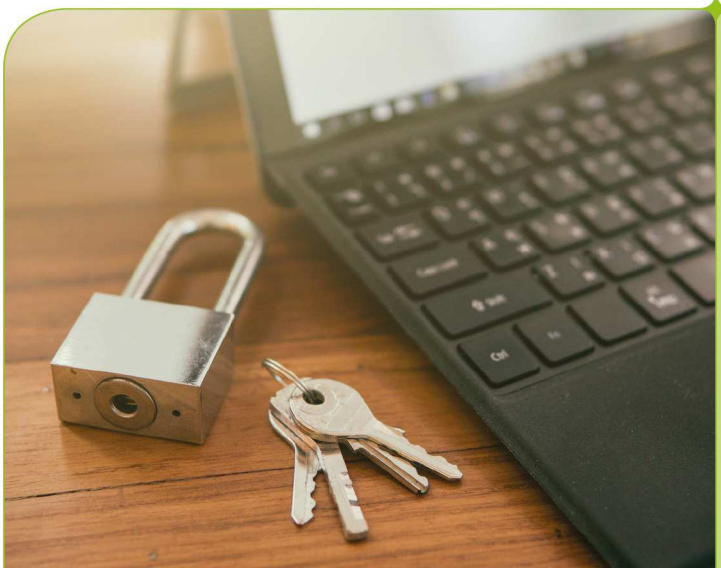
HOLGER RAASCH
STEUERBERATER

Der neue Beschäftigtendatenschutz

Welche Änderungen müssen Arbeitgeber
ab dem 25.05.2018 beachten?



Mandanten-Info

Der neue Beschäftigtendatenschutz

Holger Raasch, Alt-Kaulsdorf 51, 12621 Berlin,
Telefon: 0 30/7 20 21 22 60, Telefax: 0 30/7 20 21 22 68
E-Mail: holger.raasch@stb-raasch.de, Internet: www.stb-raasch.de

Holger Raasch, Alt-Kaulsdorf 51, 12621 Berlin,
Telefon: 0 30/7 20 21 22 60, Telefax: 0 30/7 20 21 22 68
E-Mail: holger.raasch@stb-raasch.de, Internet: www.stb-raasch.de

Holger Raasch, Alt-Kaulsdorf 51, 12621 Berlin,
Telefon: 0 30/7 20 21 22 60, Telefax: 0 30/7 20 21 22 68
E-Mail: holger.raasch@stb-raasch.de, Internet: www.stb-raasch.de

1 Einführung

Zum 25.05.2018 endet die 2-jährige Umsetzungsfrist für die Datenschutz-Grundverordnung (DS-GVO) und es tritt gleichzeitig das neue Bundesdatenschutzgesetz (BDSG n. F.) in Kraft. Damit gilt ab dem 25.05.2018 europaweit ein einheitliches Datenschutzrecht.

Auch wenn sich der Schutz und die Zulässigkeit der Verarbeitung personenbezogener Daten materiell, d. h. inhaltlich im Vergleich zum bisher geltenden Recht gar nicht so wesentlich verändert, kommen auf Verantwortliche, also diejenigen, die über die Verarbeitung personenbezogener Daten entscheiden, umfangreiche neue Verpflichtungen hinzu. Bei Verletzung der Pflichten drohen Schadensersatzansprüche der betroffenen Personen und massive Bußgelder. Dies gilt selbst dann, wenn die Grundsätze der Datenverarbeitung nach der DS-GVO objektiv eingehalten werden, aber der Nachweis hierüber nicht geführt werden kann oder notwendige Dokumentationen fehlen.

Vorliegend erhalten Sie einen Überblick über die (neuen) Verpflichtungen für Verantwortliche und die Zulässigkeit der Datenverarbeitung, speziell im Hinblick auf den Beschäftigtenkontext. Die Ausführungen zu den Neuregelungen der DS-GVO gelten aber überwiegend auch für die Verarbeitung personenbezogener Daten in anderen Zusammenhängen, z. B. im Kontakt mit Kunden oder Lieferanten.

1.1 Europaweit einheitlicher Datenschutz ab 25.05.2018

Die zentralen Rechtsvorschriften zum Datenschutz in Deutschland bilden zukünftig die Datenschutz-Grundverordnung und das neue Bundesdatenschutzgesetz.

Das **europäische Sekundärrecht** (das die Rechtsgrundlagen in den Mitgliedstaaten bildet) besteht unter anderem aus **Verordnungen** und **Richtlinien**. **Verordnungen** (wie die DS-GVO) haben allgemeine Geltung, sind in allen ihren Teilen verbindlich und **gelten unmittelbar in jedem Mitgliedstaat**.

Die DS-GVO stellt eine Verordnung in diesem Sinne dar und gilt daher unmittelbar und direkt, ohne dass es einer innerstaatlichen Umsetzung durch nationale Gesetze bedarf.

Holger Raasch, Alt-Kaulsdorf 51, 12621 Berlin,
Telefon: 0 30/7 20 21 22 60, Telefax: 0 30/7 20 21 22 68
E-Mail: holger.raasch@stb-raasch.de, Internet: www.stb-raasch.de

Hinweis

Das Bundesdatenschutzgesetz „BDSG“ in der neuen Fassung dient deshalb **nicht** der Umsetzung der DS-GVO, sondern enthält spezifischere Vorschriften für eine Datenverarbeitung im Beschäftigungskontext gem. Art. 88 Abs. 1 DS-GVO.

Nur dort, wo die DS-GVO ausdrücklich Öffnungsklauseln enthält, ist Platz für eine nationale Regelung, z. B. durch BDSG n. F.

1.2 Überblick zu den wesentlichen Neuregelungen durch die DS-GVO

Die Datenschutz-Grundverordnung enthält eine Vielzahl neuer Vorgaben, die durch Verantwortliche eingehalten werden müssen, wobei viele Regelungen bereits im alten Bundesdatenschutzgesetz enthalten waren.

Allerdings ergeben sich aus formeller Sicht umfangreiche Verpflichtungen, die Arbeitgeber zukünftig als Verantwortliche zu erfüllen haben (z. B. Dokumentations- und Nachweispflichten, Informationspflichten gegenüber betroffenen Personen und Meldepflichten bei Datenschutzverletzungen) und die aufgrund der massiven Bußgeld- und erweiterten Haftungsvorschriften ein hohes Risiko bieten. Da in vielen Unternehmen der Beschäftigtendatenschutz in der Vergangenheit „großzügig“ gehandhabt wurde, ist ein erhebliches Umdenken nötig.

2 Überblick

2.1 Anwendungsbereich

Die Datenschutz-Grundverordnung gilt nach Art. 2 DS-GVO 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.

Die in der Datenschutz-Grundverordnung verwendeten Begriffe werden in Art. 4 DS-GVO definiert bzw. klargestellt. Die DS-GVO verwendet dabei sehr ähnliche Begriffe wie das BDSG n. F., wobei durchaus maßgebliche Unterschiede bestehen.

- **„Personenbezogene Daten“** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen.

Als **identifizierbar** wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

- **„Verarbeitung"** ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

- **„Verantwortlicher"** ist die natürliche oder juristische Person (...), die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

  Bei Unternehmen ist „Verantwortlicher" die rechtliche Person, die das Unternehmen betreibt, also z. B. eine GmbH oder Aktiengesellschaft.

- Die **betroffene Person** wird in Art. 4 Nr. 1 DS-GVO definiert als diejenige identifizierte oder identifizierbare natürliche Person, auf die sich personenbezogene Daten beziehen.

2.2 Grundsätze für die Verarbeitung personenbezogener Daten nach der DS-GVO

Art. 5 DS-GVO normiert zwingend („müssen") Grundsätze für die Verarbeitung personenbezogener Daten, bei deren Missachtung nach Art. 83 Abs. 5 lit. a) DS-GVO erhebliche Bußgelder drohen. Die Grundsätze dienen gleichzeitig der Auslegung unbestimmter Rechtsbegriffe, wie etwa dem Kriterium der „Erforderlichkeit" der Datenverarbeitung, z. B. in Art. 6 und Art. 9 DS-GVO bzw. § 26 BDSG n. F.

2.2.1 Rechtmäßigkeit, Fairness und Transparenz (Art. 5 Abs. 1 lit. a) DS-GVO)

Wie schon das bisherige Bundesdatenschutzgesetz, ist die DS-GVO als „Verbot mit Erlaubnisvorbehalt" ausgestaltet. Demnach ist die Verarbeitung personenbezogener Daten grundsätzlich verboten und nur dort (ausnahmsweise!) erlaubt, wo ein Erlaubnistatbestand die Datenverarbeitung zulässt („Rechtmäßigkeit").

Verantwortliche müssen personenbezogene Daten nach **Treu und Glauben** verarbeiten, d. h. die Datenverarbeitung muss **verhältnismäßig** sein („Fairness").

Danach muss die Verarbeitung personenbezogener Daten einem legitimen Zweck dienen, das mildeste (aller gleich effektiven) Mittel zur Verwirklichung dieses Zwecks darstellen und für die betroffene Person im Rahmen einer angemessenen Interessenabwägung zumutbar sein.

Die Datenverarbeitung muss für die betroffene Person nachvollziehbar, d. h. **transparent** sein. Hieraus ergeben sich umfangreiche Informationspflichten und Betroffenenrechte, wie etwa in Art. 12 ff. DS-GVO.

2.2.2 Zweckbindung (Art. 5 Abs. 1 lit. b) DS-GVO)

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Die Daten dürfen grundsätzlich nur für diejenigen Zwecke verwendet werden, für die sie erhoben wurden. Eine Zweckänderung ist nur unter den (strengen) Voraussetzungen des Art. 6 Abs. 4 DS-GVO zulässig.

Beispiel: Übersendet ein Bewerber im Rahmen einer Stellenausschreibung seine Bewerbungsunterlagen an den (potenziellen neuen) Arbeitgeber, hat dieser mit Entgegennahme der Bewerbung die Informationspflichten aus Art. 13 DS-GVO zu erfüllen.

Der Arbeitgeber hat den Bewerber (z. B. mit einer Bestätigung über den Eingang der Bewerbungsunterlagen) über den Namen und die Kontaktdaten des Verantwortlichen, die Zwecke der Verarbeitung und die Empfänger der personenbezogenen Daten (z. B. Personalabteilung, fachlicher Vorgesetzter, Betriebsrat etc.) sowie die Dauer der Speicherung und seine Betroffenenrechte zu informieren.

2.2.3 Datenminimierung (Art. 5 Abs. 1 lit. c) DS-GVO)

Personenbezogene Daten müssen im Zweck angemessen und sachlich relevant („erheblich“) sein und auf das für den Zweck der Verarbeitung notwendige Maß beschränkt werden.

2.2.4 Weitere Grundsätze (Art. 5 Abs. 1 lit. d) bis f) DS-GVO)

Personenbezogene Daten müssen außerdem

- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein („Richtigkeit“),
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur solange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“) und
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

2.2.5 Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO)

Der Verantwortliche (z. B. Arbeitgeber) ist für die Einhaltung der Prinzipien in Art. 5 Abs. 1 DS-GVO verantwortlich und muss deren **Einhaltung nachweisen können**.

Nach Art. 24 Abs. 1 Satz 1 DS-GVO muss der Verantwortliche die Einhaltung der Vorgaben des Art. 5 Abs. 1 DS-GVO nicht nur durch geeignete technische und organisatorische Maßnahmen sicherstellen und den Nachweis dafür erbringen, dass die Verarbeitung gemäß der DS-GVO erfolgt, sondern auch den Nachweis hierfür erbringen können.

2.3 Haftung und Bußgelder

Die Datenschutz-Grundverordnung erweitert die Haftung des Verantwortlichen (und der Auftragsverarbeiter) deutlich gegenüber der früheren Regelung im BDSG a. F.

Nach Art. 82 Abs. 1 DS-GVO sind materielle und immaterielle Schäden zu erstatten, die wegen eines Verstoßes gegen die Anforderungen der DS-GVO entstanden sind. Zukünftig sind **auch immaterielle Schäden („Schmerzensgeld")** auszugleichen, was eine deutliche Erweiterung zu § 7 BDSG a. F. darstellt. Zukünftig sind auch **Verbandsklagen** nach Art. 80 Abs. 2 DS-GVO zulässig.

Art. 83 Abs. 4 und 5 DS-GVO sehen Tatbestände vor, bei deren Verwirklichung (d. h. Verletzung bestimmter Vorgaben aus der DS-GVO) massive Bußgelder durch die Aufsichtsbehörden (insb. die Landesämter für den Datenschutz/Landesdatenschutzbeauftragten) verhängt werden können.

- Bei **Verstößen aus Art. 83 Abs. 4 DS-GVO** beträgt die Geldbuße bis zu 10.000.000 Euro oder im Falle eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres (je nachdem, welcher der Beträge höher ist).

  Beispiel: Der Verantwortliche führt kein Verzeichnis aller Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DS-GVO.

- Bei **Verstößen im Sinne von Art. 83 Abs. 5 DS-GVO** beträgt die Geldbuße sogar bis zu 20.000.000 Euro bzw. 4 % des Weltjahresumsatzes.

  Beispiel: Verstoß gegen die Informationspflichten bei Erhebung von personenbezogenen Daten nach Art. 13 oder Art. 14 DS-GVO oder Verstoß gegen die Grundsätze der Datenverarbeitung nach Art. 5 DS-GVO.

Die von den Aufsichtsbehörden verhängten Bußgelder müssen nach Art. 83 Abs. 1 DS-GVO in jedem Einzelfall **wirksam, verhältnismäßig und abschreckend** sein. Hierbei sind die Aspekte aus Art. 83 Abs. 2 DS-GVO gebührend zu berücksichtigen.

3 Pflichten für Arbeitgeber nach der DS-GVO

3.1 Dokumentations- und Nachweispflichten

Nach **Art. 5 Abs. 2 DS-GVO** muss der Verantwortliche die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten in Art. 5 Abs. 1 DS-GVO (aktiv) **nachweisen** können und unterliegt diesbezüglich einer **Rechenschaftspflicht**.

Hinweis

Auch wenn Verantwortliche sämtliche materielle Verpflichtungen aus der DS-GVO (objektiv) einhalten, wäre die fehlende Nachweisbarkeit ein Verstoß nach Art. 83 Abs. 5 lit. a) DS-GVO, woraus Bußgelder von bis zu 20.000.000 Euro bzw. bei Unternehmen von bis zu 4 % des Weltjahresumsatzes des letzten Geschäftsjahres drohen können.

Art. 24 Abs. 1 DS-GVO ergänzt die Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO dahingehend, dass der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete **technische und organisatorische Maßnahmen („TOM´s")** umzusetzen hat, **um sicher zu stellen und den Nachweis dafür erbringen zu können**, dass die Verarbeitung personenbezogener Daten nach den Vorgaben der DS-GVO erfolgt.

3.2 Informationspflichten des Verantwortlichen

Der **Transparenzgrundsatz nach Art. 5 Abs. 1 lit. a) DS-GVO** zählt zu den wesentlichen Prinzipien der Datenschutz-Grundverordnung.

Die hieraus abgeleiteten **Informationspflichten nach Art. 13 und Art. 14 DS-GVO** gehen deutlich über die Vorgaben nach bisherigem Recht in § 4 Abs. 3 und § 33 BDSG a. F. hinaus.

3.2.1 Informationspflichten bei der Direkterhebung (Art. 13 DS-GVO)

Werden personenbezogene **Daten bei der betroffenen Person erhoben,** muss der Verantwortliche (spätestens) zum Zeitpunkt der Erhebung dieser Daten folgendes mitteilen:

- Name und Kontaktdaten des Verantwortlichen (und ggf. seines Vertreters), ggf. Kontaktdaten des Datenschutzbeauftragten,
- Zwecke und Rechtsgrundlage für die Datenverarbeitung,

- Ggf. berechtigtes Interesse der Datenverarbeitung, wenn die Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f) DS-GVO erfolgt,
- Ggf. Empfänger oder Kategorien von Empfängern,
- Ggf. die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland (z. B. Konzernholding außerhalb der EU) zu übermitteln,
- Dauer der Speicherung der personenbezogenen Daten oder zumindest die Kriterien für die Festlegung dieser Dauer,
- Betroffenenrechte (insb. Art. 15 ff. DS-GVO).

Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiter zu verarbeiten als den, für den sie erhoben wurden, so hat er nach Art. 13 Abs. 3 DS-GVO der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle weiteren maßgeblichen Informationen zur Verfügung zu stellen.

Die **Informationspflichten nach Art. 13 Abs. 1 bis 3 DS-GVO bestehen nicht**, wenn die betroffene Person bereits über die jeweilige Information verfügt und nach dem Erwägungsgrund 62 **wohl** auch nicht, soweit die Speicherung oder Offenlegung personenbezogener Daten **ausdrücklich durch Rechtsvorschriften** geregelt ist.

3.2.2 Informationspflichten bei sonstigen Datenerhebungen (Art. 14 DS-GVO)

Erfolgt die Datenerhebung nicht bei der betroffenen Person, sondern **bei Dritten**, sieht Art. 14 DS-GVO in Vergleich zu Art. 13 DS-GVO zusätzliche Informationspflichten durch den Verantwortlichen vor. So sind nach Art. 14 Abs. 1 lit. d) DS-GVO die Kategorien personenbezogener Daten anzugeben, die verarbeitet werden und nach § 14 Abs. 2 lit. f) DS-GVO ist die Herkunft zu benennen, aus der die personenbezogenen Daten stammen oder ggf. mitzuteilen, ob sie aus öffentlich zugänglichen Quellen bezogen wurden.

Die Information muss hier anders als nach Art. 13 DS-GVO nicht im Zeitpunkt der Erhebung, sondern innerhalb einer angemessenen Frist, längstens jedoch innerhalb eines Monats nach Erlangung der personenbezogenen Daten erfolgen.

Art. 14 Abs. 5 DS-GVO enthält erweiterte Ausnahmevorschriften. Unter Anderem entfällt die Informationspflicht nach Art. 14 Abs. 5 lit. d) DS-GVO, wenn personenbezogene Daten **von Personen erhoben werden, die einer beruflichen Geheimhaltungspflicht unterliegen, wie z. B. bei einem Rechtsanwalt oder Steuerberater**.

3.3 Löschpflichten (Art. 17 DS-GVO)

Nach Art. 17 Abs. 1 DS-GVO hat der Verantwortliche die Verpflichtung, personenbezogene Daten unverzüglich zu löschen, insbesondere dann,

- wenn personenbezogene Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind,
- die betroffene Person eine erteilte Einwilligung widerruft oder
- personenbezogene Daten unrechtmäßig verarbeitet wurden.

Die Löschpflicht aus Art. 17 Abs. 1 DS-GVO gilt nicht ausnahmslos. Vielmehr sieht Art. 17 Abs. 3 DS-GVO Ausnahmetatbestände vor, bei denen – trotz Vorliegen eines Löschgrundes nach Art. 17 Abs. 1 DS-GVO (z. B. Wegfall des Verarbeitungszwecks) – die Löschpflicht (zumindest zeitlich befristet) entfällt. Dies gilt insbesondere, wenn

- die weitere Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung (nach dem Recht der EU oder dem Recht des Mitgliedstaates) erforderlich ist oder
- für die Speicherung oder sonstige Verarbeitung personenbezogener Daten für Zwecke der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Solange daher Aufbewahrungs- oder Auskunftspflichten nach anderen Gesetzen bestehen, ist der Verantwortliche nicht zur Löschung personenbezogener Daten verpflichtet.

3.4 Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen

Art. 33 und Art. 34 DS-GVO sehen umfassende Meldepflichten gegenüber den Aufsichtsbehörden bzw. Benachrichtigungspflichten gegenüber den betroffenen Personen vor, wenn eine **Verletzung des Schutzes personenbezogener Daten** vorliegt.

Nach Art. 4 Ziffer 12 DS-GVO ist die „Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die – ob unbeabsichtigt oder unrechtmäßig – zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

3.4.1 Meldepflicht gegenüber der Aufsichtsbehörde

Im Falle einer Verletzung personenbezogener Daten muss der Verantwortliche nach Art. 33 Abs. 1 DS-GVO unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese **der zuständigen Aufsichtsbehörde melden**, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Für die Meldepflicht kommt es nicht darauf an, um welche Kategorie von personenbezogenen Daten es sich handelt und ob es zu einem Schaden für die betroffene Person kommen kann oder bereits gekommen ist.

Beispiel: Aufgrund eines Updates in der Personalverarbeitungssoftware erhalten sämtliche Mitarbeiter der Personalabteilung Zugriff auf die Daten der gesamten

Belegschaft, obwohl nach der internen Arbeitsverteilung die einzelnen Mitarbeiter der Personalabteilung nur für einen bestimmten Mitarbeiterkreis (z. B. Außendienst, Innendienst, allgemeine Verwaltung, gewerbliche Mitarbeiter im Lager etc.) zuständig sind. Damit können sämtliche Mitarbeiter der Personalabteilung potenziell unbefugt Zugang zu den personenbezogenen Daten der gesamten Belegschaft erhalten.

Der verantwortliche Arbeitgeber müsste diese Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde melden. Ob die Mitarbeiter der Personalabteilung von ihrem unbeschränkten Zugriffsrecht Gebrauch gemacht haben, spielt keine Rolle. Allein die Möglichkeit der Kenntnisnahme genügt.

Quelle: BayLDA/Erste Hilfe zur Datenschutz-Grundverordnung

3.4.2 Benachrichtigungspflicht der betroffenen Person

Hat eine Verletzung des Schutzes personenbezogener Daten darüber hinaus **voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten betroffener Personen** zur Folge, muss der Verantwortliche grundsätzlich die hiervon betroffenen Personen unverzüglich benachrichtigen (Art. 34 Abs. 1 DS-GVO).

Der Verantwortliche kann gemäß Art. 34 Abs. 3 DS-GVO ausnahmsweise von der Benachrichtigung absehen, insbesondere, wenn er geeignete **technische und organisatorische Sicherheitsvorkehrungen** getroffen hat, die den Zugang zu den personenbezogenen Daten durch Unbefugte verhindern (z. B. Verschlüsselung).

3.5 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Nach Art. 25 DS-GVO hat der Verantwortliche IT-Systeme grundsätzlich so auszugestalten, dass sie die Datenschutzgrundsätze aus Art. 5 DS-GVO wirksam umsetzen. Zudem müssen IT-Systeme so voreingestellt werden, dass das Gebot der Datenminimierung, der Transparenz und der Löschung erfüllt werden können.

Nach Art. 32 DS-GVO hat der Verantwortliche (im Rahmen des technisch und wirtschaftlich möglichen) geeignete technische und organisatorische Maßnahmen zur Datensicherheit zu treffen (z. B. Verschlüsselung, Vertraulichkeit und Integrität, Belastbarkeit der Systeme, Verfügbarkeit der Daten und regelmäßige Überprüfbarkeit), um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

3.6 Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten

Art. 30 Abs. 1 DS-GVO verpflichtet Verantwortliche, ein **Verzeichnis aller Verarbeitungstätigkeiten** zu führen, die ihrer Zuständigkeit unterliegen. Dieses Verarbeitungsverzeichnis ist eines

der zentralen **Instrumente zur Umsetzung der Dokumentations- und Nachweispflichten** nach Art. 5 Abs. 2 und Art. 24 DS-GVO.

Der Verantwortliche hat der Aufsichtsbehörde auf Anfrage das Verarbeitungsverzeichnis zur Verfügung zu stellen (Art. 30 Abs. 4 DS-GVO). Andere haben kein Einsichtsrecht (z. B. betroffene Personen oder der Betriebsrat).

Das Verzeichnis von Verarbeitungstätigkeiten muss nach Art. 30 Abs. 1 Satz 1 DS-GVO **zwingend mindestens Angaben** zu

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- die Zwecke der Verarbeitung;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie ggf. geeigneter Garantien;
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- wenn möglich, eine allgemeine Beschreibung der technischen oder organisatorischen Maßnahmen der IT-Sicherheit (Art. 32 DS-GVO)

enthalten.

Das Verzeichnis von Verarbeitungstätigkeiten ist nach Art. 30 Abs. 3 DS-GVO **schriftlich** zu führen, was auch in einem elektronischen Format erfolgen kann (z. B. PDF-Dokument).

Das Verzeichnis muss stets aktuell sein (Nachweisermöglichung). Bei Veränderungen muss ein neues Verzeichnis erstellt werden. Alte Verzeichnisse sollten aufgehoben werden.

Die Datenschutzkonferenz – DSK (unabhängige Datenschutzbehörden des Bundes und der Länder) hat ein **Muster** für ein Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher gemäß Art. 30 Abs. 1 DS-GVO (sowie ein Muster für Auftragsverarbeiter) **einschließlich umfangreicher Hinweise** herausgegeben, die bei den meisten Datenschutzbehörden der Länder zum Download bereitstehen.

4 Betroffenenrechte nach DS-GVO

Neben den deutlich erweiterten Pflichten der Verantwortlichen regeln insbesondere Art. 15 ff. DS-GVO umfangreiche Betroffenenrechte.

4.1 Recht auf Auskunft (Art. 15 DS-GVO)

Nach Art. 15 DS-GVO haben Betroffene ein umfassendes Auskunftsrecht in Bezug auf die sie betreffenden personenbezogenen Daten, das über die bisherigen Rechte in § 34 BDSG n. F. hinausgeht.

Betroffene sollen das Auskunftsrecht problemlos, (und) in angemessenen Abständen wahrnehmen können.

Anders als Art. 13 und Art. 14 DS-GVO sieht das Auskunftsrecht nach Art. 15 DS-GVO **keine Einschränkung** für den Fall vor, dass der betroffenen Person die zu erteilenden Auskünfte bereits vorliegen.

Der Verantwortliche hat der betroffenen Person nach Art 15 Abs. 3 DS-GVO eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern die betroffene Person nichts Anderes angibt.

4.2 Recht auf Berichtigung (Art. 16 DS-GVO)

Betroffene Personen haben das Recht, von dem Verantwortlichen die unverzügliche Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.

Außerdem hat die betroffene Person unter Berücksichtigung der Zwecke der DS-GVO das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

Beide Rechte können z. B. im Zusammenhang mit erteilten (und der Personalakte beigefügten) Abmahnungen eine Rolle spielen.

4.3 Weitere Rechte der betroffenen Person

Nach Art. 17 Abs. 1 DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen zu verlangen, dass personenbezogene Daten unverzüglich **gelöscht** werden, insbesondere dann,

- wenn die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind oder
- die betroffene Person eine erteilte Einwilligung widerruft.

Hat der Verantwortliche personenbezogene Daten öffentlich gemacht (Ermöglichung des Zugriffs durch einen unbestimmten Personenkreis) und ist er zur Löschung verpflichtet, hat der Verantwortliche nach Art. 17 Abs. 2 DS-GVO unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art zu treffen, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat (**Recht auf Vergessenwerden**).

Betroffene Personen haben das Recht, von dem Verantwortlichen unter bestimmten Umständen die **Einschränkung der Verarbeitung** personenbezogener Daten nach Art. 18 DS-GVO zu verlangen.

Beruht die Datenverarbeitung auf einer **Einwilligung** (Art. 6 Abs. 1 lit. a) und Art. 9 Abs. 2 lit. a) DS-GVO) oder einem **Vertrag** (Art. 6 Abs. 1 lit. b) DS-GVO) und wurden die personenbezogenen Daten **von der betroffenen Person bereitgestellt** (also durch die betroffene Person an den Verantwortlichen übermittelt), sieht Art. 20 DS-GVO das Recht vor, diese Daten von dem Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder von diesem zu verlangen, die Daten einem anderen Verantwortlichen ohne Behinderung zu übermitteln, wenn die Verarbeitung der personenbezogenen Daten mit Hilfe automatisierter Verfahren erfolgt und soweit dies technisch möglich ist.

5 Rechtmäßigkeit der Datenverarbeitung

5.1 Erlaubnistatbestände der Datenschutz-Grundverordnung

Die Verarbeitung personenbezogener Daten ist (unter Berücksichtigung der übrigen Grundsätze, insbesondere Art. 5 DS-GVO) zulässig, **unter anderem für folgende Fälle**:

- Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur **Durchführung vorvertraglicher Maßnahmen** erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;

Die Erlaubnistatbestände aus Art. 6 Abs. 1 DS-GVO stehen gleichwertig zueinander. Ist die Verarbeitung personenbezogener Daten durch den Verantwortlichen z. B. bereits zur Erfüllung eines Vertrages oder zur Erfüllung einer rechtlichen Verpflichtung erforderlich, benötigt der Verantwortliche für die Datenverarbeitung keine Einwilligung durch die betroffene Person.

Wird die Verarbeitung personenbezogener Daten auf die **Einwilligung der betroffenen Person** gestützt, muss die Einwilligung durch eine eindeutige Handlung erfolgen, mit der ohne Zwang für den konkreten Fall in Kenntnis der Sachlage und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung ihrer Daten einverstanden ist. Die Einwilligung muss eindeutig sein, d. h. ein stillschweigendes Einverständnis oder die bloße Untätigkeit der betroffenen Person sind nicht ausreichend. Gleiches gilt, wenn die Einwilligung elektronisch in Form eines vorausgefüllten Kästchens (sog. Opt-out-Wahlmöglichkeit) erfolgt.

Die betroffene Person kann ihre Einwilligung **jederzeit und grundlos mit Wirkung für die Zukunft widerrufen**. Über das Widerrufsrecht muss die betroffene Person informiert werden. Der Widerruf muss ebenso einfach wie die Einwilligung selbst erklärt werden können (Art. 7 Abs. 3 DS-GVO).

Die **Verarbeitung besonderer Kategorien** personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist im Vergleich zu Art. 6 DS-GVO nach Art. 9 DS-GVO nur eingeschränkt zulässig, und zwar unter anderem

- wenn die betroffene Person in die Verarbeitung dieser Daten für einen oder mehrere festgelegte Zwecke **ausdrücklich eingewilligt** hat oder

- die Verarbeitung erforderlich ist, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr **aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit** und des Sozialschutzes erwachsenen Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann.

5.2 Datenverarbeitung im Beschäftigungskontext

Nach **Art. 88 Abs. 1 DS-GVO** können die Mitgliedstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen „spezifischere" Vorschriften („more specific rules") zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der **Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext** vorsehen.

6 Beschäftigtendatenschutz nach § 26 BDSG n. F.

Zentrale Regelung für den neuen Beschäftigungsdatenschutz ist § 26 BDSG n. F. Der Gesetzgeber hat hier von der Öffnungsklausel in Art. 88 Abs. 1 DS-GVO Gebrauch gemacht.

Die Zulässigkeit der Verarbeitung personenbezogener Daten im Beschäftigungskontext richtet sich deshalb primär nach § 26 BDSG n. F. unter Berücksichtigung der Vorgaben aus der DS-GVO, wie etwa den Verarbeitungsgrundsätzen in Art. 5 DS-GVO.

6.1 Anwendungsbereich

Wie bereits § 32 Abs. 2 BDSG a. F. wird der **sachliche Anwendungsbereich** bei der Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis nach § 26 Abs. 7 BDSG n. F. auf solche Daten von Beschäftigten erweitert, die von Verantwortlichen (Arbeitgeber) verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen. § 26 BDSG n. F. geht damit über den sachlichen Anwendungsbereich in Art. 2 Abs. 1 DS-GVO hinaus.

Beispiel: Handschriftliche Notizen im Rahmen eines Vorstellungsgespräches oder mündliche Fragen des Vorgesetzten unterliegen damit den Anforderungen aus dem BDSG n. F./der DS-GVO. Gleiches gilt für die Personalakte in Papierform.

6.2 Zulässige Datenverarbeitung nach § 26 Abs. 1 BDSG n. F.

Der Gesetzgeber übernimmt in § 26 Abs. 1 Satz 1 BDSG n. F. den bisherigen § 32 Abs. 1 Satz 1 BDSG a. F. und ergänzt diesen durch den Erlaubnistatbestand der Erfüllung einer gesetzlichen oder kollektivrechtlichen Pflicht.

Nach § 26 Abs. 1 Satz 1 BDSG n. F. dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Wie auch § 32 Abs. 1 Satz 1 BDSG a. F. erlaubt § 26 Abs. 1 Satz 1 BDSG n. F. das Verarbeiten personenbezogener Daten von Beschäftigten, wenn dies für die dort genannten Zwecke **„erforderlich“** ist.

Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist (auch) auf der Grundlage von Kollektivvereinbarungen zulässig.

Nach § 26 Abs. 1 Satz 2 BDSG n. F. dürfen zur **Aufdeckung von Straftaten** personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Die tatsächlichen Anhaltspunkte, die den Verdacht begründen, sind vom Arbeitgeber zu dokumentieren.

Die **Verarbeitung besonderer Kategorien personenbezogener Daten i. S. v. Art. 9 Abs. 1 DS-GVO** ist nach § 26 Abs. 1 Satz 3 BDSG n. F. für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

6.3 Einwilligung zur Datenverarbeitung im Beschäftigungsverhältnis

Der Gesetzgeber lässt grundsätzlich die Einwilligung im Beschäftigungskontext zu und regelt diesbezüglich die Kriterien der Freiwilligkeit. Für die Beurteilung der Freiwilligkeit der Einwilligung ist insbesondere die im Beschäftigungsverhältnis bestehende **Abhängigkeit** der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen.

Regelmäßig wird eine Freiwilligkeit der Einwilligung vorliegen, wenn

- für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder
- Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.

Beispiel: Ein rechtlicher oder wirtschaftlicher Vorteil kann etwa bei der Einführung eines betrieblichen Gesundheitsmanagements oder bei der Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen vorliegen.

Gleichgelagerte Interessen können z. B. bei der Eintragung des Mitarbeiters auf einer Geburtstagsliste oder der Nutzung eines Fotos im Firmenintranet gegeben sein.

Nach § 26 Abs. 2 Satz 3 BDSG n. F. unterliegt die Einwilligungserklärung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist (z. B. per E-Mail bei Homeoffice).

Nach § 26 Abs. 2 Satz 4 BDSG n. F. hat der Arbeitgeber die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Art. 7 Abs. 3 DS-GVO in Textform aufzuklären. Details hierzu kennt Ihr Steuerberater.

Angaben ohne Gewähr

Titelbild: © POJCHEE/fotolia.com

Stand: April 2018

DATEV-Artikelnummer: 19899

E-Mail: literatur@service.datev.de

Holger Raasch, Alt-Kaulsdorf 51, 12621 Berlin,
Telefon: 0 30/7 20 21 22 60, Telefax: 0 30/7 20 21 22 68
E-Mail: holger.raasch@stb-raasch.de, Internet: www.stb-raasch.de