2016/679 erlassenen Vorschriften liegt darin, die Rechte und Freiheiten der Beschäftigten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext zu schützen (vgl. EuGH, Urteil vom 30. März 2023, Hauptpersonalrat der Lehrerinnen und Lehrer, C-34/21, Rn. 63). Absatz 4 schreibt insofern vor, dass das Schutzniveau der Verordnung (EU) 2016/679 durch Kollektivvereinbarungen nicht zu Lasten der Beschäftigten unterschritten werden darf. Die Verhandlungspartner können zudem nicht von den grundlegenden Prinzipien der Verordnung (EU) 2016/679, insbesondere der Artikel 5, 6 und 9 abweichen. Davon umfasst sind beispielsweise neben den Grundsätzen des Artikel 5 der Verordnung (EU) 2016/679 auch der in Artikel 6 der Verordnung (EU) 2016/679 verankerte Grundsatz des Verbots mit Erlaubnisvorbehalt. Eine Verarbeitung muss unter einen der in Artikel 6 der Verordnung (EU) 2016/679 vorgesehenen Fälle subsumierbar sein, um als rechtmäßig angesehen werden zu können (vgl. EuGH Urteil vom 30. März 2023, Hauptpersonalrat der Lehrerinnen und Lehrer, C-34/21, Rn. 70; EuGH Urteil vom 22. Juni 2021, Latvijas Republikas Saeima [Strafpunkte], C 439/19, Rn. 99). Auch die effektive Ausübung von Betroffenenrechten nach Artikel 12 ff. der Verordnung (EU) 2016/679 darf nicht durch Regelungen in Kollektivvereinbarungen gefährdet werden.

Eine Abweichung von den grundlegenden Prinzipien der Verordnung (EU) 2016/679 liegt hingegen nicht vor, wenn beispielsweise die Tatbestandsvoraussetzungen von gesetzlichen Verarbeitungsgrundlagen für bestimmte Fälle im Beschäftigungskontext konkretisiert oder zusätzliche Voraussetzungen vorgesehen werden.

Die Regelungen der Absätze 2 und 3 stehen auch nicht pauschal einem Ausschluss von bestimmten Verarbeitungszwecken oder -vorgängen in konkreten Fällen entgegen.

#### **Zu Absatz 4**

Absatz 4 verdeutlicht, dass Mindestinhalt und -umfang der Kollektivvereinbarungen unter den Voraussetzungen des Absatzes 2 anhand der konkreten Regelung im Einzelfall zu beurteilen sind. Spezifischere Regelungen und Maßnahmen sind festzulegen, soweit sie für den konkreten datenschutzrechtlichen Regelungsinhalt der Kollektivvereinbarung relevant sind. Soweit keine spezifischeren Vorschriften getroffen werden, bleiben die Bestimmungen dieses Gesetzes, des Bundesdatenschutzgesetzes und der Verordnung (EU 2016/679) unberührt.

## **Zu Absatz 5**

Absatz 5 entspricht im Wesentlichen § 26 Absatz 6 Bundesdatenschutzgesetz a. F. und stellt klar, dass die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt bleiben. Dies gilt auch für die sonstigen gesetzlichen Rechte der Interessenvertretungen.

## **Zu § 8 (Verarbeitung zu anderen Zwecken)**

§ 8 regelt die Zulässigkeit einer Verarbeitung zu anderen Zwecken im Anwendungsbereich des Beschäftigtendatenschutzgesetzes. Die Regelung stellt eine spezifischere Vorschrift zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung von Beschäftigtendaten im Beschäftigungskontext nach Artikel 88 der Verordnung (EU) 2016/679 dar. Sie sieht mit Blick auf das im Beschäftigungskontext bestehende Abhängigkeitsverhältnis und die daraus resultierende Schutzbedürftigkeit der Beschäftigten erhöhte Anforderungen für die Verarbeitung von Beschäftigtendaten zu anderen Zwecken vor.

## **Zu Absatz 1**

Absatz 1 konkretisiert die Zulässigkeit der Zweckänderung bei der Verarbeitung von Beschäftigtendaten. Nummer 1 und Nummer 2 stellen klar, dass auch im Anwendungsbereich dieses Gesetzes, wie in Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 aufgeführt, eine Weiterverarbeitung aufgrund einer Einwilligung oder aufgrund einer speziellen Rechtsvorschrift zum Schutz der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 genannten Ziele (Nummer 1 und Nummer 2) möglich ist. Hinsichtlich der Einwilligung erfolgt gegenüber Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 die Klarstellung, dass eine Einwilligung in die Verarbeitung zu anderen Zwecken den Anforderungen nach § 5 genügen muss. Durch die ausdrückliche Regelung zu Rechtsvorschriften außerhalb dieses Gesetzes zum Schutz der in Artikel 23 Absatz 1 Verordnung (EU) 2016/679 genannten Ziele (Nummer 2) erfolgt die Klarstellung, dass weder § 8 selbst noch eine andere Vorschrift aus diesem Gesetz eine solche Rechtsvorschrift zum Schutz der in Artikel 23 Absatz 1 Verordnung (EU) 2016/679 genannten Ziele darstellen, einschlägige speziellere Regelungen außerhalb dieses Gesetzes aber unberührt bleiben.

Liegt keine Einwilligung oder spezielle Rechtsgrundlage aus einem anderen Gesetz vor, gilt auch im Anwendungsbereich dieses Gesetzes nach dem Grundsatz der Zweckbindung, dass Beschäftigtendaten für festgelegte, eindeutige und legitime Zwecke erhoben werden müssen und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Nach Nummer 3 ist daher die Vereinbarkeit des geänderten Zwecks mit dem Erhebungszweck zu prüfen. Damit die speziellen Anforderungen des Beschäftigtendatenschutzes und die Rechtsgrundlagen für bestimmte Verarbeitungssituationen - wie etwa die Regelung zum Profiling nach § 24 - auch im Fall von Zweckänderungen nicht unterlaufen werden können, stellt Absatz 1 Nummer 3 präzisierend klar, dass für die Verarbeitung zu dem geänderten Zweck auch dann die Voraussetzungen für eine zulässige Verarbeitung nach diesem Gesetz vorliegen müssen, wenn die Vereinbarkeit von Erhebungszweck und geändertem Zweck festgestellt wurde. Zum Beispiel können Beschäftigte im Intranet ihres Arbeitgebers Kompetenzen und Erfahrungen angeben, um die Vernetzung und den Erfahrungsaustausch zwischen den Beschäftigten des Unternehmens zu fördern. Der Arbeitgeber möchte diese Daten durch Profiling weiterverarbeiten, um für die Beschäftigten innerhalb des Unternehmens passende Stellenangebote zu finden. Nach Nummer 3 müsste dafür zunächst der geänderte Zweck mit dem ursprünglichen Zweck vereinbar sein. Darüber hinaus müsste die Verarbeitung der Beschäftigtendaten für die unternehmens- oder behördeninterne Stellenbesetzung unter den Voraussetzungen des § 24 zulässig sein.

## **Zu Absatz 2**

Bei der Prüfung der Vereinbarkeit nach Absatz 1 Nummer 3 sind weiterhin die in Artikel 6 Absatz 4 Nummer 1 bis 4 der Verordnung (EU) 2016/679 genannten Kriterien zu berücksichtigen. Absatz 2 spezifiziert die Prüfung der Zweckvereinbarkeit im Anwendungsbereich dieses Gesetzes dahingehend, dass über die in Artikel 6 Absatz 4 Nummer 1 bis 4 der Verordnung (EU) 2016/679 genannten Kriterien hinaus die besonderen Umstände des Beschäftigungsverhältnisses zu berücksichtigen sind, insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der Beschäftigten. Insbesondere kann sich die Abhängigkeit der Beschäftigten insofern auswirken, dass Beschäftigte aufgrund ihrer Weisungsgebundenheit faktisch zur Preisgabe der Daten gezwungen sein können. Darüber hinaus kann es eine Rolle spielen, wenn durch die Weiterverarbeitung nicht absehbare nachteilige Folgen entstehen können. Wenn etwa für die Erbringung der Arbeitsleistung zwingend zu erhebende Daten nachträglich zur Leistungsbewertung weiterverarbeitet werden, dürften die Zwecke in der Regel nicht miteinander vereinbar sein. Die Weiterverarbeitung zur Leistungsbewertung kann in diesen Fällen nachteilige Folgen für das berufliche Fortkommen der Beschäftigten nach sich ziehen und die Beschäftigten müssen regelmäßig nicht mit einer solchen Zweckänderung rechnen.

## **Zu Absatz 3**

Die §§ 23 und 24 des Bundesdatenschutzgesetzes sind nationale Rechtsgrundlagen für die Weiterverarbeitung personenbezogener Daten. Diese Vorschriften sollen weiterhin auch für die Verarbeitung von Beschäftigtendaten gelten. Soweit jedoch nach den §§ 23 und 24 des Bundesdatenschutzgesetzes Interessenabwägungen vorzunehmen sind, muss der spezifische Maßstab der Interessenabwägung nach diesem Gesetz berücksichtigt werden und die Interessen des Arbeitgebers an der Verarbeitung müssen die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen. Soweit unter den Voraussetzungen der §§ 23 Absatz 2 und 24 Absatz 2 des Bundesdatenschutzgesetzes besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 weiterverarbeitet werden sollen, kann im Anwendungsbereich dieses Gesetzes nicht auf die Ausnahmetatbestände des § 22 des Bundesdatenschutzgesetzes zurückgegriffen werden, sondern die spezielleren Voraussetzungen für die Verarbeitung besonderer Kategorien von Beschäftigtendaten nach diesem Gesetz müssen vorliegen.

## **Zu § 9 (Schutzmaßnahmen)**

### **Zu Absatz 1**

Die Vorschrift stellt die Pflicht für den Arbeitgeber auf, geeignete und besondere Maßnahmen zu treffen, um die Einhaltung der Grundprinzipien und Regelungen der Verordnung (EU) 2016/679 und dieses Gesetzes sicherzustellen sowie die menschliche Würde, die berechtigten Interessen und Grundrechte der betroffenen Beschäftigten zu wahren. Die Pflicht ist im Hinblick auf alle Verarbeitungen im Beschäftigungskontext zu erfüllen. Die Vorschrift trägt den Anforderungen von Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 Rechnung und konkretisiert die Pflichten, die den Verantwortlichen einer Verarbeitung nach der Verordnung (EU) 2016/679, etwa gemäß Artikel 24 ff. treffen. Die Vorschrift spezifiziert in Satz 2, welche Umstände bei der Auswahl der Schutzmaßnahmen zu berücksichtigen sind und welche Maßnahmen insbesondere in Betracht kommen. Dabei sind neben dem Stand der Technik, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten der Beschäftigten gerade auch die Belange der Beschäftigten besonders zu berücksichtigen. Die besonderen Umstände im Beschäftigungskontext sind nicht nur bei der Auswahl der Schutzmaßnahmen, sondern auch bei deren Umsetzung und Gestaltung zu beachten. Spezifische Schutzmaßnahmen sind beispielsweise in Bezug auf Personalaktendaten vorzusehen, die gesondert (Nummer 2), sorgfältig und besonders gesichert (Nummer 4) zu

verwahren sind. Grundsätzlich darf nur ein enger Kreis von Beschäftigten Zugriff auf die Personalakten haben, dies ist durch entsprechende Maßnahmen sicherzustellen (Nummer 3).

Bei der Beschränkung des Zugangs zu Daten ist grundsätzlich zu berücksichtigen, welche Funktion die an der Verarbeitung Beteiligten innehaben, insbesondere ob es sich um direkte Vorgesetzte der jeweils betroffenen Beschäftigten handelt.

Geht mit einer Schutzmaßnahme eine Verarbeitung von Beschäftigtendaten einher, muss dies berücksichtigt und die Verarbeitung ebenfalls nach diesem Gesetz zulässig sein. Schutzmaßnahmen zur Gewährleistung der Integrität sind daher sorgfältig zu prüfen und auszugestalten und dürfen nicht zu einem Überwachungsdruck führen.

Um Transparenz und Intervenierbarkeit zu sichern und zu stärken, können insbesondere auch Interessenvertretungen von Beschäftigten frühzeitig bei der Gestaltung von Verarbeitungsvorgängen und im Rahmen von Überprüfungsmechanismen von Verarbeitungsvorgängen oder von Schutzmaßnahmen eingebunden werden (Nummer 9). Gemeint ist eine überobligatorische Einbindung, die über gesetzliche Verpflichtungen hinausgeht. Die Beteiligungsrechte und sonstigen gesetzlichen Rechte der Interessenvertretungen der Beschäftigten bleiben durch solche Maßnahmen unberührt. Es kann auch eine Schutzmaßnahme darstellen, freiwillig und überobligatorisch Datenschutzbeauftragte einzubinden (Nummer 10), nämlich in den Fällen, in denen dies nicht bereits nach der Verordnung (EU) 2016/679 vorgeschrieben ist. Dies kann zum Beispiel die Einbindung von freiwillig benannten Datenschutzbeauftragten betreffen.

Werden Systeme Künstlicher Intelligenz (KI-Systeme) zur Verarbeitung von Beschäftigtendaten eingesetzt, können sich spezifische Anforderungen stellen, um etwa die Datenminimierung, Integrität und Vertraulichkeit, Datenrichtigkeit sowie Zweckbindung gewährleisten zu können (Nummer 11). Um zu verhindern, dass während des Einsatzes des KI-Systems für den Zweck irrelevante Beschäftigtendaten verarbeitet werden, ist eine regelmäßige Evaluierung, welche der verarbeiteten Eingabe- und Ausgabedaten für die Nutzung wirklich relevant und erforderlich sind, angezeigt. Wenn sich aus den Ergebnissen Rückschlüsse auf Beschäftigte ableiten lassen, ist eine zweckwidrige, nicht von vornherein geplante Nutzung von Ergebnissen und Zwischenergebnissen auszuschließen, soweit möglich durch Anonymisierung der (Zwischen-)Ergebnisse. Auch die Risiken unrichtiger und diskriminierender Ergebnisse sind durch eine regelmäßige Überprüfung des KI-Systems möglichst zu minimieren. Dabei ist zu beachten, dass für den Arbeitgeber die Überprüfungsmöglichkeiten begrenzt sein können, wenn er nicht Entwickler des KI-Systems ist.

### **Zu Absatz 2**

Absatz 2 stellt sicher, dass bei einer Verarbeitung von besonderen Kategorien von Beschäftigtendaten besondere Schutzmaßnahmen ausgewählt und getroffen werden und dabei der Umstand berücksichtigt wird, dass diese besonders sensibel und schutzbedürftig sind. Dies trägt auch den Anforderungen von Artikel 9 der Verordnung (EU) 2016/679 Rechnung.

### **Zu Absatz 3**

Absatz 3 legt fest, dass die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 der Verordnung (EU) 2016/679 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 der Verordnung (EU) 2016/679 als Gesichtspunkt herangezogen werden können, um die Erfüllung der in Absatz 1 genannten Anforderungen nachzuweisen.

## **Zu Kapitel 3 (Betroffenenrechte, Verwertungsverbot und Datenschutzbeauftragte)**

### **Zu § 10 (Spezifische Betroffenenrechte)**

Es handelt sich um spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung von Beschäftigtendaten im Beschäftigungskontext im Sinne von Artikel 88 der Verordnung (EU) 2016/679. Die erhöhten Anforderungen berücksichtigen die Besonderheiten des Beschäftigungsverhältnisses, insbesondere das Abhängigkeitsverhältnis zwischen Beschäftigten und Arbeitgeber und die daraus resultierende, erhöhte Schutzbedürftigkeit der Beschäftigten. Die Vorschrift stellt eine geeignete und besondere Maßnahme zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Beschäftigten im Sinne von Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 dar, indem sie die Transparenz der Verarbeitung im Beschäftigungsverhältnis sicherstellt und die Pflichten, die den Verantwortlichen einer Verarbeitung nach der Verordnung (EU) 2016/679 treffen, konkretisiert und ergänzt. Im Übrigen bleiben die Betroffenenrechte aus der Verordnung (EU) 2016/679 unberührt.

#### **Zu Absatz 1**

Absatz 1 konkretisiert die Anforderungen an die Informationspflicht des Arbeitgebers nach den Artikeln 13 und 14 der Verordnung (EU) 2016/679. Für den Fall, dass eine Verarbeitung auf diesem Gesetz beruht und auf ein betriebliches oder dienstliches Interesse gestützt wird, etwa auf § 3 Absatz 1 Nummer 7 in Verbindung mit Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f der Verordnung (EU) 2016/679, stellt die Vorschrift klar, dass auf Verlangen auch die wesentlichen Erwägungen der Interessenabwägung von dem Arbeitgeber darzulegen sind. Die darzulegenden Punkte können sich insbesondere auf die Kriterien der Interessenabwägung nach § 4 beziehen. Die Regelung sieht ausdrücklich vor, dass die Erwägungen in einer für die Beschäftigten verständlichen Weise dargelegt werden müssen. Es ist ein objektivierter Maßstab anzulegen. Die Regelung soll einer effektiven Transparenz dienen und den Beschäftigten ermöglichen, die vorgenommene Abwägung nachvollziehen und überprüfen zu können. Dies ist insbesondere dann wichtig, wenn die betroffenen Beschäftigten Zweifel an einer fairen Interessenabwägung hegen oder etwa Beschwerde bei einer Aufsichtsbehörde einreichen möchten. Über das Bestehen des Auskunftsrechts nach Satz 1 sind die betroffenen Beschäftigten im Rahmen der bereits bestehenden Informationspflichten nach den Artikeln 13 und 14 der Verordnung (EU) 2016/679 zu informieren. Die Informationspflichten aus der Verordnung (EU) 2016/679 bleiben im Übrigen unberührt.

#### **Zu Absatz 2**

Um die Transparenz bei der Verarbeitung von Beschäftigtendaten durch oder aufgrund von KI-Systemen zu fördern, ist den betroffenen Beschäftigten der Einsatz kenntlich zu machen. Dadurch können Beschäftigte anschließend über die Auskunftsrechte nach Absatz 3 weitere Informationen erhalten.

#### **Zu Absatz 3**

Beim Einsatz von KI-Systemen haben die Beschäftigten ein Recht auf Auskunft über die Funktionsweise des KI-Systems sowie die Funktion der verarbeiteten Beschäftigtendaten innerhalb des KI-Systems (Nummer 1). Bei diesen typischerweise besonders intransparenten Verarbeitungsvorgängen sollen betroffene Beschäftigte verstehen können, wie ihre Daten durch das KI-System verarbeitet werden. Darüber hinaus haben Beschäftigte einen Auskunftsanspruch über die Schutzmaßnahmen nach § 9 Absatz 1 Nummer 11 (Nummer 2), um die Risiken der Verarbeitung und die entsprechenden Maßnahmen des Arbeitgebers zum Schutz vor diesen Risiken einschätzen zu können.

## **Zu § 11 (Verwertungsverbot)**

Die prozessualen Folgen eines Verstoßes gegen das Datenschutzrecht wirken sich erheblich auf die praktische Bedeutung des Datenschutzrechts für Beschäftigte und Arbeitgeber aus. Wenn Arbeitgeber nach einer unrechtmäßigen Datenverarbeitung die dadurch erlangten Daten ohne Konsequenzen in einem Prozess über die Rechtmäßigkeit einer personellen Maßnahme gegen ihre Beschäftigten verwerten können, schwächt das die tatsächliche Wirkung der datenschutzrechtlichen Vorschriften und verfestigt den Verstoß gegen das Datenschutzrecht. Aufsichtsrechtliche Maßnahmen gegen den Arbeitgeber können insoweit keinen gleichermaßen effektiven Schutz für Beschäftigte bieten. Diese befinden sich gerade bei einseitig ausgesprochenen personellen Maßnahmen des Arbeitgebers in einer besonders sensiblen Situation eines strukturellen Machtungleichgewichts. Durch die Regelung eines Verwertungsverbots werden Fragen des Datenschutzrechts zum Gegenstand des gerichtlichen Verfahrens und damit einer gerichtlichen Prüfung unterzogen.

### **Zu Absatz 1**

Ein Verwertungsverbot schützt einerseits die Persönlichkeitsrechte der betroffenen Beschäftigten und gestaltet gleichzeitig das normgeprägte grundrechtsgleiche Recht auf rechtliches Gehör für den Arbeitgeber gesetzlich aus. Neben den Persönlichkeitsrechten der beschäftigten Person sind das allgemeine Interesse an einer funktionstüchtigen Rechtspflege sowie die Grundrechte des beweisführenden Arbeitgebers, insbesondere aus Artikel 12 Absatz 1 und Artikel 14 Absatz 1 des Grundgesetzes, zu beachten. In der bisherigen Rechtsprechungspraxis wird dieses Spannungsverhältnis durch eine Güter- und Interessenabwägung im Einzelfall aufgelöst. Eine ausdrückliche gesetzliche Regelung fördert die Rechtsklarheit und kann einen Anreiz zur Beachtung datenschutzrechtlicher Vorschriften durch den Arbeitgeber schaffen.

Absatz 1 Satz 1 regelt daher ein grundsätzliches Verwertungsverbot datenschutzrechtswidrig verarbeiteter Beschäftigtendaten in einem gerichtlichen Verfahren über die Rechtmäßigkeit einer auf diese Daten gestützten personellen Maßnahme des Arbeitgebers.

Der Begriff Verwertungsverbot umfasst – je nach prozessualer Situation – Sachvortrags- und Beweisverwertungsverbote. Diese grundsätzliche Entscheidung für ein Sachvortrags- und Beweisverwertungsverbot ist sachgerecht. Das Datenschutzrecht formt die verfassungsrechtlichen Persönlichkeitsrechte der Beschäftigten einfachgesetzlich aus. Insbesondere werden das Recht auf informationelle Selbstbestimmung, das Recht am eigenen Bild und das Recht am gesprochenen Wort als Ausflüsse des allgemeinen Persönlichkeitsrechts geschützt. Verstöße gegen das Datenschutzrecht dürfen deshalb grundsätzlich nicht durch eine prozessuale Verwertung der Beschäftigtendaten verfestigt werden. Wenn eine Datenverarbeitung etwa nicht die Voraussetzungen ihrer Rechtsgrundlage erfüllt, ist daher von einem Verwertungsverbot auszugehen. Das ausdrückliche gesetzliche Verwertungsverbot erfasst wegen der erhöhten Schutzbedürftigkeit in diesen Fällen lediglich gerichtliche Verfahren über personelle Maßnahmen wie etwa Kündigungsschutzklagen. In anderen Fällen wie Schadensersatz- und Herausgabeklagen gelten weiterhin die allgemeinen Grundsätze für prozessuale Verwertungsverbote. Darüber hinaus gilt das hier geregelte ausdrückliche Verwertungsverbot nur für datenschutzrechtswidrig verarbeitete Beschäftigtendaten. Nach der bisherigen Rechtsprechung anerkannte Verwertungsverbote, die nicht durch die datenschutzrechtswidrige Verarbeitung von Beschäftigtendaten begründet sind, bleiben unberührt.

Satz 2 schafft die Möglichkeit, in eng auszulegenden Ausnahmefällen vom Grundsatz der Unverwertbarkeit abzuweichen und aus verfassungsrechtlich gebotenen Gründen eine Verwertung zuzulassen. Damit eine prozessuale Verwertung von rechtswidrig verarbeiteten Daten ausnahmsweise möglich ist, müssen bei der gerichtlichen Verwertung die grundrechtlichen Interessen beider Seiten im Einzelfall in einem offensichtlichen Missverhältnis zulasten des Arbeitgebers stehen. Das ist der Fall, wenn mit der datenschutzrechtswidrigen Verarbeitung ausnahmsweise keine Verletzung von Grundrechten derjenigen beschäftigten

Person verbunden ist, gegenüber dem die jeweilige personelle Maßnahme ergeht. Dazu zählt insbesondere die Konstellation, in der ein bloß formaler Datenschutzverstoß ohne Eingriff in die Persönlichkeitsrechte der betroffenen Person vorliegt, etwa bei einem Verstoß gegen Dokumentationspflichten mit dem Zweck, die nachträgliche Rechtmäßigkeitskontrolle zu erleichtern. Ebenso liegt keine Verletzung von Persönlichkeitsrechten der von der personellen Maßnahme betroffenen beschäftigten Person vor, wenn lediglich Rechtspositionen nicht am Prozess beteiligter Dritter durch den Datenschutzverstoß betroffen sind.

In anderen Fällen kann die Abwägung beider grundrechtlich geschützter Interessen ein offensichtliches Missverhältnis ergeben, wenn ein besonders hohes grundrechtlich geschütztes Interesse des Arbeitgebers an einer gerichtlichen Verwertung besteht und der Eingriff in das Persönlichkeitsrecht der betroffenen beschäftigten Person von geringer Intensität ist.

In einem Rechtsstreit über eine außerordentliche Kündigung kann es etwa für ein hohes grundrechtlich geschütztes Interesse des Arbeitgebers an einer gerichtlichen Verwertung sprechen, wenn aufgrund einer vorsätzlichen Straftat durch die beschäftigte Person eine Weiterbeschäftigung vor dem Hintergrund der Interessen des Arbeitgebers aus den Artikeln 12 und 14 des Grundgesetzes unzumutbar ist. Ein bloß vertragswidriges Verhalten von Beschäftigten kann auch dann kein offensichtliches Missverhältnis begründen, wenn es vorsätzlich erfolgt.

Eine eher geringe Intensität des Eingriffs in die Grundrechte der beschäftigten Person kann vorliegen, wenn, etwa bei der vorherigen Datenverarbeitung durch den Arbeitgeber die zulässige Speicherung bei einer ansonsten rechtmäßigen offenen Videoüberwachung nur geringfügig überschritten wurde und lediglich dieser Verstoß durch eine Verwertung der Daten im folgenden Prozess verfestigt wird. Anders läge der Fall bei einer Vorratsdatenspeicherung über einen längeren Zeitraum. In einer rechtswidrig verdeckten Überwachung liegt ein tiefer Grundrechtseingriff, sodass in einem solchen Fall ein offensichtliches, erhebliches Überwiegen der Arbeitgeberinteressen bereits deshalb ausscheidet.

## **Zu Absatz 2**

Absatz 2 regelt, dass Verhandlungspartner zur Aufnahme von prozessualen Verwertungsverboten in Kollektivvereinbarungen berechtigt sind. Der Begriff der Kollektivvereinbarungen ist in § 2 Absatz 4 legaldefiniert. Um die Tarif- und Betriebsautonomie zu stärken, ermächtigt Absatz 2 die Verhandlungspartner ausdrücklich, für datenschutzrechtswidrige oder kollektivvereinbarungswidrige Verarbeitungen von Beschäftigtendaten ein Verwertungsverbot in Kollektivvereinbarungen aufzunehmen. So können ausgewogene Vereinbarungen getroffen werden, welche die gegenseitigen Interessen des Arbeitgebers an einer Verwertung und den Arbeitnehmerinnen und Arbeitnehmern am Schutz ihrer personenbezogenen Daten etwa in Bezug auf bestimmte Verarbeitungsvorgänge in einzelnen Betrieben in einen angemessenen und praxistauglichen Ausgleich bringen können. Auch kann die Aufnahme eines prozessualen Verwertungsverbots in eine Betriebsvereinbarung dazu beitragen, in bestimmten betrieblichen Verarbeitungsvorgängen die Einhaltung des Zweckbindungsprinzips hinsichtlich anfallender Beschäftigtendaten abzusichern und so Verfahren zur betrieblichen Mitbestimmung in der Praxis zu erleichtern. Im Rahmen ihrer Betriebs- und Tarifautonomie können die Verhandlungspartner auch vereinbaren, dass Verstöße gegen die Kollektivvereinbarungen bei der Datenvereinbarung zu einem prozessualen Verwertungsverbot führen.

## **Zu § 12 (Mitbestimmung bei der Bestellung und Abberufung von Datenschutzbeauftragten)**

§ 12 führt ein Mitbestimmungsrecht des Betriebsrats bei der Bestellung und Abberufung der oder des betrieblichen Datenschutzbeauftragten ein. Der Arbeitgeber ist nach Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 oder § 38 des Bundesdaten-



schutzgesetzes verpflichtet, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu bestellen. Die Aufgaben der oder des Datenschutzbeauftragten richten sich nach Artikel 39 der Verordnung (EU) 2016/679 und bestehen insoweit auch gegenüber dem Betriebsrat als Teil der verantwortlichen Stelle. Die oder der Datenschutzbeauftragte wird bisher allerdings nur vom Arbeitgeber ohne Beteiligung des Betriebsrats bestellt. Um das sich hieraus ergebende Spannungsverhältnis zwischen Arbeitgeber, Betriebsrat und Datenschutzbeauftragten aufzulösen und auch dem in § 79a Absatz 1 Satz 3 Betriebsverfassungsgesetz verankerten Grundsatz der gegenseitigen Unterstützungspflicht von Arbeitgeber und Betriebsrat Rechnung zu tragen, erhält der Betriebsrat ein Mitbestimmungsrecht bei der Bestellung und Abberufung der oder des Datenschutzbeauftragten.

Entscheidet sich der Arbeitgeber freiwillig oder weil er dazu verpflichtet ist, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu bestellen, hat der Betriebsrat bei dessen Auswahl mitzubestimmen, unabhängig davon, ob eine externe Person oder eine bereits im Unternehmen beschäftigte Person zu der oder dem Datenschutzbeauftragten bestellt wird. Das Mitbestimmungsrecht umfasst auch die grundlegende Frage, ob interne oder externe Datenschutzbeauftragte bestellt werden sollen. Mögliche weitere Rechte des Betriebsrats nach den §§ 99 ff. Betriebsverfassungsgesetz bleiben in diesem Zusammenhang unberührt. Auch kann der Betriebsrat seinerseits initiativ werden.

Die Mitbestimmung bei der Abberufung soll es dem Betriebsrat ermöglichen, insbesondere dann aktiv zu werden, wenn Bedenken gegen die Unabhängigkeit der oder des Datenschutzbeauftragten wegen der Besorgnis der Befangenheit bestehen. Eine Abberufung der oder des Datenschutzbeauftragten wegen der Erfüllung seiner Aufgaben ist nach Artikel 38 Absatz 3 Satz 2 der Verordnung (EU) 2016/679 nicht zulässig. Kommt es nicht zu einer Einigung bei Bestellung oder Abberufung kann jede der beiden Seiten die Einigungsstelle nach § 76 Betriebsverfassungsgesetz anrufen. Deren Spruch ersetzt die Einigung zwischen Arbeitgeber und Betriebsrat.

## **Zu Teil 2 (Besonderer Teil)**

### **Zu Kapitel 1 (Datenverarbeitung vor Begründung des Beschäftigungsverhältnisses)**

Kapitel 1 konkretisiert die Voraussetzungen für eine Verarbeitung von Beschäftigtendaten im Beschäftigungskontext für Zwecke der Einstellung sowie die Löschpflichten in Bezug auf Bewerbungsdaten. Es handelt sich um spezifischere Vorschriften im Sinne von Artikel 88 Absatz 1 der Verordnung (EU) 2016/679 in Umsetzung der dort geschaffenen Regelungsmöglichkeit, die auch in Erwägungsgrund 155 der Verordnung (EU) 2016/679 explizit benannt wird. Soweit aufgrund der Vorschriften dieses Kapitels besondere Kategorien von Beschäftigtendaten verarbeitet werden, handelt es sich zudem um Rechtsvorschriften im Sinne von Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679. Die erhöhten Anforderungen berücksichtigen die Besonderheiten des Beschäftigungsverhältnisses, insbesondere die verstärkte Drucksituation in der Bewerbungsphase und die daraus resultierende, besondere Schutzbedürftigkeit der Bewerberinnen und Bewerber. Die Vorschriften umfassen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Beschäftigten im Sinne von Artikel 88 Absatz 2 der Verordnung (EU) 2016/679.

### **Zu § 13 (Eignungsfeststellung)**

Die Vorschrift regelt die Datenverarbeitung in der Anbahnungsphase zum Zwecke der Eignungsfeststellung oder der Erfüllung von durch Rechtsvorschrift festgelegten Pflichten des Arbeitgebers, insbesondere durch mündliche und schriftliche Befragung der Bewerberinnen und Bewerber. Für diese Zwecke stellt die Vorschrift für Verarbeitungen vor Begründung eines Beschäftigungsverhältnisses gegenüber § 3 eine speziellere und vorrangig anzuwendende Regelung dar. Die Zulässigkeit der Datenverarbeitung zu sonstigen Zwecken, etwa zur Kontaktaufnahme, richtet sich nach § 3. Die Datenverarbeitung bei der Anmeldung zur

Sozialversicherung ist Teil der Durchführung des Beschäftigungsverhältnisses und beurteilt sich ebenfalls nicht nach § 13. Bewerberinnen und Bewerber sind gemäß § 2 Absatz 2 Nummer 8 Beschäftigte im Sinne dieses Gesetzes. Die Vorschriften dieses Abschnitts finden auch auf interne Bewerbungsverfahren auf eine andere Stelle innerhalb eines Betriebs oder einer Behörde Anwendung.

### **Zu Absatz 1**

Nach Absatz 1 ist die Verarbeitung von Beschäftigtendaten in der Bewerbungsphase zulässig, wenn und soweit deren Kenntnis für die Feststellung der fachlichen und persönlichen Eignung der Bewerberin oder des Bewerbers für die vorgesehene Tätigkeit erforderlich oder durch Rechtsvorschrift vorgeschrieben ist. Ferner müssen die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen, wobei die Abwägungskriterien aus § 4 zu beachten sind. Dies gilt auch für die Verarbeitung besonderer Kategorien von Beschäftigtendaten nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679. Absatz 1 der Vorschrift ist insofern eine nationale Rechtsvorschrift im Sinne von Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679.

Welche Daten im Einzelnen unter § 13 fallen können, richtet sich nach objektiven beruflichen Kriterien und dem vom Arbeitgeber festgelegten Anforderungsprofil. Die fachliche und persönliche Eignung im Sinne von Absatz 1 Nummer 1 umfasst auch die Kriterien für den Zugang zu öffentlichen Ämtern gemäß Artikel 33 Absatz 2 des Grundgesetzes.

Die Regelung in Nummer 1 entspricht der bisherigen Rechtsprechung des Bundesarbeitsgerichts, das ein Fragerecht des Arbeitgebers bei den Einstellungsverhandlungen nur insoweit anerkennt, als der Arbeitgeber ein berechtigtes, billigenswertes und schutzwürdiges Interesse an der Beantwortung seiner Frage im Hinblick auf das Beschäftigungsverhältnis hat. Eine auszuübende Tätigkeit im Sinne der Regelung liegt auch dann vor, wenn der Arbeitgeber verschiedene Stellen in einem Verfahren ausgeschrieben hat und im Bewerbungsverfahren entscheidet, welche Bewerberinnen und Bewerber auf welchen Stellen eingesetzt werden sollen.

Nummer 2 betrifft beispielsweise die aus § 154 des Neunten Buches Sozialgesetzbuch bestehende Pflicht zur Beschäftigung schwerbehinderter Menschen. In diesem Falle darf zwar nach § 14 Absatz 2 keine Auskunft über die Schwerbehinderung oder Gleichstellung mit einer Schwerbehinderung verlangt werden. Will der Arbeitgeber der Pflicht zur Beschäftigung schwerbehinderter oder gleichgestellter Menschen gemäß § 154 des Neunten Buches Sozialgesetzbuch nachkommen, kann er dieses Ziel z.B. durch einen entsprechenden Hinweis in der Stellenausschreibung erreichen. Damit bleibt es den Bewerberinnen und Bewerbern überlassen, ob sie dieses Datum offenlegen. Sofern sie dies freiwillig tun, darf es der Arbeitgeber gemäß Absatz 1 Nummer 2 verarbeiten.

### **Zu Absatz 2**

Die Regelungen zu Verarbeitungen durch oder aufgrund von Profiling finden entsprechende Anwendung, wenn eine Verarbeitung nach diesem Kapitel durch oder aufgrund von Profiling durchgeführt wird.

### **Zu Absatz 3**

Der Arbeitgeber hat bereits nach § 9 geeignete und besondere Maßnahmen zur Einhaltung der insbesondere in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze zu ergreifen, um die Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person sicherzustellen. Ergänzend zu dieser Pflicht sind nach dieser Vorschrift erhobene Daten besonders gegen Verletzungen ihrer Vertraulichkeit und

Integrität, insbesondere durch unbefugten Zugang zu schützen. Soweit die Daten elektronisch gespeichert oder etwa innerhalb der verantwortlichen Stelle per E-Mail weitergeleitet werden, ist als eine technische Maßnahme gesetzlich vorgeschrieben, dass diese in angemessener Weise verschlüsselt werden müssen. Die Art der notwendigen Verschlüsselung richtet sich entsprechend Artikel 32 der Verordnung (EU) 2016/679 nach dem Stand der Technik.

### **Zu § 14 (Fragerecht)**

Die Vorschrift regelt, unter welchen Voraussetzungen und in Bezug auf welche Merkmale der Arbeitgeber von Bewerberinnen und Bewerbern oder von Dritten Auskunft verlangen darf. Eine Auskunft bei Dritten ist nach den Kriterien gemäß § 4, insbesondere nach dessen Nummer 2 Buchstabe g, nur im Ausnahmefall zulässig. Das Auskunftsverlangen ist eine spezielle Art der Datenverarbeitung gemäß § 3 im Sinne einer Datenerhebung bei der betroffenen Person oder bei Dritten. Es erfasst neben der mündlichen Frage auch das Anfordern auf andere Weise, etwa durch das Verlangen, eine Schufa-Auskunft oder ein polizeiliches Führungszeugnis einzureichen. Für die Datenverarbeitung in der Bewerbungsphase durch Auskunftsverlangen ist § 14 in Bezug auf die in § 14 Absatz 1 aufgeführten Merkmale spezieller als und vorrangig gegenüber § 13.

Mit der Vorschrift wird eine Regelung gemäß Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 eingeführt, die abweichend von Artikel 9 Absatz 1 der Verordnung 2016/679 die Verarbeitung besonderer Kategorien personenbezogener Daten im Beschäftigungskontext erlaubt.

### **Zu Absatz 1**

Absatz 1 beschränkt das Fragerecht des Arbeitgebers hinsichtlich besonders schutzwürdiger Beschäftigtendaten, wie zum Beispiel die Frage nach Geschlecht, Herkunft oder Behinderung, um eine Diskriminierung von Bewerberinnen und Bewerbern im Einstellungsverfahren zu verhindern. Es handelt sich mithin um eine einschränkende Regelung des Fragerechts. Das Auskunftsrecht in Bezug auf den Namen, aus dem sich unter Umständen das Geschlecht oder die Herkunft herleiten, bleibt unberührt. Die Aufzählung der besonders schutzbedürftigen Daten in dieser Vorschrift ist dem Betriebsverfassungsrecht (§ 75 Absatz 1) und dem Allgemeinen Gleichbehandlungsgesetz (§ 1) nachgebildet und um weitere in der Rechtsprechung als besonders schutzbedürftig anerkannte Merkmale, wie die Vermögensverhältnisse und Vorstrafen, ergänzt. Satz 1 Nummer 1 lässt Fragen nach diesen besonders schutzbedürftigen Beschäftigtendaten in Anlehnung an § 8 Absatz 1 des Allgemeinen Gleichbehandlungsgesetzes zu, wenn sie wegen der auszuübenden Tätigkeit eine wesentliche und entscheidende berufliche Anforderung darstellen. Ferner müssen die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen, wobei die Abwägungskriterien aus § 4 zu beachten sind. Eine berufliche Anforderung ist demnach entscheidend, wenn sie für die vertragsgemäße Erfüllung der Arbeitsleistung erforderlich ist. Sie ist wesentlich, wenn ein hinreichend großer Teil der Gesamtanforderungen des Arbeitsplatzes betroffen ist. Hinsichtlich der Frage nach Vorstrafen und laufenden Ermittlungsverfahren ist die Vorschrift zugleich eine Regelung im Sinne von Artikel 10 Satz 1, 2. Alternative der Verordnung (EU) 2016/679 im Beschäftigungskontext. Gemäß Satz 2 bleiben die Vorschriften des Bundeszentralregistergesetzes unberührt. Das bedeutet insbesondere, dass Bewerberinnen und Bewerber sich gemäß § 53 Absatz 1 des Bundeszentralregistergesetzes als unbestraft bezeichnen dürfen und den der Verurteilung zugrundeliegenden Sachverhalt nicht zu offenbaren brauchen, wenn die dortigen Voraussetzungen vorliegen. Der Arbeitgeber darf Fragen nach Vorstrafen nur stellen, soweit deren Fehlen eine wesentliche und entscheidende berufliche Anforderung darstellt, so etwa bei Tätigkeiten in der Vermögensbetreuung in Bezug auf Vermögensstraftaten. Danach ist die Anforderung eines (allgemeinen) polizeilichen Führungszeugnisses unter dem Grundsatz der Erforderlichkeit nur ausnahmsweise zulässig, denn das Führungszeugnis enthält regelmäßig auch Eintragungen über Vorstrafen, die

nicht arbeitsplatzbezogen sind. Die Anforderung eines erweiterten Führungszeugnisses und die Verarbeitung der darin enthaltenen Beschäftigendaten sind nur unter den Voraussetzungen von § 30a des Bundeszentralregistergesetzes zulässig. In einem Bewerbungsverfahren für die Tätigkeit bei einer Partei darf der Arbeitgeber Auskunft über die Parteizugehörigkeit verlangen, soweit es sich dabei wegen der Art der Tätigkeit um eine wesentliche und entscheidende berufliche Anforderung handelt. Das ist beispielsweise im Bereich der Pforte oder Reinigung nicht gegeben.

Nach Satz 3 bleibt § 7 Absatz 2 des Bundesgleichstellungsgesetzes unberührt. Die Frage nach dem Familienstand, einer bestehenden oder geplanten Schwangerschaft, oder geplanten Familien- oder Pflegeaufgaben als Ausprägung der Diskriminierung nach dem Geschlecht ist gemäß § 7 Absatz 2 des Bundesgleichstellungsgesetzes unzulässig. Hierüber darf daher auch datenschutzrechtlich keine Auskunft verlangt werden.

### **Zu Absatz 2**

Da die Datenverarbeitung auf das erforderliche Maß zu beschränken ist, und zur Absicherung des Benachteiligungsverbot aus § 164 Absatz 2 des Neunten Buches Sozialgesetzbuch, wird nach dieser Regelung bestimmt, dass vor Begründung des Beschäftigungsverhältnisses kein Fragerecht nach der Schwerbehinderten- oder Gleichstellungseigenschaft besteht. Zur Erfüllung der sich aus dem Neunten Buch Sozialgesetzbuch ergebenden Pflichten des Arbeitgebers und Rechte der schwerbehinderten und diesen gleichgestellten behinderten Menschen bedarf es des Fragerechts des Arbeitgebers nach der Schwerbehinderten- oder Gleichstellungseigenschaft vor Begründung des Beschäftigungsverhältnisses nicht. Der Pflicht zur Erfüllung der Quote nach § 154 des Neunten Buches Sozialgesetzbuch kann der Arbeitgeber nachkommen, indem er es den Bewerberinnen und Bewerbern, z.B. durch einen entsprechenden Hinweis in der Stellenausschreibung freistellt, die Schwerbehinderteneigenschaft freiwillig anzugeben. Das Gleiche gilt für den öffentlichen Arbeitgeber hinsichtlich der Verpflichtung gemäß § 165 Satz 3 des Neunten Buches Sozialgesetzbuch, schwerbehinderte und gleichgestellte Bewerberinnen und Bewerber zum Vorstellungsgespräch einzuladen. Damit bleibt es den Beschäftigten überlassen, ob sie dieses Datum offenlegen.

### **Zu Absatz 3**

Absatz 3 enthält in Anlehnung an § 9 Absatz 1 des Allgemeinen Gleichbehandlungsgesetzes eine Regelung für das über Absatz 2 hinausgehende Fragerecht von Religionsgemeinschaften und die ihnen zugeordneten Einrichtungen oder von Vereinigungen, die sich die gemeinschaftliche Pflege einer Religion oder Weltanschauung zur Aufgabe gemacht haben. Die Regelung trägt dem Selbstverständnis und dem verfassungsrechtlich garantierten Selbstbestimmungsrecht der Religions- und Weltanschauungsgemeinschaften Rechnung. Außerhalb des durch das Selbstbestimmungsrecht geprägten Bereichs wird das Fragerecht des Arbeitgebers durch das Abstellen auf die Art der Tätigkeit auf die Bewerberinnen und Bewerber beschränkt, für deren zukünftige Tätigkeit die genannten Merkmale von Bedeutung sind, was beispielsweise im Bereich der Pforte oder Reinigung nicht der Fall ist. Ferner müssen die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen, wobei die Abwägungskriterien aus § 4 zu beachten sind. Die in Artikel 91 der Verordnung (EU) 2016/679 vorgesehene Möglichkeit der Anwendung kircheneigener Datenschutzvorgaben bleibt dabei unberührt, sodass kirchliche Regelungen, welche die Anforderungen des Artikel 91 der Verordnung (EU) 2016/679 erfüllen, nationalen Regelungen zum Beschäftigendatenschutz vorgehen.

#### **Zu Absatz 4**

Damit die Beschränkungen des Fragerechts des Arbeitgebers nicht umgangen werden, wird in Absatz 4 klargestellt, dass Auskünfte, die nach den Absätzen 1 bis 3 nicht verlangt werden dürfen, auch nicht aufgrund von Profiling im Sinne des § 24 hergeleitet werden dürfen.

Die Erweiterung der gesetzlichen Verarbeitungsbefugnisse aus dieser Vorschrift durch das Einholen einer datenschutzrechtlichen Einwilligung nach § 5 ist unzulässig. Das betrifft insbesondere die Einwilligung in die Vorlage eines polizeilichen Führungszeugnisses.

#### **Zu Absatz 5**

Der Arbeitgeber hat zusätzlich zu § 9 die in § 13 Absatz 3 aufgeführten Schutzmaßnahmen zu ergreifen.]

#### **Zu § 15 (Positive Maßnahmen)**

##### **Zu Absatz 1**

Daten über die in der Vorschrift aufgezählten Merkmale darf der Arbeitgeber gemäß § 14 nur in Ausnahmefällen erheben. In Anlehnung an § 5 des Allgemeinen Gleichbehandlungsgesetzes darf der Arbeitgeber sie, über die Zwecke der Eignungsfeststellung und der Erfüllung einer rechtlichen Verpflichtung hinaus, verarbeiten, soweit sie ihm im Bewerbungsverfahren durch die Bewerberin oder den Bewerber freiwillig mitgeteilt werden und die Datenverarbeitung erforderlich und auch im Übrigen verhältnismäßig ist, um durch geeignete und angemessene Maßnahmen nach § 5 des Allgemeinen Gleichbehandlungsgesetzes bestehende Nachteile zu verhindern oder auszugleichen (z.B. Maßnahmen zur Förderung von benachteiligten oder unterrepräsentierten Personengruppen). Für die Freiwilligkeit gelten die Maßstäbe für die Freiwilligkeit einer Einwilligung nach § 5 entsprechend. Ferner müssen die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen, wobei die Abwägungskriterien aus § 4 zu beachten sind. Mit der Vorschrift wird eine Regelung gemäß Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 eingeführt, die abweichend von Artikel 9 Absatz 1 der Verordnung 2016/679 die Verarbeitung besonderer Kategorien personenbezogener Daten im Beschäftigungskontext erlaubt.

##### **Zu Absatz 2**

Der Arbeitgeber hat zusätzlich zu § 9 die in § 13 Absatz 3 aufgeführten Schutzmaßnahmen zu ergreifen.

#### **Zu § 16 (Untersuchungen und Tests)**

§ 16 regelt die Zulässigkeit der Verarbeitung von Beschäftigtendaten im Rahmen von Gesundheitsuntersuchungen sowie psychologischen Eignungstests und -untersuchungen in der Bewerbungsphase. Für diesen Anwendungsbereich ist die Vorschrift eine abschließende und gegenüber § 3 sowie § 13 vorrangig anzuwendende, speziellere Regelung. Mit der Vorschrift wird eine Regelung gemäß Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 eingeführt, die abweichend von Artikel 9 Absatz 1 der Verordnung 2016/679 die Verarbeitung besonderer Kategorien personenbezogener Daten im Beschäftigungskontext erlaubt.

## **Zu Absatz 1**

Absatz 1 regelt die Voraussetzungen für eine Untersuchung des Gesundheitszustands zur Feststellung der Eignung von Bewerberinnen und Bewerbern für die auszuübende Tätigkeit. Der Gesundheitszustand muss zum Zeitpunkt der Arbeitsaufnahme eine wesentliche und entscheidende berufliche Anforderung darstellen. Hier wird ein Gleichlauf zum Fragerecht des Arbeitgebers nach § 14 hergestellt: Was nicht im Bewerbungsgespräch erfragt werden darf, darf auch nicht durch eine Untersuchung festgestellt werden. Beschäftigten-daten zum Gesundheitszustand dürfen zudem verarbeitet werden, soweit die Feststellung der gesundheitlichen Eignung zur Erfüllung von durch Rechtsvorschrift festgelegten Pflichten des Arbeitgebers erforderlich ist. Werden bestimmte gesundheitliche Untersuchungen gesetzlich konkret vorgeschrieben, handelt es sich um speziellere Vorschriften, die nach § 1 Absatz 4 dieses Gesetzes vorgehen, zum Beispiel §§ 32 ff. des Jugendarbeitsschutzgesetzes oder § 43 des Infektionsschutzgesetzes. Ebenso stellen die Mindestanforderungen an das Seh- und Hörvermögen gemäß Tabelle 1 und 2 des G 25 etwa bei Fahr-, Steuer- und Überwachungstätigkeiten wesentliche und entscheidende berufliche Anforderungen dar, von deren Vorliegen die Einstellung abhängig gemacht werden darf. Auch Drogen- und Alkoholtests nach Satz 2 können im Ausnahmefall eine wesentliche und entscheidende Anforderung für die vorgesehene Tätigkeit darstellen. Dies gilt etwa, wenn besondere Unfallrisiken oder Fremdgefährdungen bestehen, beispielsweise bei Berufskraftfahrerinnen und -fahrern, oder wenn der Arbeitsplatz mit dem Gebrauch von Waffen verbunden ist. Tests auf übertragbare Krankheiten können im Einzelfall zulässig sein, sofern ansonsten ein unvertretbares Infektionsrisiko für Dritte, etwa Patientinnen und Patienten, bestünde. Allerdings ist insbesondere die Durchführung oder Anforderung eines HIV-Tests grundsätzlich unzulässig, da das Vorliegen einer Infektion regelmäßig nicht die Eignung zur Berufsausübung beeinträchtigt, und zudem im Rahmen moderner Behandlungsmethoden lediglich eine sehr geringfügige Ansteckungsgefahr besteht. Ferner müssen die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen, wobei die Abwägungskriterien aus § 4 zu beachten sind. Nicht von Absatz 1 erfasst werden genetische Untersuchungen nach dem Gendiagnostikgesetz. Gemäß § 19 des Gendiagnostikgesetzes darf der Arbeitgeber diese vor Begründung des Beschäftigungsverhältnisses weder vornehmen lassen, noch die Ergebnisse bereits durchgeführter Untersuchungen anfordern oder sich mitteilen lassen.

## **Zu Absatz 2**

Neben Untersuchungen zum Gesundheitszustand nach Absatz 1 kommen zur Eignungsfeststellung auch psychologische Tests und Untersuchungen in Betracht. Dies umfasst standardisierte Verfahren zur Analyse von Persönlichkeit und Charaktereigenschaften, beispielsweise Assessment Center und Fragebögen, sowie technische Verfahren, wie Stimmanalysen. Arbeitsproben und einfache Bewerbungsgespräche werden hiervon nicht erfasst. Auch diese Verfahren sind nur unter der Voraussetzung zulässig, dass die dadurch erlangten Kenntnisse erforderlich sind, um festzustellen, ob der oder die Beschäftigte eine wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung wesentliche und entscheidende berufliche Anforderung erfüllt. Ferner müssen die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen, wobei die Abwägungskriterien aus § 4 zu beachten sind. Ein Bedürfnis kann insbesondere bei Arbeitsaufgaben bestehen, die in besonders hohem Maße Zuverlässigkeit und Belastbarkeit in Krisensituationen erfordern. Auch allgemeine Intelligenz- und Persönlichkeitstests müssen einen klaren Bezug zu den jeweiligen Stellenanforderungen aufweisen.

Zusätzlich müssen die eingesetzten Verfahren, die Art und Weise der Durchführung und die Qualifikation der prüfenden Person wissenschaftlichen Standards entsprechen. Hierzu gehören insbesondere die Anforderungen der DIN 33430 in ihrer jeweils geltenden Fassung. Gegenstand der DIN 33430 sind Qualitätskriterien und -standards für berufsbezo-

gene Eignungsdiagnostik. Die Norm trifft Aussagen zu der Qualifikation der beteiligten Personen, der Qualität der verwendeten Instrumente und dem Zusammenspiel und Design von Prozessschritten und Abläufen. Durch ihre verpflichtende Einhaltung wird sichergestellt, dass Tests und Untersuchungen geltenden Standards entsprechen und durch qualifiziertes Personal durchgeführt werden. Demnach sind etwa graphologische und astrologische Tests unzulässig. Bei Personalfragebögen ist zudem das Mitbestimmungsrecht aus § 94 Absatz 1 des Betriebsverfassungsgesetzes bzw. § 80 Absatz 1 Nummer 15 Bundespersonalvertretungsgesetz zu beachten.

### **Zu Absatz 3**

Dem Arbeitgeber darf als Untersuchungsergebnis nur eine allgemeine Auskunft über die gesundheitliche Eignung der Bewerberin oder des Bewerbers erteilt werden („geeignet“ oder „nicht geeignet“), sofern das die Untersuchung durchführende Personal einer beruflichen Schweigepflicht unterliegt. Das Vorliegen einer beruflichen Schweigepflicht richtet sich nach § 203 des Strafgesetzbuches und betrifft im Zusammenhang mit Einstellungsuntersuchungen insbesondere Ärztinnen und Ärzte, sowie Berufspsychologinnen und -psychologen. Bewerberinnen und Bewerber sind hingegen auf ihr Verlangen umfassend über den Inhalt des Test- oder Untersuchungsergebnisses zu informieren. Wegen des Rechts auf Nichtwissen über den eigenen Gesundheitszustand dürfen den Bewerberinnen und Bewerbern über das Ergebnis hinausgehende Inhalte aber nicht ungefragt mitgeteilt werden.

### **Zu Absatz 4**

Der Arbeitgeber muss Bewerberinnen und Bewerber über eine Datenverarbeitung im Rahmen von Gesundheitsuntersuchungen oder psychologischen Tests und Untersuchungen stets im Sinne der Artikel 13 Absatz 1 bis 3 und Artikel 14 Absatz 1 bis 4 der Verordnung (EU) 2016/679 informieren. Gesetzliche Ausnahmen von diesen Vorschriften, insbesondere nach Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 sowie nach §§ 33, 34 des Bundesdatenschutzgesetzes, sind ausgeschlossen.

### **Zu Absatz 5**

Der Arbeitgeber hat zusätzlich zu § 9 die in § 13 Absatz 3 aufgeführten Schutzmaßnahmen zu ergreifen.

### **Zu § 17 (Löschpflichten)**

Artikel 17 der Verordnung (EU) 2016/679 regelt das Recht auf Löschung für die betroffene Person und die Pflicht zur Löschung für den Verantwortlichen. Wenn feststeht, dass ein Beschäftigungsverhältnis nicht zustande kommt, bestehen in der Praxis Unsicherheiten darüber, wann während eines Auswahlverfahrens verarbeitete Beschäftigtendaten gelöscht werden müssen. Dies führt zu unterschiedlichen Vorgehensweisen bei Arbeitgebern. § 17 präzisiert daher die Vorgaben für die Löschung vor der Eingehung eines Beschäftigungsverhältnisses verarbeiteter Beschäftigtendaten

### **Zu Absatz 1**

Absatz 1 Satz 1 konkretisiert die Regelung aus Artikel 17 Absatz 1 Buchstabe a und Absatz 3 Buchstabe e der Verordnung (EU) 2016/679. Vor Begründung eines Beschäftigungsverhältnisses verarbeitete Daten sind spätestens drei Monate nachdem feststeht, dass ein Beschäftigungsverhältnis nicht zustande kommt, zu löschen. Aus Artikel 17 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 ergibt sich, dass vor der Eingehung eines Beschäftigungsverhältnisses verarbeitete Beschäftigtendaten einer Bewerberin oder eines Bewerbers zu löschen sind, sobald feststeht, dass ein Beschäftigungsverhältnis mit dieser Person nicht zustande kommt. Eine Ausnahme besteht nach Artikel 17 Absatz 3 Buchstabe e der

Verordnung (EU) 2016/679 zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Wird eine Bewerbung abgelehnt, können Bewerberinnen und Bewerber unter Umständen Schadensersatz- oder Entschädigungsansprüche wegen eines Verstoßes gegen das Benachteiligungsverbot nach § 15 des Allgemeinen Gleichbehandlungsgesetzes geltend machen. In diesem Fall muss der Arbeitgeber in der Lage sein, sich gegen einen Schadensersatz- oder Entschädigungsanspruch zu verteidigen. Der Zeitraum von drei Monaten knüpft an die Ausschlussfrist nach § 15 Absatz 4 des Allgemeinen Gleichbehandlungsgesetzes an. Danach müssen abgelehnte Bewerberinnen und Bewerber Schadensersatz- oder Entschädigungsansprüche wegen Verstößen gegen das Benachteiligungsverbot innerhalb von zwei Monaten nach Zugang der ablehnenden Entscheidung schriftlich geltend machen. Auch unter Berücksichtigung möglicher Verzögerungen, etwa beim Zugang der Ablehnung, ist drei Monate nach einer ablehnenden Entscheidung im Regelfall nicht mehr damit zu rechnen, dass Rechtsansprüche gegen den Arbeitgeber geltend gemacht werden.

Ausnahmsweise kann nach Absatz 1 Satz 2 eine Speicherung auch über drei Monate hinaus erforderlich sein, wenn ein Rechtsstreit anhängig oder aufgrund konkreter Anhaltspunkte wahrscheinlich ist. Dazu gehört insbesondere der Fall, dass Ansprüche innerhalb der Frist des § 15 Absatz 4 des Allgemeinen Gleichbehandlungsgesetzes schriftlich geltend gemacht wurden. Um zu verhindern, dass eine ausufernde Speicherung pauschal mit dem Verweis auf einen möglichen Rechtsstreit begründet wird, ist es sachgerecht, dass Arbeitgeber ab einem Zeitpunkt von drei Monaten nach der ablehnenden Entscheidung die besonderen Gründe für eine weitere Speicherung dokumentieren müssen. Absatz 1 Satz 3 konkretisiert Artikel 17 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 für den Fall, dass eine Bewerberin oder ein Bewerber ihre Bewerbung selbst zurückzieht. In diesem Fall sind die Beschäftigtendaten grundsätzlich unverzüglich zu löschen, da sie für den Zweck der Durchführung des Bewerbungsverfahrens nicht mehr erforderlich sind und der Arbeitgeber nicht mit der Geltendmachung von Rechtsansprüchen durch die Bewerberin oder Bewerber rechnen muss.

### **Zu Absatz 2**

Absatz 2 regelt, dass personenbezogene Daten von Bewerberinnen und Bewerbern abweichend von Absatz 1 zum Zweck des Abgleichs mit offenen Stellen und der Kontaktaufnahme für spätere Auswahlverfahren gespeichert bleiben und verarbeitet werden können, wenn die betroffene Person nach der Beendigung des Auswahlverfahrens einwilligt. Damit sollen etwa „Bewerberpools“ ermöglicht werden. Voraussetzung ist eine wirksame, freiwillige Einwilligung unter Berücksichtigung von § 5. Während des Auswahlverfahrens könnten Bewerberinnen und Bewerber sich unter Druck gesetzt fühlen, dem potentiellen Arbeitgeber eine weitere Nutzung ihrer Daten nicht zu untersagen. Die Einwilligung kann deshalb erst nach dem Abschluss des Bewerbungsverfahrens Grundlage für die Speicherung sein, wenn der Druck eines konkreten Auswahlverfahrens entfällt.

### **Zu Kapitel 2 (Überwachung)**

Kapitel 2 konkretisiert die Voraussetzungen für eine Verarbeitung von Beschäftigtendaten im Beschäftigungskontext durch Überwachungsmaßnahmen. Es handelt sich um spezifischere Vorschriften im Sinne von Artikel 88 Absatz 1 der Verordnung (EU) 2016/679 in Umsetzung der dort geschaffenen Regelungsmöglichkeit. Die erhöhten Anforderungen berücksichtigen die Besonderheiten des Beschäftigungsverhältnisses, insbesondere die besondere Eingriffstiefe in das Recht auf informationelle Selbstbestimmung, die mit Überwachungsmaßnahmen einhergeht, sowie die Gefahr eines permanenten Anpassungs- und Überwachungsdrucks. Die Vorschriften umfassen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Beschäftigten im Sinne von Artikel 88 Absatz 2 der Verordnung (EU) 2016/679.



## **Zu § 18 (Überwachung von Beschäftigten)**

### **Zu Absatz 1, Absatz 2 und Absatz 3**

Die Vorschrift regelt die Zulässigkeit der Verarbeitung von Beschäftigtendaten durch Überwachungsmaßnahmen. Überwachungsmaßnahmen werden in Absatz 3 als Maßnahmen zur zielgerichteten Beobachtung von Personen oder Objekten durch Personen oder technische Einrichtungen legaldefiniert. Dies gilt nur, wenn Beschäftigtendaten ganz oder teilweise automatisiert verarbeitet werden, sowie wenn nichtautomatisiert verarbeitete Beschäftigtendaten in einem Dateisystem gespeichert werden oder gespeichert werden sollen. Ausgenommen sind rein manuelle Verarbeitungen, die nicht in einem Dateisystem gespeichert werden sollen. Damit soll sichergestellt werden, dass alltägliche Interaktionen in der Zusammenarbeit von Beschäftigten und Vorgesetzten nicht per se an den Vorschriften zu Überwachung gemessen werden müssen.

Die Überwachung ist nicht der Zweck, sondern das Mittel der Datenverarbeitung. Der Zweck kann etwa in der Verhütung und Aufdeckung von Straftaten oder im Arbeitsschutz liegen. Die Vorschrift erfasst zum einen die gezielte Überwachung von Beschäftigten, etwa um deren Gesundheit und Sicherheit zu schützen, zur Aufdeckung von Straftaten und Pflichtverletzungen oder zur Leistungskontrolle. Der Begriff der „Pflichtverletzung“ bezieht sich auf Pflichten aus dem Beschäftigungsverhältnis, einschließlich Neben- und Rücksichtnahmepflichten.

Die Überwachung als Mittel der Datenverarbeitung erfasst aber auch Maßnahmen, die sich nicht final auf Beschäftigte richten, diese aber faktisch miterfassen. So kommt es auch bei der Überwachung von beweglichen Gegenständen oder Betriebsstätten häufig zu einer Verarbeitung von Beschäftigtendaten. Dies betrifft etwa die Videoüberwachung von Eingangsbereichen, Grundstücken und Lagerräumen, oder eine Ortung von Werttransportern. Auch eine Überwachung zum Schutz vor Rechtsgutsverletzungen durch Dritte, etwa die Videoüberwachung von Supermarktregalen zum Schutz vor Diebstählen, kann mit einer Überwachung sich im Rahmen ihrer Tätigkeit im Bereich etwa der Kameras aufhaltender Beschäftigter einhergehen. Auf Überwachungsmaßnahmen, bei denen keine Beschäftigtendaten verarbeitet werden, ist die Vorschrift nicht anzuwenden. Die Überprüfung der Arbeitsergebnisse und die im Nachhinein erfolgende Durchsicht physischer oder elektronischer Dokumente beinhalten keine Beobachtung und fallen daher nicht unter den Überwachungsbegriff nach diesem Abschnitt.

Das berechtigte Interesse des Arbeitgebers oder Dienstherrn an der Aufsicht über den Betrieb und die Einhaltung gesetzlicher Pflichten erfordern die Durchführung gewisser Maßnahmen zur Kontrolle und Überwachung. Gleichzeitig greift die Überwachung von Beschäftigten tief in das Grundrecht auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 des Grundgesetzes ein. Beschäftigte dürfen keinem permanenten Anpassungs- und Überwachungsdruck ausgesetzt werden. Die Verarbeitung von Beschäftigtendaten durch Überwachungsmaßnahmen unterliegt daher einer strikten Erforderlichkeits- und Verhältnismäßigkeitsprüfung.

Absatz 1 und 2 dieser Vorschrift konkretisieren die zulässigen Zwecke, sowie die Anforderungen an die Erforderlichkeit und Verhältnismäßigkeit. So dürfen Beschäftigtendaten im Rahmen von Überwachungsmaßnahmen grundsätzlich nur kurzzeitig und anlassbezogen, also etwa bei Vorliegen des Verdachts auf eine Straftat oder Pflichtverletzung, oder aber kurzzeitig und stichprobenhaft verarbeitet werden. Die zulässige Art und Weise sowie die zulässige Dauer der Überwachungsmaßnahme bestimmen sich nach der Erforderlichkeit im Einzelfall. Eine kurzzeitige Überwachungsmaßnahme kann insbesondere vorliegen, wenn die damit einhergehende Verarbeitung von Beschäftigtendaten einen so unerheblichen Teil der Arbeitszeit betrifft, dass keine Gefahr eines permanenten Anpassungs- und Überwachungsdrucks entsteht. Die Erheblichkeit in Bezug auf die Arbeitszeit ist bei einma-

ligen Maßnahmen am einzelnen Arbeitstag zu messen, bei wiederholten Maßnahmen hingegen an dem gesamten Zeitraum, auf den sich die Maßnahmen erstrecken, etwa auf Arbeitswochen oder das Arbeitsjahr. Eine nicht nur kurzzeitige Überwachung von Beschäftigten ist grundsätzlich unzulässig. Ausnahmen hierzu regelt § 19.

Ferner müssen die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen, wobei die Abwägungskriterien aus Absatz 4 und § 4 zu beachten sind.

#### **Zu Absatz 4**

Absatz 4 der Vorschrift legt Kriterien fest, die über die allgemeinen, im Rahmen der Interessenabwägung stets zu berücksichtigenden Kriterien aus § 4 hinaus bei Datenverarbeitungen durch Überwachungsmaßnahmen zu beachten sind. Die Kriterien nach den Nummern 1 und 2 sind bei jeder Überwachungsmaßnahme zu beachten. Nummer 2 stellt auf den durch die Maßnahme entstehenden Anpassungs- und Überwachungsdruck ab. Die Nummer 3 betrifft anlassbezogene Überwachungsmaßnahmen, also solche, bei denen aufgrund eines tatsächlichen Ereignisses der Verdacht einer Straftat oder Pflichtverletzung im Raum steht. Unter den Begriff der Pflichtverletzung fallen im Sinne einer vertraglichen Nebenpflicht auch Verstöße von Beschäftigten gegen gesetzliche Pflichten, die den Arbeitgeber treffen, etwa im Bereich des Umweltrechts. Die Kriterien nach Nummer 4 beziehen sich auf präventive Überwachungsmaßnahmen zur Verhütung von Straftaten und Pflichtverletzungen.

#### **Zu Absatz 5**

Absatz 5 stellt klar, dass den Beschäftigten zum Schutz ihres Allgemeinen Persönlichkeitsrechts aus Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 des Grundgesetzes Rückzugsorte verbleiben müssen, an denen eine Überwachung nicht stattfindet. Eine Verletzung des Kernbereichs privater Lebensgestaltung ist stets unzulässig. Dies betrifft insbesondere Orte, die der Intimsphäre der Beschäftigten zuzuordnen sind, also etwa Sanitär-, Umkleide- und Schlafräume. Aber auch in kollektiven und kommunikativen Rückzugsräumen, wie etwa Kantinen und Pausenräumen, ist eine Überwachung unzulässig. An diesen Orten besteht zum einen eine berechnete Privatheitserwartung der Beschäftigten. Zum anderen dienen diese Orte nicht der Erfüllung der gegenüber dem Arbeitgeber bestehenden Verpflichtungen durch die Beschäftigten und sind dessen Kontrollbefugnis insofern grundsätzlich entzogen.

#### **Zu Absatz 6**

Durch Überwachungsmaßnahmen dürfen besondere Kategorien von Beschäftigtendaten im Sinne von § 6 Absatz 1 verarbeitet werden, sofern die Voraussetzungen für eine Datenverarbeitung durch Überwachung, sowie zusätzlich ein Ausnahmetatbestand nach Artikel 9 der Verordnung (EU) 2016/679 oder nach § 6 Absatz 1 vorliegen. Bei der Auswahl geeigneter und besonderer Schutzmaßnahmen muss der Arbeitgeber beachten, dass besondere Kategorien von Beschäftigtendaten besonders sensibel und schutzbedürftig sind.

#### **Zu § 19 (Nicht nur kurzzeitige Überwachungsmaßnahmen)**

##### **Zu Absatz 1 und Absatz 2**

Die Vorschrift regelt, wann eine entweder anlassbezogene oder stichprobenhafte, aber nicht nur kurzzeitige Überwachung von Beschäftigten zulässig ist. Eine nicht nur kurzzeitige Überwachungsmaßnahme kann insbesondere vorliegen, wenn die damit einhergehende Verarbeitung von Beschäftigtendaten einen so erheblichen Teil der Arbeitszeit betrifft, dass die Gefahr eines permanenten Anpassungs- und Überwachungsdrucks entsteht. Die Er-

heblichkeit ist bei einmaligen Maßnahmen am einzelnen Arbeitstag zu messen, bei wiederholten Maßnahmen hingegen an dem gesamten Zeitraum, auf den sich die Maßnahmen erstrecken, etwa auf Arbeitswochen oder das Arbeitsjahr. Die nicht nur kurzzeitige Überwachung beinhaltet einen besonders tiefen Eingriff in das Grundrecht auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 des Grundgesetzes und ist daher nur in eng begrenzten Ausnahmefällen zulässig. Sie kann insbesondere zulässig sein, wenn sie der Sicherheit von Beschäftigten dient, die bei ihrer Tätigkeit besonderen Gefahren ausgesetzt sind, etwa bei Feuerwehrleuten im Einsatz. Ebenso kann in bestimmten Fällen eine kontinuierliche Überwachung zum Schutz Dritter erforderlich sein, beispielsweise im Falle von Pilotinnen und Piloten oder bei medizinischem Personal während eines operativen Eingriffs. Eine nicht nur kurzzeitige Überwachung kann im Einzelfall auch zum Schutz besonders hochwertiger oder sicherheitsrelevanter Gegenstände zulässig sein, etwa bei einer Überwachung von Werttransportern oder bei Anlagen mit Bedeutung für die nationale Sicherheit. Des Weiteren kommt eine längerfristige Überwachung zum Zwecke der IT-Sicherheit in Betracht. In Anlehnung an Artikel 32 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 meint Belastbarkeit die Widerstandsfähigkeit oder Ausfallsicherheit eines IT-Systems gegenüber Störungen. Auch die Aufdeckung von Straftaten kann, bei entsprechender Schwere des Tatvorwurfes und -verdachts, im Einzelfall zulässiger Zweck einer nicht nur kurzzeitigen Überwachungsmaßnahme sein. Absatz 1 Satz 2 stellt klar, dass die allgemeinen Voraussetzungen für Überwachungsmaßnahmen auch auf die nicht nur kurzzeitige Überwachung anzuwenden sind.

Die Erforderlichkeit und Verhältnismäßigkeit der Überwachungsmaßnahme sind jeweils im konkreten Einzelfall zu prüfen, wobei vor allem im Hinblick auf den konkret erforderlichen Umfang ein strenger Maßstab anzulegen ist. Auch für die Interessenabwägung gelten aufgrund des hohen Risikos für einen permanenten Anpassungs- und Überwachungsdruck besonders strenge Maßstäbe. Der Arbeitgeber muss als positive Voraussetzung der Rechtmäßigkeit einer Verarbeitung von Beschäftigtendaten darlegen, dass die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung erheblich überwiegen. Auf der einen Seite muss der Arbeitgeber besonders wichtige eigene Interessen darlegen oder aus objektiver Sicht auch im Interesse der Beschäftigten handeln. Auf der anderen Seite müssen Risiken für die Rechte und Interessen der Beschäftigten im Einzelfall in einem beherrschbaren Rahmen liegen. Bei der Abwägung der Interessen sind die Kriterien aus § 4 und § 18 Absatz 4 zu berücksichtigen.

### **Zu Absatz 3**

Absatz 3 stellt klar, dass eine nicht nur kurzzeitige Überwachung von Beschäftigten zu Zwecken der Leistungskontrolle stets unzulässig ist, da sie hierzu kein erforderliches und angemessenes Mittel ist. Eine Leistungskontrolle kann stets in ausreichender Weise über kurzzeitige, stichprobenhafte Maßnahmen erreicht werden. Eine längerfristige Überwachung zur Leistungskontrolle setzt Beschäftigte einem unangemessenen Leistungs- und Anpassungsdruck aus. Zweckmäßig für eine Leistungskontrolle ist insbesondere eine Überprüfung der Arbeitsergebnisse, die nicht unter den Begriff der Überwachung fällt und daher datenschutzrechtlich nicht nach den speziellen Regelungen der §§ 18 und 19 zu beurteilen ist.

### **Zu Absatz 4**

Der Arbeitgeber hat bereits nach § 9 geeignete und besondere Maßnahmen zur Einhaltung der insbesondere in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze zu ergreifen, um die Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person sicherzustellen. Ergänzend zu dieser Pflicht ist vor jeder nicht nur kurzzeitigen Überwachung von Beschäftigten der oder die betriebliche oder behördliche Datenschutzbeauftragte im Sinne des Artikel 38 Absatz 1 der Verordnung (EU) 2016/679 einzubeziehen. Bei mehreren gleichgelagerten Maßnahmen genügt eine einmalige Einbeziehung.

### **Zu Absatz 5**

Durch nicht nur kurzzeitige Überwachungsmaßnahmen dürfen besondere Kategorien von Beschäftigtendaten im Sinne von § 6 Absatz 1 verarbeitet werden, sofern die Voraussetzungen für eine Datenverarbeitung durch nicht nur kurzzeitige Überwachung, sowie zusätzlich ein Ausnahmetatbestand nach Artikel 9 der Verordnung (EU) 2016/679 oder von § 6 Absatz 1 vorliegen. Bei der Auswahl geeigneter und besonderer Schutzmaßnahmen muss der Arbeitgeber beachten, dass besondere Kategorien von Beschäftigtendaten besonders sensibel und schutzbedürftig sind.

### **Zu § 20 (Verdeckte Überwachung)**

#### **Zu Absatz 1**

Die Vorschrift enthält keine Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten, sondern regelt als nationale Rechtsvorschrift im Sinne von Artikel 23 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679 eine Ausnahme von der Informationspflicht des Verantwortlichen aus Artikel 13 und 14 der Verordnung (EU) 2016/679. Danach dürfen Beschäftigtendaten durch Überwachungsmaßnahmen unter engen Voraussetzungen auch verarbeitet werden, ohne dass die betroffenen Beschäftigten hierüber informiert werden. Eine solche verdeckte Überwachung kommt in Betracht, wenn der konkrete Verdacht besteht, dass im Beschäftigungsverhältnis eine Straftat oder schwere Pflichtverletzung begangen wurde und die verdeckte Überwachung die Ultima Ratio ist, um diese Straftat oder schwere Pflichtverletzung aufzudecken. Alle anderen zumutbaren Möglichkeiten, die Straftat oder schwere Pflichtverletzung aufzuklären, müssen ausgeschöpft sein. Der Verdacht muss sich noch nicht auf einen bestimmten Beschäftigten konkretisiert haben. Er muss sich aber auf einen räumlich und funktional abgrenzbaren Kreis von Beschäftigten, sowie auf einen abgrenzbaren Ort beziehen. Unter diesen Voraussetzungen kann es auch zulässig sein, dass einzelne Beschäftigte, die nicht dem Kreis der Verdächtigen angehören, von der Überwachung betroffen sind.

#### **Zu Absatz 2**

Absatz 2 der Vorschrift regelt, dass die betroffenen Beschäftigten unverzüglich über die verdeckte Überwachungsmaßnahme im Sinne der Artikel 13 und 14 der Verordnung (EU) 2016/679 informiert werden müssen, sobald die Aufdeckung der Straftat oder schweren Pflichtverletzung hierdurch nicht mehr gefährdet wird. Dies ist insbesondere der Fall, wenn die Tat erfolgreich aufgedeckt worden ist, oder aber sich der Verdacht entkräftet hat.

#### **Zu Absatz 3**

Der Arbeitgeber hat bereits nach § 9 geeignete und besondere Maßnahmen zur Einhaltung der insbesondere in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze zu ergreifen, um die Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person sicherzustellen. Absatz 3 stellt ergänzend dazu klar, dass vor jeder verdeckten Überwachung von Beschäftigten der oder die betriebliche oder behördliche Datenschutzbeauftragte im Sinne des Artikel 38 Absatz 1 der Verordnung (EU) 2016/679 frühzeitig und ordnungsgemäß einzubeziehen ist.

### **Zu § 21 (Videoüberwachung)**

Die Vorschrift stellt für eine Videoüberwachung, bei der zugleich personenbezogene Beschäftigtendaten verarbeitet werden, zusätzliche Voraussetzungen auf. Die Videoüberwachung greift besonders tief in die informationelle Selbstbestimmung von Beschäftigten ein, da sie es ermöglicht, umfassende, und mehr als die aufgrund des Verarbeitungszwecks erstrebten Informationen über ihr Verhalten zu gewinnen.

### **Zu Absatz 1 und Absatz 2**

Die Absätze 1 und 2 verdeutlichen und konkretisieren gegenüber § 18 Absatz 1 Satz 1 für welche grundsätzlich legitimen Zwecke eine Videoüberwachung typischerweise in Betracht kommt. Danach ist die Videoüberwachung insbesondere legitim, um Straftaten durch Beschäftigte oder Dritte zu verhüten oder aufzuklären. Zum Zwecke der Leistungskontrolle ist sie hingegen regelmäßig unzulässig. Absatz 1 Satz 3 stellt klar, dass die allgemeinen Voraussetzungen für Überwachungsmaßnahmen auch auf die Videoüberwachung anzuwenden sind.

### **Zu Absatz 3**

Absatz 3 definiert den Begriff der Videoüberwachung. Aus der Definition der Videoüberwachung, die sich nur auf „optische“ Einrichtungen bezieht ergibt sich, dass Tonaufnahmen unzulässig sind. Bei Tonaufnahmen im Rahmen einer Videoüberwachung am Arbeitsplatz kann nicht ausgeschlossen werden kann, dass Informationen erhoben werden, deren Abhören und Aufzeichnen gegen § 206 des Strafgesetzbuches verstößt. Mögliche Tonaufnahmefunktionen sind dauerhaft zu deaktivieren.

### **Zu Absatz 4**

Aufgrund der erhöhten Eingriffsintensität ist eine präventive Videoüberwachung nur zulässig, wenn eine nachweisbare, konkrete Gefahrenlage besteht, die über das allgemeine Lebensrisiko hinausgeht, etwa durch Vorfälle in der Vergangenheit. Allgemeine Statistiken und subjektive Befürchtungen reichen nicht aus. Eine abstrakte Gefahr reicht ausnahmsweise aus, wenn eine Situation vorliegt, die nach allgemeiner Lebenserfahrung typischerweise gefährlich ist, etwa die Gefahr von Einbrüchen bei einem Juweliergeschäft. Zusätzlich ist eine präventive Videoüberwachung nur zur Verhütung von Straftaten oder schweren Pflichtverletzungen, nicht aber zur Verhütung von einfachen Pflichtverletzungen zulässig.

### **Zu Absatz 5 und Absatz 6**

Die Absätze 5 und 6 konkretisieren die Anforderungen an die Erforderlichkeit sowie an die gemäß § 9 zu treffenden Schutzmaßnahmen.

Der Arbeitgeber muss durch technische Mittel oder auch bloßes Abkleben verhindern, dass für die Erfüllung des Verarbeitungszwecks nicht erforderliche Personen oder Bildausschnitte aufgezeichnet werden.

Zusätzlich muss die Videoüberwachung durch Piktogramme und Kurz-Informationen erkennbar gemacht werden. Auf einer zweiten Stufe müssen im Rahmen der Informationspflichten des Verantwortlichen aus Artikel 13 und 14 der Verordnung (EU) 2016/679 die übrigen hiernach erforderlichen Informationen erteilt werden.

Die regelmäßige Speicherfrist von 72 Stunden beruht darauf, dass innerhalb dieses Zeitraums in aller Regel geklärt werden kann, ob ein Vorfall eingetreten ist, der eine weitergehende Speicherung oder Verarbeitung erfordert. Derartige Gründe sind zu dokumentieren. Eine längere Speicherdauer kommt etwa über Feiertage oder Betriebsferien in Betracht.

### **Zu Absatz 7**

Absatz 7 sieht vor, dass die Regelungen über nicht nur kurzzeitige Überwachungsmaßnahmen auch für eine Videoüberwachung gelten. Die nicht nur kurzzeitige Videoüberwachung ist demnach nur zu den Zwecken aus § 19 Absatz 1 und 2 und unter den zusätzlichen Voraussetzungen von § 19 Absatz 3 und 5 zulässig. Eine längerfristige Videoüberwachung zur Verhütung von Straftaten und schweren Pflichtverletzungen im Sinne von Absatz 4 ist unzulässig.

Eine verdeckte Videoüberwachung ist nur unter den besonderen Voraussetzungen von § 20 zulässig.

### **Zu Absatz 8**

Durch Videoüberwachung dürfen besondere Kategorien von Beschäftigtendaten im Sinne von § 6 Absatz 1 verarbeitet werden, sofern die Voraussetzungen für eine Datenverarbeitung durch Videoüberwachung, sowie zusätzlich ein Ausnahmetatbestand nach Artikel 9 der Verordnung (EU) 2016/679 oder von § 6 Absatz 1 vorliegen. Bei der Auswahl geeigneter und besonderer Schutzmaßnahmen muss der Arbeitgeber beachten, dass besondere Kategorien von Beschäftigtendaten besonders sensibel und schutzbedürftig sind.

### **Zu § 22 (Ortung)**

Ortung ist als spezieller Fall der Überwachung die Bestimmung des geografischen Standortes mittels technischer Einrichtungen, etwa durch GPS-Systeme oder RFID-Chips. Sie spielt insbesondere bei der Nutzung von Dienstfahrzeugen, zunehmend aber auch bei mobilen Endgeräten eine Rolle. Bei einem nicht nur kurzzeitigen Einsatz bietet sie die Möglichkeit, umfassende Bewegungsprofile zu erstellen, die weitreichende Rückschlüsse auf das Verhalten der betroffenen Beschäftigten zulassen. Wegen des Risikos für die Persönlichkeitsrechte von Beschäftigten gelten besondere Anforderungen.

### **Zu Absatz 1 und Absatz 2**

Absatz 1 stellt klar, dass die Ortung im Grundsatz denselben Voraussetzungen unterliegt wie Überwachungsmaßnahmen allgemein. Auch die Ortung ist nur zu bestimmten Zwecken zulässig und grundsätzlich nur kurzzeitig und entweder anlassbezogen oder stichprobenhaft. Die Interessen des Arbeitgebers an der Datenverarbeitung müssen die Interessen der Beschäftigten überwiegen, wobei die Abwägungskriterien aus § 4 und § 18 Absatz 4 zu berücksichtigen sind. Absatz 1 Satz 3 stellt klar, dass die allgemeinen Anforderungen an eine Überwachungsmaßnahme auch für die Ortung gelten.

Über die in der allgemeinen Regelung zur Verarbeitung von Beschäftigtendaten durch Überwachungsmaßnahmen aufgeführten Zwecke hinaus ist die Ortung auch zur Koordinierung wechselnder Arbeitseinsätze an verschiedenen Orten zulässig. Hiervon ist insbesondere die Disposition von Einsatzkräften, etwa von Polizei oder Rettungskräften, umfasst. Eine Ortung kann in diesen Fällen erforderlich sein, um Einsätze möglichst schnell der am nächsten befindlichen Einsatzkraft zuzuweisen.

### **Zu Absatz 3**

Absatz 3 definiert den Begriff der Ortung als Bestimmung des geografischen Standortes von Beschäftigten mit Hilfe einer technischen Einrichtung.

### **Zu Absatz 4 und Absatz 5**

Die Absätze 4 und 5 konkretisieren die Anforderungen an die Erforderlichkeit und sehen zugleich spezifische Schutzmaßnahmen ergänzend zu § 9 vor.

Demnach muss der Arbeitgeber es für die betroffenen Beschäftigten erkennbar machen, ob das Ortungssystem eingeschaltet ist, etwa durch eine Warnleuchte im Fahrzeug. Zudem müssen Beschäftigte, sofern sie ein Fahrzeug oder mobiles Endgerät auch privat nutzen dürfen, die Möglichkeit haben, das Ortungssystem hierzu abzuschalten. Nur so kann vermieden werden, dass Daten verarbeitet werden, die die private Lebensgestaltung der Beschäftigten betreffen und sich deshalb dem Zugriffsbereich des Arbeitgebers entziehen.

## **Zu Absatz 6**

Eine nicht nur kurzzeitige Ortung kann über die in § 19 Absatz 2 aufgezählten Zwecke hinaus insbesondere auch zur Koordinierung von Arbeitseinsätzen zulässig sein. Das betrifft vor allem Einsatzkräfte von Polizei und Feuerwehr, aber auch Transportdienstleister, bei denen eine Zuweisung zu wechselnden Einsatzorten erfolgt, wie etwa im Taxigewerbe. Zulässiger Zweck kann zudem sein, die Nachverfolgbarkeit von Lieferungen insbesondere für Kunden zu ermöglichen, etwa bei Postzustellungsunternehmen oder im Logistikbereich. Die in Satz 2 genannten Zwecke stellen stets ein besonders wichtiges betriebliches oder dienstliches Interesse dar. Gleichzeitig haben von nicht nur kurzzeitiger Ortung betroffene Beschäftigte ein gewichtiges Interesse am Schutz ihrer informationellen Selbstbestimmung. Bei der Prüfung der Erforderlichkeit ist ein besonders strenger Maßstab anzulegen, bei dem die Interessen des Arbeitgebers erheblich überwiegen müssen. Dies kann etwa bei Einsatzkräften und im Taxigewerbe der Fall sein, wo es besonders wichtig ist, dass die am nächsten befindlichen Fahrzeuge möglichst schnell und effizient einem Einsatzort zugewiesen werden. Ebenso kann eine erfolgreiche und möglichst reibungslose Paketzustellung es erfordern, dass Arbeitgeber nicht nur punktuell, sondern kontinuierlich nachvollziehen können, wo sich die Lieferung befindet. Der Arbeitgeber kann hier die Gewichtung der Interessen zu seinen Gunsten beeinflussen, indem er geeignete Schutzmaßnahmen ergreift, um den Grundrechtseingriff abzumildern. Je engmaschiger und präziser die Standortdaten erhoben werden, desto höher sind die Anforderungen. Der Arbeitgeber kann und muss etwa, wo möglich, die Daten anonymisieren oder pseudonymisieren, sie nur in Echtzeit erheben oder jedenfalls ein strenges Löschkonzept vorsehen sowie den Zugriff eng beschränken, so dass insbesondere der oder die direkte Vorgesetzte die Daten nicht einsehen kann. Die weiteren Voraussetzungen aus § 19 gelten auch hier. Insbesondere darf eine dauerhafte Ortung nicht zur Leistungskontrolle erfolgen. Gleichermaßen sind auch die allgemeinen Voraussetzungen für eine Ortung aus § 22 Absatz 3 bis 5 ebenso bei einer dauerhaften Ortung nach Absatz 6 einzuhalten. Absatz 6 legt für die dauerhafte Ortung lediglich abweichende Zweckbestimmungen fest.

Eine verdeckte Ortung ist nur unter den Voraussetzungen von § 20 zulässig.

## **Zu § 23 (Weiterverarbeitung zur Leistungskontrolle)**

Die Vorschrift konkretisiert die Grundsätze zur Verarbeitung zu anderen Zwecken aus Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 für die Datenverarbeitung durch Überwachungsmaßnahmen im Beschäftigungskontext. § 23 ist in Bezug auf den Zweck der Leistungskontrolle eine gegenüber § 8 speziellere, vorrangig anzuwendende Vorschrift, die eine Weiterverarbeitung gemäß § 8 Absatz 1 für die Verarbeitung von durch Überwachungsmaßnahmen erhobenen Beschäftigtendaten zur Leistungskontrolle ausschließt. Aus Überwachungsmaßnahmen gewonnene Beschäftigtendaten bieten vielfältige Möglichkeiten, Rückschlüsse auf Leistung und Verhalten von Beschäftigten zu ziehen und diese Informationen zu Leistungsprofilen zusammenzuführen. Dies birgt ein großes Missbrauchspotenzial, dem durch das Verbot der Weiterverarbeitung zur Leistungskontrolle vorgebeugt wird.

## **Zu Kapitel 3 (Profiling)**

Kapitel 3 konkretisiert die Voraussetzungen für eine Verarbeitung von Beschäftigtendaten durch oder aufgrund eines Profilings als typischerweise besonders eingriffsintensive Art der Datenverarbeitung durch den Arbeitgeber. Es handelt sich um spezifischere Vorschriften im Sinne von Artikel 88 Absatz 1 der Verordnung (EU) 2016/679 in Umsetzung der dort geschaffenen Regelungsmöglichkeit. Die erhöhten Anforderungen berücksichtigen die Besonderheiten des Beschäftigungsverhältnisses. Führt der Arbeitgeber eine automatisierte Datenverarbeitung zur Bewertung persönlicher Eigenschaften von Beschäftigten, einschließlich Bewerberinnen und Bewerbern, durch, sind die Risiken dieser Verarbeitungsform aufgrund des strukturellen Machtungleichgewichts für die Beschäftigten besonders

hoch. Der verstärkte Einsatz neuer Technologien wie Künstlicher Intelligenz und algorithmischer Entscheidungssysteme im Beschäftigungsverhältnis verstärkt den Bedarf nach einer spezifischen Regelung dieser Fälle. Die Bewertung der Persönlichkeit und Arbeitsleistung von Beschäftigten durch eine automatisierte Datenverarbeitung kann als eine besonders intensive Form der Durchleuchtung von Beschäftigten empfunden werden, und im Hinblick auf mögliche, weitreichende Konsequenzen (etwa personelle Maßnahmen wie Kündigungen) das Gefühl erzeugen, einem ständigen Bewertungs- und Überwachungsdruck ausgesetzt zu sein.

Die Vorschriften dieses Abschnitts, insbesondere die §§ 25 bis 27, umfassen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Beschäftigten im Sinne von Artikel 88 Absatz 2 der Verordnung (EU) 2016/679. Sie stellen vor allem die Transparenz der Verarbeitung sicher.

### **Zu § 24 (Profiling)**

Diese Vorschrift regelt die Anforderungen an eine Verarbeitung von Beschäftigtendaten durch oder aufgrund eines Profilings. Es gilt die Begriffsbestimmung der Verordnung (EU) 2016/679. Nach Artikel 4 Nummer 4 dieser Verordnung ist Profiling „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen“.

### **Zu Absatz 1 und Absatz 2**

Absatz 1 und Absatz 2 der Vorschrift regeln, zu welchen Zwecken und unter welchem Abwägungsmaßstab eine Datenverarbeitung durch oder aufgrund eines Profilings im Beschäftigungsverhältnis zulässig ist. Die Formulierung „durch oder aufgrund eines Profilings“ greift die verschiedenen Verarbeitungsschritte beim Profiling auf. Im Regelfall werden personenbezogene Eingabedaten durch mathematische und statistische Verfahren verarbeitet und aufgrund dieser Verarbeitung neue Informationen über eine natürliche Person erzeugt, die selbst personenbezogene Ausgabedaten darstellen können. Die Vorschrift regelt Verarbeitungen durch oder aufgrund von Profiling als solche und konkretisiert damit die Rechtmäßigkeitstatbestände des Artikel 6 Absatz 1 Unterabsatz 1 Buchstaben b, c, e und f der Verordnung (EU) 2016/679 für das Profiling im Beschäftigungskontext, indem ein strenger Maßstab für die Interessenabwägung (erhebliches Überwiegen) und über Absatz 3 Abwägungskriterien vorgegeben werden. Das Verbot vollständig automatisierter Entscheidungen nach Artikel 22 der Verordnung (EU) 2016/679 bleibt unberührt. Insbesondere handelt es sich weder um eine Rechtsvorschrift nach Artikel 22 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 noch um eine Konkretisierung des Artikel 22 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679.

Die Verarbeitung personenbezogener Beschäftigtendaten durch oder aufgrund von Profiling kann für einen konkreten Zweck für die Durchführung des Beschäftigungsverhältnisses, die Erfüllung von durch Rechtsvorschriften oder Kollektivvereinbarungen festgelegten Pflichten des Arbeitgebers oder die Wahrung wichtiger betrieblicher oder dienstlicher Interessen erforderlich sein. Die Durchführung des Beschäftigungsverhältnisses kann auch den Schutz der Beschäftigten vor Gefahren umfassen, die mit der Arbeitsausübung verbunden sind. Wichtige betriebliche und dienstliche Interessen können betroffen sein, wenn eine Verletzung wesentlicher Rechtsgüter des Arbeitgebers droht. Wertet der Arbeitgeber automatisiert Aspekte seiner Beschäftigten aus, um diesen passende Weiterbildungsmöglichkeiten anbieten zu können, ist das regelmäßig vorteilhaft für Beschäftigte. Bei konkreten



Zwecken aus dem Bereich des Einsatzes betrieblicher oder dienstlicher Systeme für Weiterbildungs- und Entwicklungsmöglichkeiten nach Absatz 2 handelt es sich daher in der Regel um legitime Verarbeitungszwecke. Wegen der hohen Risiken, die sich aus einer Durchleuchtung der Persönlichkeit und Arbeitsleistung von Beschäftigten mittels automatisierter Datenauswertung ergeben können, muss der Arbeitgeber als positive Voraussetzung der Rechtmäßigkeit einer Verarbeitung von Beschäftigtendaten durch oder aufgrund eines Profilings darlegen, dass die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung erheblich überwiegen. Damit wird ein strenger Abwägungsmaßstab festgelegt. Auf der einen Seite muss der Arbeitgeber wichtige Interessen darlegen oder aus objektiver Sicht auch im Interesse der Beschäftigten handeln. Auf der anderen Seite müssen Risiken für die Rechte und Interessen der Beschäftigten im Einzelfall in einem beherrschbaren Rahmen liegen.

Absatz 2 Satz 2 konkretisiert die Pflicht zur Festlegung eines konkreten Zwecks nach § 3 Absatz 3 für das Profiling. Ein pauschaler Verweis auf den Zweck der Profilbildung genügt nicht. Vielmehr muss erkennbar sein, welche persönlichen Aspekte mit welchem konkreten Ziel für welchen Zeitraum bewertet werden sollen. Damit sollen Umfang, Zeitraum und zulässige Verwendungsmöglichkeiten für die Ergebnisse des Profilings schon durch den Arbeitgeber bei der Festlegung des Zwecks beschränkt werden.

### **Zu Absatz 3**

Absatz 3 konkretisiert die nach Absatz 1 vorzunehmende Interessenabwägung und führt über die Kriterien des § 4 hinaus speziell für das Profiling im Beschäftigungskontext einen zusätzlichen, nicht abschließenden Katalog von Abwägungskriterien auf, die typischerweise zu berücksichtigen sind. Zu berücksichtigen ist, wie relevant die bewerteten Aspekte für die Persönlichkeit oder das berufliche Fortkommen sind („Art“, Nummer 1), wie viele Aspekte bewertet werden („Umfang“, Nummer 2) und wie detailliert einzelne Persönlichkeitsaspekte analysiert werden (Nummer 3). Bedeutsam für die Abwägung sind auch die möglichen Folgen des Profilings, die in für das berufliche Fortkommen nachteiligen Entscheidungen liegen können oder aber zu einer Verbesserung der Arbeitssicherheit von Beschäftigten führen können (Nummer 4). Auch die mit der konkreten Art und Weise der Verarbeitung verbundenen Risiken, dass Ergebnisse des Profilings missbräuchlich entgegen dem ursprünglichen Verarbeitungszweck verwendet werden, sind zu beachten (Nummer 5). Ebenso wichtig für die Abwägung sind die Fragen, wie geeignet die mathematischen und statistischen Verfahren zur Bewertung der Persönlichkeit (Nummer 6) sind, wie hoch beim jeweiligen Profilingverfahren und Anwendungskontext das Risiko diskriminierender Ergebnisse ist (Nummer 7), wie nachvollziehbar und transparent die Verfahren und Ergebnisse sind (Nummer 8) sowie welche Möglichkeiten der Arbeitgeber beim konkreten Profilingverfahren hat, die Risiken für Rechte und Interessen der Beschäftigten durch menschliche Aufsicht und zur Kontrolle der Ergebnisse des Profilings beherrschbar zu halten. Diese Anforderungen ergeben sich etwa aus den Prinzipien der Datenrichtigkeit, Transparenz und der Verarbeitung nach Treu und Glauben (wozu auch die Vermeidung von Diskriminierungen gehört) gemäß Artikel 5 der Verordnung (EU) 2016/679. Gerade beim Profiling anhand von Modellen Künstlicher Intelligenz handelt es sich um komplexe Vorgänge, bei denen Nachvollziehbarkeit, Transparenz und effektive Kontrolle häufig schwer zu gewährleisten sind, was bei der Abwägung der Interessen entsprechend zu berücksichtigen ist. Dies gilt unbeschadet der Pflichten nach Absatz 8 und § 9.

### **Zu Absatz 4**

Absatz 4 verbietet die Verarbeitung von Beschäftigtendaten zur Analyse oder Vorhersage von Emotionen der Beschäftigten sowie die Verarbeitung von Beschäftigtendaten aus Kommunikationsvorgängen zur Bewertung der sozialen Beziehungen zwischen Beschäftigten. Es handelt sich dabei um besonders tiefe Eingriffe in die Persönlichkeitsrechte der Beschäftigten. Beim Profiling zur Analyse oder Vorhersage von Emotionen (Nummer 1) geht es um

einen besonders sensiblen Fall der Persönlichkeitsbewertung. Menschliche Emotionen sind Teil der privaten, inneren Persönlichkeitsentfaltung, Beschäftigte müssen deshalb selbstbestimmt darüber entscheiden können, ob und in welcher Weise sie ihre Emotionen ausdrücken möchten. Höchstpersönliche und private Informationen über die Emotionen von Beschäftigten dürfen nicht durch eine automatisierte Auswertung etwa von unwillkürlichen, minimalen Abweichungen in Verhaltensmustern oder der Mimik abgeleitet werden. Darüber hinaus sind Methoden zur automatisierten Emotionserkennung wegen des höchstpersönlichen und individuellen Charakters von Emotionen sowie kultureller Unterschiede nicht zuverlässig.

Auch der Fall der Verarbeitung von Beschäftigtendaten aus Kommunikationsvorgängen zur Bewertung der sozialen Beziehungen zwischen Beschäftigten (Nummer 2) stellt einen nicht zu rechtfertigenden Eingriff in die Persönlichkeitsrechte dar. Dabei geht es nicht nur um den bereits für sich genommen besonders schützenswerten Inhalt der Kommunikation, sondern auch um Daten über die Häufigkeit oder Art der Kommunikation, etwa welche Beschäftigten wie häufig E-Mails an welche anderen Beschäftigten schreiben oder miteinander telefonieren. Die Erhebung solcher Daten über das Kommunikationsverhalten von Beschäftigten greift für sich bereits tief in die Persönlichkeitsrechte ein. Eine Auswertung mittels Profiling, um Beziehungen zu anderen Beschäftigten zu bewerten greift dazu sehr weit in die persönliche Sphäre der Beschäftigten ein und ist im Beschäftigungskontext auszuschließen.

### **Zu Absatz 5**

Dieser Absatz konkretisiert die Grundsätze zur Verarbeitung zu anderen Zwecken aus Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 für die Datenverarbeitung durch Überwachungsmaßnahmen im Beschäftigungskontext. § 24 Absatz 5 ist für die darin geregelten Fälle eine gegenüber § 8 speziellere, vorrangig anzuwendende, Regelung. Wegen des Unterordnungsverhältnisses zwischen Arbeitgeber und Beschäftigten und der potentiell schwerwiegenden Folgen für das berufliche Fortkommen, sind an den Grundsatz der Zweckbindung bei Datenverarbeitungen zur Bewertung der Arbeitsleistung von Beschäftigten besondere Anforderungen zu stellen. Das gilt in besonderem Maße für eingriffsintensive Datenverarbeitungen durch Profiling. Ein Profiling zur Leistungsbewertung soll nur möglich sein, wenn der Zweck bereits bei der Erhebung der Daten festgelegt und transparent gemacht wird. Es ist daher ausgeschlossen, ursprünglich zu einem anderen Zweck erhobene Daten durch ein Profiling zur Bewertung der Arbeitsleistung zu verarbeiten. Darüber hinaus ist eine Weiterverarbeitung zur Bewertung der Arbeitsleistung ausgeschlossen, wenn ein Profiling zu einem anderen konkret festgelegten Zweck durchgeführt wurde. Das gilt beispielsweise, wenn Eigenschaften von Beschäftigten zu Zwecken der Arbeitssicherheit oder des Gesundheitsschutzes bewertet werden und aus den aufgrund des Profilings hergeleiteten Daten auch vom ursprünglichen Zweck nicht erfasste Rückschlüsse auf die Arbeitsleistung gezogen werden können. Um die Beschäftigten bei der eingriffsintensiven, häufig intransparenten und schwer kontrollierbaren Datenanalyse mittels Profiling vor vom ursprünglichen Zweck nicht erfassten Folgen zu schützen, ist die Weiterverarbeitung zur Bewertung der Arbeitsleistung in diesen Fällen ausgeschlossen.

### **Zu Absatz 6**

Die Regelung stellt das Verhältnis zu den Vorschriften des Kapitel 2 klar. Wenn in dem Profiling zugleich eine Verarbeitung durch Überwachungsmaßnahmen im Sinne des Kapitel 2 liegen, sind deren Voraussetzungen grundsätzlich auch hier zu beachten.

### **Zu Absatz 7**

Um nachteilige Folgen des Profilings und zweckwidrige Verwendungen von Profilingergebnissen zu vermeiden, muss der Arbeitgeber im Rahmen seiner nach der Verordnung (EU) 2016/679 und § 9 zu treffenden Schutzmaßnahmen insbesondere auch die Risiken von

fehlerhaften Ergebnissen eines Profilings berücksichtigen, um das Prinzip der Datenrichtigkeit zu erfüllen. Zudem sollten - etwa über die Nutzeroberfläche einer Software - die Ergebnisse eines Profilings nur auf aggregierter Ebene angezeigt werden, wenn zum Erreichen des Zwecks die Kenntnisnahme der Ergebnisse zu einzelnen Beschäftigten nicht notwendig ist. Statt etwa die Kündigungswahrscheinlichkeit einzelner Beschäftigter sichtbar zu machen, sollte es für den Zweck der Personalplanung eines Unternehmens häufig ausreichend sein, wenn sichtbar wird, in welchen Abteilungen und Bereichen des Unternehmens in den nächsten Jahren eine erhöhte Personalfluktuation zu erwarten sein könnte. Darüber hinaus ist eine menschliche Aufsicht über das Profiling sicherzustellen. Um Verstöße gegen das Verbot aus Artikel 22 der Verordnung (EU) 2016/679 zu vermeiden, können dabei insbesondere Maßnahmen vorgenommen werden, die eine aktive menschliche Entscheidung erforderlich machen, wenn diese durch Profiling vorbereitet wurde. Eine sorgfältige menschliche Prüfung der Entscheidung könnte etwa durch Hinweise über die Merkmale, Fähigkeiten und Leistungsgrenzen der Profilingmethode sowie mögliche Faktoren für Ungenauigkeiten und Verzerrungen erleichtert werden. Es handelt sich bei der Regelung um eine geeignete und besondere Maßnahme zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person im Sinne des Artikel 88 Absatz 2 der Verordnung (EU) 2016/679.

### **Zu Absatz 8**

Durch oder aufgrund von Profiling dürfen besondere Kategorien von Beschäftigendaten verarbeitet werden, sofern die Voraussetzungen für eine Datenverarbeitung durch oder aufgrund von Profiling, sowie zusätzlich ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder von § 6 vorliegen. Bei der Auswahl geeigneter und besonderer Schutzmaßnahmen muss der Arbeitgeber beachten, dass besondere Kategorien von Beschäftigendaten besonders sensibel und schutzbedürftig sind.

### **Zu § 25 (Informationspflicht bei Profiling)**

Beim Profiling werden häufig große Mengen an Daten mittels komplexer Algorithmen verarbeitet, teilweise unter Verwendung Künstlicher Intelligenz. Für die Persönlichkeitsrechte Beschäftigter sehr sensible Vorgänge finden daher häufig in einer besonders intransparenten und schwer nachvollziehbaren Weise statt. Gerade im Beschäftigungskontext stellt dies ein erhebliches Problem dar, da neben das Machtungleichgewicht im Beschäftigungsverhältnis so schnell auch ein Informationsungleichgewicht treten kann. Um die Transparenz und Nachvollziehbarkeit bei der Profilerstellung im Beschäftigungskontext zu stärken, werden die nach der Verordnung (EU) 2016/679 bestehenden Informationspflichten für das Profiling im Beschäftigungskontext konkretisiert und ergänzt. Soweit in der Vorschrift Wiederholungen von Teilen der Artikel 13 und 14 der Verordnung (EU) 2016/679 enthalten sind, sind diese erforderlich, um Kohärenz zu wahren und verständlich zu machen, welche Teile der Artikel 13 und 14 der Verordnung (EU) 2016/679 konkretisiert und ergänzt werden. Die Vorschrift enthält geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, im Sinne des Artikel 88 Absatz 2 der Verordnung (EU) 2016/679. Wird im Rahmen eines Profilings ein KI-System eingesetzt, sind die Vorschriften dieses Kapitels gegenüber der Vorschrift des § 10 Absatz 2 und 3 spezieller und gehen dieser vor.

### **Zu Absatz 1**

Die Zwecke der Verarbeitung müssen in der nach § 24 Absatz 2 konkretisierten Form angegeben werden (Nummer 1). Die Kategorien von Eingabedaten sind beim Profiling im Beschäftigungskontext nicht nur in Fällen anzugeben, in denen die Daten nicht bei der betroffenen Person erhoben wurden (Nummer 2). Gerade bei der Erhebung großer Mengen an Daten durch Künstliche Intelligenz kann auch in Fällen der Erhebung beim betroffenen Beschäftigten eine Information über die Kategorien erhobener Eingabedaten notwendig

sein, um einen Überblick über erhobene Eingabedaten zu gewährleisten. Ebenso wie nach § 10 Absatz 2 ist auch beim Profiling anzugeben, ob ein KI-System bei der Verarbeitung von Beschäftigtendaten eingesetzt wird (Nummer 3).

Informationen über die involvierte Logik sind für von Profiling betroffene Beschäftigte wichtig, um zu verstehen, auf welcher Grundlage sie bewertet werden (Nummer 4). Wegen des durch das Profiling im Beschäftigungskontext an sich bereits möglicherweise erzeugten ständigen Bewertungs- und Überwachungsdrucks gilt dies auch dann, wenn das Profiling nicht unmittelbar zu einer automatisierten Entscheidung führt. Es geht hierbei nicht um die Offenlegung von Algorithmen, die häufig durch Geschäftsgeheimnisse geschützt sind und wegen ihrer Komplexität in der Regel nicht aus sich heraus verständlich sind. Vielmehr soll den Beschäftigten durch eine Beschreibung der Funktionsweise des Algorithmus und der zentralen Bewertungskriterien verständlich werden, auf welche Weise die Bewertung ihrer Person oder Arbeitsleistung zustande gekommen ist und wie ihre personenbezogenen Daten für die Bewertung genutzt wurden. Wird beim Profiling ein KI-System eingesetzt, ist diese Regelung gegenüber § 10 Absatz 3 Nummer 1 die speziellere Regelung.

Informationen über die Tragweite und die angestrebten Auswirkungen einer durch Profiling beeinflussten Entscheidung sind beim Profiling im Beschäftigungsverhältnis auch dann relevant, wenn die Entscheidung durch das Profiling bloß vorbereitet werden soll (Nummer 5). Auch wenn eine menschliche Letztentscheidung besteht, kann der Einfluss von Profiling auf den Entscheidungsprozess erheblich sein und für Beschäftigte besteht ein Interesse an diesen Informationen. Wie auch in Artikel 22 der Verordnung (EU) 2016/679 ist allerdings nicht jede Entscheidung erfasst, sondern nur solche, die gegenüber den betroffenen Beschäftigten rechtliche Wirkung entfalten oder sie in ähnlicher Weise beeinträchtigen. Dabei ist es für die Beschäftigten einerseits wichtig zu wissen, für welche Entscheidungen das Profiling genutzt werden kann und welche Folgen sich daraus ergeben können. Ebenfalls wichtig ist die Information, welche Funktion dem Profiling beim Zustandekommen der Entscheidung zukommt sowie in welcher Weise eine menschliche Aufsicht und ein Eingreifen durch Menschen vorgesehen ist, damit Beschäftigte wissen, zu welchem Grad sie einer automatisierten Entscheidung ausgesetzt sind und ob der Arbeitgeber die Grenzen des Artikel 22 der Verordnung (EU) 2016/679 einhält.

Schließlich muss auch ein Hinweis auf die speziellen Auskunftsrechte nach § 26 sowie die Rechte auf Erklärung und Überprüfung der Entscheidung nach § 27 erfolgen (Nummer 6).

### **Zu Absatz 2**

Ein Profiling, indem zugleich eine Verarbeitung durch verdeckte Überwachungsmaßnahmen liegt, ist ausgeschlossen.

### **Zu § 26 (Auskunftsrecht bei Profiling)**

Auch beim Auskunftsrecht der betroffenen Beschäftigten sind zur Stärkung von Transparenz und Nachvollziehbarkeit bei der Profilerstellung im Beschäftigungskontext Konkretisierungen und Ergänzungen nötig. Wichtig ist hier, dass die Rechte auf Auskunft und Kopie auch die Ergebnisse des Profilings bezüglich persönlicher Aspekte des Beschäftigten umfassen (Nummer 1). Hierbei handelt es sich um personenbezogene Daten, an deren Kenntnis Beschäftigte aufgrund ihrer persönlichen Betroffenheit ein herausgehobenes Interesse haben. Nummer 4 stellt klar, dass das in § 10 Absatz 3 Nummer 2 geregelte Auskunftsrecht bezüglich der Schutzmaßnahmen beim Einsatz von KI-Systemen auch gilt, wenn beim Profiling ein KI-System eingesetzt wird. Gegenüber § 10 Absatz 3 Nummer 1 ist Nummer 2 dieser Vorschrift die speziellere Regelung. Soweit in der Vorschrift Wiederholungen von Teilen des Artikels 15 der Verordnung (EU) 2016/679 enthalten sind, sind diese erforderlich, um Kohärenz zu wahren und verständlich zu machen, welche Teile des Artikels 15 der Verordnung (EU) 2016/679 konkretisiert und ergänzt werden. Es handelt sich bei der Vorschrift um eine geeignete und besondere Maßnahme zur Wahrung der menschlichen

Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, im Sinne des Artikel 88 Absatz 2 der Verordnung (EU) 2016/679. Wird im Rahmen eines Profilings ein KI-System eingesetzt, sind die Vorschriften dieses Kapitels gegenüber der Vorschrift des § 10 Absatz 3 spezieller und gehen dieser vor.

### **Zu § 27 (Erklärung und Überprüfung der Entscheidung)**

Entscheidungen durch den Arbeitgeber, die gegenüber betroffenen Beschäftigten eine rechtliche Wirkung oder ähnlich beeinträchtigende Auswirkungen haben und (zumindest vorbereitend) auf Profiling beruhen, stellen Beschäftigte vor eine besondere Situation und bergen eine erhöhte Gefahr, dass die Beschäftigten zum bloßen Objekt eines für sie undurchschaubaren und nicht beeinflussbaren automatisierten Vorgangs werden. Daher sieht Artikel 22 der Verordnung (EU) 2016/679 auch grundsätzlich ein Verbot von ausschließlich auf Profiling beruhenden Entscheidungen vor. Aber auch Fälle, in denen eine menschliche Letztentscheidung mittels Profiling vorbereitet wird, lassen einen wesentlichen Teil der Entscheidungsfindung sowohl für die entscheidenden als auch für die betroffenen Personen schwerer durchschaubar ablaufen. Sie bergen die Gefahr, dass die menschlichen Letztentscheidenden sich zu stark auf die algorithmische Empfehlung verlassen und sich Fehleinschätzungen aus dem automatisierten Profiling in der menschlichen Letztentscheidung fortsetzen. Diese Gefahren verstärken sich noch im Arbeits- und Bewerbungsverhältnis, wo Entscheidungen im Rahmen eines Unterordnungsverhältnisses getroffen werden. Daher ist es wichtig in Fällen, in denen unter den Voraussetzungen des Artikel 22 Absatz 2 der Verordnung (EU) 2016/679 Ausnahmen vom Verbot des Artikel 22 Absatz 1 der Verordnung (EU) 2016/679 bestehen oder eine menschliche Entscheidung durch Profiling bloß vorbereitet wird, den betroffenen Beschäftigten Rechte an die Hand zu geben, damit sie sich mit der Entscheidung auseinandersetzen und eine erneute Überprüfung verlangen können. Es handelt sich bei der Vorschrift um eine geeignete und besondere Maßnahme zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, im Sinne des Artikel 88 Absatz 2 der Verordnung (EU) 2016/679. Gleichzeitig knüpft die Vorschrift in der Umsetzung an den Regelungsgedanken des Artikel 22 Absatz 3 der Verordnung (EU) 2016/679 an. Dieser verpflichtet den Verantwortlichen, in Fällen von ausschließlich auf Profiling beruhenden Entscheidungen, angemessene Maßnahmen zu treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren.

#### **Zu Absatz 1**

Absatz 1 sieht als Grundlage für die weiteren Rechte daher ein Recht auf Erklärung der Entscheidung im Einzelfall vor. Die betroffenen Beschäftigten haben ein Recht auf eine Erklärung über den Einfluss ihrer personenbezogenen Eingabedaten oder ihres Verhaltens auf den konkreten Entscheidungsprozess (Nummer 1), um zu verstehen wie sie persönlich Einfluss auf die Entscheidung hatten. Zudem besteht ein Recht auf Erklärung der Funktion des Profilings im abgeschlossenen Entscheidungsprozess, insbesondere wie eine menschliche Überprüfung der Entscheidung stattgefunden hat (Nummer 2). Damit können Beschäftigte sich ein Bild machen, in welchem Maß sie einer automatisierten Entscheidung ausgesetzt waren und ob die Voraussetzungen des Artikel 22 der Verordnung (EU) 2016/679 eingehalten wurden. Schließlich sind von der Erklärung auch die konkreten Folgen der Entscheidung für die Beschäftigten umfasst, damit Beschäftigte die Auswirkungen der Entscheidung auf sich beurteilen können.

#### **Zu Absatz 2**

Die Informationen aus Absatz 1 sind Grundlage für die Rechte nach Absatz 2. Beschäftigte können sowohl zum Ergebnis des Profilings als auch zur Entscheidung Stellung nehmen und eine (erneute) Überprüfung der Entscheidung durch den Arbeitgeber verlangen. Mit dem Verlangen können Beschäftigte wählen, ob der Arbeitgeber innerhalb von vier Wochen

eine begründete Antwort auf die Stellungnahme übermitteln muss oder eine mündliche Erörterung zwischen Arbeitgeber und Beschäftigten stattfindet.

### **Zu Absatz 3**

Nach Absatz 3 kann auf Verlangen der Beschäftigten ihre Interessenvertretung in alle Schritte einbezogen werden. Die Erklärung ist auch der Interessenvertretung zu übermitteln, die Interessenvertretung kann Stellung nehmen und an der mündlichen Erörterung teilnehmen. Damit können Beschäftigte auf ihren Wunsch Unterstützung erhalten und in der Geltendmachung ihrer Rechte gestärkt werden.

### **Zu Kapitel 4 (Besondere Verarbeitungssituationen)**

Das Kapitel 4 enthält Vorschriften über die Verarbeitung von Beschäftigtendaten in besonderen Verarbeitungssituationen. Es regelt die Verarbeitung biometrischer Beschäftigtendaten und die Datenverarbeitung im betrieblichen Eingliederungsmanagement sowie im Konzern. Es handelt sich um spezifischere Vorschriften im Sinne von Artikel 88 Absatz 1 der Verordnung (EU) 2016/679 in Umsetzung der dort geschaffenen Regelungsmöglichkeit. Die Vorschriften dieses Kapitels umfassen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person im Sinne von Artikel 88 Absatz 2 der Verordnung (EU) 2016/679.

### **Zu § 28 (Datenverarbeitung zu Autorisierungs- und Authentifizierungszwecken)**

Die Vorschrift macht von den Öffnungsklauseln in Artikel 9 Absatz 1 Buchstabe b, 88 Absatz 1 der Verordnung (EU) 2016/679 Gebrauch und sieht zusätzliche Bedingungen und Beschränkungen im Sinne von Artikel 9 Absatz 4 der Verordnung (EU) 2016/679 für die Verarbeitung biometrischer Daten im Beschäftigungskontext vor. Die erhöhten Anforderungen berücksichtigen die Besonderheiten des Beschäftigungsverhältnisses, insbesondere die Risiken, die mit einer Verarbeitung besonders sensibler Daten, wie biometrischer Daten, einhergehen.

### **Zu Absatz 1**

Absatz 1 konkretisiert die Zwecke, zu denen eine Verarbeitung biometrischer Daten nach diesem Gesetz zulässig sein kann. Die Anwendbarkeit von Artikel 9 Absatz 2 sowie von spezialgesetzlichen Vorschriften über die Verarbeitung biometrischer Beschäftigtendaten wird hierdurch nicht ausgeschlossen. Die Verarbeitung biometrischer Daten aufgrund einer Einwilligung richtet sich nach § 5. Ein Rückgriff auf andere Vorschriften aus diesem Gesetz, insbesondere auf § 6 ist jedoch nicht zulässig. Die Verarbeitung aufgrund einer Einwilligung kommt in Abgrenzung zu § 28 Absatz 1 nur in Betracht, wenn eine Identifizierung auch auf andere, gleich geeignete Weise erfolgen kann und die Beschäftigten frei entscheiden können, welche Identifizierungsmöglichkeit sie nutzen wollen. Eine Verarbeitung biometrischer Daten nach § 28 scheidet dann aus, weil sie angesichts der gleichwertigen Alternative nicht erforderlich ist. Dies kann etwa der Fall sein, wenn die Identifizierung ebenso gut über ein Passwort erfolgen kann.

Die Regelung des Absatzes trägt dem Umstand Rechnung, dass der Zugang oder Zutritt zu besonders sicherheitsrelevanten Bereichen zunehmend häufiger durch biometrische Kontrollen gesichert wird. Der Begriff „Bereich“ umfasst sowohl räumlich bestimmte Teile von Betriebsstätten als auch geschützte Teile von IT-Systemen. Besonders sensible Bereiche können etwa Sicherheitsbereiche an Flughäfen sein sowie besonders sensible Bereiche in Forschungseinrichtungen, Sicherheitsbehörden oder IT-Systemen. Authentifizierung meint die Prüfung von Angaben zur Identität einer Person auf Echtheit. Autorisierung meint das sich an die Echtheitsprüfung anschließende Gewähren der Zugangs- oder Zutrittsberechtigung. Aufgrund der eher einfachen Handhabung und der eher niedrigen Fehleranfäll-

lichkeit können sowohl Arbeitgeber als auch Beschäftigte hieran ein Interesse haben. Angesichts des hohen Risikos für die Persönlichkeitsrechte im Falle einer zweckwidrigen Datennutzung, namentlich der Gefahr eines Identitätsdiebstahls oder -missbrauchs oder von Rückschlüssen auf bestimmte Erkrankungen der betroffenen Person anhand biometrischer Merkmale, unterliegt die Verarbeitung biometrischer Daten aber besonders strengen Anforderungen. Der Arbeitgeber muss als positive Voraussetzung der Rechtmäßigkeit einer Verarbeitung von Beschäftigtendaten darlegen, dass die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung erheblich überwiegen. Auf der einen Seite muss der Arbeitgeber besonders wichtige eigene Interessen darlegen oder aus objektiver Sicht auch im Interesse der Beschäftigten handeln. Auf der anderen Seite müssen Risiken für die Rechte und Interessen der Beschäftigten im Einzelfall in einem beherrschbaren Rahmen liegen. Dabei sind die Abwägungskriterien aus § 4 zu berücksichtigen.

### **Zu Absatz 2**

Absatz 2 konkretisiert die Grundsätze zur Verarbeitung zu anderen Zwecken als demjenigen, zu dem die Beschäftigtendaten erhoben wurden, aus Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 für die Verarbeitung biometrischer Beschäftigtendaten. Absatz 2 ist eine gegenüber § 8 speziellere, vorrangig anzuwendende Vorschrift, die eine Verarbeitung zu einem anderen Zweck gemäß § 8 Absatz 1 für die Verarbeitung von biometrischen Beschäftigtendaten zu einem anderen Zweck ausschließt. Aufgrund des hohen Risikos für Identitätsdiebstahl, -missbrauch oder Rückschlüsse auf den Gesundheitszustand betroffener Beschäftigter unterliegen biometrische Daten im Beschäftigungsverhältnis einer strikten Zweckbindung.

### **Zu Absatz 3**

Aufgrund der hohen Sensibilität der Daten sind besondere Anforderungen an die Transparenz der Verarbeitung zu stellen. Die betroffenen Beschäftigten müssen über eine Verarbeitung biometrischer Daten umfassend informiert werden. Ausnahmen von den Informationspflichten aus Artikel 13 Absatz 1 bis 3 und Artikel 14 Absatz 1 bis 4 der Verordnung (EU) 2016/679 sind daher ausgeschlossen.

### **Zu Absatz 4**

Der Verantwortliche hat bereits nach § 9 geeignete und besondere Maßnahmen zur Einhaltung der insbesondere in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze zu ergreifen, um die Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person sicherzustellen. Da es sich bei biometrischen Daten um besondere Kategorien von Beschäftigtendaten handelt, muss er hierbei beachten, dass diese besonders sensibel und schutzwürdig sind.

Ergänzend zu § 9 muss er daher die für die Nutzung als Referenzdaten erhobenen Rohdaten vor der Nutzung in geschützte biometrische Referenzen (Templates) umwandeln. Die Rohdaten bergen das Risiko von Rückschlüssen auf über die Zutritts- oder Zugangsberechtigung hinausgehende Informationen, etwa in Bezug auf Erkrankungen der betroffenen Person. Sofern dies technisch möglich ist, müssen die biometrischen Daten auf einem Medium, etwa einer Speicherkarte, gespeichert sein, das der alleinigen Verfügungsgewalt der beschäftigten Person unterliegt. Die Freigabe der Daten hat der aktiven Mitwirkung der Beschäftigten zu unterliegen, der Datenabgleich sollte auf dem Speichermedium selbst stattfinden (sogenannte On-Card-Comparison). Eine zentrale Speicherung der Daten hat wegen des hohen Diebstahls- und Missbrauchsrisiko zu unterbleiben. Falls sie im Einzelfall unvermeidlich ist, müssen die Daten durch geeignete Verschlüsselungs- oder Authentifizierungssysteme gegen unbefugten Zugang besonders gesichert werden. Das Speichermedium sollte nur durch die betroffenen Beschäftigten selbst und auch nicht durch den Arbeitgeber auslesbar sein.

## **Zu § 29 (Betriebliches Eingliederungsmanagement)**

Die Vorschrift macht von den Öffnungsklauseln in Artikel 9 Absatz 1 Buchstabe b, 88 Absatz 1 der Verordnung (EU) 2016/679 Gebrauch und sieht zusätzliche Bedingungen und Beschränkungen im Sinne von Artikel 9 Absatz 4 der Verordnung (EU) 2016/679 für die Verarbeitung von Gesundheitsdaten vor. Die erhöhten Anforderungen berücksichtigen die Besonderheiten des Beschäftigungsverhältnisses, insbesondere die Risiken, die mit einer Verarbeitung besonders sensibler Daten, wie Gesundheitsdaten, einhergehen. Die Vorschrift verdeutlicht die Anforderungen an eine Verarbeitung personenbezogener Beschäftigtendaten im Rahmen des betrieblichen Eingliederungsmanagements nach § 167 Absatz 2 des Neunten Buches Sozialgesetzbuch. Sie trägt dem Umstand Rechnung, dass das betriebliche Eingliederungsmanagement ein verlaufs- und ergebnisoffener Suchprozess ist, der von der Zustimmung der betroffenen Beschäftigten abhängt. Daher unterscheiden die Absätze 1 und 2 zwischen der Durchführung des betrieblichen Eingliederungsmanagements erforderlichen (Absatz 1) und darüberhinausgehenden, freiwillig mitgeteilten Informationen (Absatz 2).

### **Zu Absatz 1**

Absatz 1 normiert eine Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten, die zur Durchführung des betrieblichen Eingliederungsmanagements erforderlich sind.

Das betrifft nach Nummer 1 zunächst Daten zum Zweck der Prüfung, ob einer beschäftigten Person ein betriebliches Eingliederungsmanagement angeboten werden muss. Dies ist gemäß § 167 Absatz 2 Satz 1 des Neunten Buches Sozialgesetzbuch der Fall, wenn Beschäftigte innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig sind. Hierzu dürfen neben dem Namen, der Tätigkeit und Daten über Fehlzeiten gegebenenfalls auch, soweit bereits bekannt, Informationen über eine etwaige Schwerbehinderung, Arbeitsunfälle oder in der Vergangenheit durchgeführte Maßnahmen des betrieblichen Eingliederungsmanagements verarbeitet werden.

Zur Durchführung des betrieblichen Eingliederungsmanagements, das gemäß § 167 Absatz 2 Satz 1 des Neunten Buches Sozialgesetzbuch die Zustimmung der betroffenen Beschäftigten voraussetzt, dürfen darüber hinaus nach Nummer 2 etwa Fähigkeitsdaten in Bezug auf das Anforderungsprofil der Arbeitsumgebung sowie Daten zu Verläufen und Ergebnissen von arbeitsplatzbezogenen Maßnahmen verarbeitet werden. Entsprechend der ständigen Rechtsprechung des Bundesarbeitsgerichts müssen die Daten zur Durchführung eines zielführenden, der Gesundheit und Gesunderhaltung des oder der Betroffenen dienenden betrieblichen Eingliederungsmanagements erforderlich sein. Das kann insbesondere auch arbeitsplatz- oder tätigkeitsbezogene Gesundheitsdaten umfassen. Beschäftigte sind jedoch nicht verpflichtet, medizinische Diagnosen oder Krankheitsursachen offenzulegen.

Absatz 1 umfasst nach seiner Nummer 3 auch die Erfüllung von Verpflichtungen des Arbeitgebers aus Kollektivvereinbarungen. In diesen können die betrieblichen Rahmenbedingungen zur Ausgestaltung der gesetzlichen Verpflichtung des Arbeitgebers gemäß § 167 Absatz 2 Satz 1 des Neunten Buches Sozialgesetzbuch konkret geregelt werden.

### **Zu Absatz 2**

Die Verarbeitung von Beschäftigtendaten, die nicht im Sinne von Absatz 1 erforderlich sind, kann nach Absatz 2 bei Vorliegen einer wirksamen Einwilligung rechtmäßig sein. In Bezug auf die Wirksamkeit der Einwilligung sind die Anforderungen des § 5 dieses Gesetzes sowie von Artikel 7 der Verordnung (EU) 2016/679 zu beachten. Aus der Einwilligungserklärung muss der, im Gegensatz zu den nach Absatz 1 verarbeiteten Daten, freiwillige, einem Widerrufsrecht unterliegende Charakter der Datenverarbeitung hervorgehen. Die Einwilligung in die Verarbeitung personenbezogener Daten ist von der Zustimmung zur Durchführung



des Eingliederungsverfahrens nach § 167 Absatz 2 Satz 1 des Neunten Buches Sozialgesetzbuch zu unterscheiden. Die Unterscheidung muss für die betroffenen Beschäftigten erkennbar sein. Die Regelung betrifft insbesondere Informationen zum Hintergrund der Fehlzeiten, etwa zu Krankheitsursachen. Diese Daten müssen Beschäftigte niemals offenlegen. Da im Einzelfall seitens der Beschäftigten aber der Wunsch bestehen kann, etwa Informationen zum eigenen Gesundheitszustand zu besprechen, soll dies datenschutzrechtlich über die Einwilligung ermöglicht werden. Um der Schutzfunktion der Einwilligungserklärung gerecht zu werden, muss diese schriftlich oder elektronisch abgegeben werden. Zudem müssen Beschäftigte mindestens 24 Stunden vor Abgabe der Einwilligungserklärung über den Zweck der Datenverarbeitung und ihr Widerrufsrecht aufgeklärt werden. Die Frist dient dazu, ihnen eine ausreichende Bedenkzeit einzuräumen.

### **Zu Absatz 3**

Absatz 4 konkretisiert die Grundsätze zur Verarbeitung zu anderen Zwecken aus Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 für die Datenverarbeitung im betrieblichen Eingliederungsmanagement. Absatz 4 ist eine gegenüber § 8 speziellere, vorrangig anzuwendende Vorschrift, die eine Verarbeitung zu einem anderen Zweck gemäß § 8 Absatz 1 in Bezug auf Daten aus dem betrieblichen Eingliederungsmanagement grundsätzlich ausschließt. Das betrifft insbesondere die Weiterverarbeitung für eine personenbedingte Kündigung sowie zum Zwecke der Darlegung und Beweisführung in einem gerichtlichen Verfahren über die Wirksamkeit einer Kündigung nach § 1 des Kündigungsschutzgesetzes gegen die Beschäftigte oder den Beschäftigten. Davon ausgenommen ist das Ergebnis eines Verfahrens im betrieblichen Eingliederungsmanagement, ob also danach die Möglichkeit einer leidensgerechten Weiterbeschäftigung besteht oder nicht.

### **Zu Absatz 4**

Der Verantwortliche hat bereits nach § 9 geeignete und besondere Maßnahmen zur Einhaltung der insbesondere in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze zu ergreifen, um die Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person sicherzustellen. Sofern im Rahmen des betrieblichen Eingliederungsmanagements besondere Kategorien von Beschäftigtendaten verarbeitet werden, muss der Arbeitgeber in Bezug auf die Schutzmaßnahmen beachten, dass diese besonders sensibel und schutzbedürftig sind.

Ergänzend zu § 9 muss der Arbeitgeber vorsehen, dass nur zur Verschwiegenheit verpflichtete Personen am betrieblichen Eingliederungsmanagement mitwirken und auf die diesbezügliche Akte zugreifen dürfen. Das umfasst vor allem Personen, die einer strafrechtlich bewehrten Schweigepflicht unterliegen, wie Betriebsärzte und -ärztinnen (§ 203 Absatz 1 des Strafgesetzbuches), die allgemeinen Interessenvertretungen (§ 120 des Betriebsverfassungsgesetzes; § 203 Absatz 2 des Strafgesetzbuches) sowie die Schwerbehindertenvertretung (§ 179 Absatz 7 des Neunten Buches Sozialgesetzbuch). Sonstige am Verfahren beteiligte Personen müssen zumindest vertraglich zur Verschwiegenheit verpflichtet werden. In der Personalverwaltung beschäftigte Personen sollten keinen Zugriff auf die Akte zum betrieblichen Eingliederungsmanagement haben, sofern sie nicht selbst am konkreten Eingliederungsverfahren beteiligt sind. Die Akte ist räumlich und funktional getrennt von der Personalakte aufzubewahren und sollte gegen unbefugten Zugriff gesichert sein. Bei der Durchführung des betrieblichen Eingliederungsmanagements erhobene Gesundheitsdaten dürfen nicht in die Personalakte aufgenommen werden. Nicht darunter fallen Fehlzeiten und andere Daten, die bereits vor dem Eingliederungsverfahren vorlagen. In die Personalakte aufgenommen werden dürfen Daten, die als Nachweis über das ordnungsgemäße Eingliederungsverfahren gelten, also insbesondere der Zeitpunkt des Angebots für ein betriebliches Eingliederungsmanagement, dessen Ergebnis, sowie die konkreten Maßnahmen, die angeboten und umgesetzt wurden.

## **Zu § 30 (Datenverarbeitung im Konzern)**

Die Vorschrift konkretisiert die Voraussetzungen für eine Offenlegung von Beschäftigten-  
daten an ein anderes Unternehmen innerhalb eines Konzerns. Es handelt sich um eine  
spezifischere Vorschrift im Sinne von Artikel 88 Absatz 1 der Verordnung (EU) 2016/679 in  
Umsetzung der dort geschaffenen Regelungsmöglichkeit. Die erhöhten Anforderungen be-  
rücksichtigen die Besonderheiten des Beschäftigungsverhältnisses, insbesondere die Risi-  
ken, die mit einer unternehmensübergreifenden Übermittlung von Beschäftigtendaten ein-  
hergehen.

### **Zu Absatz 1**

Die Organisationsstruktur und effiziente Aufgabenverteilung innerhalb von Konzernen er-  
fordern in bestimmten Fällen einen Datenaustausch zwischen den Konzerngesellschaften.  
Die Zulässigkeit des konzerninternen Datentransfers ist seit langem mit Rechtsunsicherheit  
behaftet, die auch durch das Inkrafttreten der Verordnung (EU) 2016/679 nicht ausgeräumt  
wurde. Unterschiedliche Unternehmen innerhalb des Konzerns sind datenschutzrechtlich  
Dritte im Sinne von Artikel 4 Nummer 10 Verordnung (EU) 2016/679, so dass die Offenle-  
gung von Beschäftigtendaten gemäß Artikel 4 Nummer 2 der Verordnung (EU) 2016/679,  
also die Übermittlung, Verbreitung oder Bereitstellung auf andere Weise, zwischen Kon-  
zernunternehmen nur bei Vorliegen eines datenschutzrechtlichen Erlaubnistatbestandes  
zulässig ist. Regelmäßig erfordert dies eine Interessenabwägung im Einzelfall gemäß Arti-  
kel 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679. Das Bedürfnis von Konzernun-  
ternehmen nach mehr Rechtssicherheit und einer Begrenzung des bürokratischen Auf-  
wands muss mit dem Schutz des Allgemeinen Persönlichkeitsrechts der Beschäftigten in  
einen angemessenen Ausgleich gebracht werden. Die Weitergabe von Beschäftigtendaten  
an Einheiten außerhalb des Vertragsarbeitgebers ist für Beschäftigte mit einem Verlust von  
Kontrolle über ihre Daten und, aufgrund erweiterter Zugriffsmöglichkeiten, mit einem ver-  
stärkten Risiko für Datenschutzverletzungen verbunden. Die Vorschrift schafft daher kein  
generelles Konzernprivileg, sondern konkretisiert im Einklang mit Erwägungsgrund 48 der  
Verordnung (EU) 2016/679, in welchen Fällen ein berechtigtes Interesse an der Offenle-  
gung von Beschäftigtendaten im Konzern vorliegt. Eine Zulässigkeit aufgrund anderer da-  
tenschutzrechtlicher Erlaubnistatbestände wird hierdurch nicht ausgeschlossen. Die daten-  
schutzrechtliche Verantwortlichkeit richtet sich nach den allgemeinen Vorschriften. Die  
Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unterneh-  
mensgruppen an ein Unternehmen in einem Drittland bleiben unberührt. Die Interessen des  
Arbeitgebers oder des Konzernunternehmens an der Verarbeitung müssen die Interessen  
der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen, wobei die  
Abwägungskriterien aus § 4 zu beachten sind.

### **Zu Absatz 2**

Absatz 2 konkretisiert, in welchen Fällen ein berechtigtes Interesse im Sinne von Absatz 1  
insbesondere vorliegen kann.

### **Zu Nummer 1**

Konzerne sind zunehmend häufiger in Matrixstrukturen organisiert, die durch Mehrdimen-  
sionalität und ein Mehrliniensystem gekennzeichnet sind. Die Arbeit in Mehrliniensystemen  
geht damit einher, dass die betroffenen Beschäftigten Aufgaben auch auf Weisung der au-  
ßerhalb des Vertragsarbeitgebers stehenden, in dem Konzernunternehmen beschäftigten  
Führungskraft (Matrixmanager oder -managerin) ausführen. Zu diesem Zweck werden die  
Matrixmanager und -managerinnen zur Ausübung des fachlichen Weisungsrechts ermäch-  
tigt. Bei Vorliegen einer Zustimmung des Arbeitnehmers oder der Arbeitnehmerin gemäß  
§ 613 Satz 2 des Bürgerlichen Gesetzbuches kommt auch eine Übertragung des fachlichen  
Weisungsrechts in Betracht. Die Zusammenarbeit im Mehrliniensystem erfordert häufig die

Übermittlung von Beschäftigtendaten an das Konzernunternehmen, in dem die Matrixmanager und -managerinnen beschäftigt sind, etwa Kontaktdaten oder Informationen zu An- bzw. Abwesenheiten. Das Konzernunternehmen sowie ggf. die Konzernmutter haben ein berechtigtes Interesse daran, dass der Vertragsarbeitgeber dem Matrixmanager und -managerinnen die zur Ausführung der angewiesenen Aufgaben erforderlichen Daten zur Verfügung stellt.

### **Zu Nummer 2**

Ein legitimer Zweck für die Offenlegung von Beschäftigtendaten innerhalb einer Unternehmensgruppe kann auch vorliegen, wenn konzerninterne Verwaltungsaufgaben zentralisiert wahrgenommen werden, um die Arbeitsorganisation effizienter zu gestalten und Kapazitäten zu bündeln. Dies betrifft etwa eine zentrale Entgeltabrechnung, die Einrichtung eines konzernweiten elektronischen Kommunikationsverzeichnisses, oder eine zentrale IT-Infrastruktur.

### **Zu Nummer 3**

Eine dritte Fallgruppe betrifft die konzernweit einheitliche Gestaltung von Vorgängen, beispielsweise eine Vereinheitlichung der Gehaltsstrukturen. Der legitime Zweck ergibt sich hier nicht nur aus der gesteigerten Effizienz, sondern zusätzlich aus einer verbesserten Vergleichbarkeit innerhalb der Unternehmensgruppe, die auch den Beschäftigten zugutekommt.

### **Zu Absatz 3**

Die Regelung enthält selbst keine Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten, sondern erweitert den sachlichen Anwendungsbereich des Beschäftigtendatenschutzgesetzes auf Konzernunternehmen, denen Beschäftigtendaten gemäß Absatz 1 der Vorschrift offengelegt wurden. Parallel zur Zulässigkeit der Offenlegung von Beschäftigtendaten durch den Vertragsarbeitgeber erfordert die anschließende Verarbeitung der offengelegten Daten durch das Konzernunternehmen das Vorliegen eines Erlaubnistatbestandes, sofern kein Fall der Auftragsverarbeitung vorliegt. Die Vorschrift gewährleistet, dass Konzernunternehmen Daten in den in Absatz 1 genannten Fällen nicht nur unter klareren und insofern erleichterten Bedingungen erhalten, sondern, dass auch für die anschließende Nutzung der Daten durch das Konzernunternehmen ein klarer Rechtsrahmen gesetzt wird. Zum Schutz der Beschäftigten sind in diesen Fällen die Bestimmungen des Beschäftigtendatenschutzes entsprechend anzuwenden, da das Konzernunternehmen im Hinblick auf die Datenverarbeitung in eine arbeitgeberähnliche Position tritt, indem es Aufgaben wahrnimmt, die an sich dem Vertragsarbeitgeber zufallen. Die datenschutzrechtliche Verantwortlichkeit bestimmt sich nach den allgemeinen Grundsätzen. Absatz 3 trifft hierzu keine Regelung und ist nur anwendbar, sofern das Konzernunternehmen gemäß Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 als datenschutzrechtlich verantwortliche Stelle handelt. Absatz 1 ist von der entsprechenden Anwendung ausgenommen, da eine Offenlegung an weitere Konzernunternehmen gerade nicht stattfinden soll. So wird das Risiko einer unkontrollierten Datenweitergabe im Konzern begrenzt.

### **Zu Absatz 4**

Die Offenlegung besonderer Kategorien von Beschäftigtendaten im Sinne von § 6 Absatz 1 gegenüber einem anderen Konzernunternehmen ist zulässig, sofern die Voraussetzungen für eine Offenlegung nach Absatz 1, sowie zusätzlich ein Ausnahmetatbestand nach Artikel 9 der Verordnung (EU) 2016/679 oder von § 6 Absatz 1 vorliegen. Bei der Auswahl geeigneter und besonderer Schutzmaßnahmen nach § 9 muss der Arbeitgeber beachten, dass

besondere Kategorien von Beschäftigtendaten besonders sensibel und schutzbedürftig sind.

### **Zu Artikel 2 (Folgeänderungen)**

Aufgrund der Aufhebung von § 26 Bundesdatenschutzgesetz durch das Beschäftigtendatenschutzgesetz ergeben sich Folgeänderung in anderen Rechtsvorschriften.

#### **Zu Absatz 1**

#### **Zu Nummer 1**

§ 26 Bundesdatenschutzgesetz wird aufgehoben. Die Inhaltsübersicht ist entsprechend anzupassen.

#### **Zu Nummer 2**

§ 26 Bundesdatenschutzgesetz wird aufgehoben und durch die Regelungen im neuen Beschäftigtendatenschutzgesetz ersetzt.

#### **Zu Absatz 2**

Es handelt sich um eine Folgeänderung aufgrund der Aufhebung von § 26 Bundesdatenschutzgesetz.

#### **Zu Absatz 3**

Es handelt sich um eine Folgeänderung aufgrund der Aufhebung von § 26 Bundesdatenschutzgesetz.

#### **Zu Absatz 4**

Es handelt sich um Folgeänderungen aufgrund der Aufhebung von § 26 Bundesdatenschutzgesetz.

### **Zu Artikel 3 (Inkrafttreten)**

Der Artikel bestimmt, dass dieses Gesetz am Tag nach der Verkündung in Kraft tritt.