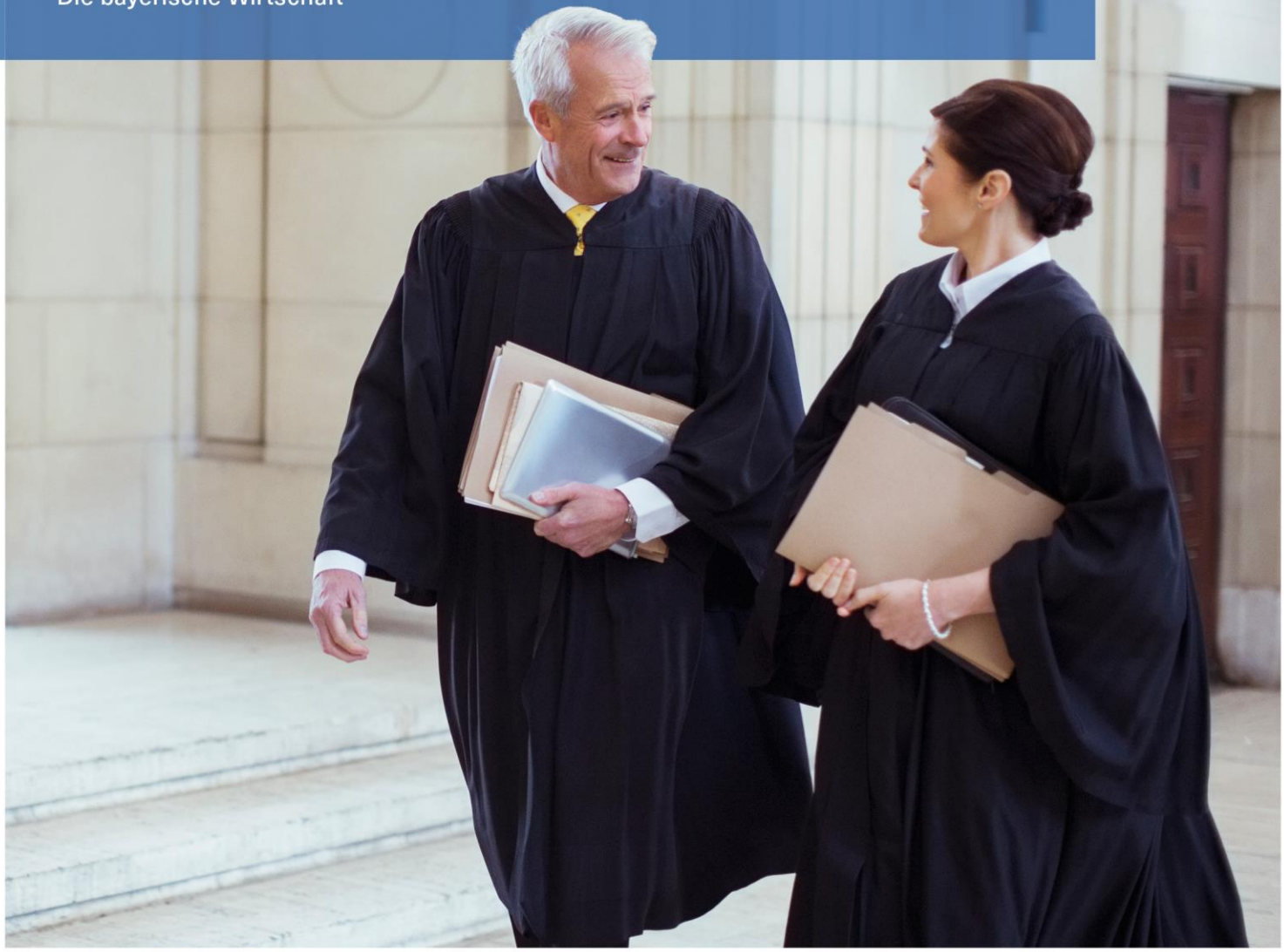
Recht

Datenschutz im Arbeitsverhältnis

vbw

Info Recht
Stand: September 2023

Die bayerische Wirtschaft



Hinweis

Diese Information ersetzt keine rechtliche Beratung im Einzelfall. Eine Haftung übernehmen wir mit der Herausgabe dieser Information nicht.

Um die Information an einen sich wandelnden Rechtsrahmen und an die höchstrichterliche Rechtsprechung anzupassen, überarbeiten wir unsere Broschüre regelmäßig. Bitte informieren Sie sich über die aktuelle Version auf unserer Homepage www.vbw-bayern.de/InfoRecht.

Vorwort

Erfahrungen und Rechtsprechung zum neuen Datenschutzrecht

Zur Anwendung des neuen Datenschutzrechts existieren mittlerweile einige Gerichtsurteile, insbesondere zum Thema Auskunftspflicht. Die Neuauflage unserer Info Recht wurde daher um diesen Teil ergänzt. Zudem gibt es Erleichterungen bei der Übermittlung von Daten in die USA. Die EU-Kommission hat dazu einen neuen Angemessenheitsbeschluss gefasst. Die Inhalte des zugrunde liegenden Data Privacy Frameworks finden Sie in dieser Broschüre.

Unsere Info Recht vermittelt alle Rechtsgrundlagen und Prinzipien, die im Beschäftigtendatenschutz zu beachten sind und enthält die aktuelle Rechtsprechung sowie die Stellungnahmen der Aufsichtsbehörden.

Bertram Brossardt
19. September 2023

Inhalt

1 Grundlagen des Beschäftigtendatenschutzes

Rechtsquellen und Definitionen

Der Datenschutz ist bestimmt durch ein ineinandergreifendes, sich ergänzendes System spezieller und allgemeiner Datenschutznormen.

1.1 Recht auf informationelle Selbstbestimmung

Grundlage des Datenschutzes ist das verfassungsrechtlich garantierte Recht eines jeden Einzelnen auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 des Grundgesetzes (GG). Dieses Recht auf informationelle Selbstbestimmung beinhaltet die Befugnis des Einzelnen, über Preisgabe und Verwendung seiner persönlichen Daten und seine Person betreffende Informationen selbst zu entscheiden. Zweck des Datenschutzes ist es, den Einzelnen vor missbräuchlicher Verwendung seiner persönlichen Daten zu schützen – das gilt auch für den Umgang mit Arbeitnehmerdaten im Arbeitsverhältnis.

Allerdings besteht dieser Schutz personenbezogener Daten des Arbeitnehmers nicht schrankenlos, denn er kollidiert mit ebenfalls verfassungsrechtlich garantierten Grundrechten des Arbeitgebers, dessen wirtschaftlicher Handlungs- und Betätigungsfreiheit (Art. 2 Abs. 1 GG), seiner Berufsfreiheit (Art. 12 Abs. 1 GG) und seinem Recht am eingerichteten und ausgeübten Gewerbebetrieb (Art. 14 GG).

Im Rahmen des Arbeitnehmerdatenschutzes gilt es immer wieder, diese gegenläufigen Interessen in Ausgleich zu bringen.

1.2 Kein eigenständiges Arbeitnehmerdatenschutzgesetz

Eine spezialgesetzliche Regelung des Beschäftigtendatenschutzes – im Sinne eines eigenständigen Arbeitnehmerdatenschutzgesetzes – gibt es bislang nicht. Der Datenschutz im Arbeitsverhältnis ist vielmehr bestimmt durch ein ineinandergreifendes, sich ergänzendes System spezieller und allgemeiner Datenschutznormen sowie arbeitsrechtlicher Prinzipien – sowohl im individualrechtlichen als auch im kollektivrechtlichen Bereich.

Der deutsche Gesetzgeber hat jedoch die in der Datenschutz-Grundverordnung (DS-GVO) vorhandenen Öffnungsklauseln in Art. 88 DS-GVO genutzt und das Bundesdatenschutzgesetz (BDSG) – u. a. im Hinblick auf den Datenschutz im Arbeitsverhältnis – überarbeitet. Der Beschäftigtendatenschutz ist seither primär in § 26 BDSG geregelt. Der Europäische Gerichtshof hat jedoch per Urteil vom 30. März 2023 (Az. C-34/21) entschieden, dass diese Norm (wohl) nicht vollends mit den Vorgaben der DS-GVO vereinbar ist. Da der EuGH allerdings bloß abstrakte Rechtsfragen bei der Auslegung der DS-GVO klärt, bleibt eine abschließende Entscheidung des Verwaltungsgerichts (VG) Frankfurt abzuwarten, welches

die entsprechenden Auslegungsfragen zur Beantwortung an den EuGH gestellt hat. Weitere Einzelheiten sowie bereits jetzt absehbare Konsequenzen der Entscheidung werden detailliert unter Gliederungspunkt 1.5 dargestellt.

Gesetzliche Grundlagen – Beispiele

- Datenschutzgrundverordnung (DS-GVO)
- Bundesdatenschutzgesetz (BDSG)
- Betriebsverfassungsgesetz (BetrVG)

Datenschutzrechtliche Regelungen finden sich des Weiteren in Betriebsvereinbarungen, Tarifverträgen und in Arbeitsverträgen.

Von großer Bedeutung sind die von der Rechtsprechung des Bundesarbeitsgerichts (BAG) entwickelten Grundsätze des allgemeinen Persönlichkeitsrechts des Beschäftigten im Arbeitsverhältnis.

Persönlichkeitsrechtsschutz bedeutet nach der Rechtsprechung des BAG, dass in die Privatsphäre des Beschäftigten nicht tiefer eingegriffen werden darf, als es der Zweck des Arbeitsverhältnisses unbedingt erfordert, und dass im Rahmen der Zweckbestimmung des Arbeitsverhältnisses für die bei Datenverarbeitungen vorzunehmende Interessenabwägung der Grundsatz der Verhältnismäßigkeit maßgebend ist.

1.3 Europäische Datenschutz-Grundverordnung

Die Datenschutzgrundverordnung findet seit 25. Mai 2018 direkt Anwendung. Mit der Einführung der DS-GVO wurde eine Vereinheitlichung des Datenschutzrechtes innerhalb der EU angestrebt, um vor allem Unternehmensgruppen und Konzernen, welche EU-weit agieren, die Einhaltung einer Datenschutz-Compliance zu vereinfachen. Es ist jedoch damit zu rechnen, dass der gewünschte Vereinheitlichungseffekt nur bedingt eintreten wird. Die DS-GVO enthält an über 60 Stellen sogenannte Öffnungsklauseln, mit denen den nationalen Gesetzgebern in der EU die Möglichkeit eingeräumt wird, eigene Regelungen und Konkretisierungen zu schaffen. Für private Unternehmen erlangen vor allem die folgenden Öffnungsklauseln Relevanz:

- Verarbeitung besonders sensibler Daten,
- Einwilligungsfähigkeit Minderjähriger,
- Ausnahmen von der Informationspflicht und dem Verbot automatisierter Einzelentscheidungen,
- Pflicht zu Ernennung eines Datenschutzbeauftragten,

1.4 Neue Begrifflichkeiten und die wichtigsten Begriffe der DS-GVO

Mit der DS-GVO wurden europaweit einheitliche Begrifflichkeiten eingeführt, die von den Begrifflichkeiten des alten BDSG abweichen.

Tabelle 1
Neue Begrifflichkeiten in der DS-GVO

BDSG-alt	**DS-GVO**
Betroffener	betroffene Person
Verantwortliche Stelle	der (für die Verarbeitung) Verantwortliche
Auftragsdatenverarbeiter	Auftragsverarbeiter
Verfahrensverzeichnis	Verzeichnis von Verarbeitungstätigkeiten
Vorabkontrolle	Datenschutzfolgenabschätzung
Standardvertragsklauseln	Standarddatenschutzklauseln

Die wichtigsten Begriffe der DS-GVO sind in Art. 4 enthalten.

Personenbezogene Daten: Sind alle Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Der Begriff ist jetzt umfassender als bisher und umfasst explizit zum Beispiel auch die Online-Kennung (z. B. IP-Adressen oder Cookie-Kennung). Auch pseudonymisierte Daten fallen unter den Anwendungsbereich der DS-GVO. Das sind Daten, die eine eindeutige Zuordnung ermöglichen. Ein Beispiel: Eine Telefonnummer allein ermöglicht noch keine Zuweisung. Die Hinzunahme eines Telefonverzeichnisses aber schon.

Der Begriff umfasst alle Daten lebender natürlicher Personen, das heißt auch zum Beispiel von Einzelfirmen und Dritter jeglicher Art, wie Arbeitgeber, bevollmächtigte Mitarbeiter im eigenen Unternehmen. Personenbezogene Daten von Verstorbenen unterliegen nicht der DS-GVO. Eine Speicherung solcher Daten ist damit zulässig.

Eine betroffene Person ist jede natürliche Person, mit der ein Verantwortlicher, also zum Beispiel ein Unternehmen aus der Metall- und Elektroindustrie, zu tun hat. Die meisten Datenarten von betroffenen Personen der Datenverarbeitung von Unternehmen sind Mitarbeiterdaten, Lieferantendaten und Kundendaten.

Der Verarbeitungsbegriff umfasst jetzt alles. Es gibt keine Differenzierung mehr zwischen dem Begriff der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten.

Ein Verantwortlicher für die Verarbeitung ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Ein Auftragsverarbeiter ist hingegen eine natürliche oder juristische Person, Behörde oder Einrichtung oder andere Stelle, die im Auftrag eines Verantwortlichen personenbezogene Daten der betroffenen Person verarbeitet. Unter der DS-GVO hat der Auftragsverarbeiter zukünftig umfangreichere Pflichten zu erfüllen als unter dem Regime des alten BDSG.

1.5 Die Regelungen des Bundesdatenschutzgesetzes (BDSG)

Zum 25. Mai 2018 ist das überarbeitete BDSG in Kraft getreten. Es überführt im Wesentlichen die bisherigen §§ 3 Abs. 11 und 32 BDSG-alt in einen neuen § 26 BDSG.

- § 26 Abs. 1 S. 1 BDSG entspricht weitestgehend dem bisherigen § 32 Abs. 1 S. 1 BDSG. Neu hinzugekommen ist, dass personenbezogene Daten der Beschäftigten für Zwecke des Beschäftigungsverhältnisses auch verarbeitet werden dürfen, wenn dies zur Ausübung oder der Erfüllung der sich aus einem Gesetz, einem Tarifvertrag oder einer Betriebsvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

- § 26 Abs. 2 BDSG betrifft die Einwilligung von Beschäftigten und weist in Hinblick auf die Wirksamkeit darauf hin, dass die Abhängigkeit der Beschäftigten sowie die Umstände, unter denen die Einwilligung erteilt wurde, bei der Beurteilung der Freiwilligkeit heranzuziehen sind. Sie kann grundsätzlich schriftlich oder elektronisch erteilt werden.

- § 26 Abs. 3 BDSG sieht vor, dass die Verarbeitung besonderer Kategorien personen-bezogener Daten zulässig ist, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit oder des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person einem Ausschluss der Verarbeitung überwiegt.

- § 26 Abs. 4 BDSG sieht vor, dass die Verarbeitung personenbezogener Daten einschließlich der besonderen Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses auf der Grundlage von Kollektivvereinbarungen zulässig ist.

- Nach § 26 Abs. 5 BDSG müssen der nationale Gesetzgeber bzw. Tarifpartner die Grundsätze der Verarbeitung nach Art. 5 DS-GVO beachten.

- § 26 Abs. 6 BDSG stellt klar, dass die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt bleiben.

– Gem. § 26 Abs. 7 BDSG findet das BDSG auch Anwendung für Beschäftigtendaten, wenn sie nicht automatisiert oder aus einer nicht automatisierten Datei verarbeitet werden.

– § 26 Abs. 8 BDSG übernimmt die Begriffsbestimmungen des § 3 Abs. 11 BDSG-alt. Neu aufgenommen wurde in der Ziff. 1, dass auch Leiharbeitnehmer als Beschäftigte im Verhältnis zum Entleiher anzusehen sind. Ausdrücklich mit in den Anwendungsbereich aufgenommen sind Bewerber.

Beschäftigte gem. § 26 Abs. 8 BDSG

– Arbeitnehmer
– zu ihrer Berufsausbildung Beschäftigte
– Rehabilitanden
– in anerkannten Werkstätten für behinderte Menschen Beschäftigte
– nach dem Jugendfreiwilligendienstegesetz Beschäftigte
– arbeitnehmerähnliche Personen; in Heimarbeit Beschäftigte
– Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist
– Beamte, Richter des Bundes, Soldaten, Zivildienstleistende
– Leiharbeitnehmer

Wie bereits eingangs kurz angerissen, hat der Europäische Gerichtshof nunmehr per Urteil vom 30. März 2023 (Az. C-34/21) entschieden, dass § 26 Abs. 1 S. 1 BDSG (wohl) nicht mit den Vorgaben der DS-GVO vereinbar ist. Da der EuGH allerdings bloß abstrakte Rechtsfragen bei der Auslegung der DS-GVO klärt, bleibt eine abschließende Entscheidung des Verwaltungsgerichts (VG) Frankfurt abzuwarten, welches die entsprechenden Auslegungsfragen zur Beantwortung an den EuGH gestellt hat. Für die Praxis sind jedoch bereits jetzt die folgenden Aspekte zu berücksichtigen:

Nach Art. 88 Abs. 1 DS-GVO können die Mitgliedsstaaten spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten vorsehen. Diese Vorschriften müssen nach Art. 88 Abs. 2 DS-GVO zudem geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen umfassen, z. B. im Hinblick auf die Transparenz der Datenverarbeitung und die Überwachungssysteme am Arbeitsplatz. Entgegen diesen Vorgaben in Art. 88 DS-GVO handelt es sich bei § 26 Abs. 1 S. 1 BDSG jedoch nicht um eine „spezifischere Vorschrift“, sondern um eine Generalklausel, welche lediglich die Vorgaben der DS-GVO wiederholt und insbesondere keine gesonderten Schutzmaßnahmen zugunsten der betroffenen Personen enthält. Im Kern führt der EuGH aus, dass es der Regelung des § 26 Abs. 1 S. 1 BDSG nicht bedurft hätte, da deckungsgleiche Regelungen bereits in der DS-GVO selbst angelegt sind. Nationale Rechtsvorschriften zum Beschäftigtendatenschutz müssen aufgrund des Anwendungsvorrangs des Unionsrechts unangewendet bleiben, wenn sie die in Art. 88 Abs. 1 und 2 DS-GVO vorgesehenen Voraussetzungen und Grenzen nicht beachten. Insoweit ist

zunächst davon auszugehen, dass das VG Frankfurt die Ausführungen des EuGH entsprechend übernehmen wird.

Wo bislang also bei der Verarbeitung von Beschäftigtendaten auf § 26 Abs. 1 S. 1 BDSG abgestellt wurde, müssen verantwortliche Stellen künftig die Regelungen der DS-GVO heranziehen. Im Regelfall wird diese Aufgabe lediglich zu einem redaktionellen Aufwand (etwa in Datenschutzhinweisen gemäß Art. 13 DS-GVO sowie im Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO) führen, da in Art. 6 Abs. 1 lit. b) DS-GVO bereits eine Regelung enthalten ist, welche die Verarbeitung personenbezogener Daten zu Zwecken der Erfüllung eines Vertrages (beispielsweise das Arbeitsverhältnis) legitimiert. „Typische" Verarbeitungstätigkeiten im Beschäftigtenkontext können daher auch künftig ohne intensive Prüfung fortgeführt werden. Gleiches gilt, sofern der Arbeitgeber beispielsweise aufgrund einer gesetzlichen Regelung zur Verarbeitung von Beschäftigtendaten verpflichtet ist, da insoweit auf Art. 6 Abs. 1 lit. c) DS-GVO abgestellt werden kann.

Daneben sind jedoch Konstellationen denkbar, in denen auch eine gründlichere Prüfung der nunmehr tauglichen Rechtsgrundlage erforderlich werden kann. Einerseits hat sich das oben zitierte Urteil des EuGH ausdrücklich nur auf Abs. 1 S. 1 von § 26 BDSG bezogen. Ob und inwieweit diese Rechtsprechung daher auf die weiteren Absätze von § 26 BDSG übertragbar ist, ist nicht abschließend geklärt. Einige rechtliche Argumente sprechen jedoch dafür, dass zumindest die Kernaussagen des Urteils auch auf weitere Absätze von § 26 BDSG übertragbar sind. Insbesondere bei der Verarbeitung personenbezogener Daten auf Basis einer Betriebsvereinbarung (vgl. hierzu § 26 Abs. 4 BDSG) sollten Unternehmen eine datenschutzrechtliche Prüfung der bisherigen Verarbeitungstätigkeiten veranlassen und die weiteren Entwicklungen im Auge behalten. Hier gilt es genau zu bewerten, ob und inwieweit das zitierte Urteil des EuGH Auswirkungen auf bestehende Prozesse und Betriebsvereinbarungen entfaltet. Da dies jedoch mitunter eine gewisse fachliche Expertise erfordert, sollte in Zweifelsfällen professioneller Rechtsrat eingeholt werden.

Auf der anderen Seite existieren in § 26 BDSG Regelungen, welche lediglich klarstellender Natur sind. Daneben ist es denkbar, dass gewisse Absätze in § 26 BDSG (insbesondere Abs. 1 S. 2) den Anforderungen der DS-GVO entsprechen und daher weiterhin anwendbar bleiben. Insoweit bleibt die weitere Entwicklung im Auge zu behalten, sodass Unternehmen schnell auf einen etwaigen Anpassungsbedarf reagieren können.

Eine gute Zusammenfassung zu Inhalt und Auswirkungen der aktuellen Rechtsprechung des EuGH zu § 26 BDSG kann einer Handreichung der Hessischen Datenschutzaufsichtsbehörde vom 25. April 2023 entnommen werden. Die Handreichung ist abrufbar unter:

https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-04/handreichung_beschaeftigtendatenschutz_eugh-urteil.pdf

1.6 Anwendungsbereich des Bundesdatenschutzgesetzes

Der Anwendungsbereich des BDSG umfasst sowohl die automatisierte als auch die nicht-automatisierte Verarbeitung von Daten. Hier sollte insbesondere im Blick behalten werden, dass die Vorgaben in § 26 Abs. 7 BDSG über den Anwendungsbereich aus Art. 2 DS-GVO hinausgehen. Die soeben dargestellten Ausführungen des EuGH beziehen sich daher nicht auf solche Datenverarbeitungstätigkeiten, welche außerhalb des Anwendungsbereichs der DS-GVO liegen. Dies gilt u. a. für rein „tatsächliche Handlungen“, wie etwa Spindkontrollen, das Protokoll des Bewerbungsgesprächs oder rein mündliche Befragungen von Beschäftigten. Insoweit gelten weiterhin die Regelungen des § 26 BDSG. Da die im Beschäftigungsverhältnis relevanten Datenverarbeitungsvorgänge jedoch im Regelfall (auch) den Anforderungen der DS-GVO unterfallen, soll hierauf nachstehend bewusst der Fokus gelegt werden.

Das BDSG unterscheidet zwischen personenbezogenen Daten und besonderen Arten personenbezogener Daten:

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person) beziehen, Art. 4 Nr. 1 DS-GVO z. B.: Geburtsdatum eines Beschäftigten, Gehalt oder Eingruppierung eines Beschäftigten.

Besondere Kategorien personenbezogener Daten sind im Sinne von Art. 9 DS-GVO Angaben über
- rassische oder ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen,
- Gewerkschaftszugehörigkeit,
- Genetische Daten,
- Biometrische Daten zur Identifikation,
- Gesundheit,
- Sexualleben oder sexuelle Orientierung.

Der Umgang mit diesen Daten unterliegt besonderen Einschränkungen.

Melde- und Benachrichtigungspflichten gem. Art. 33 und 34 DS-GVO

Art. 33 und 34 DS-GVO unterscheiden nicht nach den Kategorien von betroffenen personenbezogenen Daten.

Gehen Daten verloren und droht der betroffenen Person dadurch ein Risiko für die Rechte und Freiheiten, so besteht eine Informationspflicht gegenüber der Datenschutzaufsichtsbehörde und ggf. auch gegenüber der betroffenen Person.

Mitzuteilen sind der Datenschutzaufsichtsbehörde unverzüglich, d. h. innerhalb von 72 Stunden:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit der Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze,
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Bei einem Verstoß gegen die Informationspflicht droht ein Bußgeld in Höhe von bis zu 10.000.000,00 Euro oder im Falle eines Unternehmens von bis zu zwei Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, Art. 83 Abs. 4 DS-GVO.

Fall

Ein Vertriebsmitarbeiter verliert einen nicht verschlüsselten USB-Stick, auf dem Kundendaten enthalten sind, u. a. auch deren Kontodaten.

In diesem Fall müssen die Datenschutzaufsichtsbehörde und die betroffenen Personen über den Datenverlust informiert werden.

1.7 Datenschutzrechtlich erhebliche Vorgänge

Nach Art. 2 Abs. 1 DS-GVO gilt die Verordnung „für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“ Ob und inwieweit eine Verarbeitung in den sachlichen Anwendungsbereich der DS-GVO fällt, muss daher danach beurteilt werden,

- ob eine Verarbeitung stattfindet sowie
- ob es sich bei den Daten um personenbezogene Daten handelt.

Der Begriff der „Verarbeitung“ wird in Art. 4 Nr. 2 DS-GVO definiert. Danach handelt es sich um „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder solche Vorgangsreihen in 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 Weitergabe durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“.

Die DS-GVO erfasst somit sämtliche Formen des Umgangs mit personenbezogenen Daten von der Erhebung bis zur endgültigen Vernichtung.

Aufgrund des einheitlichen Verarbeitungsbegriffs des Art. 4 Nr. 2 DS-GVO stehen alle nachfolgenden dargestellten Verarbeitungsvorgänge Verarbeitungen im Sinne der DS-GVO dar:

- Erheben von Beschäftigtendaten findet z. B. in folgenden Formen statt:
  Durch Befragen im Bewerbungs- oder Mitarbeitergespräch oder standardmäßiges Abfragen im Personalfragebogen.

- Verarbeiten von Beschäftigtendaten findet z. B. in folgenden Formen statt:
  - Speichern (z. B. in Personalinformationssystemen)
  - Verändern
  - Übermitteln (z. B. Arbeitgeberauskünfte an Externe)
  - Einschränken und Löschen von Beschäftigtendaten (z. B. beim Ausscheiden von Beschäftigten, bei Daten deren Richtigkeit vom Beschäftigten bestritten wird, Zugriffsbeschränkungen für bestimmte Beschäftigten im Rahmen der Personaldatenverarbeitung)

- Nutzen von Beschäftigtendaten findet z. B. in folgenden Formen statt: Die betriebsinterne Weitergabe von Beschäftigtendaten an den Betriebsrat oder die Auswertung von Internetnutzungsdaten zum Zwecke der Beschäftigtenkontrolle.

2 Umgang mit Beschäftigtendaten

Prinzipien und Rechtsgrundlagen

Insbesondere wegen der Vielzahl in datenschutzrechtlicher Hinsicht zu beachtender Gesetze und der diesbezüglichen umfangreichen Rechtsprechung ist beim Umgang mit Arbeitnehmerdaten besondere Sorgfalt geboten.

2.1 Datenschutzrechtliche Grundsätze

Die bekannten Grundsätze des „Verbots mit Erlaubnisvorbehalt“, der „Datenvermeidung und Datensparsamkeit“, der „Zweckbindung“ und der „Transparenz“ prägen auch die DS-GVO. Der europäische Gesetzgeber hat damit verdeutlicht, dass diese bereits aus der Datenschutz-Richtlinie bekannten Prinzipien weiterhin Geltung erhalten sollen. Die genaue Umsetzung unterscheidet sich allerdings teilweise von der aktuellen Situation.

2.1.1 Verbotsprinzip

Für den Umgang mit personenbezogenen Daten bleibt es bei dem bekannten Verbotsprinzip: „Der Umgang mit personenbezogenen Daten ist verboten, außer soweit er nach der DS-GVO rechtmäßig ist (Art. 6 DS-GVO).“ Die wichtigsten Rechtsmäßigkeitsalternativen für private Unternehmen sind:

- die Einwilligung der betroffenen Person,
- die Vertragserfüllung oder vorvertragliche Maßnahmen,
- die Umsetzung rechtlicher Verpflichtungen sowie
- die Wahrnehmung berechtigter Interessen soweit nicht die Interessen der betroffenen Person überwiegen.

Details zu den Rechtmäßigkeitsgrundlagen finden Sie in Ziffer 2.2.

2.1.2 Datenminimierung

Eines der zentralen Prinzipien des Datenschutzes in der DS-GVO ist das Prinzip der Datenminimierung. Nach Art. 5 Abs. 1 lit. c) DS-GVO muss die Verarbeitung personenbezogener Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Hinweis

Aus Erwägungsgrund 39 S. 7 bis 10 DS-GVO lassen sich folgende Anforderungen für eine gesetzeskonforme Datenverarbeitung ableiten:

- Datenverarbeitung als ultimo ratio,
- Minimierung der Speicherfrist,
- Löschroutinen,
- Festlegung regelmäßiger Termine für eine Kontrolle, ob personenbezogene Daten noch benötigt werden.

2.1.3 Zweckbindung

Gemäß Art. 5 Abs. 1 lit. b) DS-GVO dürfen personenbezogene Daten weiterhin nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden. Zudem dürfen einmal erhobene personenbezogene Daten nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. In Art. 6 Abs. 4 stellt die DS-GVO Kriterien auf, die bei der Beurteilung der Vereinbarkeit einer Zweckänderung zu berücksichtigen sind. Dies sind unter anderem:

- die Verbindung zwischen den Zwecken der Erhebung und der Weiterverarbeitung,
- der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden,
- die Art der personenbezogenen Daten,
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffene Person sowie das Vorhandensein geeigneter Garantien.

Zu den geeigneten Garantien gehören laut DS-GVO unter anderem die Verschlüsselung oder Pseudonymisierung. Dies führt zu einer Privilegierung der Weiterverarbeitung pseudonymisierter bzw. verschlüsselter Daten. Insbesondere im Bereich der Big Data-Anwendungen kann dieser Vorteil genutzt werden.

2.1.4 Transparenz

Schon früher wurde die Transparenz im Bereich des Datenschutzes großgeschrieben. Nunmehr ist dieser Grundsatz ausdrücklich in die DS-GVO (Art. 12) aufgenommen worden. Sämtliche Informationen und Auskünfte sind danach schriftlich, leicht verständlich und in der Regel unentgeltlich zu erteilen. Grundsätzlich sollte die Auskunft spätestens einen Monat nach dem Antragseingang erfolgen.

2.1.5 Datensicherheit

Als zentrales Prinzip wurde in Art. 5 Abs. 1 lit. f) DS-GVO die Gewährleistung der Datensicherheit gesetzlich verankert. Diese umfasst neben den bereits bekannten klassischen Schutzzielen der IT-Sicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) auch die Belastbarkeit.

Um diesen Zielen gerecht zu werden, haben Verantwortliche nach Art. 32 DS-GVO geeignete technische und organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik und der Implementierungskosten umzusetzen. Somit ist zukünftig zu prüfen, was bei dem jeweiligen Verfahren als Stand der Technik angesehen wird. Jedoch ist auch die Verhältnismäßigkeit der Maßnahmen hinsichtlich des Aufwandes zu berücksichtigen. Kurzum: Das Sicherheitslevel muss im Verhältnis zum Risiko angemessen sein.

Praxistipp

Um beurteilen zu können, was ein angemessenes Schutzniveau nach Art. 32 Abs. 1 DS-GVO ist, muss der Verantwortliche im Vorfeld den Schutzbedarf der durch ihn erhobenen und gespeicherten Daten ermitteln.

2.1.6 Rechenschaftspflicht

Der Grundsatz der Rechenschaftspflicht verlangt von Unternehmen, dass die Grundsätze der DS-GVO nachweisbar eingehalten werden. Der Verantwortliche trägt die Beweislast dafür, dass er die gesetzlichen Vorgaben einhält. Sofern in Artikeln der DS-GVO geregelt ist, wie dieser Nachweis erbracht werden soll, müssen Unternehmen dafür Sorge tragen, dass entsprechende Prozesse im Unternehmen implementiert sind.

Generell sollte die Dokumentation in Schrift- oder elektronischer Form erfolgen und jederzeit auffindbar sein, um der Rechenschaftspflicht nachzukommen. Aus der Dokumentation sollte sich eine klare Beschreibung der gegenwärtigen Situation, der Rechtsgrundlagen und des Verantwortlichen innerhalb des Unternehmens ergeben.

Praxistipp

Der Grundsatz der Rechenschaftspflicht führt zu erheblichen Dokumentations- und Nachweispflichten im Unternehmen. Es muss nicht nur sichergestellt werden, dass die einzelnen Anforderungen der DS-GVO erfüllt werden, diese Tatsache muss auch nachgewiesen werden können.

Aus diesem Grunde sollte bei der Planung von Prozessen und Strukturen die entsprechende Dokumentation gleich mit geplant werden, um Bußgelder und verlorene Prozesse zu vermeiden.

2.2 Rechtmäßigkeit der Verarbeitung

Die DS-GVO regelt in Art. 6 DS-GVO verschiedene Alternativen für die Rechtmäßigkeit der Verarbeitung. Ergänzend enthält § 26 BDSG Regelungen zur Verarbeitung personenbezogener Beschäftigtendaten. Da diese Regelung – wie bereits aufgezeigt – für gewisse Verarbeitungstätigkeiten künftig nicht mehr herangezogen werden kann, soll nachstehend der Fokus auf die Rechtsgrundlagen der DS-GVO gelegt werden.

Diese Grundlagen sind von der Art her bereits aus dem alten BDSG bekannt. In Details gibt es jedoch Änderungen, welche zu beachten sind. Dies bedeutet, dass Unternehmen ihre bestehenden Verträge und Prozesse daraufhin kontrollieren müssen, ob auch die neuen Anforderungen beachtet werden. Aufgrund des Grundsatzes der Rechenschaftspflicht ist die Einhaltung der Anforderungen zu dokumentieren.

2.2.1 Einwilligung

Wenn sich die Datenverarbeitung nicht mit einer Spezialvorschrift (Art. 6 Abs. 2 und 3 DS-GVO) rechtfertigen lässt, ist eine Einwilligung (Art. 7 DS-GVO) der betroffenen Person erforderlich: Eine Einwilligung ist die vorherige Einverständniserklärung des betroffenen Beschäftigten. Ein nachträgliches Einverständnis genügt nicht und ändert auch nichts an der Rechtswidrigkeit der bis dahin erfolgten Datenverarbeitungen.

Tipp für die Praxis

Grundsätzlich sollte eine Rechtfertigung im Wege der Einwilligung nur in Fällen in Anspruch genommen werden, in denen der Beschäftigte eine echte Wahl hat. Darf der Arbeitgeber bereits aufgrund von Art. 6 Abs. 1 lit. b) DS-GVO oder einer Betriebsvereinbarung gemäß Art. 88 Abs. 1, 2 DS-GVO personenbezogene Beschäftigtendaten verarbeiten, kann es sogar irreführend sein, wenn er versucht, diese Verarbeitungen auf die Einwilligung der betroffenen Beschäftigten zu stützen. Bei dem Beschäftigten würde dann nämlich der Eindruck erweckt, er könne die Datenverarbeitung jederzeit durch Widerruf beenden. § 26 Abs. 2 BDSG enthält daneben Sonderbestimmungen für die Freiwilligkeit einer im Arbeitsverhältnis erteilten Einwilligung, welche – trotz des bereits angeführten Urteils des EuGH – nach der Auffassung der Datenschutzaufsichtsbehörden weiterhin Geltung beanspruchen (vgl. insoweit Erwägungsgründe 42 Satz 5 und 43 DS-GVO). Im Kern geht es hierbei insbesondere um das typischerweise zwischen Arbeitgeber und Arbeitnehmer bestehende Ungleichgewicht, welches bei dem Einholen einer datenschutzrechtlichen Einwilligung stets zu berücksichtigen ist.

Beispiele

Per Einwilligung zu legitimierende Beschäftigtendatenverarbeitung:

- Weitergabe von Beschäftigtenadressen zwecks Firmenrabatt, z. B. an Versicherungsunternehmen,
- Beschäftigtendaten im Internet und Veröffentlichung von Bildern und Fotos, Geburtstagsliste, Rennliste,
- Eingriffe in das Fernmeldegeheimnis, wenn der Arbeitgeber die private Nutzung von Telefon, E-Mail und Internet gestattet und den Umfang der Privatnutzung kontrollieren will,
- Aufzeichnen von dienstlichen Telefongesprächen,

Anforderungen an eine wirksame Einwilligungserklärung sind gemäß Art. 7 DS-GVO:

- Freiwilligkeit
  Die Einwilligung muss auf der freien Entscheidung der betroffenen Person beruhen. In dem Über- / Unterordnungsverhältnis von Arbeitgeber und Beschäftigten ist eine Einwilligung unfreiwillig und daher unwirksam, wenn eine wirtschaftliche Machtposition des Arbeitgebers zur Erlangung der Einwilligung ausgenutzt wurde. Dabei greifen Erleichterungen insbesondere für den Fall, dass dem Beschäftigten durch die Einwilligung ein Vorteil entsteht oder die Interessen der Parteien gleich gelagert sind; hier kann von der Freiwilligkeit der Einwilligung ausgegangen werden. Die Gesetzesbegründung des BDSG nennt als Beispiele für Vorteile des Beschäftigten eine Privatnutzung von IT-Systemen und ein betriebliches Gesundheitsmanagement zur Gesundheitsförderung. Als Beispiel für gleichgerichtete Interessen werden Geburtstagslisten oder Fotos für das Intranet angeführt. Erhöhte Anforderungen an die Freiwilligkeit werden ausweislich der Gesetzesbegründung zum BDSG bei der Begründung eines Beschäftigungsverhältnisses gestellt, weil hier laut Aussage des Gesetzgebers der Druck zum Abschluss eines Arbeitsvertrages höher liegt. Daher muss jeweils im Einzelfall entschieden werden, ob die konkrete Situation ein erhebliches Ungleichgewicht beinhaltet. Diese Anforderungen sollten auch im Anwendungsbereich der DS-GVO weiterhin berücksichtigt werden.

- Konkretheit der Einwilligung, Transparenz
  Der Beschäftigte ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. Nur wenn er die vorgesehenen Verarbeitungen kennt, kann er sich frei entscheiden. Eine pauschale Erklärung der betroffenen Person, sie sei mit jeder weiteren Form der Verarbeitung ihrer Daten einverstanden, reicht nicht aus. Das bedeutet, dass eine Einwilligung fallbezogen einzuholen ist.

- Der betroffene Beschäftigte ist über sein Widerrufsrecht mit Wirkung für die Zukunft zu informieren. Ab dem Zeitpunkt des Widerrufs wird damit jede zukünftige Verarbeitung durch den Arbeitgeber rechtswidrig, soweit kein sonstiger Erlaubnistatbestand die Verarbeitung rechtfertigt. Auf der Grundlage der konkreten Einwilligung gespeicherte

Daten müssen dann gelöscht werden, insbesondere wenn die betroffene Person dies fordert.

Beispiel

Die Konzernmutter bietet den Beschäftigten des Tochterunternehmens Unternehmensaktien zum Vorzugspreis an. Hierfür müssen allerdings Beschäftigtendaten über Einkommen, etc. an die Konzernmutter übermittelt werden. Beschäftigte, die ihre Einwilligung hierzu nicht erteilen, müssen auf den Firmenrabatt verzichten. Wird die Einwilligung erteilt, ist sie als freiwillig zu behandeln und die Übermittlung der personenbezogenen Daten erfolgt rechtmäßig.

Hinweis

Soll in die Verarbeitung besonderer Kategorien von Daten im Sinne von Art. 9 DS-GVO eingewilligt werden (z. B. Gesundheitsdaten, Daten über das Sexualleben, etc.) muss sich die Einwilligungserklärung ausdrücklich auf diese Daten beziehen (Art. 9 Abs. 2 lit. b) DS-GVO).

- Form
  Die DS-GVO knüpft eine rechtswirksame Einwilligung nicht an eine bestimmte Form. In Art. 7 Abs. 1 DS-GVO wird jedoch klargestellt, dass der Verantwortliche das Vorliegen einer Einwilligung nachweisen können muss. Neben der elektronischen Einwilligung wird daher auch künftig die schriftliche Einwilligungserklärung zu empfehlen sein. Da diese Anforderungen letztlich auch in § 26 Abs. 2 S. 3 BDSG aufgestellt werden, sollte – insbesondere aus Gründen der Rechtssicherheit – eine entsprechende Vorgehensweise eingehalten werden.

- Keine Einwilligung im „Kleingedruckten“
  Soll ein Betroffener eine Einwilligung zusammen mit anderen Erklärungen abgegeben, z. B. im Rahmen eines Arbeitsvertrages, darf die Einwilligungserklärung nicht im sogenannten „Kleingedruckten“ versteckt sein. Die Einwilligungserklärung muss dann deutlich sichtbar oder drucktechnisch von dem übrigen Text abgesetzt dargestellt werden (z. B. Fettdruck oder gesondert zu unterzeichnender Anhang), Art. 7 Abs. 2 DS-GVO.

2.2.2 Begründung, Durchführung und Beendigung eines Beschäftigungsverhältnisses

Die Verarbeitung von personenbezogenen Beschäftigtendaten zum Zwecke des Beschäftigungsverhältnisses ist zulässig, wenn dies

- für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses

– oder für dessen Durchführung
– oder dessen Beendigung

erforderlich ist. In Art. 6 Abs. 1 lit. b) DS-GVO heißt es insoweit wörtlich, dass die Verarbeitung „für die Erfüllung eines Vertrags“ erforderlich sein muss.

Grundsätzlich gilt, dass die Verarbeitung solcher Arbeitnehmerdaten zulässig ist, die zur Erfüllung der Rechte und Pflichten aus dem Arbeitsvertrag erforderlich sind, sofern damit nicht in unverhältnismäßiger Weise in das Persönlichkeitsrecht des Arbeitnehmers eingegriffen wird. Letztendlich muss die Zulässigkeit einer Datenverarbeitung immer im Einzelfall nach Abwägung der für den Einzelfall maßgeblichen Interessen beider Seiten entschieden werden.

Die Erforderlichkeit der Verarbeitung ist somit der Maßstab für die Verarbeitung. Die Verarbeitung ist jedenfalls erforderlich, wenn der Vertrag ohne Verarbeitung der Daten in dem geltend gemachten Umfang nicht erfüllt werden könnte.

2.2.3 Berechtigtes Interesse

Nach Art. 6 Abs. 1 lit. f) DS-GVO ist die Datenverarbeitung im Anschluss an eine Abwägung der berührten Interessen gestattet, soweit diese zu Gunsten des Verantwortlichen entschieden wird. Die Verarbeitung ist immer dann gestattet, wenn der folgende Dreiklang gegeben ist:

– Interessen des Verantwortlichen, welche „berechtigt“ sein müssen,
– Erforderlichkeit der Datenverarbeitung,
– kein Überwiegen der berechtigten Interessen des Betroffenen.

Festgestellt sein muss zunächst also ein berechtigtes Interesse des Verantwortlichen, zu dessen Wahrung die Verarbeitung erforderlich ist. Dieses Interesse ist weit zu verstehen. So ist schon in den Erwägungsgründen zur DS-GVO die Direktwerbung als berechtigtes Interesse des Verantwortlichen qualifiziert.

Die Verarbeitung muss ferner zur Wahrung des berechtigten Interesses erforderlich sein. Bei der Auslegung der Erforderlichkeit muss eine autonome Begriffsbildung des Unionsrechts berücksichtigt werden. Die Verarbeitung ist jedenfalls dann erforderlich, wenn sie geeignet ist den Zweck zu erreichen und es kein milderes Mittel zur Zweckerreichung gibt.

Die Verarbeitung ist jedoch auch im Falle ihrer Erforderlichkeit ausgeschlossen, wenn Interessen oder Grundrechte und Grundfreiheiten des Betroffenen überwiegen. Nach DS-GVO sind hier „vernünftige Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen“ zu berücksichtigten. Schutzgüter sind im Primärrecht der Union zu suchen, insbes. bei den Grundfreiheiten und bei den Grundrechten, ohne dass der Verantwortliche selbst an die Grundrechte gebunden wäre.

Das Interesse der betroffenen Person muss überwiegen, um die Verarbeitung auszuschließen. Für die Beurteilung ist eine Abwägung erforderlich.

Hinweis

Als berechtigtes Interesse des Verantwortlichen können unter anderem die folgenden Verarbeitungen anerkannt werden:

- Verhinderung von Betrug gegenüber dem Verantwortlichen,
- IT- und Netzwerksicherheit,
- Konzerninterne Verarbeitungen zu Verwaltungszwecken.

Es muss jedoch in jedem Einzelfall die beschriebene Abwägung stattfinden.

2.2.4 Betriebsvereinbarung

Arbeitgeber und Betriebsrat können besondere Erlaubnis-, Zweckbindungs- und Verbotsregelungen für die Verarbeitung und Nutzung von Personaldaten in Betriebsvereinbarungen regeln. Eine Betriebsvereinbarung ist eine eigenständige Zulässigkeitsnorm, Art. 88 Abs. 1 DS-GVO. Inhaltlich müssen die Betriebsvereinbarungen den Wertungen und den Grundsätzen der DS-GVO entsprechen. Die Grundsätze der Verarbeitung nach Art. 5 DS-GVO stehen damit grundsätzlich nicht zur Disposition bei Erlass nationaler Regelungen, jedoch kann der nationale Gesetzgeber unter Berücksichtigung der Grundsätze der DS-GVO die betrieblichen Begebenheiten konkretisieren und damit einheitlich für den ganzen Betrieb festlegen. In jedem Fall muss darauf geachtet werden, dass die jeweilige Betriebsvereinbarung den Anforderungen des Art. 88 Abs. 1, 2 DS-GVO entspricht. Eine bloße Wiederholung der Vorgaben der DS-GVO ist – wie bereits aufgezeigt – nicht ausreichend. Gerade bei der Festlegung und Formulierung der technischen und organisatorischen Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Personen (vgl. Art. 32 Abs. 1 DS-GVO) sollte daher mit besonderer Gründlichkeit vorgegangen werden. Zulässig ist auch, den Datenschutz zugunsten der Beschäftigten zu verstärken.

Der Gestaltungsfreiraum bleibt somit für die Betriebsparteien begrenzt. Sie müssen sich an die grundgesetzlichen Wertungen, zwingendes Gesetzesrecht und die allgemeinen Grundsätze des Arbeitsrechts halten. Aus diesem Grund sind in der Praxis kaum Fälle denkbar, in denen durch Betriebsvereinbarung das Schutzniveau der DS-GVO unterschritten werden kann.

Hinweis

Es ist erforderlich, dass die Betriebsvereinbarung die jeweiligen Verarbeitungsvorgänge von personenbezogenen Beschäftigtendaten ausdrücklich anspricht und regelt. Es genügt

nicht, dass die Verarbeitung bestimmter Informationen oder Daten „stillschweigend“ vorausgesetzt wird.

2.3 Erheben und Speichern von Personaldaten

Will der Arbeitgeber im Bewerbungsverfahren oder im laufenden Arbeitsverhältnis personenbezogene Daten erheben, dann sind seinem Informationsinteresse durch das Persönlichkeitsrecht des Bewerbers bzw. Arbeitnehmers und die arbeitsrechtliche Fürsorgepflicht Grenzen gesetzt. Zulässigerweise darf der Arbeitgeber nur Fragen stellen, an deren wahrheitsgemäßer Beantwortung er ein berechtigtes, billigenswertes und schutzwürdiges Interesse hat, aufgrund dessen die Belange des Bewerbers oder Arbeitnehmers zurücktreten müssen. Ein solches Interesse ist regelmäßig nur anzunehmen, wenn die Beantwortung der Frage für den (angestrebten) Arbeitsplatz und die zu verrichtende Tätigkeit selbst von Bedeutung sind. Unzulässig sind Fragen, die die Privat- oder Intimsphäre des Bewerbers bzw. Arbeitnehmers betreffen, ohne dass ein Zusammenhang mit dem Arbeitsplatz besteht.

Welche Informationen ein Arbeitgeber berechtigterweise ohne Verletzung des Persönlichkeitsrechts des Bewerbers oder Arbeitnehmers für seine Personalentscheidungen verwenden darf, hat die Rechtsprechung in diversen Entscheidungen zum Thema „Fragerecht und Offenbarungspflicht“ festgelegt. Daneben sind auch die Diskriminierungsverbote des Allgemeinen Gleichbehandlungsgesetzes (AGG) zu beachten.

Nach dem AGG sind Benachteiligungen von Arbeitnehmern und Bewerbern wegen der Rasse oder ethnischen Herkunft, der Religion oder Weltanschauung, des Geschlechts, des Alters, einer Behinderung oder der sexuellen Identität verboten. Verstößt der Arbeitgeber dagegen, können Arbeitnehmer und Bewerber Schadensersatz und Entschädigung geltend machen.

Das AGG gibt den Arbeitnehmern und Bewerbern bei der Geltendmachung dieser Ansprüche eine Beweislasterleichterung an die Hand, denn gemäß § 22 AGG muss der Arbeitnehmer bzw. der Bewerber nicht voll beweisen, dass er von dem Arbeitgeber gerade wegen eines der genannten Diskriminierungsmerkmale benachteiligt wurde. Es genügt vielmehr, wenn der Arbeitnehmer bzw. der Bewerber sogenannte Indiztatsachen hierfür nachweisen kann (z. B. unzulässige Fragen in Personalfragebögen, Vorstellungs- und Mitarbeitergesprächen oder diskriminierende Anforderungen in Stellenanzeigen sowie die Nennung von diskriminierenden Gründen in Absageschreiben an abgelehnte Bewerber). Kann der Arbeitnehmer bzw. Bewerber solche Indiztatsachen nachweisen, ist es Sache des Arbeitgebers, den vollen Gegenbeweis zu erbringen, dass die angegriffene Personalentscheidung nicht auf einem Diskriminierungsmerkmal beruht oder wenn das der Fall ist, dass hierfür ein Rechtfertigungsgrund vorlag. Kann der Arbeitgeber diesen Gegenbeweis nicht erbringen, muss er mit Entschädigungs- und / oder Schadensersatzforderungen rechnen.

Daher sollte der Arbeitgeber bei seinen Personalentscheidungen – insbesondere im Rahmen von Bewerbungsverfahren – darauf achten, dass er keine Indiztatsachen setzt, die im Streitfall gegebenenfalls zu einer Beweislasterleichterung für potenzielle Kläger führen könnten.

Werden Beschäftigten- oder Bewerberdaten für eine nachfolgende weitere Verarbeitung im Geltungsbereich der DS-GVO erhoben, gilt das generelle Verbot mit Erlaubnisvorbehalt. Soweit keine Spezialvorschriften gelten, richtet sich die Zulässigkeit der Datenverarbeitung grundsätzlich nach Art. 6 Abs. 1 lit. b) DS-GVO. Demnach darf der Arbeitgeber Informationen über Bewerber oder Beschäftigte verarbeiten, wenn dies für die Entscheidung über die Begründung, die Durchführung oder die Beendigung des Beschäftigungsverhältnisses erforderlich ist. Im Einzelnen gilt hinsichtlich der Daten Folgendes:

2.3.1 Stammdaten

Im laufenden Arbeitsverhältnis ist die Speicherung von Name, Adresse, Geburtsdatum und weiterer sog. Stammdaten zulässig, weil die Kenntnis dieser Daten im Verlauf des Arbeitsverhältnisses z. B. für die allgemeine Personalplanung, Zwecke der Personaleinsatzplanung (z. B. Entscheidungen über Auslandseinsätze), Personalauswahl und Sozialauswahl bei betriebsbedingten Kündigungen, erforderlich sein kann. Solche Stammdaten sind zum Beispiel:

- Geschlecht
- Familienstand
- (Hoch-) Schulausbildung
- Ausbildung in Lehr- und anderen Berufen
- Fachschulausbildung / Fachrichtung / Abschluss
- Sprachkenntnisse

In Bewerbungsverfahren sollte der Arbeitgeber aber auf die Abfrage von Geschlecht, Familienstand, Alter bzw. Geburtsdatum in Fragebögen, Vorstellungsgesprächen etc. wegen der eventuellen Indizwirkung im Rahmen der Geltendmachung von Schadensersatz- und Entschädigungsansprüchen nach dem AGG verzichten. Aus dem gleichen Grund sollten Sprachkenntnisse nicht als „Muttersprache“ verlangt werden, da dies eine Anknüpfung an die Rasse oder ethnische Herkunft impliziert.

Zulässig sind aber insbesondere Fragen nach dem beruflichen Werdegang, Aus- und Weiterbildungszeiten, Fragen nach früheren Arbeitgebern und der jeweiligen Beschäftigungsdauer.

Soweit Lohn und Gehalt unbar ausgezahlt werden, darf der Arbeitgeber zum Zwecke der Entgeltüberweisung auch die Bankverbindung des Arbeitnehmers erfragen und speichern.

2.3.2 Gesundheitsdaten

Gesundheitsdaten sind besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO. Da es sich hierbei um einen besonders sensiblen Bereich handelt, ist die Verarbeitung von Gesundheitsdaten erheblich eingeschränkt.

In § 22 Abs. 1 BDSG werden über die DS-GVO hinaus weitere Zulässigkeitstatbestände zur Verarbeitung personenbezogener Personaldaten genannt. So ist beispielsweise eine solche Datenverarbeitung explizit gestattet, soweit dies erforderlich ist, um die aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und den diesbezüglichen Pflichten nachzukommen. Generell sind nach § 22 Abs. 2 BDSG angemessene und spezifische Maßnahmen – unter Berücksichtigung des Stands der Technik – zur Wahrung der Interessen der Beschäftigten vorzusehen.

Hinweis

An die Stelle des früher in der Anlage des § 9 BDSG-alt enthaltenen konkreten technischen und organisatorischen Maßnahmen zum Zwecke der Datensicherheit ist die etwas allgemeine Regelung des Art. 32 der DS-GVO sowie § 22 Abs. 2 BDSG getreten. Statt bestimmter konkreter Schutzmaßnahmen wird die Einhaltung der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit sowie Belastbarkeit gefordert und beispielhaft als Maßnahmen die Pseudonymisierung und die Verschlüsselung personenbezogener Daten genannt. Der Arbeitgeber als Verantwortlicher muss nachweisen, dass er die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat.

2.3.3 Krankheiten / allgemeiner Gesundheitszustand

Nach der Rechtsprechung des BAG sind Fragen nach dem Gesundheitszustand nur insoweit zulässig, als gezielt die Beeinträchtigungen bei der Verwendung auf dem konkreten Arbeitsplatz ermittelt werden sollen:

- Krankheiten bzw. Beeinträchtigungen des Gesundheitszustandes, durch die die Eignung für die vorgesehene Tätigkeit auf Dauer oder wiederkehrend eingeschränkt wird (z. B. beeinträchtigende Körperbehinderungen),
- ansteckende Krankheiten, die Kollegen oder Kunden gefährden können,
- absehbare Arbeitsunfähigkeit zum vorgesehenen Dienstantritt oder in absehbarer Zeit, z. B. durch eine geplante Operation, eine bewilligte Kur oder auch durch eine derzeit bestehende, akute Erkrankung.

Die „nur“ allgemeine Frage nach dem Gesundheitszustand ist dagegen unzulässig.

2.3.4 Krankheitszeiten- und Fehlzeitendaten im laufenden Arbeitsverhältnis

Das Verarbeiten von Krankheitszeiten- und Fehlzeitendaten im laufenden Arbeitsverhältnis ist zulässig. Dies folgt zum einen aus dem Gesichtspunkt der Verpflichtung des Arbeitgebers zur Lohn- und Gehaltsabrechnung. Außerdem hat der Arbeitgeber auch ein berechtigtes Interesse daran festzustellen, inwiefern das arbeitsvertragliche Austauschverhältnis durch Krankheits- und Fehlzeiten gestört ist, also im Hinblick auf eine etwaige personenbedingte Kündigung des Arbeitsverhältnisses.

Keine Angaben muss der Arbeitnehmer hingegen zum Krankheitsgrund machen. Der Krankheitsgrund kann ausnahmsweise von Bedeutung für das Arbeitsverhältnis sein, wenn es sich um eine arbeitsplatzbezogene Krankheit handelt, z. B. um ein Rückenleiden durch die Produktionsstätte oder einen ungeeigneten Stuhl.

Auch in diesen Fällen ist die Angabe des Krankheitsgrundes durch den Arbeitnehmer freiwillig. Über diese Freiwilligkeit muss der Arbeitnehmer ausdrücklich belehrt werden. Die Einwilligung des Arbeitnehmers muss sich sowohl auf die Erhebung des Krankheitsgrundes als auch auf dessen Speicherung und weitere Verwendung der Information erstrecken.

2.3.5 Alkohol- und Drogentests

Bei der Frage der Zulässigkeit von Alkohol- und Drogentests ist hinsichtlich des Bewerbungsverfahrens und dem nachfolgenden Arbeitnehmerverhältnis zu unterscheiden.

Ohne entsprechende gesetzliche oder tarifvertragliche Verpflichtung ist ein Arbeitnehmer ohne konkrete Verdachtsmomente nicht verpflichtet, sich im laufenden Arbeitsverhältnis routinemäßig auf eine eventuelle Alkohol- oder Drogenabhängigkeit untersuchen zu lassen. Will sich ein Arbeitnehmer freiwillig einem Test unterziehen, z. B. um einen bestehenden Verdacht zu widerlegen und um sich so zu entlasten, muss er diesen Wunsch äußern. Von sich aus braucht der Arbeitgeber den Test nicht anzubieten.

Anders ist dies jedoch im Bewerbungsverfahren. Dort gilt eine Drogen- oder Alkoholabhängigkeit als eine Krankheit, welche die Erfüllung der Arbeitspflicht generell erheblich beeinträchtigen wird und nach der demzufolge auch gefragt werden darf.

2.3.6 AIDS-Erkrankung / HIV-Infizierung

Die Frage nach einer AIDS-Erkrankung ist zulässig, da mit einer Heilung nicht gerechnet werden kann und der Bewerber deshalb zumindest in absehbarer Zeit nicht mehr in der Lage sein wird, seiner Arbeitspflicht weiter nachzukommen.

Anders ist es allerdings bei einer HIV-Infizierung. In diesem Falle ist die Frage nur dann zulässig, wenn aufgrund der Tätigkeit ein erhöhtes Risiko der Ansteckung von Kollegen oder Kunden besteht, also zum Beispiel bei

– Tätigkeiten im Gesundheitsdienst,
– Küchenpersonal,
– Tätigkeiten, die mit der Herstellung von Lebensmitteln beschäftigt sind.

2.3.7 Genom- / DNA-Analysen

Die Frage nach der genetischen Veranlagung ist grundsätzlich unzulässig – ebenso Genom- / DNA-Analysen. Hier gilt das Gendiagnostikgesetz.

2.3.8 Schwerbehinderteneigenschaft

Die pauschale Frage nach einer bestehenden Schwerbehinderung oder Gleichstellung im Bewerbungsverfahren ist unzulässig.

Etwas anderes gilt aber nach getroffener Auswahlentscheidung. Sobald sich der Arbeitgeber endgültig für einen Bewerber entschieden hat und das Bewerbungsverfahren abgeschlossen ist, kann der letztendlich eingestellte Bewerber nach einer bestehenden Schwerbehinderung oder Gleichstellung gefragt werden. Eine Benachteiligung wegen einer Behinderung ist dann – zumindest hinsichtlich der Einstellungsentscheidung – nicht mehr möglich, da die Auswahlentscheidung bereits getroffen wurde.

Der Arbeitgeber darf aber in Erfahrung bringen, ob ein Bewerber gesundheitlich für den konkreten Arbeitsplatz geeignet ist. Deshalb darf der Arbeitgeber nach Krankheiten bzw. (körperlichen) Beeinträchtigungen des Gesundheitszustandes fragen, durch die die Eignung für die vorgesehene Tätigkeit auf Dauer oder wiederkehrend eingeschränkt wird.

2.3.9 Schwangerschaft

Die Frage nach einer bestehenden Schwangerschaft ist unzulässig. Dies gilt auch, wenn die Bewerberin befristet eingestellt werden soll und für die vorgesehene Vertragsdauer oder wesentliche Teile davon eine Beschäftigung aus Gründen des Mutterschutzes ausscheidet. Gleiches gilt bei Rückkehr aus der Elternzeit bei erneuter Schwangerschaft.

2.3.10 Bisheriges Entgelt

Die Frage nach dem bisherigen Entgelt betrifft die Einkommensverhältnisse des Bewerbers und greift daher in dessen geschützte Individualsphäre ein. Die Frage ist deshalb nur insoweit zulässig, als das bisherige Entgelt

– Aussagen über die Qualifikation des Bewerbers für den zu besetzenden Arbeitsplatz trifft oder Rückschlüsse auf dessen Eignung zulässt (z. B. bisherige und angestrebte Position erfordern vergleichbare Kenntnisse und Fähigkeiten oder der Bewerber hat zuvor eine leistungsabhängige Vergütung erhalten, deren Höhe für seine Einsatzbereitschaft kennzeichnend ist) oder
– vom Bewerber selbst zur Mindestbedingung für sein zukünftiges Einkommen erhoben wird.

Ansonsten ist die Frage nach dem bisherigen Entgelt unzulässig, weil sie den Bewerber bei den Gehaltsverhandlungen in eine schlechtere Position drängt.

2.3.11 Vorstrafen und Ermittlungsverfahren

Nach Vorstrafen darf nur gefragt werden, wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert – und dann darf der Arbeitgeber auch nur nach einschlägigen Vorstrafen fragen, d. h. nach solchen Vorstrafen, die für den zu besetzenden Arbeitsplatz relevant sind. Unter diesen Voraussetzungen darf auch nach laufenden Ermittlungsverfahren gefragt werden.

Einschlägigkeit ist beispielsweise zu bejahen bei der Frage nach

– vermögensrechtlichen Vorstrafen eines Bankkassiers,
– verkehrsrechtlichen Vorstrafen eines Kraftfahrers,
– Sittlichkeitsdelikten eines Erziehers.

Es gelten die Löschungsfristen des Bundeszentralregistergesetzes (BZRG). Vorstrafen, die nicht mehr in dem polizeilichen Führungszeugnis genannt werden (§ 51 BZRG), braucht der Bewerber auch auf Befragen nicht zu offenbaren.

2.3.12 Lohnpfändungen / -abtretungen, Vermögensverhältnisse

Die Frage nach den Vermögensverhältnissen (Überschuldung, Pfändungen, Leistung des „Offenbarungseids“) und Lohnpfändungen / -abtretungen ist nur zulässig, wenn der Bewerber / Arbeitnehmer eine Position ausfüllen soll, in der Seriosität, eine besondere Vertrauenswürdigkeit und finanzielle Zuverlässigkeit relevant sind, z. B. Finanzberater oder Buchhalter.

2.3.13 Wettbewerbsverbote

Die Frage nach Wettbewerbsverboten, die sich auf das einzugehende Arbeitsverhältnis beziehen, ist zulässig.

2.3.14 Gewerkschaftszugehörigkeit, politische und religiöse Überzeugungen

Die Frage nach der Gewerkschaftszugehörigkeit ist wegen der in Art. 9 Abs. 3 GG verfassungsrechtlich garantierten Koalitionsfreiheit unzulässig. Gleichfalls unzulässig vor Abschluss eines Arbeitsvertrages sind Fragen nach der Konfession oder sonstigen religiösen Überzeugungen, Fragen nach der Mitgliedschaft in Parteien oder politischen und philosophischen Überzeugungen. Ausnahmen bestehen aber unter bestimmten Voraussetzungen für sogenannte Tendenzbetriebe (z. B. Presseunternehmen, Verlage, Parteien).

2.3.15 Gesetzliche Aufzeichnungs- und Aufbewahrungspflichten

Der Arbeitgeber hat sowohl im laufenden Arbeitsverhältnis als auch nach dessen Beendigung verschiedene Aufbewahrungs- und Aufzeichnungspflichten, die steuerrechtlicher, sozialversicherungsrechtlicher und arbeitsrechtlicher Natur sind. Das Erheben und Speichern dieser personenbezogenen Arbeitnehmerdaten ist selbstverständlich nicht nur zulässig, sondern sogar verpflichtend. Solche Aufbewahrungs- und Aufzeichnungspflichten beziehen sich beispielsweise auf

- die Überschreitung der werktäglichen Arbeitszeit von acht Stunden,
- das Verzeichnis der Arbeitnehmer, die in eine Verlängerung der Arbeitszeit eingewilligt haben,
- das Verzeichnis der beschäftigten Jugendlichen,
- den Nachweis der Beschäftigungszeiten werdender und stillender Mütter.

2.4 Nutzen von Personaldaten

Ein Nutzen von gespeicherten Arbeitnehmerdaten liegt dann vor, wenn die Daten mit einer bestimmten Zweckbestimmung ausgewertet, zusammengestellt, abgerufen oder ansonsten betriebsintern zielgerichtet zur Kenntnis genommen werden (z. B. betriebsinterne Veröffentlichung von Personaldaten, Datenfluss zwischen Personalabteilung und Betriebsrat).

Rechtmäßig gespeicherte Daten dürfen zu dem Zweck genutzt werden, für den sie ursprünglich erhoben wurden (z. B. Stammdaten für eine Sozialauswahl, Bankverbindung für die Überweisung des Gehalts).

Sollen legitim gespeicherte Daten nachträglich für weitere – andere als die ursprünglich festgelegten – Zwecke genutzt werden, muss gem. Art. 6 Abs. 4 DS-GVO eine Vereinbarkeitsprüfung mit dem ursprünglichen Zweck stattfinden.

2.4.1 Daten für die Einbehaltung der Lohnsteuer

Gemäß § 39 Abs. 8 und 9 EStG darf der Arbeitgeber die früher auf der Lohnsteuerkarte enthaltenen Merkmale nur für die Einbehaltung der Lohnsteuer verwenden. Eine Weitergabe nach innen oder eine Übermittlung nach außen ist nur mit Einwilligung des Betroffenen zulässig oder wenn eine spezielle gesetzliche Regelung dies gestattet.

2.4.2 Sozialversicherungsnummer und Sozialversicherungsausweis

Die Sozialversicherungsnummer und der Sozialversicherungsausweis dürfen vom Arbeitgeber nur entsprechend der Vorgaben der §§ 18 f, h verwendet werden. Jede anderweitige Nutzung ist unzulässig.

Der Sozialversicherungsausweis darf nur zum Zwecke der Aufdeckung bzw. Vermeidung illegaler Beschäftigung und zur Erhebung der Versicherungsnummer genutzt werden.

Gemäß § 18f Abs. 3 SGB IV darf der Arbeitgeber die Sozialversicherungsnummer nur verarbeiten, soweit dies zur Erfüllung einer gesetzlichen Aufgabe der Sozialversicherungsträger, ihrer Verbände, ihrer Arbeitsgemeinschaften, der Bundesagentur für Arbeit, etc. erforderlich ist. Der Beschäftigte ist nach § 18 h Abs. 2 S. 1 SGB IV zur Vorlage des Sozialversicherungsausweises zu Beginn der Beschäftigung beim Arbeitgeber verpflichtet.

2.4.3 Telefonverzeichnisse, Organisationspläne, etc.

Die Bekanntgabe von dienstlichen Arbeitnehmerdaten im Rahmen des betrieblichen Arbeitsablaufs ist häufig unumgänglich und datenschutzrechtlich zulässig. Beispielsweise dürfen die dienstlichen Telefonnummern in einem betrieblichen Telefonverzeichnis geführt oder betriebliche Funktionen bzw. Positionen in Organisationsplänen genannt werden.

Privatnummern der Arbeitnehmer dürfen regelmäßig nur mit deren Zustimmung veröffentlicht werden.

2.4.4 Geburtstagslisten

Geburtstagslisten dürfen nicht ohne Zustimmung der betroffenen Arbeitnehmer bekanntgegeben werden, weil ein gewichtiges Interesse des Arbeitgebers an der Veröffentlichung der Geburtsdaten kaum angenommen werden kann.

Im Regelfall werden die Beschäftigten nichts dagegen haben, dass sie in einer Geburtstagsliste geführt werden. Eine praxisgerechte Vorgehensweise des Arbeitgebers könnte folgendermaßen aussehen: der Arbeitgeber informiert die einzelnen Beschäftigten im Vorfeld über sein Vorhaben, eine Geburtstagsliste zu veröffentlichen, räumt ihnen die Möglichkeit

ein, ihr Geburtsdatum hierfür zu melden und holt eine informierte Einwilligung nach Art. 6 Abs. 1 lit. a) DS-GVO ein.

2.4.5 Rang- und Bestenlisten

In betriebsinternen sogenannten „Rang-“ oder „Rennlisten“ werden die Leistungen, z. B. Verkaufs- und Werbeaktivitäten aller Arbeitnehmer, vergleichend gegenübergestellt und bekannt gemacht. Diese Rennlisten sollen den einzelnen Arbeitnehmern Leistungsvergleiche ermöglichen und ihnen Leistungsanreize und -ziele geben. Datenschutzrechtlich sind solche Rennlisten allerdings problematisch. Zumindest bei den leistungsschwächeren Arbeitnehmern wird der Veröffentlichung regelmäßig ein schutzwürdiges Interesse entgegenstehen, weil die Veröffentlichung schlechter Arbeitsergebnisse erhebliche Auswirkungen auf das Ansehen des Betroffenen innerhalb und außerhalb des Betriebs haben kann. Eine Veröffentlichung ist daher grundsätzlich nur zulässig, wenn sie im Arbeitsvertrag vorgesehen ist oder soweit der Arbeitnehmer wirksam eingewilligt hat.

Leistungsanreize können auch durch bloße „Bestenlisten“ (z. B. „Mitarbeiter des Monats“) erreicht werden. Deren interne Veröffentlichung begegnet datenschutzrechtlich erheblich weniger Bedenken, weil hier nicht alle Arbeitnehmer veröffentlicht werden, sondern nur der Leistungsstärkste – die Leistungsschwachen werden nicht aufgeführt.

Die veröffentlichten leistungsstarken Arbeitnehmer werden in der Regel kein schutzwürdiges Interesse haben, das einer solchen „Auszeichnung“ entgegensteht. Um jedoch eine Verletzung von Arbeitnehmerbelangen auch in diesem Fall auszuschließen, empfiehlt es sich, die Arbeitnehmer über die beabsichtigte Veröffentlichung zu unterrichten und ihnen Gelegenheit zu geben, der Veröffentlichung zu widersprechen.

2.4.6 Bewerberdaten

Bewerberdaten dürfen nur im Rahmen der Auswahlentscheidung für die Besetzung der Stelle verwendet werden, auf die sich der Bewerber beworben hat. Daher ist es grundsätzlich unzulässig, eine auf eine bestimmte Stelle ausgerichtete Bewerbung innerhalb des Betriebs, Unternehmens oder Konzerns anderen möglicherweise interessierten Organisationseinheiten zugänglich zu machen. Hierfür muss entweder die Einwilligung des Bewerbers eingeholt werden oder es wird bereits im Rahmen der Ausschreibung auf dieses Vorgehen hingewiesen.

Bei Initiativbewerbungen allerdings bewirbt sich der Kandidat in der Regel bereits von sich aus nicht auf eine konkrete Stelle, sondern zeigt Interesse an jeglichen freien Arbeitsplätzen des Unternehmens oder Betriebs, die seiner Qualifikation entsprechen. Soweit keine entgegenstehenden Anhaltspunkte ersichtlich sind, dürfen seine Bewerbungsunterlagen daher auch an andere gegebenenfalls interessierte Organisationseinheiten weitergegeben werden.

Sobald der Arbeitgeber kein berechtigtes Interesse mehr an den Bewerberdaten hat, muss er diese Daten löschen. Seit Inkrafttreten des AGG darf der Arbeitgeber die Bewerberdaten auch nach Abschluss des Bewerbungsverfahrens speichern, solange er noch mit Schadensersatz- und Entschädigungsansprüchen von Bewerbern rechnen muss. Erst danach muss der Arbeitgeber die Bewerberdaten vernichten. Wie lange der Arbeitgeber die Daten behalten darf ist derzeit unklar – Rechtsprechung gibt es hierzu nicht. Zulässig ist jedenfalls, die Daten bis Ablauf der Zwei-Monats-Frist des § 15 Abs. 4 AGG zu behalten, aber auch danach muss dem Arbeitgeber noch ein angemessener „Sicherheitszuschlag“ gewährt werden.

Die bayerische Aufsichtsbehörde sieht eine Speicherung von maximal sechs Monaten als angemessen an. Dies ist aber keine allgemein gültige, starre Frist, sondern nur eine Richtgröße für den „Normalfall“. Es bleibt dabei, dass sich die Frage der Löschungspflicht von Bewerberdaten nur für jeden Einzelfall gesondert und unter Berücksichtigung der konkreten Interessenlage beantworten lässt.

Fall

Das Unternehmen möchte einen „Bewerberpool“ anlegen und auch die Daten abgelehnter, aber für künftige Stellen interessanten Bewerber über die möglichen sechs Monate hinaus speichern.

Hierfür benötigt das Unternehmen die Einwilligung der Bewerber. Die Daten sollten maximal für einen Zeitraum von ein bis zwei Jahren vorgehalten werden.

2.4.7 Weitergabe von Daten an den Betriebsrat

Der Arbeitgeber darf dem Betriebsrat nur Informationen über die Beschäftigten zugänglich machen, soweit

– dies für die Entscheidung über die Begründung, die Durchführung oder die Beendigung des Beschäftigungsverhältnisses erforderlich ist (Art. 6 Abs. 1 lit. b) DS-GVO),

Tipp für die Praxis

Der Arbeitgeber wird dem Betriebsrat die Stammdaten der Beschäftigten (Name, Geburtsdatum, Berufsbezeichnung, Arbeitsplatz, Vergütungsgruppe, Beginn des Beschäftigungsverhältnisses, Voll- / Teilzeitbeschäftigung etc. – nicht jedoch die Privatanschrift) mitteilen müssen, weil der Betriebsrat wissen muss, wen er vertritt. Der Arbeitgeber kann dem Betriebsrat hierzu eine eigene „Grunddatei“ zur Verfügung stellen oder ihm entsprechend beschränkte Zugriffsrechte auf das Personalverwaltungssystem einräumen.

- der Arbeitgeber durch spezielle Vorschriften des BetrVG dazu verpflichtet ist,
- Unterrichtungsanspruch im Rahmen der allgemeinen Überwachungs- und Kontrollaufgaben des Betriebsrats nach § 80 Abs. 2 BetrVG (z. B. Informationen über Beginn und Ende der täglichen Arbeitszeit der Beschäftigten zur Überprüfung der Einhaltung des Arbeitszeitgesetzes),
- Unterrichtungsanspruch bei Betriebsänderungen nach § 111 BetrVG,
- Mitbestimmung bei personellen Angelegenheiten nach § 99 BetrVG: Unterrichtung des Betriebsrats vor jeder Einstellung, Eingruppierung, Umgruppierung und Versetzung unter Vorlage der erforderlichen (Bewerbungs-)Unterlagen,
- Informations- und Unterrichtungsanspruch über die Personalplanung, insbesondere den gegenwärtigen und künftigen Personalbedarf sowie über die sich daraus ergebenden personellen Maßnahmen (§ 92 BetrVG),
- Unterrichtungsanspruch über vorläufige personelle Maßnahmen nach
- § 100 Abs. 2 BetrVG,
- Anhörung des Betriebsrats vor jeder Kündigung (§ 102 BetrVG),
- Einsicht in die Personalakten nur mit Einwilligung des jeweiligen Beschäftigten
- (§ 83 BetrVG),
- Einsichtsrecht in die Bruttolohn- und -gehaltslisten gemäß § 80 Abs. 2 S. 2 BetrVG.

Hinweis

Soweit dem Betriebsrat nur ein Einsichtsrecht zusteht, darf er die entsprechenden Daten darüber hinaus weder kopieren, noch speichern oder auswerten. Eine eigene, vom Betriebsrat geführte, Lohn- und Gehaltsdatei der Beschäftigten ist unzulässig.

Die Beschränkung der personenbezogenen Informationsansprüche des Betriebsrats soll dem Datenschutz der Beschäftigten Rechnung tragen. Der Arbeitgeber ist daher nicht befugt, freiwillig Informationen zu liefern oder Unterlagen zur Verfügung zu stellen, die das BetrVG nicht vorsieht.

Tipp für die Praxis

Verantwortlich für den rechtmäßigen Umgang mit personenbezogenen Daten nach dem BDSG ist grundsätzlich der Arbeitgeber. Ist der Arbeitgeber verpflichtet, Daten z. B. nach den Art. 16 ff DS-GVO zu berichtigen, zu löschen oder einzuschränken, dann muss er auch dafür sorgen, dass die Löschung, Berichtigung, Einschränkung unternehmensweit erfolgt – also auch bei dem Betriebsrat.

Mit der Einführung des neuen § 79a BetrVG wurde eine klarstellende gesetzliche Regelung geschaffen. Soweit der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, ist der Arbeitgeber der für die Verarbeitung

Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften. Bei der Einhaltung der datenschutzrechtlichen Vorschriften sollen sich Arbeitgeber und Betriebsrat jedoch gegenseitig unterstützen. Zudem ist der oder die Datenschutzbeauftrage gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet, sofern es um Informationen geht, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen.

2.5 Übermitteln von Personaldaten

Der Begriff der Verarbeitung wird in Art. 4 Nr. 2 DS-GVO definiert. Umfasst vom Begriff der Verarbeitung von Daten wird auch die Weitergabe durch eine Übermittlung. Ein Übermitteln von Personaldaten liegt z. B. dann vor, wenn gespeicherte oder durch Datenverarbeitung gewonnene personenbezogene Daten an einen Betriebsfremden (nicht betriebsintern) bekannt gegeben werden. Auf welche Art und Weise die Weitergabe erfolgt, ist unerheblich.

2.5.1 Gesetzliche Melde-, Berichts- und Auskunftspflichten

Datenübermittlungen, die aufgrund von speziellen gesetzlichen Regelungen erfolgen, sind selbstverständlich nicht nur zulässig, sondern gegebenenfalls sogar zwingend gesetzlich geboten. Das gilt insbesondere für den Arbeitgeber gegenüber staatlichen Instanzen, wie Finanzämter oder Bundesagentur für Arbeit, Sozialversicherungsträgern, Industrie- und Handels- oder Handwerkskammer auferlegte Melde-, Berichts- und Auskunftspflichten, also beispielsweise

- die Meldepflicht nach § 28a SGB IV,
- Meldung des Arbeitgebers an die Einzugsstelle für jeden in der Kranken-, Pflege-, Rentenversicherung oder nach dem Recht der Arbeitsförderung kraft Gesetzes versicherten Beschäftigten, z. B. bei Beginn und Ende der Beschäftigung, bei Änderung des Familiennamens, Änderung der Staatsangehörigkeit, Beginn und Ende der Altersteilzeitarbeit,
- die Meldepflichten an das Finanzamt im Rahmen der Durchführung des Lohnsteuerabzugs.

2.5.2 Geheimhaltungsgebote

Verboten ist die Datenübermittlung, wenn besondere Schweige- und Geheimhaltungsgebote bestehen, beispielsweise

- das Gebot zur vertraulichen Behandlung der Personalakte,
- das Geheimhaltungsgebot des Arbeitgebers bezüglich der Angaben für die Lohnsteuer, vgl. hierzu § 39 Abs. 8 und 9 EstG,
- die Geheimhaltungspflichten des Betriebsrats, vgl. § 79 BetrVG,
- die Schweigepflicht der Betriebsärzte, vgl. § 8 Abs. 1 ASiG und § 203 StGB,

– das Gebot zur Wahrung der Geschäftsgeheimnisse seitens des einzelnen Arbeitnehmers, vgl. § 4 GeschGehG.

2.5.3 Gläubigeranfragen

Durch „Arbeitgeberanfragen“ soll häufig aufgeklärt werden, inwieweit Forderungen gegebenenfalls durch Lohn- oder Gehaltspfändungen oder andere Zwangsvollstreckungsmaßnahmen beizutreiben sind. Hintergrund sind meist offene Forderungen gegen den Arbeitnehmer.

Wenn ein Gläubiger oder eine von diesem beauftragte Inkassofirma bei dem Arbeitgeber in Erfahrung zu bringen versucht, ob ein Schuldner bei dem Arbeitgeber beschäftigt ist und wenn ja, wie viel er verdient, besteht für den Arbeitgeber keine Auskunftspflicht und ohne die Einwilligung des betroffenen Arbeitnehmers darf der Arbeitgeber in diesen Fällen auch keine Auskunft erteilen. Anders wäre es nur bei der sogenannten Drittschuldnererklärung nach § 840 ZPO.

2.5.4 Anfragen von Sicherheitsbehörden, Polizei

Datenübermittlungen zur Verfolgung von Straftaten sind zulässig nach Art. 6 Abs. 1 lit. f) DS-GVO, ggf. aber auch Art. 6 Abs. 1 lit. c) oder e) DS-GVO, soweit nicht bereits eine speziell geregelte Mitteilungspflicht besteht (z. B. Auskunft über Telekommunikationsverbindungsdaten nach § 100g StPO, Auskünfte an Finanzbehörden nach § 93 Abgabenordnung).

2.5.5 Arbeitgeberauskünfte

Häufig genügen dem Arbeitgeber im Einstellungsverfahren die vom Bewerber erhaltenen Informationen und Zeugnisse für eine fundierte Einstellungsentscheidung nicht. Das gilt insbesondere bei der Besetzung leitender Positionen oder besonderer Vertrauensstellungen. Der Arbeitgeber ist daher oftmals daran interessiert ist, zusätzliche Informationen über in die engere Wahl gezogene Bewerber bei bisherigen oder früheren Arbeitgebern einzuholen.

Dieses Vorgehen ist datenschutzrechtlich problematisch, denn der angefragte Arbeitgeber verarbeitet – sofern er sich nicht darauf beschränkt, die vom Bewerber gemachten Angaben zu bestätigen – gegebenenfalls Daten, die er jedenfalls nach dem Zeugnisrecht nicht mitteilen dürfte.

Auf der sicheren Seite befindet sich der angefragte Arbeitgeber jedenfalls, wenn er Auskünfte über (ehemalige) Arbeitnehmer nur mit deren Einwilligung erteilt – eine Auskunftspflicht besteht in jedem Fall nicht. Auskunft darf nicht erteilt werden, wenn sich der Arbeitgeber dem Arbeitnehmer gegenüber zur Vertraulichkeit verpflichtet hat. Inhaltlich darf die Auskunft nur auf solche Informationen gerichtet sein, die auch vom Fragerecht des

Arbeitgebers abgedeckt sind. Wenn sich also der Personalleiter des potenziellen neuen Arbeitgebers beim Personalleiter des ehemaligen Arbeitgebers danach erkundigt, ob der Bewerber während seines Arbeitsverhältnisses bei diesem häufig krankheitsbedingt gefehlt habe, dann darf der Personalleiter des ehemaligen Arbeitgebers keine Auskunft erteilen. Diese Frage ist nicht vom Fragerecht im Bewerbungsverfahren gedeckt.

Ein Auskunftsersuchen muss aber in jedem Fall unterbleiben, wenn der Bewerber sich Nachfragen bei seinem (bisherigen) Arbeitgeber verbeten hat, z. B. weil sich der Arbeitnehmer in ungekündigter Stellung befindet.

2.5.6 Weitergabe von Arbeitnehmerdaten an Versicherungsunternehmen

Von der Zweckbestimmung des Arbeitsverhältnisses nicht gedeckt ist die Weitergabe von Arbeitnehmerdaten an Versicherungsunternehmen zur Bewerbung mit Versicherungsleistungen. Die Erlaubnis zur Weitergabe der Daten kann sich hier nur aufgrund einer Einwilligung des betroffenen Arbeitnehmers ergeben, deren Freiwilligkeit hier regelmäßig vorliegen wird, wenn der Arbeitgeber seinen Beschäftigten mit der Weitergabe der Adressen nur einen Vorteil verschaffen möchte, weil das Versicherungsunternehmen den Beschäftigteneinen besonderen Firmenrabatt gewährt.

2.5.7 Arbeitnehmerdaten und Fotos im Internet

Die externe Veröffentlichung von Arbeitnehmerdaten ist bei herkömmlichen Publikationsformen (z. B. auf Briefbögen, Prospekten, Verzeichnissen, Werkszeitungen) ohne Einwilligungserklärung des Arbeitnehmers nur dann zulässig, wenn dies in der Zweckbestimmung des Arbeitsverhältnisses liegt. Zulässig ist demnach die Veröffentlichung erforderlicher Daten

– zur Erfüllung arbeitsvertraglicher Pflichten, z. B. bei Kundenberatern oder Außenmitarbeitern oder
– zur Erfüllung gesetzlicher Publikationspflichten, z. B. Veröffentlichung der Geschäftsführer einer GmbH im Handelsregister.

Die Besonderheit bei der Einstellung von Beschäftigtendaten in das Internet besteht darin, dass die Daten – im Gegensatz zu herkömmlichen Medien – nicht nur einem abgrenzbaren, interessierten Personenkreis zur Verfügung stehen, sondern sofort weltweit und grenzüberschreitend abrufbar sind. Die Daten sind damit auch in Ländern zugänglich, in denen kein oder kein hinreichender Datenschutz besteht. Daher kann nicht automatisch der Rückschluss gezogen werden, dass die Berechtigung zur Publikation in herkömmlicher Form auch die Befugnis zur Einstellung der Daten in das Internet einschließt. Vielmehr ist davon auszugehen, dass eine Veröffentlichung von Arbeitnehmerdaten ohne deren Einwilligung nur in Ausnahmefällen zulässig ist. Gegebenenfalls sollte den betroffenen Arbeitnehmern zur Wahrung der informationellen Selbstbestimmung ein Widerspruchsrecht gegen die Veröffentlichung im Internet eingeräumt werden.

Denkbar wäre beispielsweise die Bekanntgabe des Namens, der Funktion, der Spezialkenntnisse und der dienstlichen Telefonnummer und E-Mail-Adresse von Arbeitnehmern in Funktionen mit Außenwirkung und unmittelbarem Kundenkontakt. Zur Vermeidung datenschutzrechtlicher Probleme können Kontaktmöglichkeiten per Internet auch nur mit bloßer Funktionsbezeichnung angeboten werden, z. B. Bearbeitung von Bestellungen: Telefonnummer: 1234; E-Mail: bestellung@xyz.de.

Die Veröffentlichung von Bildern und Fotos eines Arbeitnehmers bedarf immer der Einwilligung des Arbeitnehmers. Eine ohne Einschränkung erteilte Einwilligung des Arbeitnehmers erlischt nicht automatisch mit dem Ende des Arbeitsverhältnisses. Sie kann aber widerrufen werden.

3 Die Rechte der Beschäftigten

Information, Auskunft, Löschen

3.1 Transparenz- und Informationspflichten des Arbeitgebers

Der Grundsatz der Transparenz bedeutet, dass eine für den betroffenen Beschäftigten bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente enthält (vergleiche Erwägungsgrund 58 der DS-GVO). Zur Erfüllung dieser Anforderung hat der Arbeitgeber als Verantwortlicher geeignete Maßnahmen zu treffen.

Die Informationspflichten dienen dem Schutz des betroffenen Beschäftigten. Ausreichende Informationen über die Verarbeitung seiner personenbezogenen Daten sollen dem Beschäftigten zum einen die Verarbeitungsvorgänge transparent machen und zum anderen eine wirksame Wahrnehmung seiner Rechte ermöglichen.

Die Informationspflichten des Arbeitgebers sind in Art. 13 und Art. 14 DS-GVO geregelt. Die DS-GVO differenziert hinsichtlich der Informationspflichten danach, ob der Verantwortliche die personenbezogenen Daten direkt bei den betroffenen Beschäftigten erhoben hat (Art. 13 DS-GVO) oder nicht (Art.14 DS-GVO). Inhaltlich sind die Informationspflichten dabei in weiten Teilen identisch, allerdings sieht Art. 14 DS-GVO einige Erleichterungen für den Verantwortlichen vor, z. B. bezüglich des Zeitpunkts der Zurverfügungstellung der Information. Zu den zahlreichen Informationspflichten der Art. 13 und 14 DS-GVO gehören unter anderem:

- Kontaktdaten des Verantwortlichen und seines Datenschutzbeauftragten,
- Zwecke der Datenverarbeitung,
- Berechtigte Interessen des Verantwortlichen oder eines Dritten an der Datenverarbeitung,
- Empfänger oder Kategorie von Empfängern personenbezogener Daten,
- Übermittlung von Daten in ein Drittland,
- Dauer der Speicherung,
- Bestehen von Auskunftsrechten,
- Bestehen von Rechten auf Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragbarkeit,
- Recht auf Beschwerde bei Aufsichtsbehörden,
- Automatisierte Entscheidungsfindung einschließlich Profiling (zumindest in diesen Fällen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite der Verarbeitung),
- Zweckänderung.

Anders als bei der Informationspflicht in Art. 13 DS-GVO sind bei den Informationspflichten nach Art. 14 DS-GVO weitergehende Ausnahmeregelungen von den Informationspflichten

geregelt (vgl. Art. 14 Abs. 5 DS-GVO). Ist eine dieser Ausnahmereglungen einschlägig, entfallen Informationspflichten für Arbeitgeber.

Tipp für die Praxis

Unternehmen sollten die verpflichtenden Informationen im Internet oder auf Formularen bereitstellen. In der Praxis hat sich auch das Einfügen eines entsprechenden Links in die E-Mail-Signatur bewährt.

Es ist schon bei der Dokumentation der betroffenen IT-Systeme und Prozesse darauf zu achten, dass diese die Informationen bereitstellen können.

3.2 Betroffenenrechte

Die betroffenen Beschäftigten haben ein Recht auf Auskunft, Berichtigung, Sperrung und Löschung ihrer Daten. Die Rechte der betroffenen Beschäftigten sind in Kapitel III. der DS-GVO geregelt. Dabei stehen dem betroffenen Beschäftigten alle Rechte ausschließlich gegenüber dem Arbeitgeber als für den Datenschutz Verantwortlichen zu. Der Arbeitgeber ist über Art. 13 Abs. 2 lit. b), Art. 14 Abs. 2 lit. b) DS-GVO verpflichtet, die betroffenen Beschäftigten über die ihnen zustehenden Rechte zu informieren.

Die Rechte der betroffenen Beschäftigten dienen als sichere Grundsätze der Verarbeitung personenbezogener Daten aus Art. 5 DS-GVO aus Sicht des betroffenen Beschäftigten.

3.2.1 Auskunfts- und Einsichtsrecht der Beschäftigten

Der Beschäftigte hat das Auskunftsrecht gemäß Art. 15 DS-GVO gegenüber seinem Arbeitgeber bezüglich der über ihn gespeicherten Daten. Er kann eine Bestätigung darüber verlangen, ob ihn betreffende personenbezogene Daten verarbeitet werden, und wenn dies der Fall ist, welche Daten dies sind. Darüber hinaus sind vom Arbeitgeber nach Art. 15 Abs. 1 DS-GVO vor allem noch folgende Informationen mitzuteilen:

- über die Verarbeitungszwecke,
- über die Kategorien personenbezogener Daten, die verarbeitet werden,
- über die gegebenen und möglichen Datenempfänger bzw. Kategorien von Empfängern,
- soweit möglich über die geplante Speicherdauer,
- Informationen über die Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung sowie ein Widerspruchsrecht,
- über das Beschwerderecht bei der Aufsichtsbehörde,
- die Herkunft der Daten, soweit diese nicht von der betroffenen Person selbst erhoben wurden,

– soweit zutreffend über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling,
– Datenübermittlungen in EU-Drittländer und die insoweit gegebenen Garantien nach Art. 46 DS-GVO.

Im Zusammenhang mit der Angabe von Datenempfängern bzw. Kategorien von Datenempfängern ist auf eine aktuelle Entscheidung des EuGH vom 12. Januar 2023 (Az. C-154/21) hinzuweisen. Vor der nunmehr klarstellenden Entscheidung des EuGH war es umstritten, ob der Verantwortliche stets konkrete Datenempfänger (namhaft) benennen muss, oder ob die Nennung von Kategorien von Datenempfängern ausreicht. Insoweit war insbesondere unklar, wem das in Art. 15 Abs. 1 lit. c) DS-GVO angelegte Wahlrecht zusteht. Der EuGH hat in der angeführten Entscheidung nunmehr klargestellt, dass betroffenen Personen – auf deren Wunsch – konkrete Datenempfänger namhaft zu benennen sind. Wo bislang also die bloß generische Angabe von Kategorien von Datenempfängern ausreichend war, müssen künftig präzise Angaben getroffen werden. Für Unternehmen bedeutet dies konkret, dass insbesondere eine lückenlose Kenntnis über sämtliche eingesetzten Dienstleister bestehen muss, an welche personenbezogene Daten übermittelt werden. Der effizienteste Weg um diese Anforderungen umzusetzen, kann in einem aktuellen und vollständigen Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DS-GVO gesehen werden.

Auskunftserteilungen müssen gemäß Art. 12 Abs. 3 DS-GVO unverzüglich erfolgen, spätestens aber innerhalb eines Monats. Nur in begründeten Ausnahmefällen kann die Monatsfrist überschritten werden.

Hinweis

§ 33 BDSG schränkt für nicht-öffentliche Stellen die Informations- und Auskunftspflichten ein, wenn die Information die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würden oder eine Gefährdung der öffentlichen Sicherheit und Ordnung droht. Sofern die Information unterbleibt, muss der verantwortliche Arbeitgeber geeignete Maßnahmen zum Schutz der berechtigten Interessen des betroffenen Beschäftigten ergreifen. In diesen Fällen ist nach § 34 BDSG auch das Auskunftsrecht des betroffenen Beschäftigten beschränkt. Allerdings müssen die Gründe für die Verweigerung der Auskunft durch den Arbeitgeber dokumentiert werden.

Tipp für die Praxis

Arbeitgeber müssen geeignete organisatorische Maßnahmen treffen, damit die Beschäftigten eine beantragte Auskunft zeitnah und in verständlicher Form erhalten können. IT-Systeme sind dahingehend zu prüfen, ob die Herausgabe einer Kopie der personenbezogenen Daten möglich ist, ohne die Rechte Anderer zu verletzen.

Über einen langen Zeitraum war zudem umstritten, wie genau der in Art. 15 Abs. 3 DS-GVO angelegte Anspruch auf Herausgabe einer Kopie zu verstehen ist. In Art. 15 Abs. 3 DS-GVO heißt es hierzu wörtlich: „Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung". Der EuGH hat nunmehr per Urteil vom 04. Mai 2023 (Az. C-478/21) zunächst klargestellt, dass es sich bei Art. 15 Abs. 1 und 3 DS-GVO um einen einheitlichen Anspruch auf Auskunftserteilung handelt. Der betroffenen Person ist daher – bei Auskunftserteilung – eine Kopie ihrer personenbezogenen Daten zu erteilen. Zum konkreten Inhalt einer solchen Kopie hat der EuGH zudem festgehalten, dass es sich hierbei um eine „originalgetreue und verständliche Reproduktion der personenbezogenen Daten" handelt. Art. 15 DS-GVO soll es der betroffenen Person insbesondere ermöglichen, zu prüfen, ob die verarbeiteten personenbezogene Daten korrekt sind und rechtmäßig verarbeitet werden. Diese Anforderung bestimmt zugleich den Umfang der erteilenden Kopie. Um eine Rechtmäßigkeitsprüfung durchzuführen, kann dies also dazu führen, dass die Reproduktion von Auszügen von Dokumenten oder von ganzen Dokumenten anzufertigen ist. Insbesondere, sofern die bereitgestellten Daten kontextabhängig erhoben wurden (beispielsweise in Dokumenten mit Freitextfeldern), kann es erforderlich sein, das zugrundeliegende Dokument in die Auskunft nach Art. 15 Abs. 1, 3 DS-GVO aufzunehmen. In jedem Fall sind jedoch die Rechte und Freiheiten anderer zu berücksichtigen, womit ggf. Schwärzungen in dem entsprechenden Dokument vorzunehmen sind. Um auch diese Anforderungen des EuGH umsetzen zu können, sollten Unternehmen zunächst einen erprobten Maßnahmenplan zur Prüfung und Erfüllung von Betroffenenrechten vorhalten. Daneben ist auch hier die lückenlose Kenntnis über die eingesetzten IT-Systeme und Verarbeitungsvorgänge erforderlich.

Zudem können Beschäftigte jederzeit Einsicht in ihre Personalakten nehmen (§ 83 Abs. 1 BetrVG, § 26 Abs. 2 Sprecherausschussgesetz). Sie sind berechtigt, bei der Einsichtnahme ein Mitglied des Betriebsrats bzw. Sprecherausschusses hinzuzuziehen. Schwerbehinderte Beschäftigte können zudem die Schwerbehindertenvertretung hinzuziehen (§ 95 Abs. 3 S. 1 SGB IX). Die hinzugezogenen Personen müssen über den Inhalt der Personalakte Stillschweigen bewahren, es sei denn sie wurden von dem Beschäftigten im Einzelfall von dieser Schweigepflicht entbunden.

3.2.2 Recht auf Berichtigung

Die Verarbeitung unrichtiger oder unvollständiger personenbezogener Daten kann für den betroffenen Beschäftigten zum Nachteil führen, wenn der Arbeitgeber hierdurch zu unrichtigen Ergebnissen gelangt. Art. 16 S. 1 DS-GVO entspricht dem früheren § 35 Abs. 1 S. 1 BDSG-alt. Jeder betroffene Beschäftigte hat danach das Recht, vom Arbeitgeber unverzüglich die Benachrichtigung ihn betreffender unrichtiger personenbezogener Daten zu verlangen. Ein Dritt-Berichtigungsrecht schließt Art. 16 S. 1 DS-GVO aus. Über die Berichtigung hat der verantwortliche Arbeitgeber nach Art. 19 S. 1 DS-GVO alle Empfänger der von der Berichtigung betroffenen personenbezogenen Daten zu unterrichten, soweit ihm dies nicht ausnahmsweise unmöglich oder nur mit unverhältnismäßigem Aufwand durchführbar ist.

3.2.3 Recht auf Löschung, einschließlich dem Recht auf Vergessenwerden

Das Recht des betroffenen Beschäftigten auf Löschung und eine Pflicht des Arbeitgebers personenbezogene Beschäftigtendaten zu löschen, besteht in den in Art. 17 Abs. 1 DS-GVO verzeichneten Fällen. Art. 17 Abs. 1 DS-GVO benennt folgende Gründe für eine Löschung personenbezogener Daten:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig (lit. a)),
- Der betroffene Beschäftigte widerruft seine Einwilligung, auf die sich die Verarbeitung gemäß Art. 6 Abs. 1 lit. a) und Art. 9 Abs. 2 lit. a) DS-GVO stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung (lit. b)),
- Der betroffene Beschäftigte legt gemäß Art. 21 Abs. 1 DS-GVO Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder der betroffene Beschäftigte legt gemäß Art. 21 Abs. 2 DS-GVO Widerspruch gegen die Verarbeitung ein (lit. c)),
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet (lit. d)),
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht und dem Recht der Mitgliedsstaaten erforderlich, denen der verantwortliche Arbeitgeber unterliegt (lit. e)),
- Personenbezogene Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DS-GVO von Kindern erhoben (lit. f)).

Nicht wirklich neu ist das so genannte Recht auf Vergessenwerden nach Art. 17 Abs. 2 DS-GVO. Bereits nach früher geltendem Recht war die Benachrichtigung der Empfänger bei Berichtigung, Sperrung oder Löschung erforderlich.

Der EuGH hat jedoch per Urteil vom 04. Mai 2023 (Az. C-60/22) eine erfreuliche Konkretisierung des Begriffs der unrechtmäßigen Datenverarbeitung vorgenommen: Eine Datenverarbeitung ist insbesondere dann nicht unrechtmäßig im Sinne des Art. 17 Abs. 1 lit. d) DS-GVO), sofern die verantwortliche Stelle lediglich ihren Dokumentations- und Nachweispflichten nicht nachkommt. Dies ist beispielsweise dann der Fall, sofern der Verantwortliche kein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DS-GVO führt oder keinen Vertrag zur gemeinsamen Verantwortlichkeit gemäß Art. 26 DS-GVO abgeschlossen hat. Da die Rechtmäßigkeit der Datenverarbeitung (im Sinne der Art. 5 ff. DS-GVO) von den weiteren formellen Verpflichtungen der DS-GVO zu trennen ist, hat die betroffene Person in einem solchen Fall insbesondere keinen Anspruch auf Löschung der Daten oder auf Einschränkung der Datenverarbeitung. Dies ist auch nachvollziehbar, da die Nichteinhaltung dieser Pflichten keine unmittelbaren Auswirkungen auf die betroffene Person entfaltet.

3.2.4 Recht auf Einschränkung der Verarbeitung

Neu ist der Begriff „Einschränkung der Verarbeitung“ in Art. 18 Abs. 1 DS-GVO. Liegt eine der Voraussetzungen für eine Einschränkung der Verarbeitung nach Art. 18 Abs. 1 DS-GVO

vor, hat dies nach Art. 18 Abs. 2 DS-GVO zur Folge, dass sich das Recht zur Verarbeitung des verantwortlichen Arbeitgebers auf die Speicherung der von der Einschränkung betroffenen personenbezogener Daten beschränkt. Die von der Einschränkung betroffenen personenbezogenen Daten dürfen dann über die reine Speicherung hinaus nur in folgenden Fällen verarbeitet werden:

- Einwilligung des betroffenen Beschäftigten,
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder
- zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedsstaates.

3.2.5 Recht auf Datenübertragbarkeit

Das in Art. 20 DS-GVO geregelte Recht auf Datenübertragbarkeit ist ein neues Recht, das es vor der DS-GVO weder im europäischen noch deutschen Datenschutzrecht gab. Danach kann der betroffene Beschäftigte verlangen, die von ihm auf Basis einer Einwilligung oder eines Vertrages zur Verfügung gestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Erfolgt die Verarbeitung auf einer anderen Rechtsgrundlage, gilt dieses Recht nicht. Der Beschäftigte kann weiter verlangen, dass die Daten direkt an einen anderen Arbeitgeber übermittelt werden, soweit dies technisch machbar ist.

Hinweis

Das Recht auf Datenübertragbarkeit darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Die Regelung richtet sich erkennbar an die Anbieter sozialer Netzwerke, dem Wortlaut nach gilt sie aber auch für Arbeitgeber.

Tipp für die Praxis

Die vorhandenen Systeme in der Personalabteilung sind daher darauf zu prüfen, ob sie die Datenübertragbarkeit unterstützen und ob eine Übertragung die Rechte und Freiheiten anderer Personen beeinträchtigt. Dies dürfte immer dann der Fall sein, wenn der relevante Datensatz andere als den betroffenen Beschäftigten tangiert.

3.2.6 Widerspruchsrecht

Das Widerspruchsrecht in Art. 21 Abs. 1 DS-GVO gibt dem betroffenen Beschäftigten das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, der weiteren Verarbeitung seiner Daten zu widersprechen, wenn die Verarbeitung

- für die Wahrnehmung einer Aufgabe im öffentlichen Interesse erforderlich ist oder
- in der Ausübung einer dem Arbeitgeber übertragenen öffentlichen Gewalt erfolgt
- (Art. 6 Abs. 1 lit. e)) oder
- auf einem berechtigten Interesse des Verarbeiters beruht (Art. 6 Abs. 1 lit. f)).

Das Widerspruchsrecht ist kein grundsätzlich neues Instrument und entspricht im Wesentlichen den §§ 20 Abs. 5, 35 Abs. 5 BDSG-alt. Neu ist aber, dass der verantwortliche Arbeitgeber zukünftig „zwingende Gründe“ nachweisen muss, die den Interessen des betroffenen Beschäftigten überwiegen.

Tipp für die Praxis

Es empfiehlt sich insbesondere nach einer auf die Interessenabwägung gestützten Verarbeitung die zwingenden Gründe bereits bei der Datenverarbeitung nachvollziehbar zu dokumentieren, gegebenenfalls im Zeitverlauf zu aktualisieren und zum Nachweis bereitzuhalten.

Neu ist auch, dass der betroffene Beschäftigte auf sein Widerspruchsrecht hinzuweisen ist und der Hinweis verständlich und von anderen Informationen getrennt zu erfolgen hat (vergleiche Art. 20 Abs. 4 DS-GVO).

3.2.7 Einschränkung von Betroffenenrechten

§ 29 BDSG beschränkt Informationspflichten des Verantwortlichen im Falle von Geheimhaltungspflichten, insbesondere wenn durch die Pflichterfüllung Informationen offenbart würden, für die ein Geheimhaltungsbedarf besteht. Auch sind Berufsgeheimnisträger (z. B. Rechtsanwälte, Wirtschaftsprüfer und Ärzte) nicht zur Erfüllung von Informationspflichten gegenüber betroffenen Personen verpflichtet, sofern deren Interesse an der Informationserteilung überwiegt.

Weitere Einschränkungen von Betroffenenrechten ergeben sich aus den §§ 32 und 33 BDSG. § 35 BDSG beinhaltet Ausnahmen vom Löschungsrecht, nämlich dann, wenn diese im Falle nicht automatisierter Datenverarbeitung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Dann ist die Datenverarbeitung einzuschränken. Dies gilt nicht, wenn die Daten zu Unrecht verarbeitet wurden.

Das Widerspruchsrecht wird in § 36 BDSG eingeschränkt, wenn und soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, welches die Interessen der betroffenen Person überwiegt oder bei einer Verpflichtung zur Verarbeitung durch eine Rechtsvorschrift.

4 Datensicherung und Vertraulichkeit

Rechtliche und technische Maßnahmen

4.1 Verpflichtung auf die Vertraulichkeit und Integrität

Die DS-GVO und das BDSG enthalten für einen Verantwortlichen keine vergleichbare ausdrückliche Pflicht zur Verpflichtung auf das Datengeheimnis, wie dies das BDSG-alt in § 5 Abs. 1 vorschreibt. Nur für Auftragsverarbeiter besteht nach Art. 28 Abs. 3 lit. b) DS-GVO die klar formulierte Pflicht, dass nur Personen mit der Verarbeitung personenbezogener Daten betraut werden dürfen, die sich entweder zur Vertraulichkeit und Integrität verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.

Hinweis

Die Regelung zum Datengeheimnis in § 53 BDSG gilt nur für öffentliche Stellen.

Eine ausdrückliche und dokumentierte Verpflichtung auf die Vertraulichkeit und Integrität ist dennoch zu empfehlen, da sie eine geeignete und zweckmäßige Maßnahme ist, die sicherstellt, dass Personen, die Zugang zu personenbezogenen Daten haben, diese datenschutzkonform verarbeiten. Eine solche Verpflichtung ist für einen Verantwortlichen auch einfach zu dokumentieren und daher zum Nachweis dafür geeignet, dass Verarbeitungen gemäß den Vorgaben der Verordnung erfolgen.

Umgekehrt bedeutet dies, dass Beschäftigte, die ausschließlich an Maschinen arbeiten und nicht mit personenbezogenen Daten in Berührung kommen, grundsätzlich nicht auf die Vertraulichkeit und Integrität verpflichtet werden müssen.

Tipp für die Praxis

Obwohl für die Verpflichtung auf die Vertraulichkeit und Integrität vom Gesetz nicht ausdrücklich für Verantwortliche vorgeschrieben ist, sollte aus Beweisgründen eine individuelle schriftliche Belehrung mit Verpflichtung vorgenommen werden. Das ergibt sich schon aus der allgemeinen Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO sowie aus dem Rechtsgedanken des Art. 28 Abs. 3 lit. b) DS-GVO.

Durch die Verpflichtung muss dem Beschäftigten die Bedeutung des korrekten Umgangs mit Personaldaten und die Schwere der Pflichtverletzung bei unbefugtem Umgang mit Daten bzw. bei Verstößen gegen Datenschutzregelungen bewusst werden.

Neben der Verpflichtung auf Vertraulichkeit und Integrität gelten für die Beschäftigten gegebenenfalls auch weitere spezielle Geheimhaltungspflichten aus anderen Gesetzen (z. B. § 4 GeschGehG – Geheimhaltung von Geschäftsgeheimnissen, § 79 BetrVG – Geheimhaltungspflicht der Mitglieder des Betriebsrats, § 3 TTDSG – Fernmeldegeheimnis und § 206 StGB – Post- und Fernmeldegeheimnis).

Der Arbeitgeber als Verantwortlicher hat gemäß Art. 32 DS-GVO sicherzustellen, dass einerseits ein angemessenes Sicherheitsniveau gewährleistet ist und andererseits keine unberechtigte oder ungesetzliche Verarbeitung stattfindet. Demnach obliegt der Geschäftsführung ein Organisationsschuld, der sie unter anderem durch eine Verpflichtung der Beschäftigten auf die Vertraulichkeit und Integrität nachkommen kann.

4.2 Technische und organisatorische Sicherungsmaßnahmen nach der DS-GVO

Nach Art. 32 DS-GVO hat der Arbeitgeber unter Berücksichtigung des Stands der Technik, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Welche technischen und organisatorischen Datensicherungsmaßnahmen zu treffen sind, ist daher jeweils an den konkreten Umständen des Einzelfalls unter Berücksichtigung des Standes der Technik zu messen. Der Schutzbedarf bestimmt den Umfang der Sicherungsmaßnahmen, wobei der Grundsatz der Verhältnismäßigkeit in Hinblick auf das Risiko anzuwenden ist. Für die Bewertung der Verhältnismäßigkeit wird also eine Risikobewertung vorausgesetzt. So stellt beispielsweise der Einsatz von Cloud-Technologien anders geartete Anforderungen an Datensicherungsmaßnahmen, als es beim herkömmlichen Client-Server-Einsatz der Fall ist.

Zur Bestimmung der Sicherheitsmaßnahmen sind nach der DS-GVO folgende Schritte erforderlich:

- Der Schutzbedarf ist festzustellen,
- Die Risiken sind zu bewerten,
- Es sind im Hinblick auf das Risiko verhältnismäßige Maßnahmen zu ergreifen,
- Nachweise sind zu erbringen.

Damit unterstellt die DS-GVO im Grundsatz, dass im Unternehmen ein IT-Sicherheits-management umgesetzt wird.

Hinweis

Ein Beispiel zur Etablierung eines IT-Sicherheitsmanagements bietet der BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS).

Die angemessene Etablierung und Erhaltung eines IT-Sicherheitsmanagements kann der Arbeitgeber durch die Einhaltung von Verhaltensregeln oder Zertifizierungsverfahren im Sinne der DS-GVO nachweisen. Durch das Zusammenwirken von Datenschutz- und IT-Sicherheitsmanagement sowie die Einbeziehung von Nachweisen und Zertifizierungsmaßnahmen ergibt sich ein angemessenes Schutzkonzept nach den Vorgaben der DS-GVO für die Verarbeitung personenbezogener Daten.

Art. 32 Abs. 1 DS-GVO sieht folgende Maßnahmen hierfür vor:

- Die Pseudonymisierung und Verschlüsselung personenbezogener Daten,

- Die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen (siehe hierzu die ehemaligen „8 Gebote“ aus § 9 BDSG und dessen Anlage),

- Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall wiederherzustellen (Reaktions- und Wiederherstellverfahren),

- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Kontrolle).

Die ehemals bestehenden „8 Gebote“ verlieren damit nicht ihre Gültigkeit. Sie bleiben im Wesentlichen über den zweiten Spiegelstrich erhalten und werden durch die neuen Begrifflichkeiten in Art. 32 DS-GVO ergänzt. Im Einzelnen gelten also weiterhin folgende Maßnahmen:

- Zutrittskontrolle
  Die Zutrittskontrolle verlangt, Unbefugten den „körperlichen“ Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Damit soll verhindert werden, dass Personen, die dazu nicht berechtigt sind, unkontrolliert in die Nähe von Datenverarbeitungsanlagen kommen (z. B. durch Türen, die sich nur bei richtiger PIN-Eingabe oder mit freigeschalteten Chipkarten öffnen lassen).

- Zugangskontrolle
  Die Zugangskontrolle soll verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Gemeint ist damit das Eindringen in ein EDV-System seitens einer unberechtigten externen Person (z. B. „Hacker“).

- Zugriffskontrolle
  Die Zugriffskontrolle soll gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Dateien zugreifen können. Zudem muss verhindert werden, dass

personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beispiel

Vergabe individueller Passwörter an jeden Beschäftigten, mit dem der Beschäftigte nur auf diejenigen Personaldaten zugreifen kann, die er zur Erledigung seiner Arbeit benötigt.

- Weitergabekontrolle
  Die Weitergabekontrolle soll gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, sowie dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Eingabekontrolle
  Die Eingabekontrolle soll gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Diese Maßnahme wird regelmäßig durch manuell oder automatisiert erfolgende Protokollierungen realisiert.

Beispiele

- handschriftliche Eingabevermerke
- automatisierte Protokolldateien

- Auftragskontrolle
  Im Rahmen der Auftragskontrolle muss der Auftragnehmer gewährleisten, dass im Auftrag zu verarbeitende Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

- Verfügbarkeitskontrolle
  Die Verfügbarkeitskontrolle zielt darauf ab, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und meint damit Wasserschäden, Brand, Blitzschlag, Stromausfall etc. Sicherungsmaßnahmen sind beispielsweise die Auslagerung von Sicherungskopien oder Notstromaggregate.

- Trennungsgebot
  Der Arbeitgeber muss die Zweckgebundenheit der Datenverarbeitung auch technisch sicherstellen. Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt

verarbeitet werden können. Dieser Grundsatz ist zwar so nicht mehr ausdrücklich in Art. 32 DS-GVO genannt, ergibt sich aber indirekt aus Art. 5 Abs. 1 lit. b) DS-GVO und verdient wegen Art. 5 Abs. 2 DS-GVO gesonderte Beachtung.

– Die Belastbarkeit und Wiederherstellbarkeit von Datenverarbeitungssystemen sollte durch entsprechende Krisenreaktionspläne sichergestellt werden (K-Fall-Szenarien, Business-Continuity-Pläne). Idealerweise wird deren Funktionsfähigkeit regelmäßig getestet.

Hinweis

Die Verschlüsselungsverfahren müssen dem Stand der Technik entsprechen.

Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Tipp für die Praxis

Der Arbeitgeber unterliegt auch in Bezug auf die ergriffenen Sicherheitsmaßnahmen der Rechenschaftspflicht. Zur Nachweiserbringung sind daher insbesondere die Maßnahmen selbst als auch ihre regelmäßige Überprüfung, Bewertung und Evaluierung zu dokumentieren.

4.3 Maßnahmen zum Schutz des Fernmeldegeheimnisses

Gestattet der Arbeitgeber die private Nutzung von Telefon, E-Mail und Internet, wird er seinen Beschäftigten gegenüber zum „Anbieter“ von Telekommunikationsdiensten im Sinne des Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG). Als solcher ist er insbesondere gemäß § 3 TTDSG zur Wahrung des Fernmeldegeheimnisses verpflichtet. Im Rahmen dessen muss er technische und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses treffen. In Betracht kommen Zutritts- und Zugriffsbeschränkungen, Verschlüsselungen sowie der Schutz der Firewall-Auswertungsprotokolle vor unbefugter Einsichtnahme.

Hinweis

Dass der Arbeitgeber bei der Erlaubnis der privaten Nutzung Telekommunikationsanbieter wird, ist trotz einiger anderslautender Urteile von Landesarbeitsgerichten herrschende Meinung. Leider ist auch mit Einführung des TTDSG keine gesetzliche Klarstellung erfolgt. Arbeitgeber, die die Privatnutzung erlauben, sollten sich auf jeden Fall an die Vorschriften des TTDSG halten, um ein strafbares Handeln auszuschließen.

5 Auftragsverarbeitung

Personaldatenverarbeitung durch Auftragnehmer

5.1 Allgemeines

Viele Unternehmen lagern – nicht zuletzt aus Kostengründen – ihre Datenverarbeitung (zumindest teilweise) aus.

Beispiele

- Ausgliederung von IT-Abteilungen und Rechenzentren
- zentrale, einheitliche Personaldatenverarbeitung eines Konzerns bei der Konzernmutter
- Auslagerung der Lohn- und Gehaltsabrechnung
- Einschalten eines Personalberatungsunternehmens im Bewerbungsverfahren Beauftragung eines externen Entsorgungsunternehmens mit dem Vernichten (= Löschen) von Dokumenten (z. B. Computerausdrucke, Personalakten)

Der Begriff des Auftragsverarbeiters wird in Art. 4 Nr. 8 DS-GVO definiert. Danach ist Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des verantwortlichen Arbeitgebers verarbeitet.

Die Auftragsverarbeitung isan die Voraussetzungen des Art. 28 DS-GVO geknüpft. Wesentliches Kriterium ist hierbei die Weisungsgebundenheit des Auftragsverarbeiters. Das Unternehmen (= der Arbeitgeber) muss „Herr der Daten“ bleiben, also die volle Verfügungsgewalt behalten und damit auch allein über die bestimmen. Sobald dem Auftragsverarbeiter eine „rechtliche Zuständigkeit“ oder eine „tatsächliche Entscheidungskompetenz“ zugewiesen wird, liegt keine Auftragsverarbeitung mehr vor, sondern ggf. eine gemeinschaftliche Verantwortlichkeit ober eben eine Datenübermittlung. Konsequenz wäre, dass die Datenverarbeitung, insbesondere der (Personal-) Datentransfer, wieder einer ausdrücklichen Ermächtigungsgrundlage bedürfte.

Beispiele

Ein Arbeitgeber schaltet bei der Stellenausschreibung, z. B. um zunächst anonym zu bleiben, einen Personalberater ein. Dieser nimmt nur die Bewerbungsunterlagen entgegen, sortiert sie nach Vorgaben und leitet sie an den Arbeitgeber weiter. Hierbei handelt sich um eine Auftragsverarbeitung.

Trifft der Personalberater aus dem Kreis der Bewerber eine eigene Vorauswahl, dann ist ihm ein Teil der eigentlichen Aufgabe übertragen worden, so dass keine Auftragsverarbeitung mehr vorliegt, sondern eine Auftragsdurchführung aufgrund eigener Kompetenz und damit weisungsunabhängig. Die vorausgehende Datenübermittlung ist aber im Sinne einer arbeitsteiligen Wirtschaft interessengerecht und damit zulässig (vgl. Art. 6 Abs. 1 lit. f) DS-GVO).

Hinweis

Der Vertrag zur Auftragsverarbeitung konkretisiert den zwischen den Parteien geschlossenen Hauptvertrag. Der Ausdruck „Auftragsverarbeitung“ ist im Hinblick auf die Vertragsgestaltung zwischen den Parteien untechnisch zu verstehen. Das Rechtsverhältnis zwischen Unternehmen und Auftragsverarbeiter muss nicht zwingend ein „Auftrag“ im Sinne des § 662 BGB sein – es kann auch als Dienst-, Werk- oder Geschäftsbesorgungsvertrag ausgestaltet sein.

5.2 Sorgfältige Auswahl des Auftragnehmers

Werden personenbezogene Daten im Auftrag verarbeitet, ist der Auftraggeber auch insoweit für die Einhaltung der Datenschutzvorschriften verantwortlich (Art. 4 Nr. 7 i. V. m. Art. 28 Abs. 1 DS-GVO). Der Auftraggeber hat deshalb einen Auftragnehmer sorgfältig auszuwählen, und zwar unter besonderer Berücksichtigung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen („hinreichende Garantien“) zum Schutz der Daten (Art. 28 Abs. 1 DS-GVO).

5.3 Schriftliche oder elektronische Auftragserteilung

Ist ein geeigneter Auftragnehmer gefunden, so ist der Auftrag schriftlich oder in elektronischer Form zu erteilen, wobei im Einzelnen u. a. festzulegen sind:

- Gegenstand und Dauer sowie Art und Zweck der Verarbeitung,
- Art der personenbezogenen Daten sowie Kategorien von betroffenen Personen,
- Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen,
- Verpflichtung der Beschäftigten zur Vertraulichkeit (ähnlich dem heutigen Datengeheimnis),
- Treffen angemessener technischer und organisatorischer Schutzmaßnahmen,
- Regelung des Einsatzes von Unterauftragsnehmern,
- Unterstützung des Verantwortlichen bei der Wahrnehmung der Rechte der betroffenen Personen,
- Unterstützung des Verantwortlichen bei der Meldung von Datenpannen und Durchführung von Datenschutzfolgenabschätzung,
- Rückgabe und Löschung personenbezogener Daten nach Beendigung des Auftrags,

– Kontrollrechte des Verantwortlichen und entsprechende Duldungs- und Mitwirkungspflichten des Auftragsverarbeiters,
– Hinweispflicht bei Weisungen, die gegen datenschutzrechtliche Vorschriften verstoßen.

Hinweis

Folgende Änderungen lassen sich somit im Hinblick auf den Inhalt des Vertrages feststellen:

– Elektronische Form ist ausreichend,
– Weisungen des Auftraggebers müssen dokumentiert werden,
– Auftragsverarbeiter wird verpflichtet:
– Bei der Datenverarbeitung ausschließlich Personen einzusetzen, die sich zur Verschwiegenheit verpflichtet sind,
– Den Verantwortlichen zu unterstützen, wenn betroffene Personen ihre entsprechenden Rechte gemäß Art. 12 ff. DS-GVO geltend machen,
– Den Verantwortlichen bei der Erfüllung seiner gesetzlichen Verpflichtungen zu unterstützen.

Als weitere Neuerung im Bereich der Auftragsverarbeitung kommt hinzu, dass die sowohl die EU-Kommission als auch die nationalen Aufsichtsbehörden Standardvertragsklauseln für die Auftragsverarbeitung veröffentlichen können.

Der Nachweis von Garantien des Auftragnehmers kann zukünftig durch Zertifizierungen und genehmigte Verhaltensregelungen (Art. 40, 42 DS-GVO) erfolgen.

Darüber hinaus müssen Auftragsverarbeiter zukünftig eine Reihe von Neuerungen beachten. Anders als bislang müssen sie zukünftig nach Art. 30 DS-GVO ebenfalls ein Verzeichnis von Verarbeitungstätigkeiten führen und darin sämtliche Tätigkeiten aufnehmen, welche für den Verantwortlichen durchgeführt werden.

Inhalte eines solchen Verzeichnisses des Auftragsverarbeiters nach Art. 30 Abs. 2 DS-GVO sind:

– Name und Kontaktdaten des Auftragsverarbeiters,
– Auch alle Daten der Verantwortlichen, auf deren Weisung der Auftragsverarbeiter personenbezogene Daten verarbeitet, gegebenenfalls deren Vertreter,
– Name und Kontaktdaten des Datenschutzbeauftragten,
– Kategorien von Verarbeitungen, die im Auftrag eines jeden Verantwortlichen geführt werden,
– Gegebenenfalls die Übermittlung von Daten in ein Drittland sowie
– Die technischen und organisatorischen Maßnahmen in allgemeiner Art und Weise.

Zudem ist der Auftragsverarbeiter unabhängig von seinem Sitz zukünftig dazu verpflichtet, einen Datenschutzbeauftragten zu bestellen, wenn die Bestellvoraussetzungen des Art. 37 DS-GVO vorliegen oder das nationale Datenschutzrecht dies verlangt.

Ferner wird in der DS-GVO die Haftung des Auftragsverarbeiters verschärft. Haftete dieser bislang nicht direkt gegenüber der betroffenen Person, ändert sich dies nunmehr. Nach Art. 82 Abs. 1 DS-GVO haften der Verantwortliche und der Auftragsverarbeiter zukünftig gemeinsam gegenüber der betroffenen Person.

Tipp für die Praxis

Diese Neuerungen sind von Auftragsverarbeitern bei der Vertrags- und Preisgestaltung zu berücksichtigen. Insbesondere die Haftungsfolgen bergen erhebliche Risiken für Auftragsverarbeiter.

5.4 Weisungsgebundenheit

Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten (Art. 28 Abs. 3 lit. a) DS-GVO). Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen die DS-GVO oder andere Datenschutzvorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen (Art. 28 Abs. 3 a. E. DS-GVO).

5.5 Kontrolle und Dokumentation

Art. 28 Abs. 3 lit. h) DS-GVO konkretisiert Kontrollrechte des Verantwortlichen. Kontrollen können danach sowohl durch den Verantwortlichen als auch durch einen Auditor, der durch den Verantwortlichen beauftragt wird, durchgeführt werden. Die DS-GVO erwähnt zwar nicht ausdrücklich das Recht, Kontrollen auch als Vor-Ort-Kontrollen durchzuführen. Die besondere Erwähnung der Möglichkeit, Inspektionen durchzuführen, legt aber nahe, dass die Kontrollrechte auch Vor-Ort-Kontrollen erfassen.

Tipp für die Praxis

Es empfiehlt sich die Erarbeitung eines Prüfkonzepts, wer auf welche Art und in welchem Umfang die Kontrollen durchführt und dokumentiert.

5.6 Einsatz von Unterauftragnehmern

Die Einschaltung von Unterauftragnehmern ist nach der DS-GVO nicht ohne Weiteres zulässig. Es bedarf vielmehr nach Art. 28 Abs. 2 DS-GVO der vorherigen Zustimmung des Verantwortlichen. Der Verantwortliche kann die Zustimmung für einzelne Unterauftragnehmer oder pauschal für mehrere Unterauftragnehmer erklären. Für den letztgenannten Fall ist der Auftragsverarbeiter verpflichtet, den Auftraggeber über den Austausch von Unterauftragnehmern und über neu hinzukommende Unterauftragnehmer zu informieren. Damit erhält der Auftraggeber die Möglichkeit des Einspruchs.

Wenn der Auftragsverarbeiter Unterauftragnehmer einschaltet, müssen die Parteien nach Art. 28 Abs. 4 DS-GVO eine Vereinbarung abschließen, wonach im Unterauftragsverhältnis alle Regelungen verbindlich zu treffen sind, die in Art. 28 Abs. 3 DS-GVO für den Vertrag zur Auftragsverarbeitung vorgeschrieben sind.

Der Auftragsverarbeiter hat für alle Datenschutzverstöße des Unterauftragnehmers einzustehen und ist für diese Verstöße gegenüber dem Verantwortlichen und der betroffenen Person haftbar.

6 Personaldatenübermittlung innerhalb des Konzerns

Zentralisierte Personalverwaltung

6.1 Allgemeines

Konzerne bestehen aus einzelnen juristischen Personen (Unternehmen), die sich jedoch als wirtschaftliche Einheit verstehen und daher dementsprechend z. B. mit einer konzernweiten Personalplanung oder -verwaltung agieren möchten. Für das Datenschutzrecht ist jedoch das einzelne Unternehmen als juristische Person maßgeblich. Dieses ist Normadressat der DS-GVO (siehe Art. 4 Nr. 7 DS-GVO). Eine Weitergabe von Beschäftigtendaten zwischen rechtlich selbständigen Unternehmen ist datenschutzrechtlich nur unter den allgemeinen Voraussetzungen zulässig – ein sogenanntes „Konzernprivileg“, das die wirtschaftlichen Zusammenhänge und Abhängigkeiten innerhalb konzernangehöriger Unternehmen berücksichtigt, kennt die DS-GVO nicht, obwohl Erwägungsgrund 48 im Rahmen der Interessenabwägung berücksichtigt werden kann.

Hinweis

Eine gewisse Erleichterung sieht die DS-GVO lediglich in Erwägungsgrund 48 hinsichtlich der Verarbeitung zu internen Verwaltungszwecken vor. Hierdurch sollen Unternehmen der Datenaustausch innerhalb einer Unternehmensgruppe zu administrativen Zwecken erleichtert werden. Auch derartiger Datenaustausch innerhalb einer Unternehmensgruppe bedarf zwar einer rechtlichen Legitimation. In Erwägungsgrund 48 wird es aber als berechtigtes Interesse bezeichnet, personenbezogene Daten zu internen Verwaltungszweck innerhalb einer Unternehmensgruppe auszutauschen.

Im Geltungsbereich der DS-GVO ist die Weitergabe von Beschäftigtendaten innerhalb eines Konzerns als „Übermittlung“ anzusehen und daher nur zulässig, wenn

- die DS-GVO selbst (z. B. Art. 6 Abs. 1 lit. b) DS-GVO),
- eine Betriebsvereinbarung, (Art. 88 DS-GVO) oder
- der Beschäftigte selbst (Einwilligung, Art. 7 DS-GVO)

dies erlaubt.

Fall

Die Konzernmutter aus den USA möchte sämtliche Beschäftigtendaten aller Konzernunternehmen verarbeiten.

Der Zweck des Beschäftigungsverhältnisses macht eine Verarbeitung von Beschäftigtendaten im Konzern in der Regel nicht erforderlich. Beschäftigtendaten sind grundsätzlich nur zur Information des eigenen Arbeitgebers und zur Wahrnehmung von dessen Rechten und Pflichten gegenüber dem Beschäftigten bestimmt. Unerheblich sind auch vertragliche Rechtsbeziehungen zwischen den einzelnen konzernangehörigen Unternehmen untereinander, insbesondere z. B. sogenannte Beherrschungsverträge zwischen Unternehmen und Konzernspitze. In Ausnahmefällen kann ein „konzernbezogenes“ Arbeitsverhältnis den konzerninternen Personaldatenaustausch legitimieren, z. B. wenn sich der Beschäftigte in seinem Arbeitsvertrag bereit erklärt hat, auch in anderen Konzernunternehmen tätig zu werden. Gleiches gilt für Führungskräfte, denen die Konzernstrukturen und die Notwendigkeit konzerninterner Mobilität bei Aufnahme ihrer Tätigkeit ersichtlich waren. Unter diesen Voraussetzungen ist es auch bei Personen, die als Nachwuchskräfte an Führungsaufgaben herangeführt werden sollen, durch den Arbeitsvertrag gerechtfertigt, dass ihre Beschäftigtendaten in konzerneinheitliche Personalfortentwicklungssysteme eingespeist und damit innerhalb des Konzerns verarbeitet werden.

Hinweis

Klarheit kann in diesen Fällen allerdings nur eine ausdrückliche arbeitsvertragliche Regelung bringen.

Die Verarbeitung der Personaldaten ist auch in den genannten Ausnahmefällen selbstverständlich nur in dem Umfang gerechtfertigt, wie er für den Arbeitgeber selbst gelten würde (zweckgebunden!): die Verarbeitung von Beschäftigtendaten für einen im Konzern frei verfügbaren Datenpool wäre unzulässig. Legitim können lediglich streng zweckgebundene Personaldatensammlungen sein, z. B. Bereitstellen der Beschäftigtendaten in einem zentralen „human-resource-System“ zum Zwecke der konzerninternen Personalplanung.

Das Einholen einer Einwilligung der betroffenen Beschäftigten während des laufenden Arbeitsverhältnisses als Rechtfertigung für die Verarbeitung seiner Personaldaten in einem konzernangehörigen Unternehmen kommt nur dann in Betracht, wenn der Beschäftigte eine echte, auf Freiwilligkeit beruhende Wahl hat.

Für die Übermittlung von personenbezogenen Daten an ein Konzernunternehmen in Staaten außerhalb der Europäischen Union und außerhalb des Europäischen Wirtschaftsraums gelten die besonderen Anforderungen nach Art. 44 ff. DS-GVO.

Tipp für die Praxis

Die in der Praxis wohl praktikabelste Lösung ist der Abschluss einer (Konzern-) Betriebsvereinbarung, in der die Verarbeitung von Beschäftigtendaten innerhalb des Konzerns geregelt wird. Diese wird als Legitimation zur Datenverarbeitung anerkannt, wenn folgende Voraussetzungen vorliegen:

- Einhaltung der allgemeinen Datenschutzgrundsätze (vgl. Art. 5 DS-GVO),
- Einhaltung der Transparenz- und Informationspflichten über den Beschäftigten
- (vgl. Art. 12 bis 14 DS-GVO),
- Abbildung der Rechte der betroffenen Beschäftigten nach Art. 15 ff. DS-GVO,
- Gewährleistung eines angemessenen Datensicherheitsniveaus (vgl. Art. 32 DS-GVO).

6.2 Konzernweite Telefon-, Namens- und E-Mail-Verzeichnisse

In vielen Konzernen werden im konzerninternen Intranet Namens-, Telefon und E-Mail-Verzeichnisse genutzt. Nach den Vorgaben der Verordnung und des BDSG ist dies zulässig,

- sofern es für die Erbringung der Arbeitsleistung jedes Beschäftigten aktuell erforderlich ist, dass er auf die dienstlichen „Kommunikationsdaten“ (Name, Abteilung, dienstliche Telefon- und Faxnummer, E-Mail-Adresse) aller anderen Konzernbeschäftigten zugreifen kann, weil es erforderlich ist, dass er mit jedem kommunizieren kann,
- ein berechtigtes Interesse des konzernangehörigen Arbeitgebers oder anderer konzernangehöriger Unternehmen besteht (z. B. zentrale Versendung von E-Mails zur zeitgleichen Information aller Beschäftigten).

Um jedoch den schutzwürdigen Belangen der betroffenen Beschäftigten, insbesondere der Nicht-Funktionsträger (z. B. Schreibkräfte, LKW-Fahrer), Rechnung zu tragen, sollte die beabsichtigte Erstellung eines solchen Verzeichnisses vorher bekanntgegeben werden, damit die betroffenen Beschäftigten besondere Gründe vortragen können, die der Aufnahme in das Verzeichnis entgegenstehen. Soll das Verzeichnis im Internet veröffentlicht werden, müssen Nicht-Funktionsträger ein Widerspruchsrecht haben.

6.3 Zentralisierte Personalverwaltung

Eine zentralisierte Personalverwaltung ist zulässig, sofern sie als Auftragsverarbeitung ausgestaltet ist oder besondere Datenschutzregelungen, z. B. (Konzern)Betriebsvereinbarung, geschaffen wurden.

6.4 Übertragung wichtiger Personalentscheidungen (Sozialauswahl, Einstellung)

Werden wichtige Personalentscheidungen isoliert auf andere Konzernunternehmen übertragen, so ist die Zulässigkeit der hierfür erfolgenden Übermittlung von Personaldaten besonders kritisch zu prüfen.

Hinweis

Eine Konzernmutter fordert die Übermittlung personenbezogener Personaldaten, um über betriebsbedingte Kündigungen in der Tochtergesellschaft zu entscheiden, vor allem um die Sozialauswahl zu treffen.

Hier besteht die Gefahr, dass die Daten aus dem üblichen Kontext gerissen werden und gegebenenfalls nicht in sachlich gerechtfertigter Weise genutzt werden. Legitim dürfte allenfalls die Verarbeitung statistischer Daten sein. Wenn die Konzernmutter die Entscheidung über die Einstellung eines neuen Beschäftigten trifft, so ist die hierfür erforderliche Verarbeitung der Bewerberdaten zulässig, wenn der Arbeitgeber den Bewerber darüber informiert hat.

7 Personaldatenübermittlung ins Ausland

Länder mit und ohne angemessenes Datenschutzniveau

7.1 Beschäftigtendatentransfer an Stellen innerhalb der EU bzw. des EWR

Mit der DS-GVO soll das Datenschutzrecht innerhalb von Europa vereinheitlicht werden. In einem noch größeren Umfang als bislang ist somit künftig davon auszugehen, dass in den EU-Ländern und in den Ländern des EWR ein einheitliches Datenschutzniveau herrscht und ein Datentransfer in derartige Länder bei Beachtung der Regelungen der DS-GVO problemlos möglich ist.

7.2 Beschäftigtendatentransfer an Stellen außerhalb der EU bzw. des EWR

Für den Fall, dass personenbezogene Daten über die EU-Grenzen transferiert werden, bleiben die bislang bekannten Grundbausteine zum internationalen Datenschutz erhalten. Neben der einschlägigen Rechtsgrundlage für die Übermittlung an sich muss zusätzlich ein angemessenes Datenschutzniveau bei der empfangenden Stelle vorliegen (Zwei-Stufen-Prüfung). Ausnahmsweise kann auf der zweiten Stufe eine Datenübermittlung in das Drittland trotz fehlendem angemessenem Datenschutzniveaus erfolgen, wenn die Voraussetzungen des Art. 48 oder 49 DS-GVO vorliegen. Eine gesetzliche Beschränkungsmöglichkeit der internationalen Verarbeitung hat der Gesetzgeber aber in Art. 49 Abs. 5 DS-GVO für bestimmte Kategorien personenbezogener Daten im Sinne von Art. 9 DS-GVO vorgesehen.

7.3 Länder mit gleichwertigem Datenschutzniveau

Die Europäische Kommission hat in Bezug auf einige Länder, z. B. UK, Schweiz, Kanada, Argentinien, Uruguay, Israel und Neuseeland und Japan entschieden, dass ein vergleichbares und damit hinreichendes Schutzniveau besteht. Ein Datentransfer in diese Staaten ist daher wie innerhalb der EU, das heißt wie im Inland möglich, vgl. Art. 45 DS-GVO.

Weiterführende Informationen / Link

Die Liste aller Länder mit gleichwertigem Datenschutzniveau und die entsprechenden Entscheidungen der Europäischen Kommission sowie weitere Informationen stehen Ihnen unter folgendem Link zur Verfügung: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

7.4 USA

Mit Urteil vom 16. Juli 2020 („Schrems II“) hat der EuGH entschieden, dass europäische Unternehmen ihre Datenübermittlung in die USA nicht mehr auf das zwischen der EU-Kommission und der US-Regierung ausgehandelte Privacy Shield-Abkommen stützen können.

Aufgrund der weitreichenden Zugriffsmöglichkeiten der amerikanischen Sicherheitsbehörden auf elektronisch gespeicherte Daten seien die europäischen Anforderungen an den Datenschutz für in die USA übertragene Nutzerdaten nicht gewährleistet. Auch sei der Rechtsschutz für Betroffene unzureichend. Seit dieser Entscheidung haben sich jedoch mittlerweile einige erfreuliche Neuerungen ergeben, welche nachstehend aufgezeigt werden.

Nachdem der Europäische Gerichtshof das sog. „EU-US Privacy Shield“ in o. g. Urteil für ungültig erklärt hat, mussten Unternehmen zunächst auf alternative Mechanismen zur datenschutzrechtlichen Legitimierung des Drittlandtransfers ausweichen. Neben Standardvertragsklauseln kamen hierzu beispielsweise sog. „Binding Corporate Rules“ oder – zumindest in Ausnahmefällen – datenschutzrechtliche Einwilligungen der betroffenen Personen in Betracht. Allen Fällen war dabei jedoch gemein, dass gewisse datenschutzrechtliche Risiken bestehen blieben, welche nur schwerlich vollends ausgeräumt werden konnten.

Bereits am 25. März 2022 wurde in Anbetracht dieser datenschutzrechtlichen Risiken seitens der Europäischen Kommission und den Vereinigten Staaten eine gemeinsame Erklärung für einen „Transatlantischen Datenschutzrahmen“ veröffentlicht. Festgehalten wurde hierbei explizit, dass die in der „Schrems-II“ Entscheidung genannten Bedenken künftig ausgeräumt werden sollen und sich die USA insoweit einer „Selbstverpflichtung“ zum Ergreifen geeigneter Garantien unterziehen. Am 07. Oktober 2022 unterzeichnete Präsident Joe Biden sodann eine Executive Order „Enhancing Safeguards for United States Signals Intelligence Activities“ (EO 10486), welche der erste Schritt zur Gewährleistung eines angemessenen Datenschutzniveaus darstellen sollte.

Seit dem 13. Dezember 2022 liegt der erste Entwurf für ein neues „EU-US Data Privacy Framework“ vor, welcher den sog. Drittlandtransfer in die USA legitimieren soll. Am 10. Juli 2023 wurde sodann verkündet, dass die Europäische Kommission den Angemessenheitsbeschluss final angenommen hat. Darin wird bestätigt, dass die USA ein hinreichendes Schutzniveau für personenbezogene Daten gewährleisten. Der Datentransfer an US-Unternehmen wird dadurch künftig deutlich vereinfacht.

Hinweis

US-Unternehmen, an die Daten auf Basis des Angemessenheitsbeschlusses übermittelt werden soll, müssen sich in den USA zunächst noch zertifizieren lassen.

Die Zertifizierung ist über die vom US-Handelsministerium betriebene Website www.dataprivacyframework.gov vorzunehmen, die aktuell allerdings noch nicht live geschaltet ist. Es ist davon auszugehen, dass sich die meisten US-Unternehmen, die Daten aus Europa empfangen, mittelfristig um diese Zertifizierungen bemühen werden. Auf der o. g. Website des US-Handelsministeriums wird künftig eine aktualisierte Liste der zertifizierten und der ehemals zertifizierten Unternehmen (mit Angabe der Gründe für die Streichung) veröffentlicht. Die Zertifizierung muss jährlich aktualisiert werden.

Alle bisherigen Rechtsgrundlagen für Datentransfers in die USA, wie beispielsweise Standardvertragsklauseln, bleiben wirksam und bis zur Zertifizierung des die Daten empfangenden US-Unternehmens auch erforderlich. Nicht vom Angemessenheitsbeschluss abgedeckt sind zudem Datentransfers aus den USA an Subunternehmer in anderen Drittstaaten. Insoweit bedarf es alternativer Rechtsgrundlagen (z. B. Standardvertragsklauseln). Im Übrigen werden Unternehmen auch weiterhin ihre datenschutzrechtlichen Hausaufgaben zu erledigen haben, insbesondere müssen sie ihre Datenströme genau kennen und dokumentieren („Know your data transfers“). Sofern Datentransfers künftig auf den Angemessenheitsbeschluss gestützt werden, sind Verträge und Datenschutzhinweise entsprechend anzupassen.

7.5 Länder ohne angemessenes Datenschutzniveau

Fehlt es an einem angemessenen Schutzniveau, ist eine Übermittlung von personenbezogenen Daten in den in Art. 49 DS-GVO geregelten Ausnahmen möglich:

- Zulässig ist die Datenübermittlung, die im Rahmen eines Vertrages erforderlich ist, den der betroffene Beschäftigte entweder selbst abgeschlossen hat oder der in seinem Interesse abgeschlossen wurde, z. B. Weitergabe von Beschäftigtendaten im Rahmen von Auslandseinsätzen zur Buchung von Hotelzimmern, Flügen, etc.
- Die Einwilligung des betroffenen Beschäftigten kann die Übermittlung seiner personenbezogenen Daten in ein „datenschutzloses“ Land rechtfertigen. Dazu gehört in diesem Fall auch, dass der Arbeitgeber auf die spezifischen Risiken des Datentransfers hinweist und den Beschäftigten darüber informiert, welche Daten an welchen Empfänger und zu welchem Zweck übermittelt werden sollen (Art. 49 DS-GVO). Je nach Einzelfall stellt sich auch hier die Frage, inwiefern die Einwilligung des Beschäftigten freiwillig erfolgte. Ebenfalls ist zu berücksichtigen, dass eine entsprechende Einwilligung nach der restriktiven Auffassung der Datenschutzaufsichtsbehörden nur für Ausnahmefälle herangezogen werden kann. Für regelmäßige und kontinuierliche Datenübermittlungen sollte daher primär auf andere Mechanismen abgestellt werden.
- Der Datenschutz bei dem Datenempfänger kann auch aufgrund aufsichtsbehördlich genehmigter vertraglicher Vereinbarungen gewährleistet werden (Art. 46 Abs. 3 DS-GVO).

7.6 EU-Standarddatenschutzklauseln

Für die Übermittlung von Daten an Drittstaaten, die nicht über ein angemessenes Datenschutzniveau verfügen, hat die Europäische Kommission Standardvertragsklauseln entworfen. Mittels derer kann ein Unternehmer ein ausreichendes Datenschutzniveau bei dem Empfänger gewährleisten und so den Datentransfer ermöglichen. Mit den Standardvertragsklauseln verpflichten sich die Beteiligten, d. h. der Datenexporteur in der EU und der Datenimporteur in dem Drittstaat, die Daten entsprechend den europäischen Datenschutzbestimmungen zu erheben und zu verarbeiten. Die Vertragsklauseln legen also die notwendigen Mindeststandards, die in den Drittstaaten nicht gesetzlich garantiert sind, vertraglich zwischen den Parteien fest.

Eigene Vertragsklauseln können zwar formuliert werden, müssen jedoch individuell genehmigt werden und dürfen inhaltlich nicht wesentlich von den EU-Standardvertragsklauseln abweichen, Art 46 Abs. 3 DS-GVO.

Hinweis

In seinem Urteil vom 16. Juli 2020 hat der EuGH entschieden, dass die Standardvertragsklauseln als mögliche weitere Grundlage für den Datentransfer in Drittstaaten weiterhin gültig sind. Allerdings müssen die Aufsichtsbehörden im Einzelfall letztlich prüfen und sicherstellen, dass die Standardklauseln in dem jeweiligen Drittland eingehalten werden (können). Gegebenenfalls bedürfen diese Klauseln der Ergänzung zusätzlicher Vereinbarungen oder Elemente, um im Empfängerland ein gleichwertiges Datenschutzniveau zu gewährleisten. Dies betrifft primär technische Maßnahmen (wie etwa die Pseudonymisierung der Daten), daneben allerdings auch organisatorische und vertragliche Maßnahmen. Sollte ein angemessenes Datenschutzniveau auch durch sonstige Maßnahmen nicht gewährleistet werden können, muss die Datenübermittlung in das betreffende Land ausgesetzt oder verboten werden.

7.7 Konzernweiter Verhaltenskodex

Eine weitere Möglichkeit, hinreichenden Datenschutz zu gewährleisten, ist die Schaffung eines konzernweiten Verhaltenskodex, der für den gesamten Konzern den Umgang mit Daten verbindlich festlegt. Auf diese Weise können konzernweit personenbezogene Daten übermittelt werden – unabhängig von der Frage des jeweiligen Datenschutzniveaus. Ein solcher Kodex muss sich allerdings an den strengen Vorgaben des europäischen Datenschutzrechts orientieren und bedarf der individuellen Genehmigung durch die zuständige Aufsichtsbehörde nach Art. 47 DS-GVO.

8 Kontrolle von Arbeitnehmern

Verhältnismäßigkeit beachten

Die gezielte Überwachung von Arbeitnehmern an ihrem Arbeitsplatz ist ein erheblicher Eingriff in das allgemeine Persönlichkeitsrecht der Arbeitnehmer und daher nur unter sehr engen Voraussetzungen zulässig. Wie eingangs bereits dargestellt, ist es derzeit nicht eindeutig klar, inwieweit die Regelung des § 26 BDSG künftig anwendbar bleibt. Gerade für die Aufdeckung von Straftaten existiert in § 26 Abs. 1 S. 2 BDSG eine Sonderregelung. Es ist jedoch davon auszugehen, dass die inhaltlichen Anforderungen an eine Kontrolle von Arbeitnehmern – allen voran die stets durchzuführende Interessenabwägung – losgelöst von der datenschutzrechtlichen Rechtsgrundlage beachtet werden müssen. So stellt es primär eine dogmatische Fragestellung dar, ob weiterhin auf § 26 BDSG oder etwa auf Art. 6 Abs. 1 lit. f) DS-GVO abzustellen ist. Gleichwohl sprechen einige Argumente dafür, dass zumindest die Sonderregelung in § 26 Abs. 1 S. 2 BDSG mit den Anforderungen der DS-GVO vereinbar ist. Dies vorangestellt, gelten die folgenden Grundsätze:

8.1 Videoüberwachung von Arbeitnehmern am Arbeitsplatz

Erfolgt die Überwachung zur Aufdeckung einer Straftat, gelten die Anforderungen des § 26 Abs. 1 S. 2 BDSG (hilfsweise Art. 6 Abs. 1 lit f) DS-GVO). Für präventive Überwachungen und solche zur Aufdeckung von schweren Verfehlungen, die keine Straftaten sind, findet Art. 6 Abs. 1 lit. f) DS-GVO Anwendung. Die Überwachung muss somit zur Wahrung von berechtigten Interessen des Arbeitgebers, beispielsweise zum Schutz seines Eigentums erforderlich sein. Zudem darf nicht das Interesse der betroffenen Beschäftigten überwiegen. Bei der Abwägung sind insbesondere Umfang und Dauer der Überwachung sowie die Intensität der Auswertung der Aufzeichnungen zu berücksichtigen.

Beispiele aus der Praxis

- Kontrolle von Arbeitsvorgängen, die aus technischen Gründen besonderer Beobachtung bedürfen, z. B. Walzstraßen, Hochöfen,
- Kontrolle bestimmter Bereiche aus Sicherheitsgründen, z. B. Tresorraum, Bankschalter, kerntechnische Anlagen, Tore,
- Vorliegen konkreter Anhaltspunkte oder Verdachtsmomente für Straftaten oder andere schwere Verfehlungen gegen den Arbeitgeber (z. B. Diebstahl oder Unterschlagung von Firmeneigentum, Verrat von Betriebsgeheimnissen, etc.). Lediglich vage Vermutungen oder ein pauschaler Verdacht gegen die gesamte Belegschaft reichen nicht aus.

Sämtliche weniger einschneidende Mittel zur Aufklärung des Verdachts müssen bereits ausgeschöpft sein, bevor eine Videoüberwachung als verhältnismäßiges Mittel in Frage kommt.

– Eine unter diesen Voraussetzungen zulässige Videoüberwachung ist grundsätzlich offen mittels einer sichtbaren Anlage und nach vorheriger Information der Belegschaft durchzuführen.

– Eine heimliche Überwachung durch eine verdeckte Kamera ist nur ausnahmsweise zulässig, z. B. bei Verdacht von Straftaten oder anderen schweren Verfehlungen gegen den Arbeitgeber, wenn keine andere Möglichkeit besteht, den Täter zu überführen und Beweismaterial zu sichern. Das wird regelmäßig dann der Fall sein, wenn der Täter selbst heimlich handelt, z. B. nur dann stiehlt, wenn er sich unbeobachtet fühlt.

Fall

Eine Beschäftigte eines Getränkemarkts erstellt fiktive Leergutbons, scannt diese ein und entnimmt den entsprechenden Betrag heimlich aus ihrer Kasse. Das Verhalten der Beschäftigten führt zu erheblichen Inventurdifferenzen und begründet einen konkreten Tatverdacht des Arbeitgebers. Der Arbeitgeber überprüft daraufhin sein Warenwirtschaftssystem, um die Inventurdifferenzen aufzuklären. Sämtliche Arbeitsabläufe werden auf mögliche Fehlerquellen untersucht. Letztendlich kommt nur noch ein Beschäftigtenfehlverhalten als Ursache in Betracht. Eine effektive Überwachung durch Beschäftigte oder Vorgesetzte ist nicht möglich, weshalb eine heimliche Videoüberwachung das einzig verbleibende – und in diesem Fall auch gerechtfertigte – Mittel zur Sachverhaltsaufklärung darstellt.

Die Videoüberwachung unterliegt gemäß § 87 Abs. 1 Nr. 6 BetrVG der Mitbestimmung des Betriebsrates und bedarf daher seiner vorherigen Zustimmung.

Hält der Arbeitgeber sich nicht an diese Vorgaben, läuft er Gefahr, die gewonnenen Erkenntnisse in einem nachfolgenden (Kündigungsschutz-) Prozess nicht als Beweise verwerten zu dürfen (Beweisverwertungsverbot).

Tipp für die Praxis

Das Bundesarbeitsgericht (BAG) hat am 22. September 2016 zur Verwertbarkeit von Zufallsfunden aus einer heimlichen Videoüberwachung ein wichtiges Urteil gefällt (Az: 2 AZR 848/15). Die Entscheidung des BAG zeigt, unter welchen Voraussetzungen Ermittlungs- und Kontrollmaßnahmen des Arbeitgebers ohne Kenntnis der davon betroffenen Beschäftigten zulässig sind. Ebenso zeigt die Entscheidung, unter welchen Voraussetzungen Arbeitsgerichte sogar unstreitige Tatsachen unbeachtet lassen müssen, wenn der

Arbeitgeber diese datenschutzwidrig erhoben hat. Besonders wichtig ist die Aussage des BAG, wonach Eingriffe in das Recht der Beschäftigten auf informationelle Selbstbestimmung durch verdeckte Videoüberwachungen dann zulässig sind, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht. Es müssen aber andere, weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft worden sein. Die Kontrollmaßnahme darf zudem insgesamt nicht unverhältnismäßig sein.

Für die Praxis ist besonders wichtig, dass Arbeitgeber nicht nur konkret vermutete Straftaten, sondern auch sonstigen schweren Pflichtverletzungen nachgehen dürfen. Zudem stellt das BAG fest, dass § 32 BDSG-alt für den Datenschutz im Beschäftigungsverhältnis eine abschließende Regelung darstellt. Es steht zu erwarten, dass diese Entscheidung des BAG auch für eine Videoüberwachung nach der DS-GVO Gültigkeit hat.

8.2 Videoüberwachung an öffentlich zugänglichen Arbeitsplätzen

Die Videoüberwachung von öffentlich zugänglichen Räumen – die zugleich Arbeitsplätze sind – regelt § 4 BDSG. Solche öffentlich zugänglichen Arbeitsplätze sind z. B. Schalterhallen eines Kreditinstituts, Verkaufsräume, öffentlich zugängliche Eingangshallen, Tankstellen, Gaststätten.

In diesen Bereichen ist die Videoüberwachung nach § 4 BDSG zulässig

– zur Wahrnehmung des Hausrechts,
– zur Wahrnehmung berechtigter Interessen für konkret festzulegende Zwecke.

Beispiele

– Videoüberwachung einer Schalterhalle eines Kreditinstituts zum Schutz gegen Überfälle,
– Videoüberwachung der Verkaufsräume eines Kaufhauses zum Schutz vor Diebstählen.

Hinweis

Das Bundesverwaltungsgericht hat entschieden, dass im Fall einer Videoüberwachung öffentlich zugänglicher Räume durch Private zum Schutz individueller Rechtsgüter – seien es die eigenen oder diejenigen Dritter – Art. 6 Abs. 1f DS-GVO als Rechtsgrundlage herangezogen werden muss und nicht § 4 Abs. 1 S. 1 BDSG. Dies führt im Ergebnis insbesondere dazu, dass z. B. bei einer Videoüberwachung zum Schutz öffentlich zugänglicher großflächiger Anlagen im Sinne von § 4 Abs. 1 S. 2 BDSG der Schutz von Leben, Gesundheit und Freiheit von dort aufhältigen Personen nicht mehr zwingend als besonders schützenswertes Interesse anzusehen ist. Es ist nun in diesen Fällen, ebenso wie bei sonstigen

Videoüberwachungen öffentlich zugänglicher Räume, eine Abwägung nach Art. 6 Abs. 1 lit. f) DS-GVO vorzunehmen.

Für die Anwendung von § 4 Abs. 1 BDSG verbleiben Fälle, in denen Privatpersonen durch einen staatlichen Übertragungsakt im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt auf der Grundlage von Art. 6 Abs. 1 lit. e) DS-GVO tätig werden.

In der Regel richtet sich die Videoüberwachung hier gegen Betriebsfremde (z. B. Kunden, Besucher). Beschäftigte in diesen öffentlich zugänglichen Bereichen werden eine solche Videoüberwachung als „arbeitsplatzimmanent“ hinnehmen müssen. Sofern sie nicht der eigentliche „Gegenstand“ der Beobachtung sind, ist eine Auswertung der Beobachtungsergebnisse zum Zweck einer beschäftigtenbezogenen Leistungs- und Verhaltenskontrolle unzulässig.

8.3 Videoüberwachung durch Detektiv

Lässt ein Arbeitgeber einen Beschäftigten ohne berechtigten Anlass von einem Detektiv überwachen, so handelt er rechtswidrig. Dies ist der Fall, wenn sein Verdacht nicht auf konkreten Tatsachen beruht. Für dabei heimlich hergestellte Videoaufnahmen gilt dasselbe. Eine solche rechtswidrige Verletzung des allgemeinen Persönlichkeitsrechts kann einen Geldentschädigungsanspruch („Schmerzensgeld“) begründen.

Hinweis

Gemäß Art. 82 Abs. 1 DS-GVO hat jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Ersatz des entstandenen Schadens gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Insbesondere Art und Umfang eines immateriellen Schadensersatzes waren bislang sowohl in Literatur als auch in Rechtsprechung höchst umstritten.

Der EuGH hat per Urteil vom 04. Mai 2023 (Az. C-300/41) nunmehr ausdrücklich festgehalten, dass der bloße Verstoß gegen die DS-GVO keinen Anspruch aus Art. 82 DS-GVO auf Schadensersatz nach sich zieht. Vielmehr ist es die Aufgabe der betroffenen Person, einen etwaig erlittenen immateriellen Schaden substantiiert darzulegen und ggf. zu beweisen. Andererseits hat der EuGH klargestellt, dass ein immaterieller Schaden an keinerlei Erheblichkeitsschwelle zu knüpfen ist. Dies bedeutet, dass auch „geringfügige“ Schäden – sofern sie im jeweiligen Fall tatsächlich vorliegen und vorgetragen werden – ersatzfähig sind. Die nationalen Gerichte haben daher künftig zu entscheiden, wann es sich um einen ersatzfähigen immateriellen Schaden handelt und in welcher Höhe dieser zu ersetzen ist. Trotz des Umstands, dass die DS-GVO keinen Strafschadensersatz kennt, darf die Abschreckungswirkung des Art. 82 DS-GVO nicht unterlaufen werden.

8.4 Sonstige Voraussetzungen für eine Videoüberwachung nach der DS-GVO

Die Videoüberwachung ist in das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DS-GVO aufzunehmen. Dieses Verzeichnis ersetzt das Verfahrensverzeichnis nach dem BDSG-alt. Die neu durch Art. 35 DS-GVO eingeführte Datenschutzfolgenabschätzung ist auch für die systematische und umfangreiche Überwachung öffentlich zugänglicher Bereiche erforderlich. Darin sind vorab die Folgen der vorhergesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten abzuschätzen. Diese Datenschutzfolgenabschätzung soll sich insbesondere mit den Maßnahmen, Garantien und Verfahren befassen, durch die ein hohes Risiko für die Rechte der betroffenen Beschäftigten eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen der DS-GVO nachgewiesen werden können.

8.5 Sonstige Überwachung bzw. Kontrolle

Die Regelungen in Art. 6 Abs. 1 lit. b) DS-GVO sowie § 26 Abs. 1 S. 2 BDSG konkretisieren die Kontrollbefugnisse des Arbeitgebers für den Fall der Aufdeckung von erkannten oder konkret vermuteten Straftaten. Sollte die Norm künftig nicht mehr anwendbar sein, werden dessen inhaltliche Voraussetzungen jedoch perspektivisch weiterhin seitens der Arbeitsgerichte herangezogen.

8.5.1 Aufdecken und Verhindern von Straftaten

Die Verarbeitung von Daten ist demnach nur dann erlaubt, wenn bereits ein aufgrund dokumentierter und tatsächlicher Anhaltspunkte begründeter Anfangsverdacht gegen den konkreten Arbeitnehmer besteht und sie zur Aufdeckung der Straftat oder einer vertraglichen Pflichtverletzung erforderlich ist. Zudem dürfen keine überwiegenden schutzwürdigen Interessen des Betroffenen entgegenstehen. Das Prinzip der Verhältnismäßigkeit muss sowohl für die Art als auch für das Ausmaß der Maßnahme gewahrt werden. Zu berücksichtigen ist die Schwere der Straftat bzw. der Pflichtverletzung und die Intensität des Verdachts.

Nicht unter § 26 Abs. 1 S. 2 BDSG fallen allgemeine verdachtsunabhängige Kontrollen, die gem. Art. 6 Abs. 1 lit. b) DS-GVO zur Durchführung des Beschäftigungsverhältnisses erforderlich sind, z. B. Kontrolle von Leistung und Verhalten oder zur Verhinderung von Pflichtverletzungen und Straftaten. Das Prinzip der Verhältnismäßigkeit ist bei jeder Kontrollmaßnahme zu wahren.

In der betrieblichen Praxis empfiehlt sich nach alledem die folgende Vorgehensweise:

– Durchführung einer Gefährdungsanalyse mit anonymisierten oder pseudonymisierten Daten,

- Bei Anhaltspunkten für Rechtsverstöße bei konkreten Geschäftsvorgängen: Herstellung eines Personenbezugs,
- Dokumentation jedes Schrittes des Gesamtprozesses hinsichtlich Motive, Ziele, Analysen und Ergebnisse,
- Hinreichende Vornahme der Interessenabwägung,
- Einbindung des Datenschutzbeauftragten und des Betriebsrats.

8.5.2 Überwachung mittels RFID

RFID ist die Abkürzung für „Radio Frequency Identification“ und steht für technische Verfahren, in denen durch Funkwellen eine kontaktlose Kommunikation zwischen RFID-Transponder und den dazugehörigen Lese- und / oder Schreibgeräten ermöglicht wird.

Die Überwachung von Arbeitnehmern mittels RFID stellt ebenfalls einen erheblichen Eingriff in das Persönlichkeitsrecht der Arbeitnehmer dar. Will der Arbeitgeber die RFID-Transponder während der Arbeitszeit zur Überwachung von Arbeitnehmern einsetzen, kann sich die Zulässigkeit der Überwachung aus Art. 6 Abs. 1 lit. b) DS-GVO oder aus einer Betriebs- oder Dienstvereinbarung ergeben. Hierzu müssen die Erhebung und Verarbeitung der Arbeitnehmerdaten mithilfe der RFID-Transponder „erforderlich“ sein. Da bei der RFID-Überwachung nur die Anwesenheit einer Identifikationsnummer an einem bestimmten Ort zu einer bestimmten Zeit festgestellt werden kann und eine sichere Identifizierung einer bestimmten Person nicht möglich ist, stellen die RFID-Systeme gegenüber der Videoüberwachung ein weniger belastendes Mittel dar.

Der Einsatz der RFID-Systeme muss zudem angemessen sein. Die Angemessenheit lässt sich jedoch nur im Einzelfall unter Berücksichtigung der mit dem Einsatz verfolgten Zwecke feststellen. Erfolgt die RFID-Überwachung beispielsweise dazu, wertvolle Arbeitsmittel zu verfolgen, ist es angemessen, dieses mit einem aktiven RFID-Transponder zu versehen, der regelmäßig oder gar in Echtzeit überwacht wird. Nicht angemessen, und damit nicht zulässig, ist es hingegen, eine flächendeckende RFID-Überwachung zu installieren. Diese dient lediglich dazu, lückenlose Bewegungsprofile von Arbeitnehmern zu erstellen, was grundsätzlich nicht zulässig ist.

8.5.3 Einsatz von Ortungssystemen im Arbeitsverhältnis

GPS ist die Abkürzung für „Global Positioning System“ und ermöglicht eine satellitengestützte Positionsbestimmung. Im Arbeitsverhältnis wird diese Technik nicht selten zur Lokalisierung von Arbeitnehmern und damit zu Überwachungszwecken eingesetzt. Sogenannte standortbezogene Dienste im Mobilfunk („Location Based Services“) erlauben eine Orts- und Zeiterfassung des Mobiltelefons (Handys) in Abhängigkeit von den Funkzellen des Mobilfunkdienstanbieters. Durch Auswertung der von GPS-Satelliten abgestrahlten und vom GPS-Empfangsgerät aufgezeichneten Signale kann festgestellt werden, zu welchem Zeitpunkt sich das Empfangsgerät, das etwa in einem von einem Arbeitnehmer genutzten Fahrzeug angebracht ist, an welchem Ort befunden hat. Das System ermöglicht

damit, den genauen Aufenthalt von Arbeitnehmern in zeitlicher und örtlicher Hinsicht auch ohne menschliche Kontrolle permanent abzubilden und zu verfolgen. Auch wenn sich diese Angaben unmittelbar nur auf das Empfangsgerät beziehen, entsteht durch die Gerätezuordnung zu den jeweiligen Arbeitnehmern regelmäßig ein Personenbezug.

Grundsätzlich setzt der Einsatz von Ortungstechnik, sobald damit die Ortung von Arbeitnehmern verbunden ist, nach Art. 6 Abs. 1 DS-GVO voraus, dass ein Erlaubnistatbestand vorliegt, der die Verarbeitung von Daten zulässt oder dass die betroffenen Arbeitnehmer eingewilligt haben.

Im Rahmen der Prüfung der Zulässigkeit der Datenerhebung und -verarbeitung kommt es im Einzelnen auf den Zweck der Datenverarbeitung, die technischen Möglichkeiten des Systems und dessen tatsächlichen Gebrauch an. So wäre es datenschutzrechtlich unproblematisch, wenn die Ortung durch das System technisch etwa erst nach einem Kfz-Diebstahl einsetzen würde. Andere Einsatzmöglichkeiten sind in der Logistik denkbar, beispielsweise können Speditionen zur Warenverfolgung ihren Fuhrpark orten. Solche der Ortung von Gegenständen dienende Zwecke, die offensichtlich im berechtigten Interesse des Unternehmens liegen, sind grundsätzlich zulässig.

Systeme, die nur zum Zwecke der allgemeinen persönlichen Überwachung von Arbeitnehmern eingesetzt werden (wie etwa Geschwindigkeitsaufzeichnungen, Dauer von Fahrtunterbrechungen), sind grundsätzlich unzulässig. Ein System, das beispielsweiseüber eine Alarmierungsfunktion verfügt, die den Arbeitgeber informiert, wenn Arbeitnehmer eine definierte Zone verlassen oder sich zu lange in einer solchen aufhalten, würde einen permanenten Kontrolldruck erzeugen und ist deswegen nicht zulässig.

Der Einsatz von Ortungstechnik, die der gezielten Überwachung des Verhaltens von Arbeitnehmern dient, kommt nur in ganz begründeten Einzelfällen in Betracht. Solche Kontrollen sind nur dann zulässig, wenn sie unter Beachtung des Verhältnismäßigkeitsgrundsatzes geeignet und erforderlich sind, um etwa konkreten Verdachtsmomenten auf arbeitsrechtliche Verfehlungen nachzugehen. Es müssen tatsächliche Anhaltspunkte bestehen, die den Verdacht rechtfertigen, dass die überwachten Personen gegen ihre arbeitsrechtlichen Pflichten verstoßen. In solchen Fällen ist außerdem der Betriebsrat vor Beginn der Überwachungsmaßnahme zu beteiligen.

9 Der betriebliche Datenschutzbeauftragte

Bestellpflicht und Aufgaben

Die Kontrolle der Einhaltung der in den Betrieben zu beachtenden Bestimmungen des Datenschutzes obliegt

- den Unternehmen / dem Arbeitgeber selbst (Art. 4 Nr. 7 DS-GVO),
- dem betrieblichen Datenschutzbeauftragten (Art. 37 DS-GVO),
- den externen Aufsichtsbehörden und
- dem Betriebsrat (§§ 75 Abs. 2, 80 Abs. 1 Nr. 1 und Abs. 2 BetrVG).

9.1 Voraussetzungen für die Bestellpflicht

Unternehmen sind nach Art. 37 DS-GVO dazu verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen, wenn die Datenverarbeitung im Unternehmen ein bestimmtes Gefährdungspotential birgt. Das ist dann der Fall, wenn

- die Kerntätigkeit des Arbeitgebers in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und / oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder
- die Kerntätigkeit des Arbeitgebers in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftagen gemäß Art. 10 DS-GVO besteht.

Zudem muss gem. § 38 Abs. 2 BDSG i. V. m. § 6 BDSG ein Datenschutzbeauftragter bestellt werden, soweit sich in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

Hinweis

Die Schwelle wurde durch das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz EU von zehn auf 20 ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen Personen erhöht.

Tipp für die Praxis

Beispiele für die Bestellpflicht nach Art. 37 Abs. 1 lit. b) DS-GVO:

- Auskunfteien
- Detekteien
- Versicherungsunternehmen
- Marketingunternehmen

Beispiele für die Bestellpflicht nach Art. 37 Abs. 1 lit. c) DS-GVO:

- Gesundheitseinrichtungen
- Dienstleister mit biometrischen ID-Management
- Anbieter von Erotikartikeln

Hinweis

Wird ein Datenschutzbeauftragter nicht bestellt, obwohl die verpflichtenden Voraussetzungen des Art. 37 hierfür vorliegen, kann dies als Ordnungswidrigkeit mit einer Geldbuße bis zu 10.000.000,00 Euro geahndet werden (Art. 83 Abs. 4 DS-GVO i. V. m. § 41 BDSG).

9.2 Aufgaben des Datenschutzbeauftragten

Die allgemeinen Aufgaben des Datenschutzbeauftragten sind in Art. 39 DS-GVO geregelt. Er hat insbesondere

- zu unterrichten und zu beraten, Art. 39 Abs. 1 lit. a) DS-GVO,

- die Einhaltung des Datenschutzes zu überwachen, d. h. die Vorschriften der DS-GVO, anderer Datenschutzvorschriften der Union bzw. der Mitgliedsstaaten, sowie die Strategien des Arbeitgebers oder seiner Auftragsverarbeiters, einschließlich der Sensibilisierung (Schulungsfunktion),

- bei der Durchführung einer Datenschutzfolgenabschätzung nach Art. 35 DS-GVO zu beraten, Art. 39 Abs. 1 lit. c) DS-GVO,

- mit der Aufsichtsbehörde zusammenzuarbeiten, Art. 39 Abs. 1 lit. d) und e) DS-GVO (s. auch Art. 57 Abs. 3 DS-GVO),

- bei alledem risikoorientiert vorzugehen, Art. 39 Abs. 2 DS-GVO.

9.3 Person des Datenschutzbeauftragten

Zum Datenschutzbeauftragten kann sowohl ein Beschäftigter des Unternehmens, als auch eine Person außerhalb des Unternehmens – ein „Externer“ – bestellt werden. Als persönliche Voraussetzungen fordert das Gesetz Fachkunde und Zuverlässigkeit (Art. 37 Abs. 6 DS-GVO).

Für die erforderliche Fachkunde benötigt der Datenschutzbeauftragte ein allgemeines Grundwissen (z. B. Datenschutzrecht, Verständnis für betriebswirtschaftliche Zusammenhänge, Grundkenntnisse über Verfahren und Techniken der automatisierten Datenverarbeitung). Darüber hinaus muss er auch mit der Organisation und den Funktionen des Betriebes vertraut sein und sich einen Überblick über alle Fachaufgaben verschaffen, zu deren Erfüllung personenbezogene Daten verarbeitet werden (vgl. Art 37 Abs. 5 DS-GVO).

Neben der Fachkunde muss der Datenschutzbeauftragte auch die zur Erfüllung seiner Aufgaben erforderliche Zuverlässigkeit besitzen. Das umfasst zum einen charakterliche Zuverlässigkeit und persönliche Integrität – zum anderen darf der Datenschutzbeauftragte bei seiner Tätigkeit nicht in einen Interessenkonflikt geraten (siehe auch Art. 38 Abs. 6 DS-GVO). Das Problem stellt sich insbesondere, wenn ein Beschäftigter „nebenamtlich“ zum Datenschutzbeauftragten bestellt werden soll. Die Tätigkeit als Datenschutzbeauftragter bringt es mit sich, gegebenenfalls auch gegen die Interessen bzw. Auffassungen des Arbeitgebers zu handeln. Daher ist eine Interessenkollision bei bestimmten Personen vorprogrammiert, weshalb diese nicht zum Datenschutzbeauftragten bestellt werden dürfen. Die Zuverlässigkeit des Datenschutzbeauftragten bedingt auch, dass ihm die hierfür erforderliche Arbeitszeit, z. B. durch Freistellung von bisheriger Tätigkeit, gewährt wird.

Der Datenschutzbeauftragte hat ein Fort- und Weiterbildungsrecht auf Kosten des Unternehmens.

Praxishinweis

Nicht als interner Datenschutzbeauftragter bestellt werden dürfen zum Beispiel

- Unternehmensinhaber,
- Vorstand,
- Geschäftsführer,
- Leiter der EDV,
- Personalleiter.

9.4 Bestellung und Widerruf des Datenschutzbeauftragten

Die Bestellung des Datenschutzbeauftragten ist formlos möglich, sollte aus Dokumentationsgründen zumindest aber in Textform erfolgen.

Anforderungen an die Dauer der Bestellung enthält die DS-GVO nicht. Einen Benachteiligungs- und Abberufungsschutz gibt es nur noch nach Maßgabe von Art. 38 Abs. 3 S. 2 DS-GVO.

Der deutsche Gesetzgeber hält durch den Verweis in § 38 Abs. 2 BDSG auf § 6 Abs. 4 BDSG an dem Fortwirken eines besonderen Kündigungsschutzes für den Datenschutzbeauftragten über die Amtszeit hinaus für ein Jahr fest. Somit ändert sich auch in diesem Bereich nichts für den Datenschutzbeauftragten.

Tipp für die Praxis

Soll ein Beschäftigter des Unternehmens zum Datenschutzbeauftragten bestellt werden, sind neben den Bestimmungen der DS-GVO und des BDSG auch die arbeitsrechtlichen Regelungen zu beachten. Die Bestellung eines Beschäftigten zum Datenschutzbeauftragten ist in der Regel nicht vom Direktionsrecht des Arbeitgebers umfasst, so dass der Beschäftigte der Beauftragung zustimmen muss (= Ergänzung des Arbeitsvertrages). Soll dem Beschäftigten die Sonderaufgabe des Datenschutzbeauftragten wieder entzogen werden, ist neben dem Widerruf nach der DS-GVO auch eine Teilkündigung dieser nunmehr arbeitsvertraglich geschuldeten Sonderaufgabe erforderlich.

9.5 Die organisatorische Stellung des Datenschutzbeauftragten

Der Datenschutzbeauftragte wäre angesichts seiner Sonderstellung innerhalb des Betriebes überfordert, wenn er die ihm gesetzlich übertragenen Aufgaben nur durch persönlichen Einsatz erfüllen müsste. Art. 38 DS-GVO legt daher fest, dass der Datenschutzbeauftragte

- organisatorisch direkt der Unternehmensleitung zu unterstellen ist, Art. 38 Abs. 3 S. 3 DS-GVO,
- in der Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei ist, Art. 38 Abs. 3 S. 1 DS-GVO,
- wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden darf, Art. 38 Abs. 3 S. 2 DS-GVO,
- von der Unternehmensleitung bei der Erfüllung seiner Aufgaben zu unterstützen ist, Art. 38 Abs. 2 DS-GVO.

10 Die Personalakte

Inhalt und Vertraulichkeit

Arbeitgeber in der Privatwirtschaft sind nicht verpflichtet, Personalakten zu führen. Für eine erfolgreiche Personalplanung und -verwaltung des Arbeitgebers ist in aller Regel aber eine systematische Anlage und Führung von Personalakten unerlässlich.

10.1 Inhalt der Personalakte und Rechte der betroffenen Beschäftigten

Inhalt der Personalakte können alle Unterlagen werden, die sich unmittelbar auf das Arbeitsverhältnis beziehen und an deren Aufnahme der Arbeitgeber ein sachliches, berechtigtes Interesse hat. Das Persönlichkeitsrecht des Beschäftigten und sein Interesse am Schutz seiner Privatsphäre begrenzt hierbei den Umfang der Unterlagen, die der Arbeitgeber legitimerweise in die Personalakte aufnehmen darf. Jedenfalls darf der Arbeitgeber solche Unterlagen aufnehmen, nach denen er im Rahmen seines Fragerechts auch zulässigerweise fragen darf. Ferner darf der Arbeitgeber den Beschäftigten im laufenden Arbeitsverhältnis hinsichtlich Eignung, Befähigung und fachlicher Leistung beurteilen und diese Beurteilungen zu der Personalakte nehmen.

Inhalt der Personalakte – Beispiele

- Bewerbungsunterlagen
- Personalfragebogen
- Zeugnisse, Bescheinigungen
- Arbeitsvertrag
- Beurteilungen
- Abmahnungen, Rügen
- Urlaubsanträge
- Krankheitsbescheinigungen
- Lohn- und Gehaltsveränderungen

Die in der Personalakte enthaltenen Beschäftigtendaten müssen inhaltlich richtig sein und ein zutreffendes Bild über den Beschäftigten in dienstlichen und persönlichen Beziehungen abgeben. Die Art. 16 ff. DS-GVO enthalten ausführliche Vorschriften über Berichtigung, Löschung und Einschränkungen von Daten, wenn sie unrichtig oder unzulässig verarbeitet worden sind. Nationale Detaillierungen enthalten die §§ 32 ff BDSG. Neben den als Rechte der betroffenen Person ausgestalteten Vorschriften treffen den Arbeitgeber aus Art. 5 DS-GVO auch originär durch ihn zu erfüllende Pflichten. So muss er nach Art. 5 Abs. 1 lit. d) DS-DGVO selbst dafür sorgen, dass die Daten stets richtig sind. Ebenso dürfen personenbezogene Daten – unabhängig von der Ausübung eines Löschungsanspruch durch die

betroffene Person – nur so lange gespeichert bleiben, wie dies erforderlich ist, Art 5 Abs. 1 lit. e) DS-GVO.

Der Beschäftigte kann die Entfernung unrichtiger, ihn zu Unrecht belastender oder unzulässig aufgenommener Unterlagen aus der Personalakte verlangen. Er kann außerdem die Entfernung einer Abmahnung verlangen, wenn der Arbeitgeber kein schutzwürdiges Interesse mehr an deren Verbleib in der Akte hat. Eine feste Frist gibt es hierfür nicht. Vielmehr muss dies anhand einer Gesamtabwägung im Einzelfall bestimmt werden. Berücksichtigt werden dabei insbesondere die Umstände des konkreten Falles, die Schwere des Vorwurfs und die Beeinträchtigung der Interessen des Beschäftigten. Ein lange zurückliegender, nicht schwerwiegender und durch beanstandungsfreies Verhalten faktisch überholter Pflichtverstoß kann seine Bedeutung auch für eine später erforderlich werdende Interessenabwägung gänzlich verlieren. Eine nicht unerhebliche Pflichtverletzung im Vertrauensbereich hingegen ist länger zu berücksichtigen.

Hinweis: Entfernung einer Abmahnung

Eine Abmahnung muss nicht allein wegen Zeitablaufs aus der Personalakte entfernt werden. Nach der Emmely-Entscheidung des Bundesarbeitsgerichts wird im Rahmen der Interessenabwägung bei der Entscheidung über die Rechtsmäßigkeit einer fristlosen Kündigung dem „erarbeiteten Vorrat an Vertrauen“ durch ein über lange Jahre unbeanstandet geführtes Arbeitsverhältnis maßgebliche Bedeutung beigemessen.

Das Recht des Beschäftigten nach § 83 Abs. 2 BetrVG seiner Personalakte eigene Erklärungen beizufügen besteht auch im Geltungsbereich des BDSG.

10.2 Vertraulichkeit der Personalakte

Der Arbeitgeber hat Personalakten sowohl innerhalb des Betriebes als auch gegenüber Externen vertraulich zu behandeln. Der Kreis der zugriffsberechtigten Personen ist möglichst klein zu halten und auf die für Personalentscheidungen zuständigen Beschäftigten zu beschränken (sogenanntes Need-to-know-Prinzip).

Hinweis

Für besonders schützenswerte Informationen (Daten / Dokumente) innerhalb der Personalakte, wie z. B. Gesundheitsdaten von Mitarbeitern, müssen erweiterte Schutzmaßnahmen Anwendung finden, damit sie nicht bei der regelmäßigen Sachbearbeitung der Personalakte ohne konkreten Anlass ins Auge fallen. Ein sinnvolles Verfahren ist der Kennwortschutz auf Objektebene. Der Mitarbeiter der Personalverwaltung setzt bei entsprechend sensiblen Informationen ein Merkmal, welches die Eingabe eines globalen Kennwortes bei

jedem Zugriff verlangt, um diese Informationen sehen zu können – unabhängig davon, ob man aufgrund der linearen Rechte alle Dokumente der Akte sehen darf. Dieses Kennwort ist nur einem kleinen Benutzerkreis bekannt und sollte in einem geschützten Bereich (Aktenschrank, Tresor, etc.) schriftlich hinterlegt werden.

Unter der Geltung der DS-GVO wird das Gebot der Vertraulichkeit und Integrität durch Art. 5 Abs. 1 lit. e) und die Bedingung der Erforderlichkeit der Datenverarbeitung für die Entscheidung über die Begründung, die Durchführung oder die Beendigung von Arbeitsverhältnissen durch Art. 6 Abs. 1 lit. b) DS-GVO sichergestellt. Des Weiteren fallen die betriebsinterne und externe weitere Verarbeitung von Beschäftigtendaten (= Nutzen und Übermitteln) unter das „Verbot mit Erlaubnisvorbehalt“ (Art. 6 Abs. 1 DS-GVO).

10.3 Elektronische Personalakte

In Zeiten der Digitalisierung hält die elektronische Personalakte in vielen Personalabteilungen Einzug. Durch die Verwendung der elektronischen Personalakte ergeben sich viele Verwendungs- und Verknüpfungsmöglichkeiten, welche die Arbeit der Personalabteilung deutlich erleichtern.

Die Einführung einer elektronischen Personalakte ist in datenschutzrechtlicher Hinsicht möglich und zulässig, wenn die Speicherung der Daten des Arbeitnehmers der Zweckbestimmung des Beschäftigungsverhältnisses entspricht, vgl. Art. 6 Abs. 1 lit. b) DS-GVO.

Im Hinblick auf den Inhalt einer elektronischen bzw. digitalen Personalakte ergeben sich im Vergleich zur Papierakte keine Besonderheiten. Auch bei einer digitalen Datendokumentation muss ein unmittelbarer innerer Zusammenhang zum Arbeitsverhältnis bestehen, das allgemeine Persönlichkeitsrecht darf nicht verletzt werden und die Vorgaben der DS-GVO und des BDSG müssen eingehalten werden.

Bei der Verwendung einer elektronischen Personalakte ist zu beachten, dass in einigen gesetzlichen Vorschriften geregelt ist, dass die Daten trotz der Aufbewahrung in digitaler Form auch (noch zusätzlich) im Original beim Arbeitgeber vorliegen müssen. Dies gilt z. B. für sozialversicherungsrechtliche Nachweise. Zur Vermeidung etwaiger Beweisschwierigkeiten im Prozess empfiehlt es sich, Originaldokumente, deren formelle Wirksamkeit von der Einhaltung der strengen Schriftform nach § 126 BGB abhängt, weiterhin aufzubewahren – gegebenenfalls neben deren digitaler Archivierung.

Praxistipp

– Unterlagen, deren Aufbewahrung im Original zwingend ist.
  Grundsätzlich sind sozialversicherungsrechtliche Nachweise nach § 28f SGB IV, wie zum Beispiel Lohn- und Beitragsabrechnungsunterlagen sowie Meldungen an die Krankenkasse und Berufsgenossenschaft bis zum Ablauf des auf die letzte

Sozialversicherungsprüfung (§ 28 p SGB IV) folgenden Kalenderjahres im Original aufzubewahren. Gemäß § 9 Abs. 5 Beitragsverfahrensordnung (BVV) kann die Aufbewahrung sozialversicherungsrechtlicher Entgeltunterlagen (§ 28f SGB IV i. V. m. § 8 BVV) unter Einhaltung bestimmter Voraussetzungen aber auch in elektronischer Form erfolgen.

– Unterlagen, deren Aufbewahrung im Original zweckmäßig ist.
  Bei Dokumenten mit konstitutivem Schriftformerfordernis empfiehlt es sich aus Beweiszwecken, die Originale weiterhin in einer analogen Personalakte aufzubewahren. Beispiele hierfür sind:
  – Kündigung (§ 623 BGB)
  – Aufhebungsvertrag (§ 623 BGB)
  – Befristung eines Arbeitsvertrages (§ 14 Abs. 4 TzBfG)
  – Nachvertragliches Wettbewerbsverbot (§ 74 Abs. 1 HGB)
  – Geltendmachung von Elternzeit (§ 16 Abs. 1 BEEG)

  Weitere konstitutive Schriftformerfordernisse können sich beispielsweise aus Tarifverträgen ergeben.

– Unterlagen, die – auch wenn häufig davon ausgegangen wird – nicht im Original aufbewahrt werden müssen.
  Trotz etwaiger gesetzlich angeordneter Aufbewahrungspflichten für bestimmte Unterlagen, z. B. Lohnberechnungsunterlagen (§ 147 AO), Quittungsbelege über den Arbeitslohn (§ 257 HGB), betriebliche Altersversorgung (§ 11 BetrAVG) besteht keine Pflicht zu deren Aufbewahrung im Original. Gleiches gilt für Unter lagen nach dem Jugendarbeitsschutzgesetz (§ 50 Abs. 2 JArbSchG), dem Mutterschutzgesetz (§ 19 Abs. 2 MuSchG) sowie Arbeitnehmerüberlassungsunterlagen (§ 7 Abs. 2 AÜG).

10.4 Einsichtsrecht des Arbeitnehmers

Der Arbeitnehmer kann jederzeit Einsicht in seine Personalakte nehmen, vgl. § 83 Abs. 1 BetrVG und § 26 Abs. 2 SprAuG. Er ist berechtigt, bei der Einsichtnahme ein Mitglied des Betriebsrats bzw. des Sprecherausschusses hinzuzuziehen. Schwerbehinderte Arbeitnehmer können zudem die Schwerbehindertenvertretung hinzuziehen, vgl. § 95 Abs. 3 S. 1 SGB IX. § 83 Abs. 1 S. 1 BetrVG gibt dem einzelnen Arbeitnehmer das höchstpersönliche Recht zur Einsichtnahme in die über ihn geführten Personalakten. Die Vorschrift gilt auch in betriebsratslosen Betrieben und unabhängig davon, ob der Betrieb überhaupt betriebsratsfähig ist. Leiharbeitnehmern steht im Entleiherbetrieb kein Anspruch auf Einsichtnahme und Erklärung zu, § 14 Abs. 2 S. 3 AÜG Der Arbeitgeber kann die Hinzuziehung eines Rechtsanwalts des Arbeitnehmers zur Einsichtnahme jedenfalls dann verweigern, wenn dem Arbeitnehmer gestattet wurde, Fotokopien vom Inhalt seiner Personalakte anzufertigen.

Die hinzugezogenen Personen müssen über den Inhalt der Personalakte Stillschweigen bewahren, es sei denn sie wurden von dem Arbeitnehmer im Einzelfall von dieser Schweigepflicht entbunden.

Im Geltungsbereich der DS-GVO hat der Arbeitnehmer zusätzlich das Auskunftsrecht gemäß Art. 15 DS-GVO gegenüber seinem Arbeitgeber bezüglich der über ihn gespeicherten Daten.

Der betroffene Beschäftigte kann von dem Arbeitgeber eine Bestätigung darüber verlangen, ob ihn betreffende personenbezogene Daten verarbeitet werden und, wenn dies der Fall ist, welche Daten dies sind. Darüber hinaus sind vom Arbeitgeber nach Art. 15 Abs. 1 DS-GVO vor allem noch folgende Informationen mitzuteilen:

- die Verarbeitungszwecke,
- die Kategorien personenbezogener Daten, die verarbeitet werden,
- die gegebenen und möglichen Datenempfänger bzw. Kategorien von Empfängern,
- soweit möglich die geplante Speicherdauer,
- Informationen über die Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung sowie ein Widerspruchsrecht,
- das Beschwerderecht bei der Aufsichtsbehörde,
- die Herkunft der Daten, soweit diese nicht von der betroffenen Person selbst erhoben wurden,
- soweit zutreffend über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling.

Auskunftserteilungen müssen gemäß Art. 12 Abs. 3 DS-GVO unverzüglich erfolgen, spätestens aber innerhalb eines Monats. Nur in begründeten Ausnahmefällen kann die Monatsfrist überschritten werden.

11 Privatnutzung von Telefon, Telefax, E-Mail und Internet

Kontrollmöglichkeiten

Bei der Nutzung von Telefon, E-Mail und Internet werden automatisch Nutzungs-, Verbindungs- und Inhaltsdaten erfasst und gespeichert, insbesondere wenn der Arbeitgeber sogenannte Proxyserver oder technische Überwachungssysteme (z. B. Firewall-System) einsetzt.

Telefon / Telefax

- Telefon- bzw. Telefaxnummern des Anrufers und Angerufenen
- Information, dass ein Verbindungsversuch fehlgeschlagen ist (z. B. besetzt, Angerufener nimmt nicht ab)
- Datum, Beginn und Ende einer Verbindung
- Gebühren

E-Mail

- E-Mail-Adressen des Absenders und Empfängers
- Datum und Uhrzeit des E-Mail-Verkehrs
- Inhalt der E-Mail

Internet

- IP-Adresse des benutzten Rechners
- Adresse der besuchten Websites
- Datum, Beginn und Ende der Internetverbindung
- Umfang des Datenverkehrs

Unabhängig von der Frage, ob der Arbeitgeber die private Nutzung von Telefon, E-Mail und Internet gestattet, darf er diese Daten zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage vorübergehend in Protokolldateien speichern (vgl. Art. 32 DS-GVO). Diese Protokolldateien sind hinsichtlich ihrer Nutzung allerdings streng zweckgebunden und dürfen ohne Einwilligung oder betriebliche Regelung nur zu diesen genannten Zwecken verwendet werden.

Sollen die Protokolldaten auch für Auswertungen im Rahmen einer zulässigen Leistungs- und Verhaltenskontrolle der Beschäftigten zur Verfügung stehen, muss diese Nutzungsmöglichkeit zuvor am besten durch entsprechende Betriebsvereinbarungen festgelegt werden (strenge Zweckbindung der Protokolldateien). Eine nachträgliche zweckfremde Verwendung der Protokolldaten ist nur ausnahmsweise unter Rückgriff auf Art. 6 Abs. 1 und 4 DS-GVO zulässig.

Es empfiehlt sich daher, die technischen und organisatorischen Fragen der Protokollierung und Auswertung von vornherein ausdrücklich in einer Betriebsvereinbarung zu regeln.

Sobald die Protokolldateien nicht mehr benötigt werden, sind sie zu löschen oder einzuschränken.

Träger von Berufsgeheimnissen (z. B. Betriebsärzte, Psychologen, Geistliche, Sozialarbeiter) sind – zumindest hinsichtlich der Daten der Gesprächs- oder E-Mail-Partner – aus der Telefon- und E-Mail-Datenerfassung herauszunehmen. Diese Sonderstellung hat nach der Rechtsprechung des BAG zwei Gründe:

– Das besondere Vertrauensverhältnis zwischen Betriebsarzt und Arbeitnehmer
  Insbesondere für Werksärzte und Psychologen gilt: soll eine ärztliche Behandlung Aussicht auf Erfolg haben, dann ist hierfür ein besonderes Vertrauensverhältnis zwischen Arzt / Psychologe und dem betreuten Patienten erforderlich. Ein solches Vertrauensverhältnis kann jedoch nur entstehen, wenn ein Patient davon ausgehen kann, dass seine Behandlung vertraulich ist – also auch dem Arbeitgeber gegenüber geheim bleibt.

– Schweigepflicht nach § 203 StGB / Fürsorgepflicht des Arbeitgebers
  Die in § 203 Strafgesetzbuch (StGB) genannten Träger von Berufsgeheimnissen unterliegen einer besonderen Schweigepflicht, deren Verletzung sogar unter Strafe gestellt ist. Unter diese Schweigepflicht fällt bereits die Tatsache, dass ein Arbeitnehmer die Beratung oder Behandlung des Werksarztes, Werkspsychologen, etc. in Anspruch nimmt. Dieses Berufsgeheimnis muss der Werksarzt, Werkspsychologe, etc. auch gegenüber dem Arbeitgeber wahren. Das wiederum hat zur Folge, dass der Arbeitgeber kraft seiner Fürsorgepflicht alles zu unterlassen hat, was den Geheimnisträger in Konflikt mit seiner Geheimhaltungspflicht bringen kann. Dazu gehört auch, dass der Arbeitgeber die Arbeitsbedingungen seiner Berufsgeheimnisträger entsprechend vertraulich ausgestaltet, beispielsweise muss er vermeiden, dass Werksärzte / Werkspsychologen etc. bei der Nutzung der ihnen zur Verfügung gestellten Arbeitsmittel unwillkürlich und unvermeidlich preisgeben, wen sie betreuen. Würden Daten der Telefon- und E-Mail-Partner von dem Arbeitgeber erfasst, wäre das aber der Fall, daher sind sie aus der Datenerfassung auszunehmen.

11.1 Privatnutzung nicht erlaubt

Ob und inwieweit der Arbeitgeber die Arbeitnehmer bei der Nutzung bereitgestellter Kommunikationstechniken, wie z. B. Telefon, E-Mail und Internet, kontrollieren und überwachen darf, hängt wesentlich davon ab, ob den Arbeitnehmern neben der dienstlichen auch die private Nutzung am Arbeitsplatz gestattet ist.

Sind dem Arbeitnehmer Telefon, E-Mail und Internet ausschließlich zur dienstlichen Nutzung überlassen, richtet sich die Zulässigkeit der Datenverarbeitung zu Kontrollzwecken nach dem BDSG und dem allgemeinen Anspruch des Arbeitnehmers auf Persönlichkeitsrechtsschutz. Damit beruht die Zulässigkeit einer Kontrolle regelmäßig auf einer

Einzelfallentscheidung, bei der die Erforderlichkeit der Datenverarbeitung und das Interesse der Arbeitnehmer an einer möglichst geringen Überwachung gegeneinander abgewogen und in Ausgleich gebracht werden müssen.

Bei ausschließlich dienstlicher Nutzung darf der Arbeitgeber stichprobenartig prüfen, ob das Telefonieren, E-Mail-Versenden oder Internet-Surfen auch tatsächlich dienstlicher Natur ist. Eine automatisierte Vollkontrolle bzw. eine Totalüberwachung der Arbeitnehmer ist aber als schwerwiegender Eingriff in das Persönlichkeitsrecht der Arbeitnehmer allenfalls bei konkretem Missbrauchsverdacht im Einzelfall zulässig.

Zu diesem Zweck können beispielsweise die Protokolldateien, die für die Datensicherheit erhoben werden, stichprobenhaft und zeitnah ausgewertet werden. Aufgrund der strengen Zweckbindung dieser Protokolldateien ist dies aber nur zulässig, wenn diese Auswertungsmöglichkeit zuvor schon festgelegt war.

Grundsätzlich gilt jedoch: präventive Maßnahmen sind nachträglichen Kontrollen vorzuziehen, z. B. Positivlisten erlaubter Internetadressen, Sperren bestimmter Internetadressen.

11.1.1 Konkreter Missbrauchsverdacht, Kostenkontrolle

Der Arbeitgeber darf Verbindungs-, Nutzungs- und Inhaltsdaten zu Zwecken der Kostenkontrolle verarbeiten, z. B. zur Aufklärung einer Kostensteigerung.

Wenn der Arbeitgeber beispielsweise eine allgemeine Kostensteigerung feststellt, dann muss er zunächst prüfen, ob er statt der Kontrolle der Daten auch präventive Maßnahmen ergreifen könnte, die regelmäßig einen weniger starken Eingriff in das Recht der Arbeitnehmer auf Datenschutz darstellen (z. B. temporäre Zugangssperren zum Internet).

Kann die Kostensteigerung einem bestimmten Arbeitnehmer zugeordnet werden, kann dies einen Missbrauchsverdacht begründen, der die Kontrolle der Verbindungs-, Nutzungs- und Inhaltsdaten rechtfertigt.

Bei konkret vorliegendem Missbrauchsverdacht wegen schwerwiegender Verfehlungen der Arbeitnehmer dürfen Verbindungs-, Nutzungs- und Inhaltsdaten kontrolliert werden.

11.1.2 Kenntnisnahme des Inhalts von E-Mails

Zu der Frage, in welchem Umfang der Arbeitgeber den dienstlichen E-Mail-Verkehr kontrollieren darf, liegt Rechtsprechung bislang nicht vor. Hier wird man jedoch eine Parallele zu den Kontrollmöglichkeiten bei dienstlichem Schriftverkehr ziehen können: von ein- und ausgehenden dienstlichen E-Mails seiner Arbeitnehmer darf der Arbeitgeber in demselben Maß Kenntnis nehmen wie von deren dienstlichen Schriftverkehr. Beispielsweise kann der Vorgesetzte verfügen, dass ihm jede ein- und ausgehende dienstliche E-Mail seiner

Arbeitnehmer zur Kenntnis gegeben wird. Persönlichkeitsrechte werden dann nicht verletzt, wenn die Arbeitnehmer über dieses Verfahren des Arbeitgebers informiert sind.

In der Praxis sollte diese Information der Arbeitnehmer in einfacher allgemeiner Form, beispielsweise durch eine Mitteilung, aber auch durch eine entsprechende Klausel in einer Betriebsvereinbarung erfolgen.

Zulässig ist auch die Einsichtnahme in das elektronische Postfach des Arbeitnehmers aus dringenden betrieblichen Gründen, insbesondere bei krankheitsbedingter oder urlaubsbedingter Abwesenheit des Arbeitnehmers.

11.1.3 Mithören und Aufzeichnen betrieblicher Telefonate

Beim Mithören und Aufzeichnen von betrieblichen Gesprächen greift der Arbeitgeber in das allgemeine Persönlichkeitsrecht des Arbeitnehmers ein, insbesondere in das sogenannte „Recht am gesprochenen Wort“. Demnach entscheidet der Arbeitnehmer auch bei dienstlichen Gesprächen, ob seine Worte allein dem Gesprächspartner oder auch dem Arbeitgeber zugänglich sein sollen oder gar auf Tonträger aufgenommen werden dürfen.

Eingriffe des Arbeitgebers sind nur im Einzelfall zulässig, soweit das Interesse des Arbeitgebers Vorrang vor den Interessen des Arbeitnehmers verdient. Mit Kenntnis bzw. Einwilligung des Arbeitnehmers ist das offene Mithören und Aufzeichnen von dienstlichen Gesprächen beispielsweise zulässig, wenn es „arbeitsplatzimmanent“ ist und dem Grundsatz der Verhältnismäßigkeit hinsichtlich Menge und Auswertung der mitgehörten bzw. aufgezeichneten Gesprächen Rechnung getragen ist (z. B. die Aufzeichnung von Gesprächen beim Telefonbanking zu Beweiszwecken oder das stichprobenartige Mithören zur Ausbildung und Schulung von Arbeitnehmern in Call-Centern).

Nur ausnahmsweise kann das heimliche Mithören und Aufzeichnen von betrieblichen Gesprächen zulässig sein, z. B. zur Ermittlung des Täters sexuell belästigender Anrufe, bei konkretem Verdacht des Verrats von Betriebsgeheimnissen oder bei begründetem Verdacht anderer strafbarer Handlungen.

11.2 Privatnutzung erlaubt

Bei gestatteter Privatnutzung wird der Arbeitgeber gegenüber seinen Beschäftigten zum „Anbieter“ von Telekommunikationsdiensten im Sinne des TTDSG. Als solcher unterliegt er einem weitgehenden Kontrollverbot. Ohne Einwilligung der Beschäftigten darf der Arbeitgeber Nutzungs- und Verbindungsdaten nur wie folgt verarbeiten:

– Soweit die private Nutzung eine Entgeltzahlungspflicht des Beschäftigten nach sich zieht, darf der Arbeitgeber auch die Abrechnungsdaten erheben und bis zur Abrechnung aufbewahren (vgl. § 10 TTDSG).

– Zur Erkennung, Eingrenzung oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen (§ 19 TTDSG),
– zum Aufklären und Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und -dienste (§ 12 TTDSG),
– zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs in Protokolldateien (vgl. Art. 32 DS-GVO).

Hinweis

Eine darüber hinaus gehende Kontrolle, insbesondere eine Leistungs- und Verhaltenskontrolle der Beschäftigten, ist unzulässig – auch die Kontrolle, ob die Beschäftigten den vorgegebenen erlaubten Nutzungsrahmen tatsächlich einhalten. Kontrolliert der Arbeitgeber trotzdem, hat er nicht nur strafrechtliche Konsequenzen zu befürchten, sondern kann die bei einer unzulässigen Kontrolle gewonnenen Beweise in einem nachfolgenden (Kündigungsschutz-)Prozess nicht verwenden (Beweisverwertungsverbot).

Unzulässig wäre auch die Einsichtnahme in das elektronische Postfach des Beschäftigten, die aber insbesondere bei nicht absehbaren, z. B. krankheitsbedingten Abwesenheiten des Beschäftigten regelmäßig erforderlich sein wird, um einen reibungslosen betrieblichen Ablauf zu sichern.

Auch das Ausfiltern von Spam ist bei erlaubter Privatnutzung nicht ohne Einwilligung der Beschäftigten möglich – das Ausfiltern und Löschen einer privaten E-Mail wäre dann ein strafbares Verhalten.

Der Arbeitgeber hat jedoch ein berechtigtes Interesse daran, Missbrauch und strafbare Handlungen nicht nur bei dienstlicher, sondern auch bei privater Nutzung des Internets zu unterbinden, sowie in Abwesenheitszeiten Einsicht in die dienstlichen Mails des Beschäftigten zu nehmen. Daher sollte er die private Nutzung an bestimmte Bedingungen, z. B. hinsichtlich des Zeitrahmens, der zugelassenen Bereiche und regelmäßig durchzuführende Kontrollen knüpfen.

Tipp für die Praxis

Jeder Beschäftigte ist umfassend über die Bedingungen und Kontrollen bei der privaten Nutzung zu informieren. Geregelt werden müssen in jedem Fall folgende Punkte:

– Stichproben bzgl. der Einhaltung des vorgegebenen (Zeit-)Rahmens,
– Archivierung von E-Mails,
– Ausfilterung von Spam,
– Einsichtnahme in das Postfach bei Abwesenheit.

In diese Maßnahmen müssen die Beschäftigten einwilligen. Wenn ein Beschäftigter diese Kontrollmaßnahmen nicht akzeptieren will, dann muss er die private Nutzung unterlassen.

12 Mitwirkungsrechte des Betriebsrats

Mitbestimmung und Kontrolle

Auch in datenschutzrechtlicher Hinsicht bestehen Mitwirkungsrechte des Betriebsrats, die der Arbeitgeber beachten muss.

12.1 Mitbestimmungsrechte

Will der Arbeitgeber in allgemeingültiger Weise das Verhalten der Arbeitnehmer im Betrieb regeln und damit die Ordnung im Betrieb gestalten, so unterliegen derartige Regelungen und Anweisungen einem Mitbestimmungsrecht des Betriebsrats, vgl. § 87 Abs. 1 Nr. 1 BetrVG. Das gilt auch für Regelungen im Rahmen der Arbeitnehmerdatenverarbeitung. Hierunter fallen beispielsweise

- die Einführung von Stechuhren oder anderen automatisierten Zeiterfassungsgeräten sowie biometrischen Zugangskontrollen,
- die Benutzung von Telefon, E-Mail und Internet für private Zwecke, soweit der Arbeitgeber die Privatnutzung gestatten will,
- die Verwendung von Formblättern zur Erfüllung vertraglicher Mitteilungspflichten.

12.1.1 Einführung und Anwendung von technischen Einrichtungen

§ 87 Abs. 1 Nr. 6 BetrVG begründet ein Mitbestimmungsrecht des Betriebsrats bei der Einführung und Anwendung technischer Überwachungseinrichtungen. Entgegen dem Wortlaut des § 87 Abs. 1 Nr. 6 BetrVG kommt es hierfür nach der Rechtsprechung nicht darauf an, ob der Arbeitgeber die technische Einrichtung zur Kontrolle der Arbeitnehmer tatsächlich einsetzen will, sondern nur darauf, ob sie „objektiv“ dafür geeignet ist.

Das ist insbesondere immer dann der Fall, wenn personenbezogene Arbeitnehmerdaten technisch erfasst und festgehalten werden, z. B. durch automatisierte Personalinformationssysteme, in Datenprotokollen einer Internetsoftware, eines Firewall-Systems oder sonstigen Überwachungsprogrammen – sei es auch nur als „Nebenprodukt“. Hierunter fallen beispielsweise

- Fingerprint-Scanner-System als Zugangskontrollsystem,
- Das Aufstellen von Video- und Fernsehkameras,
- Telefonanlagen, die Telefondaten erfassen und / oder das Abhören oder Aufzeichnen von Gesprächen ermöglichen,
- Stechuhren und andere, automatisierte Zeiterfassungsgeräte,
- Technische Sicherungsmaßnahmen,
- Personalabrechnungs- und Personalinformationssysteme (z. B. PAISY, AiSAS, SAP),

– Datenverarbeitungssysteme, EDV-Anlagen,
– Die Einführung von Internet und E-Mail im Betrieb.

Das Mitbestimmungsrecht bei der Einführung einer technischen Einrichtung umfasst das „Ob“ der Anschaffung sowie die hierzu erforderlichen näheren Modalitäten. Dazu gehören Modalitäten über die Zweckbestimmung, die Art und Anzahl einzelner Komponenten / Geräte, der Zeitpunkt der Einführung, der Ort der Verwendung, die Art der Installation, der Zeitraum der Verwendung sowie unmittelbar auf die Einführung bezogene Vorbereitungsmaßnahmen (z. B. Veränderung des Arbeitsplatzes bzw. Arbeitsablaufs).

Die Mitbestimmung bei der Anwendung der technischen Einrichtung umfasst die Art und Weise, in der die Einrichtung zur Überwachung verwendet wird, z. B. generelle oder fallweise Kontrolle, Einschaltzeiten, die Festlegung des zu überwachenden Teils der Arbeitnehmer, Festlegung des Aufstellungsortes.

Im Rahmen des Mitbestimmungsrechts hat der Betriebsrat auch bei der Festlegung des Verwendungszwecks gespeicherter Leistungs- und Verhaltensdaten mitzubestimmen.

Der Betriebsrat hat daher bei der Einführung und Anwendung von Telefonanlagen sowie von E-Mail, Telefon und Internet im Betrieb ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG, wenn in den dabei eingesetzten technischen Systemen Informationen und Daten der Arbeitnehmer erfasst werden, die eine Leistungs- und Verhaltenskontrolle ermöglichen. Das wird regelmäßig der Fall sein, denn die meisten Telefon- und EDV-Anlagen, E-Mail- und Internetsysteme oder Überwachungssysteme erfassen automatisch Verbindungs-, Nutzungs- und Inhaltsdaten der Arbeitnehmer (z. B. in Firewall-Protokollen). Bei der Entscheidung, ob der Arbeitgeber die Privatnutzung von E-Mail, Telefon und Internet erlaubt, ist er aber frei – ein Mitbestimmungsrecht des Betriebsrats besteht diesbezüglich nicht.

Die Mitbestimmung findet ihre Grenze im Persönlichkeitsrecht der einzelnen Beschäftigten (Art. 88 Abs. 2 DS-GVO i. V. m. § 26 Abs. 5 BDSG, § 75 Abs. 2 BetrVG). Unzulässige Eingriffe in das Persönlichkeitsrecht der Beschäftigten können daher nicht durch die Mitbestimmung des Betriebsrats legitimiert werden (z. B. keine gezielte präventive Dauervideoüberwachung der Beschäftigten am Arbeitsplatz; keine automatisierte Vollkontrolle bzw. Totalüberwachung der Beschäftigten durch Auswertung von Verbindungs- und Nutzungsdaten im Rahmen der dienstlichen Nutzung von Telefon, E-Mail und Internet).

Die vom Arbeitgeber initiierte Abschaffung einer technischen Kontrolleinrichtung unterfällt dagegen nicht mehr dem Mitbestimmungsrecht des Betriebsrates.

12.2 Kontroll- und sonstige Beteiligungsrechte

Der Betriebsrat hat im Rahmen des Arbeitnehmerdatenschutzes ferner folgende Kontroll- und Beteiligungsrechte:

- Personalfragebögen bedürfen der Zustimmung des Betriebsrats, vgl. § 94 Abs. 1 BetrVG,
- Die Aufstellung allgemeiner Beurteilungsrichtlinien / -grundsätze bedarf der Zustimmung des Betriebsrats, vgl. § 94 Abs. 2 BetrVG,
- Auswahlrichtlinien bedürfen der Zustimmung des Betriebsrats, vgl. § 95 BetrVG,
- Beratungs- und Unterrichtungsrecht des Betriebsrats bei der Personalplanung gemäß § 92 BetrVG.

Gemäß § 80 Abs. 1 Nr. 1 BetrVG hat der Betriebsrat die Durchführung der zugunsten der Arbeitnehmer geltenden Gesetze und sonstigen Rechtsvorschriften zu überwachen. Dazu gehört auch die Einhaltung des BDSG. Demnach muss der Betriebsrat nicht nur die Rechtmäßigkeit der Verarbeitung von Personaldaten überprüfen, sondern auch die Ordnungsgemäßheit der betrieblichen Datenschutzkontrolle und der Datensicherung.

Ferner ist der Betriebsrat im Rahmen seines Schutzauftrags aus § 75 Abs. 2 BetrVG verpflichtet, die freie Entfaltung der Persönlichkeit der Arbeitnehmer – und damit auch den Persönlichkeitsrechtsschutz bei der automatisierten Datenverarbeitung – zu schützen und zu fördern.

Ansprechpartner/Impressum

Kristina Fink
Grundsatzabteilung Recht

Telefon 089-551 78-234
kristina.fink@vbw-bayern.de

Impressum
Alle Angaben dieser Publikation beziehen sich ohne jede Diskriminierungsabsicht grundsätzlich auf alle Geschlechter.

Herausgeber

vbw
Vereinigung der Bayerischen
Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.vbw-bayern.de