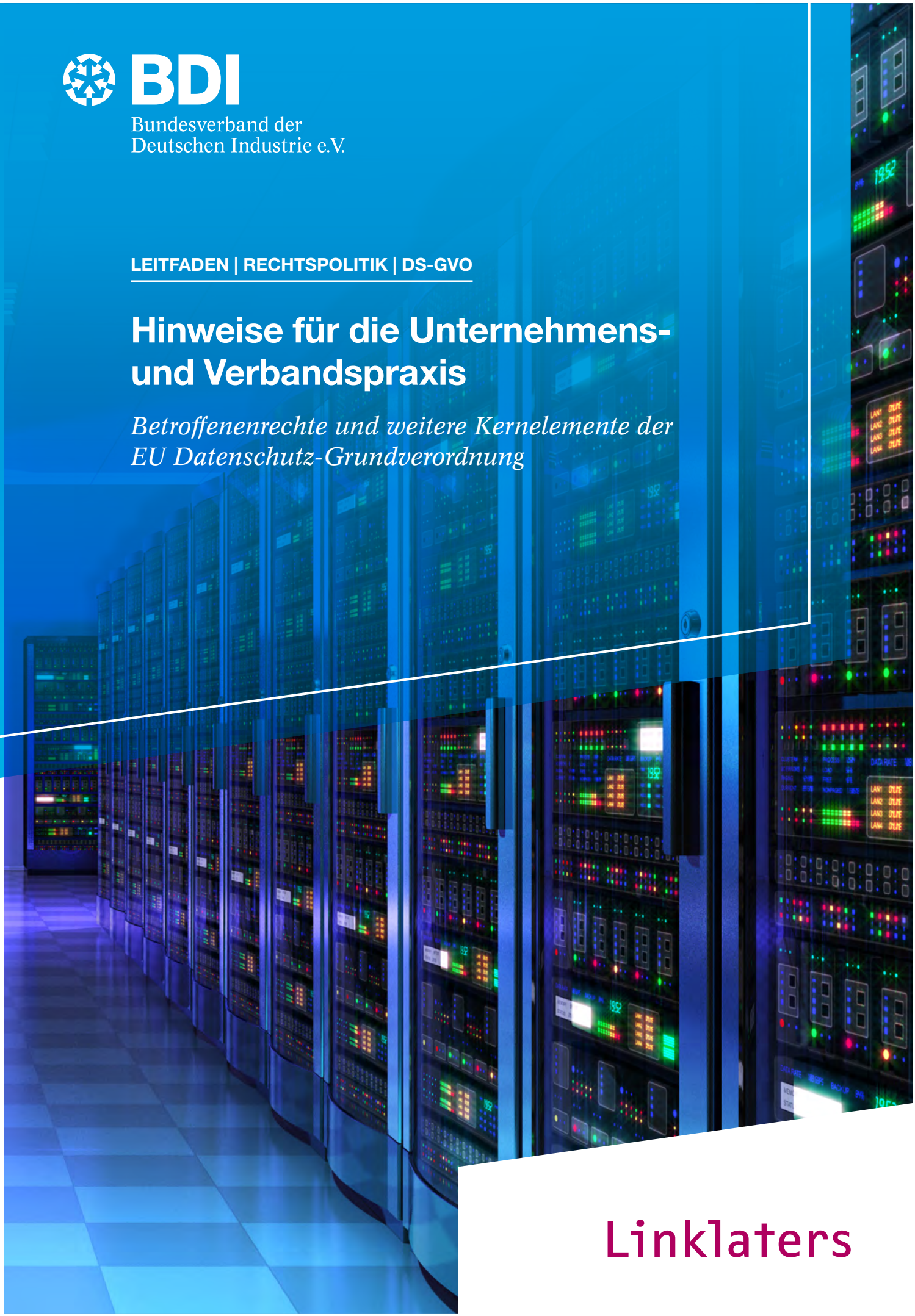
BDI
Bundesverband der
Deutschen Industrie e.V.

LEITFADEN | RECHTSPOLITIK | DS-GVO

Hinweise für die Unternehmens- und Verbandspraxis

Betroffenenrechte und weitere Kernelemente der EU Datenschutz-Grundverordnung



Linklaters

Digitale Version

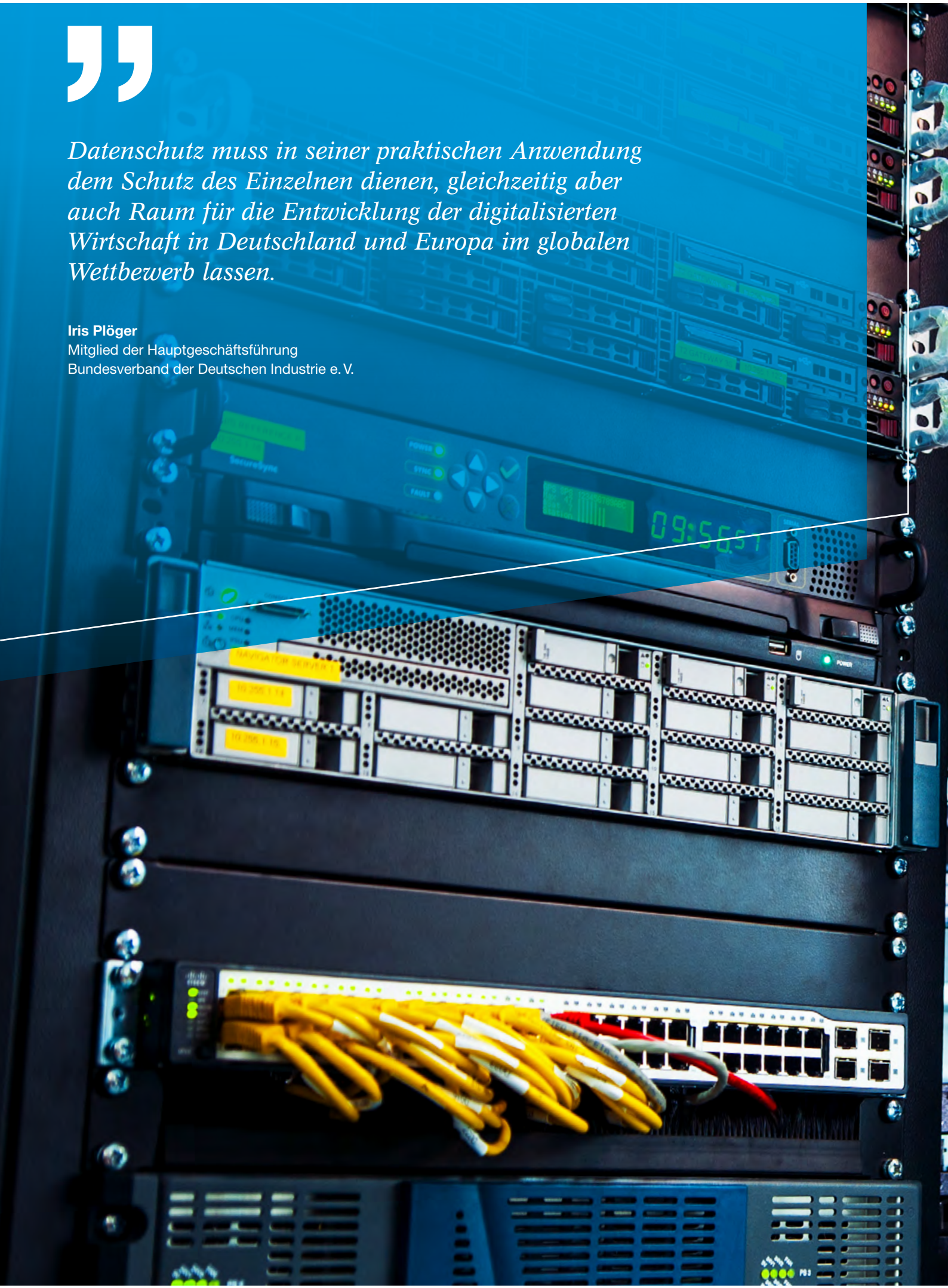
Einfach den QR-Code mit dem Smartphone oder Tablet einscannen, und die digitale Version öffnen.

www.bdi.eu/publikation/news/Hinweise-fuer-die-Unternehmens-und-Verbandspraxis

Inhaltsverzeichnis

Datenschutz muss in seiner praktischen Anwendung dem Schutz des Einzelnen dienen, gleichzeitig aber auch Raum für die Entwicklung der digitalisierten Wirtschaft in Deutschland und Europa im globalen Wettbewerb lassen.

Iris Plöger
Mitglied der Hauptgeschäftsführung
Bundesverband der Deutschen Industrie e. V.



Vorwort

Seit dem 25. Mai 2018 gilt die EU Datenschutz-Grundverordnung (DS-GVO) und das neue Bundesdatenschutzgesetz (BDSG). Die DS-GVO erfüllt die Erwartungen – im positiven wie im negativen Sinne. Sie greift tief in die Prozesse der Unternehmen und Verbände ein, führt bei vielen Wirtschaftsakteuren zu Verunsicherung und verlangt erhebliche, z. T. kostspielige, Anpassungen und ein Umdenken beim praktizierten Datenschutz. Dabei generiert sie signifikanten Aufwand, insbesondere auch bei jenen, die in der Vergangenheit beim Datenschutz „Fünfe haben gerade sein lassen".

Andererseits wurde mit der DS-GVO ein konsistentes Regelwerk geschaffen, das den Datenschutz ganzheitlich begreift und ein für die deutsche und europäische Wirtschaft wichtiges Level-Playing-Field herstellt. Die Allgemeinverständlichkeit der DS-GVO ist ein großer Vorteil. Wer jemals mit den §§ 28 ff. des alten BDSG arbeiten musste, begrüßt die klare Struktur und Wortwahl der DS-GVO.

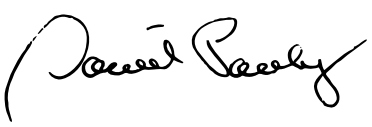
Es ist sicher ein nicht fernliegender Vorwurf, die DS-GVO „verkaufe alten Wein in neuen Schläuchen", indem sie sich weitgehend bei den bereits aus der EU Datenschutz-Richtlinie von 1995 bekannten – und veralteten – Instrumenten bedient. Allerdings sollte keinesfalls verschwiegen werden, dass die DS-GVO einige ausgesprochen innovative Elemente enthält, allen voran die Prinzipien „Datenschutz durch Technikgestaltung" (Privacy by Design) und „Datenschutzfreundliche Voreinstellungen" (Privacy by Default). Wer diese Prinzipien ernst nimmt und beachtet, genießt Gestaltungsspielraum und erspart sich in der praktischen Anwendung viel Zeit und mögliche Konflikte.

Datenschutz muss in seiner praktischen Anwendung dem Schutz des Einzelnen dienen, gleichzeitig aber auch Raum für die Entwicklung der digitalisierten Wirtschaft in Deutschland und Europa im globalen Wettbewerb lassen. Die föderale Struktur der Datenschutzaufsicht in Deutschland darf nicht zu einem Datenschutz-Flickenteppich mit unterschiedlicher Auslegung und Handhabung führen. Datenschutz muss ein Standortvorteil sein und darf nicht Hemmnis für innovative, digitale Geschäftsmodelle werden. Möglicherweise entwickelt sich die DS-GVO aber auch zum weltweiten Standard für den Datenschutz, wie es erste Tendenzen wohl vermuten lassen.

Vor diesem Hintergrund und unter Berücksichtigung, dass die Anwendung der DS-GVO unvermeidlich ist, sei allen empfohlen, die DS-GVO als Chance zu begreifen. Der vorliegende Leitfaden wird dabei unterstützen und den Zugang zu den in der konkreten Umsetzung, zugegebenermaßen komplexen und herausfordernden, Kernelementen der DS-GVO erleichtern – allen voran den Betroffenenrechten und angrenzenden -pflichten. Wir wünschen bei der Umsetzung im Unternehmen und Verband viel Erfolg.

Iris Plöger

Mitglied der Hauptgeschäftsführung
Bundesverband der Deutschen
Industrie e. V.



Dr. Daniel Pauly

RA und Partner
Linklaters LLP

01 Informationspflichten bei der Datenerhebung (Art. 13, 14)

1.1 Überblick

Direkterhebung: Jeder Person sind von demjenigen, der personenbezogene Daten direkt von ihr erhebt (der Verantwortliche), allgemeine Informationen (Art. 13 Abs. 1 DS-GVO) sowie weitere Informationen zur Gewährleistung einer fairen und transparenten Verarbeitung (Art. 13 Abs. 2 DS-GVO) zur Verfügung zu stellen.

Dritterhebung: Jeder Person sind von demjenigen, der personenbezogene Daten nicht direkt von ihr selbst erhebt (der Verantwortliche), diese aber von Dritten bezieht (z. B. Adresshändler), allgemeine Informationen (Art. 14 Abs. 1 DS-GVO) sowie die für eine faire und transparente Verarbeitung notwendigen Informationen (Art. 14 Abs. 2 DS-GVO) mitzuteilen.

1.2 Rahmenbedingungen

Allgemeines:

- Jede Person, deren Daten erhobenen werden, hat ein Recht auf Information.
- Das Recht auf Information ergibt sich aus der Erhebung selbst und muss nicht beantragt werden.
- Der Informationspflicht kann sowohl schriftlich als auch in elektronischer Form, z. B. durch aussagekräftige Bilder, nachgekommen werden.
- Die Information muss in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form sowie in einer klaren und einfachen Sprache erbracht werden.
- Für jede weitere Erhebung ist erneut zu informieren.
- Ändern sich die Zwecke der Verarbeitung, muss der betroffenen Person diese Änderung genannt und den Informationspflichten zur Gewährleistung einer fairen und transparenten Verarbeitung (Art. 13 Abs. 2, Art. 14 Abs. 2 DS-GVO) erneut nachgekommen werden.
- Eine Übermittlung der Daten an Dritte stellt oftmals auch eine Zweckänderung dar, sodass die oben genannte Informationspflicht auch hier besteht. Zusätzlich sind bei einer Weitergabe der neue Empfänger oder die neue Empfängerkategorie zu nennen.
- Die Information erfolgt unentgeltlich. Ein angemessenes Entgelt kann nur bei offenkundig unbegründeten oder exzessiven Anträgen verlangt werden.

Direkterhebung:

- Bei der Direkterhebung hat die Information unverzüglich zum Zeitpunkt der Erhebung zu erfolgen.
- Die Pflicht zur Mitteilung besteht für:
  - Namen und Kontaktdaten des Verantwortlichen sowie gegebenenfalls seiner Vertreter und des Datenschutzbeauftragten;
  - Verarbeitungszwecke der Datenverarbeitung;
  - berechtigte Interessen der Verantwortlichen oder eines Dritten (sofern sich die Verarbeitung darauf stützt);
  - Empfänger oder Kategorien von Empfängern der Daten; und
  - etwaige Absichten zur weiterleitung an einen Empfänger in einem Drittland oder eine internationale Organisation sowie das Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses der Kommission.
- Darüber hinaus sind die folgenden Informationen zur Verfügung zu stellen:
  - Speicherdauer der Daten;
  - Rechte der Betroffenen (z. B. auf Auskunft, Löschung);
  - Widerrufbarkeit von Einwilligungen;
  - Beschwerderecht bei der Aufsichtsbehörde;
  - ggf. gesetzliche oder vertragliche Verpflichtung zur Bereitstellung der Daten; und
  - ggf. bei automatisierter Entscheidungsfindung oder Profiling Informationen über die Auswirkungen und Tragweite der Verarbeitung.

Dritterhebung:

- Bei der Dritterhebung muss die Information innerhalb einer angemessenen Frist, jedoch spätestens nach einem Monat nach Erhalt der Daten erfolgen. Werden die Daten zur Kommunikation mit der betroffenen Person verwendet, hat die Information spätestens bei der Kontaktaufnahme zu erfolgen.

- Zusätzlich zu den bei der Direkterhebung erforderlichen Informationen sind die Kategorien der verarbeiteten personenbezogenen Daten mitzuteilen. Dabei müssen die Folgen der Verarbeitung für die betroffene Person erkennbar sein.

- Etwaige berechtigte Interessen des Verantwortlichen an der Verarbeitung sind nunmehr innerhalb der Verpflichtung zur Gewährleistung eines fairen und transparenten Verfahrens zu nennen. Im Rahmen dieses Punktes ist bei Dritterhebungen auch die Datenquelle sowie ggf. deren öffentliche Zugänglichkeit anzugeben. Kann die genaue Herkunft der Daten nicht mehr nachvollzogen werden, ist eine allgemeine Information ausreichend.

1.3 Warum sollte dies ernst genommen werden?

- Die Information der betroffenen Person ist notwendig, damit diese ihre Rechte erfahren und durchsetzen kann. Insbesondere die Betroffenenrechte können nur durch vorherige Information ausgeübt werden, z. B. das Recht auf Löschung oder Einschränkung der Verarbeitung.

- Verstöße gegen die Informationspflichten können zudem zu sehr hohen Geldbußen führen sowie erhebliche Reputationsschäden nach sich ziehen.

1.4 Praktisches Vorgehen

Zum Entsprechen der Informationspflicht bietet sich das folgende Vorgehen an:

- **Schritt 1:** Werden Informationen über eine Person erhoben, so ist bei der Direkterhebung sofort sowie bei der Dritterhebung zumindest innerhalb eines Monats nach Erhalt der Daten der Informationspflicht nachzukommen.

- **Schritt 2:** Je nach Direkterhebung oder Dritterhebung sind die Daten zu ermitteln, über die informiert werden muss (siehe oben).

- **Schritt 3:** Alle Personen, deren Unterstützung erforderlich sein könnte, sind einzubinden (z. B. Personalabteilung, IT).

- **Schritt 4:** Die Informationen sind in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form sowie in einer klaren und einfachen Sprache bereitzustellen und der betroffenen Person zu übermitteln. Dies kann schriftlich oder beispielsweise elektronisch geschehen.

- **Schritt 5:** Das Einhalten der Informationspflichten ist durch den Verantwortlichen stets zu dokumentieren.

Hinweis: Der Informationspflicht darf nur unter besonderen Voraussetzungen nicht nachgekommen werden, so unter anderem, wenn die betroffene Person bereits über die Informationen verfügt, wenn die Information der betroffenen Person einen unverhältnismäßigen Aufwand erfordern würde, die Daten einem Berufsgeheimnis unterliegen oder die Erlangung durch Rechtsvorschrift ausdrücklich geregelt ist. Auch das BDSG-neu enthält gewisse Ausnahmeregelungen, deren Anwendbarkeit jedoch sehr beschränkt und im Allgemeinen noch nicht abschließend geklärt ist.

1.5 Weitere praktische Hinweise

Hinweis 1: Es bietet sich an, für eine effiziente und sichere Bearbeitung von Informationspflichten im Unternehmen, entsprechende Prozesse zu implementieren und Zuständigkeiten festzulegen.

Hinweis 2: Auch ist es sinnvoll, die Informationspflicht bereits in die Datenschutzerklärung auf der Webseite zu integrieren.

Einschlägige Hilfestellungen:

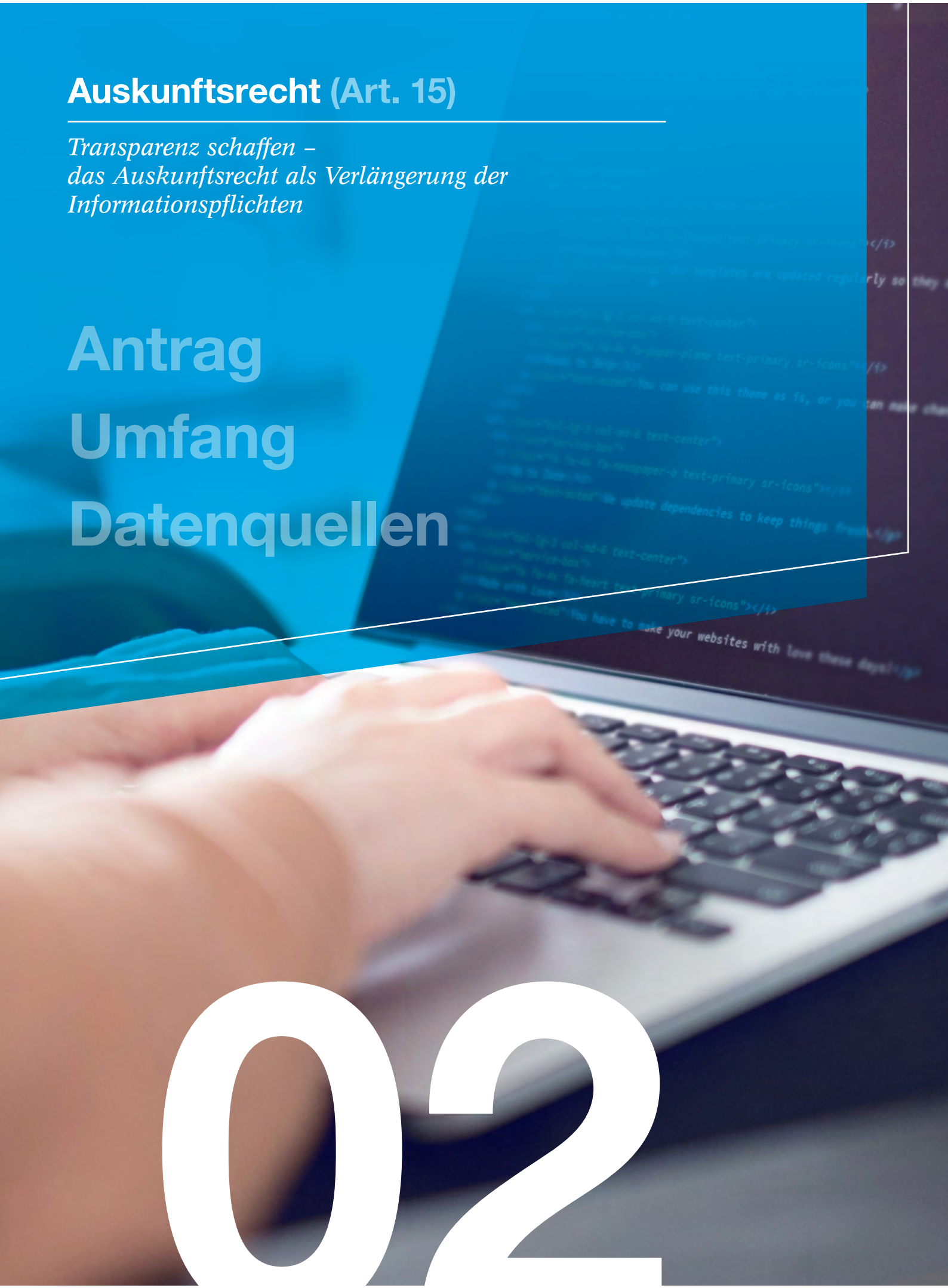
Datenschutzkonferenz des Bundes und der Länder, Informationspflichten bei Dritt- und Direkterhebung (Kurzpapier Nr. 10 vom 16. Januar 2018)

Abrufbar unter:
www.lda.bayern.de/media

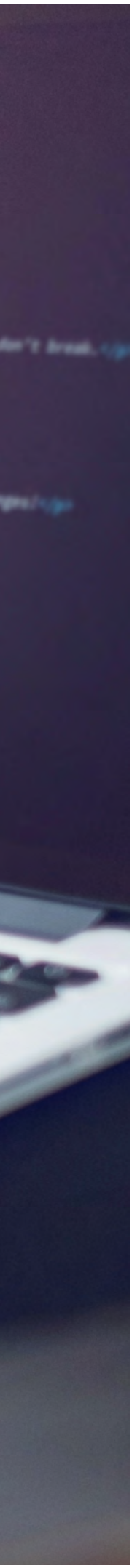
Auskunftsrecht (Art. 15)

Transparenz schaffen –
das Auskunftsrecht als Verlängerung der Informationspflichten

Antrag
Umfang
Datenquellen



02



2.1 Überblick

Jede Person kann von jeder öffentlichen (z. B. einer Behörde) oder privaten Stelle (z. B. einem Unternehmen), die Daten über diese Person verarbeitet (der Verantwortliche), Auskunft darüber verlangen, ob – und wenn ja – welche Daten über sie verarbeitet werden und eine Kopie der Daten anfordern (Art. 15 DS-GVO).

Als solche Daten gelten z. B. die Personalakte, E-Mails, Protokolle und Vermerke, vorausgesetzt, diese Datenbestände enthalten personenbezogene Daten der auskunftsverlangenden Person.

2.2 Rahmenbedingungen

- Jede natürliche Person kann einen Antrag auf Auskunftserteilung stellen, d. h. Mitarbeiter, Kunden und sonstige Dritte. Unternehmen haben dieses Recht nicht.
- Der Antrag kann formlos gestellt werden, insbesondere mündlich (z. B. per Telefon), aber natürlich auch schriftlich (z. B. per Brief oder E-Mail).
- Ist der Antrag elektronisch gestellt, sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen (z. B. Excel). Damit die auskunftserteilende Stelle ihre Auskunft dokumentieren kann, sollten alle übrigen Anträge immer schriftlich beantwortet werden. Sind keine Daten vorhanden, ist dies auch mitzuteilen.
- Generell sind alle Anträge innerhalb eines Monats zu beantworten. Kann diese Frist nicht eingehalten werden, muss dies der antragstellenden Person unter Angabe der (verlängerten) Antwortfrist mitgeteilt werden.
- Die Informationen sind unentgeltlich zur Verfügung zu stellen. Ein angemessenes Entgelt kann nur bei offenkundig unbegründeten oder exzessiven Anträgen verlangt werden.

2.3 Warum sollte dies ernst genommen werden?

- Transparenz schafft Vertrauen.
- Verstöße gegen das Recht einer Person, Auskunft über die Verarbeitung ihrer personenbezogenen Daten zu erhalten, können mit sehr hohen Geldbußen geahndet werden und zu erheblichen Reputationsschäden führen.

2.4 Praktisches Vorgehen

Im Falle eines konkreten Auskunftsverlangens müssen der antragstellenden Person eine Vielzahl an Informationen und eine Kopie ihrer Daten gegeben werden. Insofern bietet sich das folgende Vorgehen an:

- **Schritt 1:** Bestehen Zweifel an der Identität der antragstellenden Person, so sind weitere Informationen anzufordern, um die Identität zweifelsfrei festzustellen. Die Monatsfrist zur Beantwortung beginnt erst mit zweifelsfreier Identitätsfeststellung.
- **Schritt 2:** Es bietet sich an, zu ermitteln, ob die antragstellende Person zuvor bereits vergleichbare Anträge gestellt hat. Exzessive Anträge können verweigert oder durch ein angemessenes Entgelt für den Aufwand entschädigt werden.
- **Schritt 3:** Werden sehr viele Daten über die antragstellende Person verarbeitet und sollte der Antrag unspezifisch sein, bietet es sich an zu erwägen, die antragstellende Person um Spezifizierung zu bitten.
- **Schritt 4:** Umfang und Reichweite des Auskunftsbegehrens sind zu ermitteln. Bleibt der Antrag trotz Bitte um Spezifizierung unspezifisch und würde die Bereitstellung der Informationen ganz erheblichen Aufwand generieren (z. B. Durchsuchung aller E-Mail-Konten), könnte das Begehren exzessiv sein. In einem solchen Fall wäre zu erwägen, die Rechtsabteilung einzuschalten.
- **Schritt 5:** Alle Personen, deren Unterstützung erforderlich sein könnte, sind einzubinden (z. B. Personalabteilung, IT).

- **Schritt 6:** Die Datenquellen sind zu identifizieren, die nach den maßgeblichen Informationen durchsucht werden sollen. Informiert werden muss über:
  - die Verarbeitungszwecke;
  - die Kategorien personenbezogener Daten, die verarbeitet werden;
  - die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt werden;
  - die Dauer der Speicherung personenbezogener Daten;
  - das Bestehen eines Rechts auf Berichtigung, Löschung, Einschränkung oder Widerspruch (siehe die entsprechenden Praktischen Hinweise);
  - das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
  - soweit die personenbezogenen Daten nicht bei der antragstellenden Person erhoben wurden: alle verfügbaren Informationen über die Herkunft der Daten;
  - das Bestehen einer automatisierten Entscheidungsfindung (z. B. bei Anträgen im Internet) und *Profiling*, einschließlich Informationen über die involvierte Logik, die Tragweite und angestrebten Auswirkungen einer derartigen Verarbeitung für die antragstellende Person; und
  - bei Übermittlung der Daten in Länder außerhalb der EU: Informationen über geeignete Garantien bei der Übermittlung (z. B. EU Standardvertragsklauseln).
- **Schritt 7:** Daten, die nicht von dem Auskunftsbegehren erfasst sind, sind zu entfernen. Daten, die vertraulich sind wie etwa Geschäftsgeheimnisse oder die sich auf andere Personen beziehen, können z. B. geschwärzt werden.
- **Schritt 8:** Die zu übermittelnden Informationen und die Kopien der Daten sind sodann zusammenzustellen und der antragstellenden Person zu übermitteln.
- **Wichtig:** Die Auskunft darf nur unter sehr wenigen Umständen verweigert, eingeschränkt oder aufschoben werden. Dies ist insbesondere der Fall, wenn der Adressat des Antrags nicht Inhaber der Daten ist – in der Regel wird er dann Auftragsverarbeiter sein – oder wenn Geschäftsgeheimnisse oder eine potentielle Schädigung von Dritten einer Auskunft entgegenstehen. Unter keinen Umständen dürfen Informationen über Dritte offengelegt werden. Darüber hinaus sehen die §§ 32-34 BDSG-neu bestimmte Ausschlüsse vor, die im regelmäßigen Geschäftsverkehr jedoch nur ausnahmsweise anwendbar sein werden.

2.5 Weitere praktische Hinweise

Siehe praktischen Hinweis *Recht auf Datenübertragbarkeit*.

Hinweis: Es bietet sich an, für die effiziente und sichere Bearbeitung von Auskunftsverlangen einen Prozess aufzusetzen und im Unternehmen zu implementieren. In diesem Zusammenhang könnten auch vorformulierte Antwortschreiben erstellt und zur Verfügung gestellt werden.

Einschlägige Hilfestellungen:

Bayerisches Landesamt für Datenschutzaufsicht, Das Auskunftsrecht der betroffenen Person (Stand: 21. Februar 2017)

Abrufbar unter:
www.lda.bayern.de/media

03

Recht auf Berichtigung (Art. 16)

3.1 Überblick

Jede Person kann von demjenigen, der personenbezogene Daten von ihr verarbeitet (der Verantwortliche), verlangen, dass er unverzüglich ihre Person betreffende unrichtige Daten berichtigt (Art. 16 DS-GVO). Darüber hinaus besteht auch ohne einen entsprechenden Berichtigungsantrag die Pflicht, unrichtige personenbezogene Daten zu korrigieren.

3.2 Rahmenbedingungen

- Jede natürliche Person kann einen Antrag auf Berichtigung stellen, d. h. Mitarbeiter, Kunden und sonstige Personen.
- Der Antrag kann formlos gestellt werden, d. h. mündliche Anträge (z. B. per Telefon) sind ebenso zu berücksichtigen und zu bearbeiten wie schriftliche (z. B. per Brief oder E-Mail).
- Der Berichtigungsanspruch verpflichtet den Verantwortlichen, unrichtige Tatsachen zu korrigieren. Demgegenüber müssen unrichtige Werturteile, die auf Grundlage richtiger Daten getroffen wurden, nicht korrigiert werden.
- Das Recht auf Berichtigung besteht auch bei nur minimaler oder durch die betroffene Person selbst verursachter Unrichtigkeit.
- Berichtigung meint gegebenenfalls auch die Vervollständigung oder Aktualisierung von Daten.
- Um ein unzutreffendes Bild im Hinblick auf den Verarbeitungszweck zu korrigieren, müssen unter Umständen weitere zutreffende Daten oder eine Erläuterung zu den bereits gespeicherten Daten hinzugespeichert werden. Ein Recht auf Vervollständigung besteht jedoch nicht, sollte das Unternehmen die zusätzlichen Informationen nicht für den Verarbeitungszweck benötigen.
- Daten sind grundsätzlich aktuell zu halten. Dies gilt nur dann nicht, wenn für den spezifischen Verarbeitungszweck der veraltete Datenbestand relevant ist, z. B. bei der Entscheidung über einen Kreditantrag oder die Begründung eines Arbeitsverhältnisses.
- Die Berichtigung muss durch die jeweils angemessene Maßnahme erfolgen. Mit Blick auf die tatsächlichen Gegebenheiten kann dies die Veränderung, die teilweise oder vollständige Löschung oder die Speicherung ergänzender oder neu erhobener Daten sein.
- Unrichtige personenbezogene Daten sind unverzüglich zu berichtigen.
- Das Unternehmen muss die betroffene Person unverzüglich, spätestens einen Monat nach Eingang des Antrags, über die auf ihren Berichtigungsantrag hin unternommenen Maßnahmen informieren. Kann diese Frist nicht eingehalten werden, muss dies dem Antragsteller unter Angabe von Gründen für die Verzögerung und der (verlängerten) Frist mitgeteilt werden.
- Die Berichtigung hat unentgeltlich zu erfolgen. Ein angemessenes Entgelt kann nur bei offenkundig unbegründeten oder exzessiven Anträgen verlangt werden.

3.3 Warum sollte dies ernst genommen werden?

- Unrichtige Daten können schwerwiegende Auswirkungen auf die betroffene Person haben, z. B. zur Ablehnung eines Kreditantrags oder Arbeitsverhältnisses führen.
- Verstöße gegen das Recht auf Berichtigung können zudem zu sehr hohen Geldbußen führen und erhebliche Reputationsschäden nach sich ziehen.

3.4 Praktisches Vorgehen

Zur Bearbeitung des Berichtigungsantrags bietet sich das folgende Vorgehen an:

- **Schritt 1:** Bestehen Zweifel an der Identität des Antragstellers, sind weitere Informationen anzufordern, um diese zweifelsfrei festzustellen. Die Monatsfrist zur Beantwortung beginnt erst mit zweifelsfreier Identitätsfeststellung.

Hinweis: Sobald zur Bestätigung der Identität weitere Informationen vom Antragsteller eingeholt wurden, müssen diese Informationen nach Bestätigung der Identität wieder gelöscht werden.

- **Schritt 2:** Es bietet sich an, zu prüfen, ob der Antragsteller bereits zuvor vergleichbare Berichtigungsanträge gestellt hat. Bei exzessiven Anträgen kann ein angemessenes Entgelt für den Aufwand verlangt werden.

- **Schritt 3:** Es sollten sämtliche Datenbestände identifiziert werden, in denen die unrichtigen personenbezogenen Daten des Antragstellers gespeichert sind. Der Berichtigungsanspruch umfasst alle Datenbestände (einschließlich Backup-Daten), in denen die unrichtigen Daten gespeichert sind.

- **Schritt 4:** Dabei sind die Personen einzubinden, deren Unterstützung zur Bearbeitung des Antrags benötigt wird (z. B. Personalabteilung, IT, Finance, Marketing, Legal, Datenschutzbeauftragter).

- **Schritt 5:** Die Berichtigung der unrichtigen Daten muss hinsichtlich sämtlicher Datenbestände veranlasst werden, gegebenenfalls auch – unter Beachtung der vorstehend beschriebenen Einschränkungen – durch Aktualisierung oder Vervollständigung.

- **Schritt 6:** Der Antragsteller muss entsprechend informiert werden.

3.5 Besonderheiten

- Übermittelt der Verantwortliche die gespeicherten personenbezogenen Daten der betroffenen Person an andere Empfänger, müssen diese über die Berichtigung der Daten informiert werden, sofern dies vernünftigerweise möglich ist.

- Auf einen Antrag der betroffenen Person hin müssen ihr diese Empfänger genannt werden.

3.6 Weitere praktische Hinweise

Siehe die praktischen Hinweise *Recht auf Löschung und Löschpflicht*, *Recht auf Einschränkung und Auskunftsbegehren.*

Hinweis: Es bietet sich an, für eine effiziente und sichere Bearbeitung von Berichtigungsbegehren sowie zum Nachkommen der Berichtigungspflicht, im Unternehmen entsprechende Prozesse aufzusetzen.

Recht auf Löschung („Recht auf Vergessenwerden“) und Löschpflicht (Art. 17)

04

4.1 Überblick

Recht auf Löschung: Jede Person kann unter gewissen Voraussetzungen von demjenigen, der personenbezogene Daten von ihr verarbeitet (der Verantwortliche), verlangen, dass diese Daten unverzüglich gelöscht werden (Art. 17 DS-GVO).

Löschpflicht: Auch ohne ein entsprechendes Löschverlangen besteht die Pflicht, personenbezogene Daten bei Vorliegen gewisser Voraussetzungen zu löschen.

4.2 Rahmenbedingungen

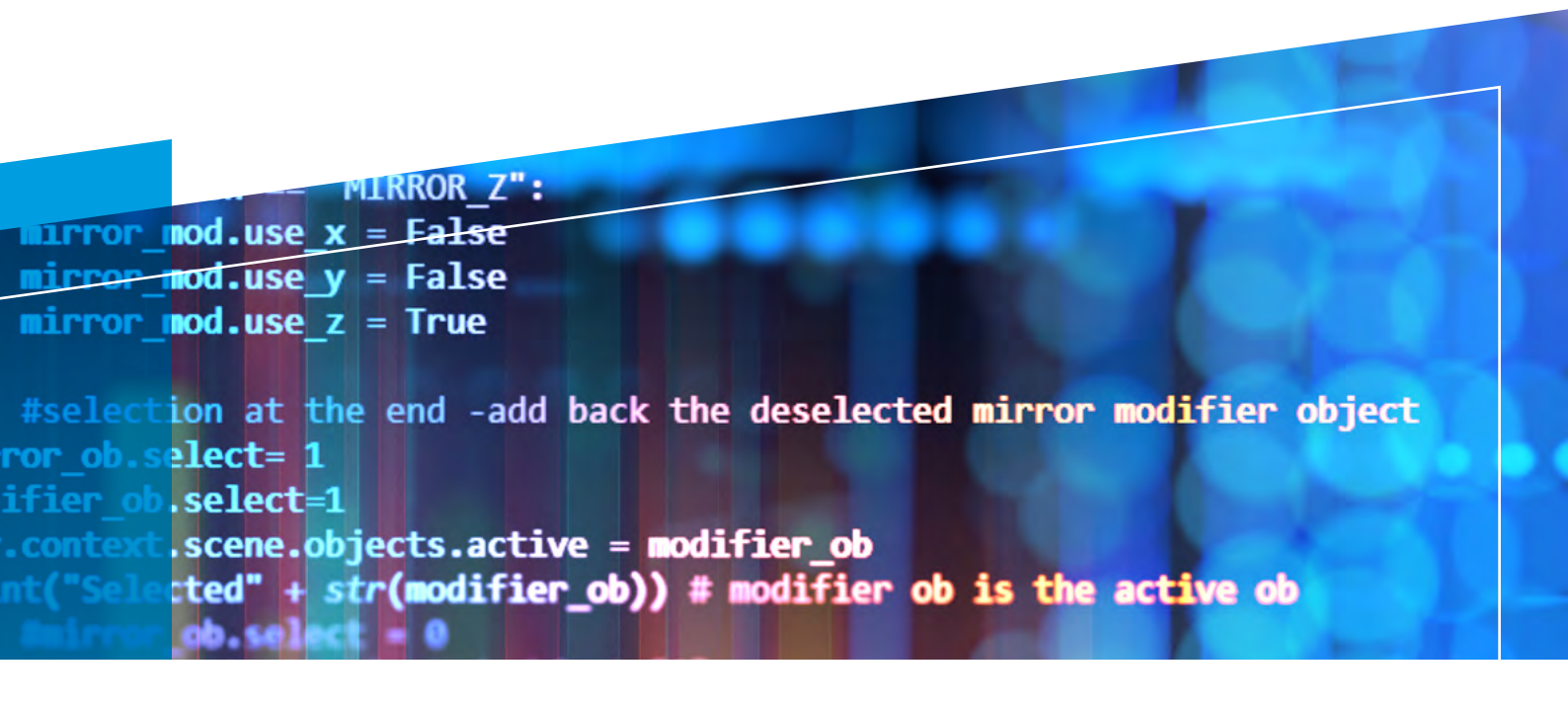
- Jede natürliche Person kann die Löschung ihrer personenbezogenen Daten verlangen, d. h. Mitarbeiter, Kunden und sonstige Dritte. Unternehmen haben dieses Recht nicht.
- Löschanträge können formlos gestellt werden, d. h. mündliche Anträge (z. B. per Telefon) sind ebenso zu berücksichtigen und zu bearbeiten wie schriftliche (z. B. per Brief oder E-Mail).
- Löschanträgen ist unverzüglich, jedoch spätestens nach Ablauf eines Monats ab Zugang des Löschantrags, zu entsprechen. Kann diese Frist nicht eingehalten werden, muss dies dem Antragsteller unter Angabe von Gründen und der (verlängerten) Frist mitgeteilt werden. Die Löschung hat unentgeltlich zu erfolgen.

4.3 Warum sollte dies ernst genommen werden?

- Das Recht, die Löschung seiner Daten verlangen zu können, genießt in einer sich immer weiter digitalisierenden Welt einen hohen Stellenwert. Mit dem sog. „Recht auf Vergessenwerden“ soll dem mit der Digitalisierung verbundenen Risiko für den Einzelnen begegnet werden, nicht mehr „Herr seiner Daten“ zu sein.
- Verstöße gegen das Recht auf Löschung und/oder gegen die Löschpflicht können mit sehr hohen Geldbußen geahndet werden und zu erheblichen Reputationsschäden von Unternehmen führen.

4.4 Wer wird typischerweise die Löschung verlangen?

- (Ehemalige) Mitarbeiter (z. B. Löschung von Personaldaten);
- (Abgelehnte) Bewerber (z. B. Löschung von Bewerberdaten); oder
- Kunden (z. B. Löschung von Kundenprofilen).



4.5 Löschantrag und Löschpflicht

Einem Löschantrag und der Löschpflicht muss nur entsprochen bzw. nachgekommen werden, sofern einer der folgenden Gründe vorliegt:

- Die Daten sind nicht mehr für die Zwecke notwendig, für die sie erhoben bzw. verarbeitet wurden.
- Die Verarbeitung der Daten beruht auf einer vom Antragsteller erteilten Einwilligung, die jedoch widerrufen wurde und es liegen auch keine sonstigen Gründe vor, die eine Verarbeitung rechtfertigen.
- Der Antragsteller hat der Datenverarbeitung widersprochen (Art. 21 DS-GVO).
- Die Datenverarbeitung erfolgte unrechtmäßig.
- Einem Löschantrag muss hingegen nicht nachgekommen werden und es besteht auch keine Löschpflicht, wenn die Verarbeitung der Daten insbesondere erforderlich ist zur:
  - Ausübung des Rechts auf freie Meinungsäußerung und Information;
  - Erfüllung einer rechtlichen Verpflichtung; oder
  - Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (z. B. bei Garantiefällen).

4.6 Praktisches Vorgehen

Zur Bearbeitung eines Löschantrags sollten die folgenden Schritte durchgeführt werden:

- **Schritt 1:** Bestehen Zweifel an der Identität des Antragstellers, sollten von diesem weitere Informationen angefordert werden, um diese zweifelsfrei festzustellen. Die Frist zur Beantwortung beginnt erst mit zweifelsfreier Identitätsfeststellung.
- **Hinweis:** Sobald die Identität aufgrund der Preisgabe weiterer Informationen durch den Antragsteller erfolgreich festgestellt worden ist, müssen diese Informationen wieder gelöscht werden.
- **Schritt 2:** Die zu dieser Person gespeicherten Daten inkl. der folgenden Informationen müssen identifiziert werden:
  - Datenquelle(n) (Herkunft der Daten);
  - Angaben über den Zweck der Verarbeitung, sowie (falls vorhanden) die Rechtsgrundlage der Verarbeitung (z. B. Einwilligung);
  - Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt wurden; und
  - bestehende Widersprüche gegen die Verarbeitung oder Widerrufe der Einwilligung.
- **Schritt 3:** Es müssen die Personen eingebunden werden, deren Unterstützung benötigt wird (z. B. Personalabteilung, IT, Finanzen, Marketing).
- **Schritt 4:** Es muss geprüft werden, ob der Antragsteller aufgrund des Vorliegens einer der unter *Nummer 4.5* genannten Gründe einen Anspruch auf Löschung hat bzw. ob der Antrag aufgrund der unter *Nummer 4.5* genannten Gründe abgelehnt werden kann.
- **Schritt 5:** Abhängig von Schritt 4 muss entweder die Löschung beantragt und dem Antragsteller eine entsprechende Bestätigung gesendet oder der Antrag unter Angaben von Gründen abgelehnt werden.
- **Hinweis:** Löschung bedeutet entweder die physische Vernichtung oder Unbrauchbarmachung der personenbezogenen Daten oder – vermutlich der Regelfall – die technische Löschung von einem Datenträger. Die zuständige IT-Abteilung sollte stets miteinbezogen werden, um eine ordnungsgemäße Löschung sicherzustellen.
- Um der Löschpflicht in angemessenem Umfang nachkommen zu können, muss regelmäßig geprüft werden, ob die unter *Nummer 4.5* genannten Gründe, die eine Speicherung rechtfertigen, weiterhin vorliegen. Sind diese nicht mehr gegeben, sollte wie vorstehend beschrieben verfahren werden.

4.7 Besonderheiten

- Sollten personenbezogene Daten eines Antragstellers öffentlich gemacht worden sein, müssen im Falle eines Löschantrags nicht nur diese Daten gelöscht werden, sondern auch andere Verantwortliche (z. B. weitere Gruppengesellschaften) vom Löschantrag in Kenntnis gesetzt werden, die diese Daten ebenfalls verarbeiten.

- Gemäß dem neuen BDSG besteht im Falle einer nicht automatisierten Datenverarbeitung das Recht des Betroffenen auf Löschung bzw. die Verpflichtung zur Löschung seitens des Verantwortlichen gemäß der DS-GVO nicht, sofern die Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und das Interesse des Betroffenen an der Löschung als gering anzusehen ist (§ 35 BDSG). In einem solchen Fall tritt an die Stelle des Rechts auf Löschung das Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO).

4.8 Weitere praktische Hinweise

Siehe praktischen Hinweis *Recht auf Einschränkung der Verarbeitung*.

Hinweis: Es bietet sich an, für die effiziente und sichere Bearbeitung von Löschanträgen einen Prozess im Unternehmen aufzusetzen.

Einschlägige Hilfestellungen:

Datenschutzkonferenz (DSK) des Bundes und der Länder, Recht auf Löschung „Recht auf Vergessenwerden“ (Kurzpapier Nr. 11 vom 29. August 2017)

Abrufbar unter:
www.lda.bayern.de/media

Recht auf Einschränkung der Verarbeitung (Art. 18)

Vorläufiges Schutzrecht, wenn die Löschung (noch) nicht angemessen ist

Einschränkungsvermerk
Sperrung
Umsetzung

05

5.1 Überblick

Jede Person kann von jeder öffentlichen (z. B. einer Behörde) oder privaten Stelle (z. B. einem Unternehmen), die personenbezogene Daten von ihr verarbeitet (der Verantwortliche), die Einschränkung der Verarbeitung dieser Daten verlangen (Art. 18 DS-GVO).

Das Recht auf Einschränkung ist lediglich ein vorläufiges Schutzrecht und somit „weniger" als das Recht auf Löschung.

5.2 Rahmenbedingungen

- Jede natürliche Person kann die Einschränkung der Verarbeitung ihrer personenbezogenen Daten verlangen, d. h. Mitarbeiter, Kunden und sonstige Dritte. Unternehmen haben dieses Recht nicht.

- Der Antrag auf Einschränkung der Datenverarbeitung kann formlos gestellt werden, d. h. mündliche Anträge (z. B. per Telefon) sind ebenso zu berücksichtigen und zu bearbeiten wie schriftliche (z. B. per Brief oder E-Mail).

- Anträgen auf Einschränkung der Datenverarbeitung ist unverzüglich, jedoch spätestens nach Ablauf eines Monats ab Zugang des Antrags, zu entsprechen. Kann diese Frist nicht eingehalten werden, muss dies dem Antragsteller unter Angabe von Gründen für die Verzögerung sowie der (verlängerten) Frist mitgeteilt werden. Die Einschränkung hat unentgeltlich zu erfolgen. Ein angemessenes Entgelt kann lediglich bei offenkundig unbegründeten oder exzessiven Anträgen verlangt werden.

5.3 Warum sollte dies ernst genommen werden?

- Das Recht auf Einschränkung der Verarbeitung dient einem (vorläufigen) Ausgleich zwischen den Interessen des Antragstellers an seinen personenbezogenen Daten und den Interessen des Verantwortlichen an deren Verarbeitung.

- Verstöße gegen das Recht auf Einschränkung der Verarbeitung können mit sehr hohen Geldbußen geahndet werden und zu erheblichen Reputationsschäden führen.

5.4 Wer wird typischerweise einen Antrag auf Einschränkung der Datenverarbeitung stellen?

- (Ehemalige) Mitarbeiter (z. B. Einschränkung von Personaldaten);

- (Abgelehnte) Bewerber (z. B. Einschränkung von Daten in Bewerberdatenbank); oder

- Kunden (z. B. Einschränkung von Kundendaten).

5.5 Das Recht auf Einschränkung der Verarbeitung personenbezogener Daten im Detail

Einem Antrag auf Einschränkung der Verarbeitung personenbezogener Daten muss entsprochen werden, sofern eine der folgenden Voraussetzungen erfüllt ist:

- Der Antragsteller bestreitet die Richtigkeit der von dem Verantwortlichen gespeicherten Daten. In diesem Fall erfolgt die Einschränkung der Datenverarbeitung begrenzt für die Dauer der Überprüfung der Richtigkeit der in Frage stehenden Daten durch den Verantwortlichen.

- Die Verarbeitung von personenbezogenen Daten des Antragstellers durch den Verantwortlichen ist unrechtmäßig, aber der Antragsteller lehnt die Löschung der Daten ab und verlangt stattdessen die Einschränkung der Nutzung.

- Der Verantwortliche benötigt die personenbezogenen Daten des Antragstellers nicht mehr für Zwecke der Verarbeitung, der Antragsteller benötigt sie allerdings zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

- Der Antragsteller hat allgemein Widerspruch gegen die Verarbeitung seiner Daten durch den Verantwortlichen eingelegt (Art. 21 DS-GVO). In diesem Fall erfolgt die Einschränkung der Datenverarbeitung bis zu dem Zeitpunkt, in dem endgültig feststeht, ob die Interessen des Antragstellers die berechtigten Interessen des Verantwortlichen an der Verarbeitung der Daten überwiegen.

5.6 Umsetzung der Einschränkung

Ist eine der vorstehend genannten Voraussetzungen erfüllt, sind die personenbezogenen Daten des Antragstellers einzuschränken. Hierfür:

- müssen die betreffenden Daten, Datensätze oder gegebenenfalls auch ganze Dateien dahinter mit einem Einschränkungsvermerk dahingehend kenntlich gemacht werden, dass sie gespeichert bleiben, aber nicht mehr anderweitig verarbeitet werden dürfen; und

- muss technisch und organisatorisch effektiv sichergestellt werden, dass die Daten tatsächlich nicht mehr verarbeitet und auch nicht mehr verändert werden können. Hierzu kann man sie z. B. vorübergehend auf ein anderes Verarbeitungssystem übertragen, für Nutzer sperren (z. B. durch ein Passwort), oder veröffentlichte Daten (z. B. auf einer Webseite) entfernen.

Die eingeschränkten Daten dürfen in Ausnahmefällen trotz der Einschränkung verarbeitet werden, jedoch nur noch:

- mit Einwilligung des Antragstellers;

- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Antragstellers;

- zum Schutz der Rechte einer anderen natürlichen oder juristischen Person; oder

- aus Gründen öffentlichen Interesses (z. B. Forschungszwecke).

5.7 Praktisches Vorgehen

Zur Bearbeitung des Antrags auf Einschränkung bietet sich das folgende Vorgehen an:

- **Schritt 1:** Bestehen Zweifel an der Identität des Antragstellers, sollten von ihm weitere Informationen angefordert werden, um diese zweifelsfrei feststellen zu können. Die Frist zur Beantwortung beginnt erst mit zweifelsfreier Identitätsfeststellung.

Hinweis: Sobald die Identität aufgrund der Preisgabe weiterer Informationen durch den Antragsteller erfolgreich festgestellt worden ist, müssen diese Informationen wieder gelöscht werden.

- **Schritt 2:** Anhand der in *Nummer 4* genannten Vorgaben muss geprüft werden, ob eine der Voraussetzungen erfüllt ist, die eine Einschränkung der Verarbeitung von personenbezogenen Daten des Antragstellers notwendig macht.

- **Schritt 3:** Die zur Person des Antragstellers gespeicherten Daten müssen identifiziert werden. Möglicherweise sind nicht alle gespeicherten Daten von dem Einschränkungsbegehren erfasst.

- **Schritt 4:** Es müssen die Personen eingebunden werden, deren Unterstützung benötigt werden könnte (z. B. Personalabteilung, IT, Finance, Marketing, Legal, Datenschutzbeauftragter).

- **Schritt 5:** Abhängig von Schritt 2 muss entweder die Einschränkung der Verarbeitung veranlasst und dem Antragsteller eine entsprechende Bestätigung gesendet oder der Antrag unter Angaben von Gründen abgelehnt werden.

- **Schritt 6:** Im Falle einer Einschränkung der Verarbeitung muss die Umsetzung entsprechend den Vorgaben in *Nummer 5* veranlasst werden. In diesem Zusammenhang sollte die zuständige IT-Abteilung eingeschaltet werden, um sicherzustellen, dass die Einschränkung ordnungsgemäß erfolgt.

- **Schritt 7:** Es muss sichergestellt werden, dass der Antragsteller vorab unterrichtet wird, wenn zu einem späteren Zeitpunkt die Einschränkung der Verarbeitung wieder aufgehoben wird.

5.8 Weitere praktische Hinweise

Siehe praktischen Hinweis *Recht auf Löschung („Recht auf Vergessenwerden“) und Löschpflicht*.

Hinweis: Es bietet sich an, für die effiziente und sichere Bearbeitung von Anträgen auf Einschränkung der Datenverarbeitung einen Prozess im Unternehmen aufzusetzen. Wie auch für die Bearbeitung von Auskunftsverlangen, empfiehlt es sich, vorformulierte Antwortschreiben zu erstellen.

Einschlägige Hilfestellungen:

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz – Texte und Erläuterungen, Juni 2018, S. 59 ff.

Abrufbar unter:
www.bfdi.bund.de

06 Recht auf Datenübertragbarkeit (Art. 20)

6.1 Überblick

Jede Person kann unter bestimmten Voraussetzungen von demjenigen, dem sie personenbezogene Daten bereitgestellt hat (der Verantwortliche), verlangen, diese Daten zu erhalten oder diese Daten an einen anderen Verantwortlichen zu übermitteln (Art. 20).

Dieses Recht auf Datenübertragbarkeit ist besonders bei der Beendigung von Arbeitsverhältnissen sowie beim Onlinehandel relevant.

6.2 Rahmenbedingungen

- Jede natürliche Person kann die Übertragung der von ihr bereitgestellten Daten verlangen. Typischerweise machen (ehemalige) Mitarbeiter (z. B. bei der Übertragung von Personaldaten an einen neuen Arbeitgeber) oder Kunden (z. B. bei der Übertragung von Kundendaten im Online Handel) von diesem Recht Gebrauch.

- Übertragungsbegehren können formlos gestellt werden, d. h. mündliche Anträge (z. B. per Telefon) sind ebenso zu berücksichtigen und zu bearbeiten wie Schriftliche (z. B. per Brief oder E-Mail).

- Übertragungsbegehren ist so schnell wie vernünftigerweise möglich, jedoch spätestens nach Ablauf eines Monats ab Zugang des Übertragungsbegehrens, zu entsprechen. Kann diese Frist nicht eingehalten werden, muss dies der gesuchstellenden Person unter Angabe der (verlängerten) Frist mitgeteilt werden. Die Übertragung hat unentgeltlich zu erfolgen. Ein angemessenes Entgelt kann nur bei offenkundig unbegründeten oder exzessiven Begehren verlangt werden.

- Erfüllt ein Übertragungsbegehren alle Voraussetzungen, kann die gesuchstellende Person bestimmen, ob der Verantwortliche die Daten der Person selbst bereitstellen soll oder diese direkt an einen anderen, von der Person benannten Verantwortlichen, übermitteln soll.

6.3 Warum sollte dies ernst genommen werden?

- Ähnlich dem Recht auf Auskunft, soll der Person im Rahmen der automatischen Verarbeitung die Kontrolle über ihre personenbezogenen Daten gegeben werden. Darüber hinaus soll ein unkomplizierter Datenwechsel von einem Verantwortlichen zu einem anderen (z. B. Arbeitgeber oder Diensteanbieter) ermöglicht werden.

- Verstöße gegen das Recht auf Datenübertragbarkeit können mit sehr hohen Geldbußen geahndet werden und zu erheblichen Reputationsschäden führen.

6.4 Praktisches Vorgehen

Zur Bearbeitung des Übertragungsbegehrens sind beispielsweise die folgenden Schritte empfehlenswert:

- **Schritt 1:** Soweit Zweifel an der Identität der gesuchstellenden Person bestehen, sollte der Verantwortliche von dieser weitere Informationen anfragen, um die Identität zweifelsfrei festzustellen. Die Monatsfrist zur Beantwortung beginnt erst mit zweifelsfreier Identitätsfeststellung. Informationen, die hierfür erhoben worden sind, müssen nach erfolgreicher Identitätsfeststellung gelöscht werden.

- **Schritt 2:** Der Verantwortliche sollte prüfen, ob die gesuchstellende Person einen Anspruch auf Datenübertragung hat oder der Antrag abgelehnt werden kann. Einem Übertragungsbegehren muss nur nachgekommen werden, soweit die Daten:

  – von der gesuchstellenden Person selbst bereitgestellt worden sind und sie selbst betreffen;

  – auf der Grundlage einer wirksamen Einwilligung der Person oder eines Vertrags mit der Person durch den Verantwortlichen verarbeitet worden sind; und

  – unter Einsatz einer Datenverarbeitungsanlage (automatisiertes Verfahren) verarbeitet worden sind.

Einem Übertragungsbegehren muss demnach nicht für solche Daten entsprochen werden, die:

– nicht von der gesuchstellenden Person selbst bereitgestellt worden sind. Als bereitgestellt von der Person gelten auch Daten, die bei einer Nutzung von Diensten durch die Person automatisch generiert worden sind (z. B. online login). Ausgenommen sind aber Daten, die der Verantwortliche selbst erstellt hat (z. B. bei einer Bonitätsprüfung);

– nicht die gesuchstellende Person, sondern einen Dritten betreffen oder anonym sind;

– durch den Verantwortlichen nicht auf der Grundlage einer wirksamen Einwilligung oder eines Vertrags verarbeitet worden sind, sondern aufgrund einer anderen gesetzlichen Erlaubnisnorm; oder

– nicht unter Einsatz einer Datenverarbeitungsanlage, sondern manuell verarbeitet worden sind.

- **Schritt 3:** Der Verantwortliche sollte diejenigen Personen einbinden, deren Unterstützung zur Bearbeitung des Übertragungsbegehrens benötigt wird (z. B. Personalabteilung, IT, Finanzen, Marketing).

- **Schritt 4:** Anhand der in Schritt 2 genannten Vorgaben sollten die personenbezogenen gespeicherten Daten ermittelt werden, für die der Anspruch auf Datenübertragung besteht. Besteht kein Anspruch, so sollte der Antrag unter Angaben von Gründen abgelehnt werden.

- **Schritt 5:** Soweit ein Anspruch besteht, sollte der Verantwortliche prüfen, ob die Person den Erhalt der Daten oder die direkte Übermittlung der Daten an einen anderen Verantwortlichen verlangt hat. In letzterem Fall sollte weiter geprüft werden, ob die Übermittlung an den Verantwortlichen technisch möglich ist.

- **Schritt 6:** Daraufhin sollte die Bereitstellung der Daten an die gesuchstellende Person oder die Übermittlung an den anderen Verantwortlichen veranlasst werden und der gesuchstellenden Person eine entsprechende Bestätigung zugesendet werden.

6.5 Weitere praktische Hinweise

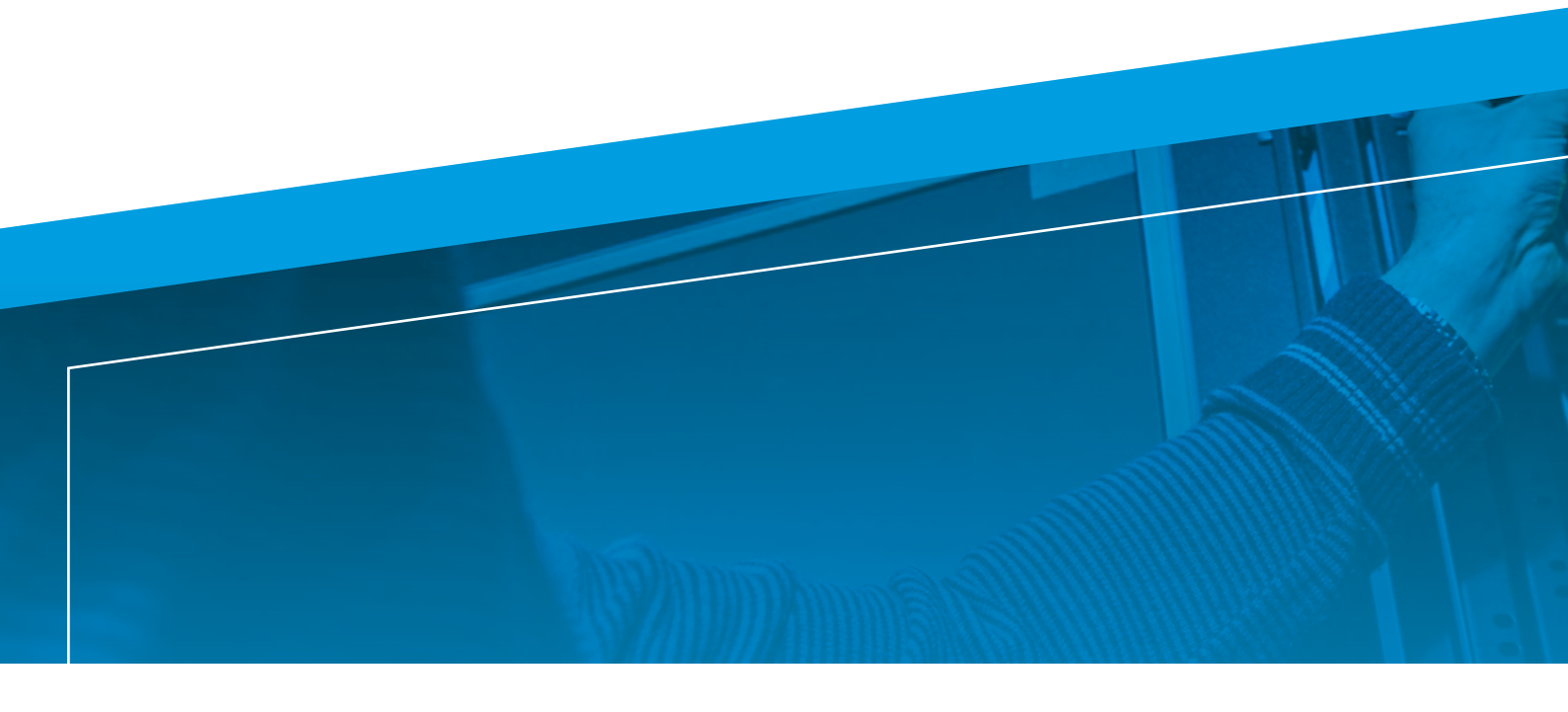
Siehe die praktischen Hinweise *Recht auf Einschränkung der Verarbeitung*, *Recht auf Löschung und Löschpflicht* sowie *Auskunftsrecht*.

Hinweis: Die Daten müssen in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden. Dabei ist ein konkretes Format nicht vorschrieben. Nach dem derzeitigen Stand sind etwa XML, HTML, Microsoft Excel oder PDF möglich. Es bietet sich an, für die effiziente und sichere Bearbeitung von Datenübertragbarkeitsverlangen, einen Prozess aufzusetzen und im Unternehmen zu implementieren. In diesem Zusammenhang können auch vorformulierte Antwortschreiben erstellt und zur Verfügung gestellt werden.

Einschlägige Hilfestellungen:

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz – Texte und Erläuterungen, Juni 2018, S. 62 f.

Abrufbar unter:
www.bfdi.bund.de



Widerspruchsrecht (Art. 21)

07

7.1 Überblick

Jede Person kann unter bestimmten Umständen der Verarbeitung ihrer personenbezogenen Daten widersprechen, (i) soweit die Datenverarbeitung für Aufgaben im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt oder zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erfolgt, (ii) bei Direktwerbung sowie (iii) bei einer Verarbeitung zu Forschungs- oder Statistikzwecken (Art. 21 DS-GVO).

7.2 Rahmenbedingungen

- Liegen die einschlägigen Voraussetzungen vor, kann ein Widerspruch von der Person eingelegt werden, deren personenbezogene Daten verarbeitet werden.

Hinweis: Der Verarbeiter muss die betroffene Person auf ihr Widerspruchsrecht ausdrücklich hinweisen. Dies sollte spätestens bei der ersten Kommunikation sowie getrennt von anderen Informationen geschehen. Ein ausdrückliches Hinweisen wird bereits bei getrennten Absätzen oder Unterstreichen der Information anzunehmen sein. Einzig bei Verarbeitungen zu Forschungs- oder Statistikzwecken besteht eine solche Hinweispflicht nicht.

- Der Widerspruch kann formlos erfolgen. Er erfordert lediglich eine in irgendeiner Weise erfolgte Artikulation des Widerspruchswillens der betroffenen Person gegenüber dem Verantwortlichen.

- Das Widerspruchsbegehren ist innerhalb einer angemessenen Frist, spätestens jedoch innerhalb eines Monats zu beantworten. Kann diese Frist nicht eingehalten werden, ist der betroffenen Person dies unter Angabe von Gründen sowie der neuen Frist mitzuteilen.

- Ein wirksamer Widerspruch bewirkt automatisch ein Verbot der weiteren Verarbeitung für die vom Widerspruch erfassten Zwecke.

- Die Prüfung und gegebenenfalls Umsetzung eines Widerspruchsbegehrens hat unentgeltlich zu erfolgen.

7.3 Warum sollte dies ernst genommen werden?

- Das Widerspruchsrecht trägt dem Gedanken Rechnung, dass auch eigentlich rechtmäßige Datenverarbeitungen dem Interesse der schutzbedürftigen betroffenen Person zuwiderlaufen können.

- Verstöße gegen das Widerspruchsrecht können mit sehr hohen Geldbußen geahndet werden und zu erheblichen Reputationsschäden führen.

7.4 Praktisches Vorgehen

Im Falle eines Widerspruchs bietet sich das folgende Vorgehen an:

- **Schritt 1:** Bestehen Zweifel an der Identität der widersprechenden Person, so sind weitere Informationen anzufordern, um die Identität zweifelsfrei festzustellen. Die Monatsfrist zur Beantwortung beginnt erst mit zweifelsfreier Identitätsfeststellung.

- **Schritt 2:** Alle Personen, deren Unterstützung erforderlich sein könnte, sind einzubinden (z. B. Personalabteilung, IT, Finance, Marketing, Legal, Datenschutzbeauftragter).

- **Schritt 3:** Für die Prüfung der Voraussetzungen eines Widerspruchs sowie der möglichen Ausnahmen ist zwischen den unterschiedlichen Verwendungszwecken zu unterscheiden:

  – Bei Verarbeitungen zur Wahrnehmung von Aufgaben, die im öffentlichen Interesse liegen oder die zur Ausübung öffentlicher Gewalt dienen, kann die betroffene Person grundsätzlich nur Widerspruch einlegen, wenn die Verarbeitung ausschließlich auf diesen Zwecken beruht. Die betroffene Person muss weiterhin Widerspruchsgründe nennen, die sich aus ihrer besonderen Situation ergeben. Eine solche folgt aus einer besonderen Schutzwürdigkeit der betroffenen Person (z. B. durch besondere familiäre Umstände oder geschäftliche Geheimhaltungsinteressen).

Hinweis: Im Einzelfall kann eine Datenverarbeitung durch den Verantwortlichen dennoch zulässig sein. Dafür muss der Verantwortliche darlegen, dass die Datenverarbeitung aus zwingenden schutzwürdigen Gründen nötig ist, welche die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen. Dies ist der Fall, wenn der Betroffene seine legitimen Ziele nur durch die Verarbeitung erreichen kann. Geringfügige Mehrkosten oder Umsatzverluste sind davon nicht umfasst. Weiterhin kann eine Verarbeitung zulässig sein, wenn diese der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

– Ein Widerspruch gegen Direktwerbung ist jederzeit möglich. Die einzige Voraussetzung ist, dass sich die Verarbeitung nicht noch auf weitere Zwecke und Erlaubnistatbestände stützt. Direktwerbung umfasst unmittelbare Ansprachen eines Nachfragers, z. B. durch Prospekte, Kataloge, automatische Anrufsysteme, E-Mails oder SMS, mit dem Ziel, den entgeltlichen Absatz von Waren oder die Erbringung von Dienstleistungen zu fördern.

– Bei einem Widerspruch gegen Verarbeitungen zu Forschungs- oder Statistikzwecken muss die betroffene Person ebenfalls Widerspruchsgründe darlegen, die sich aus ihrer besonderen Situation ergeben.

Hinweis: Eine Ausnahme von dem Recht zum Widerspruch kann vorliegen, soweit die Verarbeitung für eine im öffentlichen Interesse liegende Aufgabe unbedingt notwendig ist. Der Verantwortliche hat dabei darzulegen, warum das Interesse an dieser Verarbeitung gegenüber dem Interesse des Betroffenen überwiegt.

- **Schritt 4:** Sind die oben genannten Voraussetzungen für einen Widerspruch erfüllt und legt der Verantwortliche keine entgegenstehenden Gründe dar, ist dem Widerspruchsbegehren zu entsprechen und die weitere Verarbeitung der Daten zu unterlassen.
- **Schritt 5:** Stimmt der Verantwortliche einer Beendigung der Verarbeitung nicht zu, ist dies zu begründen. Die betroffene Person ist über ihre Möglichkeit zur Beschwerde bei einer Aufsichtsbehörde bzw. zu einem gerichtlichen Rechtsbehelf zu informieren.

Wichtig: Bis zur endgültigen Prüfung des Widerspruchs hat die betroffene Person einen Anspruch auf Einschränkung der Verarbeitung.

Wichtig: Bei Vorliegen eines zulässigen Widerspruchs besteht für den Verantwortlichen grundsätzlich auch eine Löschverpflichtung. Soweit der Verantwortliche die Daten veröffentlicht hat, sind auch Dritte über das Bestehen einer Löschpflicht zu informieren.

7.5 Weitere praktische Hinweise

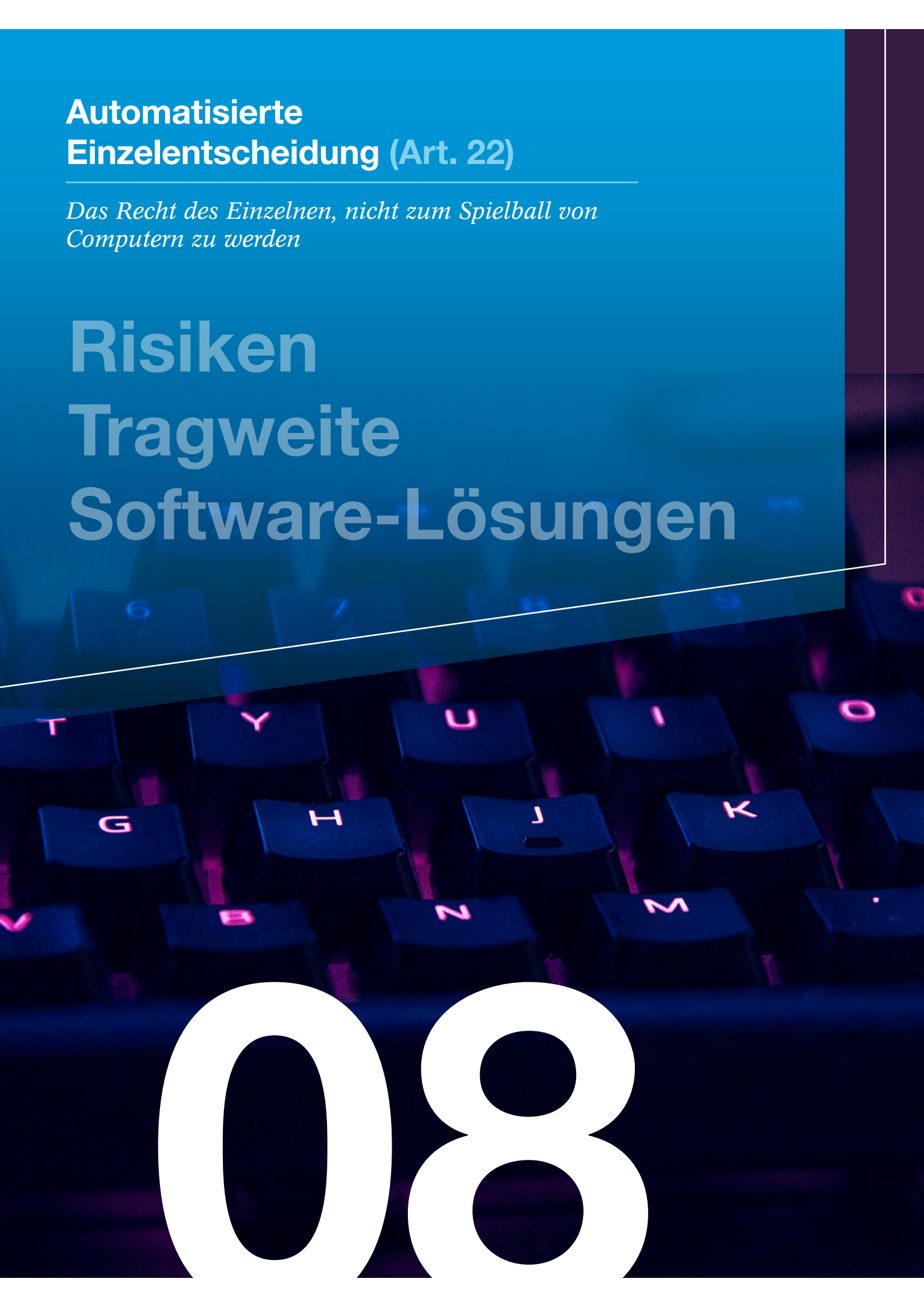
Siehe die praktischen Hinweise *Recht auf Löschung und Löschpflicht*; *Recht auf Einschränkung der Verarbeitung* sowie *Informationspflicht*.

Hinweis: Es bietet sich an, für die effiziente und sichere Bearbeitung von Widersprüchen einen Prozess aufzusetzen und im Unternehmen zu implementieren. In diesem Zusammenhang können auch vorformulierte Antwortschreiben erstellt und zur Verfügung gestellt werden.

Automatisierte Einzelentscheidung (Art. 22)

Das Recht des Einzelnen, nicht zum Spielball von Computern zu werden

Risiken
Tragweite
Software-Lösungen



08

8.1 Rahmenbedingungen

Das Verbot der automatisierten Einzelentscheidung besteht, wenn:

- eine Entscheidung ausschließlich automatisiert (d. h. ohne menschliches Zutun) getroffen wird; und
- diese Entscheidung einer Person gegenüber rechtliche Wirkung entfaltet (z. B. Nichtgewähren bestimmter Leistungen) oder diese Person in ähnlicher Weise erheblich beeinträchtigt (z. B. Ablehnung einer bestimmten Zahlungsart).

Hinweis: Ausnahmsweise sind automatisierte Entscheidungen erlaubt, wenn diese z. B. für den Abschluss eines Vertrags erforderlich sind (z. B. Bonitätsprüfung bei Online-Käufen) oder wenn sie auf der Grundlage besonderer Rechtsvorschriften (z. B. zur Betrugsbekämpfung) oder auf Basis einer wirksamen Einwilligung erfolgen.

Hinweis: Selbstverständlich muss auch die der Entscheidung zugrundeliegende Datenverarbeitung als solche rechtmäßig erfolgen. Dies ist wie immer nach den allgemeinen Grundsätzen zu bestimmen.

8.2 Warum sollte dies ernst genommen werden?

- Es soll verhindert werden, dass Betroffene (z. B. Kunden) zum bloßen Objekt eines automatisierten Entscheidungsprozesses werden.
- Risiken für die Persönlichkeit und Diskriminierungen aufgrund computergesteuerter Abläufe sollen vermieden werden.
- Jeder Mensch hat ein Recht auf ein faires und transparentes Verfahren.

8.3 Wann ist die automatisierte Einzelentscheidung verboten?

- Das Verbot betrifft nur automatisch ausgeführte Entscheidungen, die auf einer automatisierten, maschinellen Verarbeitung beruhen.
- **Automatische Entscheidung:** Immer, wenn maschinell verarbeitete Daten unmittelbar zu einer Entscheidung führen, diese ausschließlich computergestützt erfolgt und jeder Mitbestimmung oder Bewertung durch eine natürliche Person entzogen ist.
  - **Beispiel 1:** Werden automatisch Bewerberrankings erstellt, entscheidet letztlich aber die Personalabteilung über die Eignung von Bewerbern, so liegt keine ausschließlich computergestützte Entscheidung vor.
  - **Beispiel 2:** Erhält ein Bewerber im Laufe eines Online-Bewerbungsprozesses automatisch eine Absage, weil er beim Eintragen in vorbestimmte Felder eine Punktzahl nicht erreicht, fehlt eine menschliche Beurteilung. Es liegt eine automatisierte Einzelentscheidung vor.
  - **Beispiel 3:** Bei einem automatisierten Scoring-Prozess über die Kreditwürdigkeit eines Kunden liegt eine automatisierte Einzelentscheidung nur vor, wenn der Kreditgeber keine inhaltliche Prüfung mehr vornimmt und das Scoring-Ergebnis damit nicht nur eine Grundlage für eine folgende, menschliche Entscheidung darstellt, sondern selbst schon zur Entscheidung führt.
- Die Entscheidung muss für den Betroffenen in irgendeiner Weise negative Rechtswirkungen haben oder ihn in ähnlicher Weise erheblich beeinträchtigen, (z. B. Verweigerung einer Leistung; Nichterfüllung eines Anspruchs; Kündigung eines Vertrags; ehrverletzende Darstellungen). Wird lediglich ein Vertragsabschluss verweigert, bewirkt dies in der Regel aber weder eine negative Rechtsfolge (weil kein Anspruch auf einen Vertragsabschluss besteht) noch eine vergleichbare erhebliche Beeinträchtigung.

8.4 Wann greift das Verbot nicht?

Das Verbot der automatisierten Einzelentscheidung greift nicht, wenn die Entscheidung:

- für einen Vertragsschluss erforderlich ist (allerdings dürfen hierfür keine besonders schützenswerten Daten wie z. B. Gesundheitsdaten verwendet werden);
- aufgrund von Rechtsvorschriften der Mitgliedsstaaten zulässig ist. So erlaubt § 37 Abs. 1 BDSG-neu in Deutschland beispielsweise explizit eine automatisierte Einzelentscheidung, wenn die Entscheidung

im Rahmen der Leistungserbringung nach einem Versicherungsvertrag ergeht und

  - dem Begehren der betroffenen Person stattgegeben wurde oder

  - die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht und der Verantwortliche für den Fall, dass dem Antrag nicht vollumfänglich stattgegeben wird, angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person trifft; oder

- mit ausdrücklicher Einwilligung des Betroffenen erfolgt. Eine solche Einwilligung ist aber nur wirksam, wenn der Betroffene auch deren Tragweite verstehen konnte. Daher ist zu beachten, dass bei der Einholung einer solchen Einwilligung aussagekräftige Informationen über die verwendete Logik sowie die Tragweite und die angestrebten Auswirkungen der Einzelfallentscheidung(en) zur Verfügung zu stellen sind.

8.5 Was außerdem zu beachten ist

- Wenn eine automatisierte Einzelentscheidung ausnahmsweise zulässig ist (siehe *Nummer 8.4*), muss das Unternehmen Vorkehrungen treffen, damit der Betroffene die Entscheidung korrigieren bzw. anfechten kann.

- Daher gilt: Das Unternehmen muss die Betroffenen frühzeitig informieren (Art. 13 Abs. 2 (f) und 14 Abs. 2 (g) DS-GVO), wenn es plant automatisierte Entscheidungen zu verwenden. Diese Information muss aussagekräftig sein mit Blick auf die verwendete Logik, die angestrebten Auswirkungen der Entscheidungen sowie ihre Konsequenzen für den Betroffenen.

8.6 Praktisches Vorgehen

Zur Prüfung, ob die im Unternehmen eingesetzten automatisierten Einzelfallentscheidungen zulässig sind, bietet sich das folgende Vorgehen an:

- **Schritt 1:** Zunächst sind die im Unternehmen existierenden automatisierten Entscheidungsprozesse zu ermitteln und daraufhin zu prüfen, ob die Entscheidung tatsächlich vollständig automatisch erfolgt.

- **Schritt 2:** Falls solche Prozesse bestehen, ist zu prüfen, ob eine Ausnahme gemäß obiger *Nummer 8.4* anwendbar ist.

- **Schritt 3:** Alle Personen, deren Unterstützung erforderlich sein könnte, sind einzubinden (z. B. Personalabteilung, IT, Finance, Marketing, Legal, Datenschutzbeauftragter).

- **Schritt 4:** Greift keine der unter obiger *Nummer 8.4* beschriebenen Ausnahmen, sind die Prozesse sofort einzustellen. Greift eine der Ausnahmen ist sicherzustellen, dass:

  - der Betroffene über die Tatsache der maschinellen Entscheidung informiert wird;

  - der Betroffene über die Gründe für die Ablehnung seines Begehrens informiert wird, falls der Betroffene danach fragt; und

  - der Betroffene das Recht erhält, seinen eigenen Standpunkt darzulegen und die automatisierte Einzelfallentscheidung anzufechten.

- **Schritt 5:** Die vorstehenden Überlegungen sind sorgfältig schriftlich zu dokumentieren und die entsprechende Dokumentation ist an zentraler Stelle im Unternehmen dauerhaft verfügbar zu halten.

Schritte 1 bis 5 gelten entsprechend bei der Überlegung, ob automatisierte Entscheidungsprozesse aufgesetzt oder entsprechende Software-Lösungen beschafft werden dürfen.

8.7 Weitere praktische Hinweise

Siehe praktischen Hinweis *Profiling*.

Hinweis: Es bietet sich an, für den effizienten und sicheren Umgang mit automatisierten Einzelentscheidungen einen Prozess aufzusetzen und im Unternehmen zu implementieren.

09

Profiling (Art. 22)

9.1 Überblick

Ein Profiling im Sinne der Datenschutzgrundverordnung (DS-GVO) liegt vor, wenn ein Unternehmen personenbezogene Daten einer betroffenen Person automatisiert verarbeitet, um persönliche Aspekte, z. B. bezüglich deren Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen oder Verhalten zu analysieren und/oder vorherzusagen. Ein Beispiel hierfür ist die Auswertung des Surf-Verhaltens der Besucher einer Internetseite mittels Analysesoftware.

Ob Profiling und ggf. die anschließende Verwendung eines Profils zulässig ist, ist gemäß den Regeln der DS-GVO zu ermitteln.

Unzulässig ist Profiling regelmäßig jedoch dann, wenn Profiling automatisiert zu Einzelentscheidungen führt, d. h. wenn diese aufgrund eines Profils ausschließlich computergestützt ohne menschliches Zutun gegenüber Individuen getroffen werden (Art. 22 DS-GVO). Dies ist nur in Ausnahmefällen rechtmäßig (siehe praktischer Hinweis *automatisierte Einzelentscheidung*).

Hinweis: Für das Profiling gelten die allgemeinen Regeln der DS-GVO sowie insbesondere das Verbot, gemäß dem Profil ausschließlich automatisiert, eine Entscheidung für oder gegen eine Person zu treffen.

9.2 Rahmenbedingungen

Die Zulässigkeit von Profiling und die Verwendung eines Profils ist in zwei Schritten zu ermitteln:

- Die Erstellung eines Profils ist rechtmäßig, wenn die allgemeinen Grundsätze der Verarbeitung von personenbezogenen Daten eingehalten werden. Dies ist der Fall, wenn die betroffene Person in die Erhebung und Verarbeitung ihrer Daten für die Profilbildung eingewilligt hat oder die Erstellung des Profils gesetzlich erlaubt ist. Dabei ist die Verwendung der personenbezogenen Daten immer auf das erforderliche Minimum zu beschränken.

- Dieselben Voraussetzungen gelten auch für die Verwendung des Profils, soweit dadurch keine Einzelentscheidung getroffen wird.

- Ob diese Voraussetzungen erfüllt sind, ist im Einzelfall zu untersuchen.

  – **Beispiel 1:** Im Rahmen ihres Marketings erstellen Unternehmen häufig Kundenprofile, um bestimmte Gruppen zielgenau werblich ansprechen zu können. Eine damit verbundene Direktwerbung (= Verwendung des Profils) ist rechtmäßig, wenn die betroffene Person (= der Kunde) eingewilligt hat oder das Unternehmen ein überwiegendes legitimes Interesse an der Direktwerbung hat. Das ist unter der DS-GVO regelmäßig der Fall, wenn es sich um einen Bestandskunden handelt, und die Daten des Kunden bei der Einteilung in Zielgruppen für bestimmte Werbung in pseudonymisierter Weise verwendet werden. Direktmarketing sollte daher stets rechtlich geprüft werden. In vielen Ländern bestehen weitere gesetzliche Anforderungen an ein Direktmarketing.

  – **Beispiel 2:** Auch kann es beispielsweise bei Rückrufaktionen rechtmäßig sein, Profile innerhalb der CRM Datenbank zu bilden und diese für einen solchen Zweck zu verwenden. Zu prüfen ist jedoch stets, ob im Einzelfall Interessen der betroffenen Personen entgegenstehen.

9.3 Warum sollte dies ernst genommen werden?

- Big Data Anwendungen, Robotik und künstliche Intelligenz beeinflussen Arbeitsabläufe in Unternehmen. Insbesondere Personaldaten und CRM Daten werden systematisch und automatisiert verarbeitet, um Profile zu bilden und aus diesen Schlüsse zu ziehen.

- Der Einzelne soll davor geschützt werden, zum bloßen Objekt eines automatisierten Entscheidungsprozesses zu werden.

- Risiken für die Persönlichkeit sowie Diskriminierungen durch computergesteuerte Abläufe sollen verhindert werden.

9.4 Widerspruchsrecht beim Profiling auf Basis einer Interessenabwägung

- Die betroffene Person kann der Verwendung ihres Profils jederzeit widersprechen – selbst wenn die Erstellung des Profils rechtmäßig ist – wenn (i) das Profil auf Basis einer Interessenabwägung (Art. 6 Abs. 1 (f) DS-GVO) erfolgt und (ii) der Widerspruch mit der Sondersituation der betroffenen Person begründet wird.

- Als Sondersituation gelten atypische Situationen besonders schutzwürdiger Interessen (z. B. Krankheit, familiäre Krisen).

Hinweis: Die betroffene Person kann formlos widersprechen und muss den Widerspruch auch nicht ausdrücklich als solchen bezeichnen. Sie muss den Widerspruch aber mit ihrer Sondersituation begründen. Ein allgemeiner Widerspruch ist unzureichend.

9.5 Widerspruchsrecht bei Profiling für Direktmarketing

- Die betroffene Person kann der Verwendung ihres Profils insbesondere auch dann widersprechen, wenn das Unternehmen das Profil für gezielte und an die betroffene Person gerichtete Werbung, gleich in welcher Form, verwendet. Dazu reicht es, dass die Werbung mit dem Profiling in Zusammenhang steht.

Hinweis: Die betroffene Person muss den formlosen Widerspruch gegen das Direktmarketing auf Basis des erstellten Profils nicht begründen.

9.6 Wie ist mit einem Widerspruch umzugehen?

Hinweis: Das Unternehmen sollte der betroffenen Person immer unverzüglich bestätigen, dass ihr Widerspruch eingegangen ist und dieser sodann geprüft wird.

- Widerspruchsrecht bei Profiling, das auf einer Interessenabwägung basiert: Das Unternehmen muss unverzüglich, spätestens jedoch innerhalb eines Monats, über den Widerspruch entscheiden und die betroffene Person über die Entscheidung informieren. Dazu führt das Unternehmen eine erneute Interessenabwägung durch, die nunmehr auch die im Rahmen des Widerspruchs geltend gemachte Sondersituation einbezieht. Auch muss das Unternehmen die Verwendung des Profils bis zu einer Entscheidung aussetzen.

- Widerspruchsrecht bei Profiling für Direktmarketing: Das Unternehmen muss die Werbung auf Basis des Profiling unmittelbar einstellen. Es besteht dabei kein Entscheidungsspielraum.

9.7 Hinweispflicht bezüglich Widerspruchsrecht

- Das Unternehmen muss die betroffene Person informieren, dass sie dem Profiling widersprechen kann. Der Hinweis sollte spätestens zum Zeitpunkt der ersten Kommunikation erfolgen und in jedem Fall vor Beginn der Verarbeitung.

- Die betroffene Person muss die Zusammenhänge verstehen können. Der Hinweis muss daher in klarer und einfacher Sprache verfasst sein.

- Erfolgt der Hinweis in einer Werbe-E-Mail, sollte dieser immer hervorgehoben werden (z. B. Fettschrift und Box).

9.8 Was ist außerdem zu beachten?

- Wenn ein Unternehmen Profiling verwendet, muss es die betroffenen Personen darüber informieren (Art. 13 und 14 DS-GVO). Das Unternehmen muss sie informieren, dass ihre personenbezogenen Daten für Profilbildungen und anknüpfende Maßnahmen (z. B. Direktwerbung) verwendet werden. Auch müssen die betroffenen Personen informiert werden, welche Konsequenzen damit verbunden sind.

- Die durch das Profiling gewonnene Bewertung darf nur sehr eingeschränkt, im Rahmen von automatisierten Einzelentscheidungen, genutzt werden (siehe praktischer Hinweis *automatisierte Einzelentscheidung*).

- Jede Person kann von dem Verantwortlichen Auskunft darüber verlangen, ob – und wenn ja – welche Daten über sie verarbeitet werden und eine Kopie der Daten anfordern (Art. 15 DS-GVO) (siehe Praktischer Hinweis *Auskunftsrecht*).

- Ein Unternehmen muss bei Profiling-Aktivitäten eine Datenschutz-Folgenabschätzung durchführen (siehe praktischer Hinweis *Datenschutz-Folgenabschätzung*).

9.9 Praktisches Vorgehen

- **Schritt 1:** Bestehende Profiling-Aktivitäten sind zu identifizieren. Weiter müssen die Hinweis- und Informationspflichten (d. h. insbesondere, dass bestehende Datenschutzerklärungen anzupassen sind, wie in *Nummern 9.7* und *9.8* näher beschrieben) umgesetzt werden. Bei neuen Verarbeitungen ist darauf zu achten, dass betroffene Personen über die Profiling-Aktivitäten informiert und auf das Widerspruchsrecht hingewiesen werden.

- **Schritt 2:** Handelt es sich um Profiling gemäß *Nummer 9.2*, sollte – ggf. mit Hilfe von Rechtsberatern oder dem etwaig in einem Unternehmen bestellten Datenschutzbeauftragten – vor der Erstellung und Verwendung eines Profils geprüft werden, ob die Verarbeitung der personenbezogenen Daten zum Zwecke des Profiling rechtmäßig ist.

- **Schritt 3:** Ggf. mit Hilfe von Rechtsberatern oder dem etwaig im Unternehmen bestellten Datenschutzbeauftragten ist, vor der Erstellung und Verwendung des Profils, auch eine Datenschutz-Folgenabschätzung durchzuführen.

- **Schritt 4:** Die Schritte 1 bis 3 und alle Überlegungen sollten sorgfältig schriftlich dokumentiert werden. Es ist sicherzustellen, dass diese Dokumentation an zentraler Stelle in Ihrem Unternehmen dauerhaft verfügbar gehalten wird.

- **Schritt 5:** Bei Widersprüchen gegen Profiling-Aktivitäten sollte umgehend die für Widersprüche zuständige Abteilung des Unternehmens informiert und mit allen Informationen zu der Profiling-Aktivität versorgt werden.

- **Schritt 6:** Bei einem berechtigten Widerspruch ist sicherzustellen, dass das erstellte Profil nicht weiterverwendet wird und auch die personenbezogenen Daten nicht für weitere Profilbildungen verwendet werden.

9.10 Weitere praktische Hinweise?

Siehe die praktischen Hinweise:
Automatisierte Einzelentscheidung, *Auskunftsrecht* sowie *Datenschutz-Folgeabschätzung*.

10 Datenschutzfreundliche Voreinstellungen (Art. 25)

10.1 Überblick

So viel wie nötig – so wenig wie möglich: Als Standard sollen Unternehmen nur die personenbezogenen Daten verarbeiten, die sie im konkreten Einzelfall tatsächlich benötigen (Art. 25 Abs. 2 DS-GVO).

Im Rahmen der Konzeption und Entwicklung von Datenverarbeitungsprozessen sollten Unternehmen aufgrund der Pflicht zur datenschutzfreundlichen Voreinstellung die folgenden Punkte unbedingt beachten.

10.2 Rahmenbedingungen

- Die Pflicht zur datenschutzfreundlichen Voreinstellung umfasst:
  - die Menge der erhobenen personenbezogenen Daten;
  - den Verarbeitungsumfang;
  - die Speicherdauer; und
  - die Zugänglichkeit der personenbezogenen Daten für Dritte.
- Alle diese Anforderungen sind am Kriterium der Erforderlichkeit zu messen. Erforderlich ist nur, was nicht auf einem weniger eingriffsintensiven Weg erreicht werden kann.
- Die Pflicht zur datenschutzfreundlichen Voreinstellung gilt nicht rückwirkend, d. h. betroffen sind lediglich Datenverarbeitungen, die nach dem 25. Mai 2018 erfolgen.

Hinweis: Unternehmen, die ein datenschutzspezifisches Zertifizierungsverfahren erfolgreich durchlaufen, genießen dadurch gewisse Vorteile. Dazu zählt insbesondere, dass sie gegenüber Aufsichtsbehörden leichter nachweisen können, dass sie die Anforderungen an datenschutzfreundliche Voreinstellungen einhalten.

10.3 Warum sollte dies ernst genommen werden?

- Im Zeitalter von Big Data, in dem der Daten-Sammelleidenschaft kaum Grenzen gesetzt sind, dient die Pflicht zu datenschutzfreundlichen Voreinstellungen der Datenminimierung.
- Ein Horten von Daten z. B. in Form eines „Data Warehouses“ soll verhindert werden.
- Von diesem sogenannten „privacy by default“-Konzept profitieren insbesondere Personen, die selbst nicht in der Lage sind, Verarbeitungsvorgänge umfassend zu verstehen und deshalb datenschutzfreundliche Einstellungen – auch wenn diese grundsätzlich angeboten werden – nicht auf eigene Initiative vornehmen würden (z. B. bei Sozialen Netzwerken, Smartphones oder Betriebssystemen).
- Betroffene sollen vor Überrumpelung und Unerfahrenheit geschützt werden.

10.4 Die Anforderungen im Einzelnen

- Grundsätzlich sollen entsprechende Voreinstellungen gewährleisten, dass nur personenbezogene Daten verarbeitet werden, wenn dies für den jeweiligen Zweck auch im engeren Sinn erforderlich ist.
- Konkret ist dieser Grundsatz auf die Rahmenbedingungen der Verarbeitung (Art, Umfang, Speicherfristen und Zugänglichkeit) anzuwenden.

Hinweis: Häufigster Anwendungsfall dürften internetbasierte Dienste sein, wie beispielsweise Online-Shops. Durch die standardmäßige Konfiguration der Privatsphäre-Einstellungen von Nutzern muss sichergestellt sein, dass Nutzer Ihre Daten nur den Personenkreisen und nur in dem Umfang zugänglich machen, die für die Zweckerreichung, d. h. für die Abwicklung des Online-Geschäfts, erforderlich sind.

- Ziel ist es, allgemeinen Verarbeitungsgrundsätzen zu entsprechen, wie insbesondere dem Grundsatz der Datenminimierung oder dem Zweckbindungsgrundsatz.
- Als Grundsatz gilt: Als Voreinstellung ist stets die kleinstmögliche Einheit zu wählen: Geringstmögliche Menge an personenbezogenen Daten, geringstmögliche Verarbeitung, kleinster Empfängerkreis und kürzeste Speicherfrist.
- Für den Betroffenen heißt das konkret: Er sollte im Normalfall keine Änderungen an den Einstellungen

vornehmen müssen, um unter den gegebenen Umständen ein Maximum an „Privatheit“ für seine Daten zu erreichen. Im Wege einer Einwilligung („Opt-In“) kann der Betroffene dann entscheiden, ob und inwiefern er diese Einstellungen zum Nachteil seiner Privatsphäre abändern möchte.

10.5 Möglichkeit des genehmigten Zertifizierungsverfahrens

- Sogenannte genehmigte Zertifizierungsverfahren (siehe Art. 42 DS-GVO) bieten Unternehmen die Möglichkeit, die Einhaltung der Anforderungen an datenschutzfreundliche Voreinstellungen nachzuweisen.

- Wird ein Zertifikat nach Art. 42 DS-GVO erteilt, entbindet dies nicht von den oben erwähnten Pflichten. Stattdessen dient es primär der Vereinfachung der Kommunikation mit Aufsichtsbehörden, Geschäftspartnern und Betroffenen.

- Der Erwerb eines solchen Zertifikats ist nicht verpflichtend, sondern freiwillig.

Achtung: Unternehmen sind auch nach Erhalt eines Zertifikats weiterhin für die fortlaufende Kontrolle und Umsetzung des verwendeten Datenschutzkonzepts verantwortlich.

10.6 Praktisches Vorgehen

- **Schritt 1:** Bestehende technologische Verarbeitungsprozesse sind zu identifizieren.

- **Schritt 2:** Kommen datenschutzfreundliche Voreinstellungen aufgrund der konkreten Prozessausgestaltung grundsätzlich in Betracht, ist vor einer möglichen Verarbeitung zunächst zu prüfen, welche Datenverarbeitung zur Zweckerreichung in welchem Umfang erforderlich ist. Die Voreinstellungen sollten daraufhin entsprechend gestaltet werden. Unternehmen, die einen Datenschutzbeauftragten bestellt haben, können sich unter Umständen dessen Unterstützung bedienen.

- **Schritt 3:** Vor einer möglichen Verarbeitung sollte darüber hinaus geprüft werden, ob eine Zertifizierung nach Art. 42 DS-GVO machbar und sinnvoll wäre. Auch insofern sollte bei Unternehmen, die einen Datenschutzbeauftragten bestellt haben, dessen Unterstützung in Erwägung gezogen werden.

- **Schritt 4:** Um die einst ausgewählten Voreinstellungen regelmäßig auf ihre anhaltende Rechtmäßigkeit zu untersuchen, sind agile Prozesse mit variablen Intervallen zu implementieren.

- **Schritt 5:** Wird im Rahmen der Schritte 1-4 Änderungsbedarf identifiziert, so sind diese Anpassungen vorzunehmen.

Die Schritte 1 bis 5 sind ebenfalls zu befolgen, wenn entsprechende Verarbeitungsprozesse, die Voreinstellungen erlauben, aufgesetzt oder Software-Lösungen mit solchen Funktionen beschafft werden sollen.

10.7 Weitere praktische Hinweise

Siehe praktischen Hinweis *Datenschutz durch Technikgestaltung*.

Hinweis: Bei Unternehmen, die einen Datenschutzbeauftragten bestellt haben, sollte stets dessen Unterstützung bei Fragen zu datenschutzfreundlichen Voreinstellungen in Erwägung gezogen werden.

Einschlägige Hilfestellungen:

Hinweise der Datenschutzkonferenz (DSK) des Bundes und der Länder, Zertifizierung nach Art. 42 DS-GVO (Kurzpapier Nr. 9 vom 15. August 2017)

Abrufbar unter:
www.lda.bayern.de/media

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz – Texte und Erläuterungen, Juni 2018, S. 95.

Abrufbar unter:
www.bfdi.bund.de

11 Datenschutz durch Technikgestaltung (Art. 25)

Achtung Innovation: Wer seine Produkte und Dienstleistungen bereits im Lichte des Datenschutzes entwickelt, hat Gestaltungsspielraum und spart viel Zeit und Ärger

11.1 Überblick

Bereits bei der Planung von Systemen für die Datenverarbeitung muss ein Unternehmen die wirksame Umsetzung der Datenschutzgrundsätze durch Technikgestaltung sowie datenschutzfreundliche Voreinstellungen sicherstellen (Art. 25 Abs. 1 DS-GVO).

Die Verantwortlichen für die Entwicklung, Beschaffung/Einkauf oder Planung technologischer Datenverarbeitungssysteme, sollten die folgenden Punkte unbedingt beachten, die bereits (weit) vor der konkreten Erhebung der Daten zu beachten sind.

11.2 Rahmenbedingungen

- Die Pflicht zur datenschutzkonformen Technikgestaltung entfaltet eine Art „Vorfeldwirkung“, da das Unternehmen bereits bei Planung und Einsatz der für die Verarbeitung genutzten Technik proaktiv technisch und organisatorisch einen angemessenen Datenschutz sicherzustellen hat.
- Im digitalen Zeitalter ist adäquater Schutz der Privatheit ohne datenschutzgerechte Technikgestaltung nicht denkbar. Daher ist der Anwendungsbereich der DS-GVO faktisch bereits weit vor der eigentlichen Verarbeitung personenbezogener Daten eröffnet.
- Werden IT-Systeme bereits systemseitig im Einklang mit dem Grundsatz des „privacy by design“ eingerichtet, wird wesentlich dazu beigetragen, dass die spätere Datenverarbeitung sozusagen „automatisiert“ datenschutzkonform erfolgt.
- Im Einzelfall kann es sinnvoll sein, bereits bei der Planung eines Verarbeitungsprozesses eine Datenschutz-Folgenabschätzung durchzuführen (siehe dazu den praktischen Hinweis *Datenschutz-Folgenabschätzung*).

11.3 Warum sollte dies ernst genommen werden?

- Im Zeitalter von Big Data sind der Daten-Sammelleidenschaft kaum Grenzen gesetzt. Die Vorschrift dient daher insbesondere der Umsetzung der Datenschutzgrundsätze (Datenminimierung, Transparenz, Zweckbindung, Integrität und Vertraulichkeit der Datenverarbeitung) und damit der Einhaltung der DS-GVO und dem Schutz der Rechte der betroffenen Personen.

- Verstöße gegen die Verpflichtung, die Datenschutzgrundsätze bereits bei der Technikgestaltung der Verarbeitungsprozesse zu berücksichtigen, können mit sehr hohen Bußgeldern geahndet werden und zu erheblichen Reputationsschäden führen.

11.4 Die Anforderungen im Einzelnen

- Bereits zum Zeitpunkt der Festlegung der Mittel für die Datenverarbeitung und selbstverständlich auch während der Verarbeitung muss ein Unternehmen angemessene technische und organisatorische Maßnahmen zur wirksamen Umsetzung der Datenschutzgrundsätze treffen, um den Anforderungen der DS-GVO zu genügen und die Rechte der betroffenen Personen zu schützen.

- Das Gesetz macht keine Vorgaben, welche Maßnahmen das Unternehmen konkret treffen muss. Es muss vielmehr stets im Wege einer Einzelfallbetrachtung eine Analyse des konkreten Systems sowie der Datenverarbeitungsvorgänge vornehmen und die daraus erforderlich werdenden Maßnahmen ermitteln und umsetzen.

- Das Unternehmen muss dabei jeweils wirksame Maßnahmen ergreifen, die z. B. folgende Bereiche betreffen:

  - Technische Maßnahmen, z. B. Pseudonymisierung (d. h. das Ersetzen der Merkmale zur Identifikation der Person durch Pseudonyme wie etwa Buchstaben- oder Zahlenfolgen) sowie Verschlüsselung;

  - Organisatorische Maßnahmen, z. B. klare Regelungen zu Verantwortlichkeiten, Verhaltensregeln sowie Schulung und Sensibilisierung von Mitarbeitern;

  - Datenminimierung (d. h. die Datenverarbeitung ist auf das für den jeweiligen Zweck notwendige Mindestmaß zu beschränken);

  - Datensicherheit (z. B. Sicherung datenverarbeitender Anlagen durch Zugangs- und Zutrittskontrollen);

  - Transparenz durch Dokumentation der Datenverarbeitung und Information der betroffenen Personen; und

  - Stetige Selbstkontrolle und Weiterentwicklung der Maßnahmen. So muss etwa eine veraltete Technik, gegebenenfalls auf der Grundlage nachstehender Aspekte durch eine neue Technik ersetzt werden.

- Die Auswahl der richtigen Maßnahmen steht grundsätzlich im Ermessen des Unternehmens, wobei es aber immer die folgenden Aspekte berücksichtigen muss:

  - Stand der Technik (d. h. Einsatz von technologischen Werkzeugen, die bereits ausreichend getestet sind, um z. B. eine angemessene Verschlüsselung oder eine verlässliche Pseudonymisierung zu gewährleisten).

  - Implementierungskosten (d. h. Herstellung eines angemessenen Verhältnisses zwischen wirtschaftlichem Aufwand und reellem Mehrwert für den Schutz der betroffenen Daten).

  - Art, Umfang, Umstände und Zwecke der Datenverarbeitung.

  - **Beispiele:** Höhere Anforderungen an die Maßnahmen können sich ergeben, soweit durch die Datenverarbeitung betroffene Personen die Möglichkeit verlieren, ihre Daten zu kontrollieren. Zu nennen sind beispielsweise die Verarbeitung sensibler Daten (wie z. B. Gesundheitsdaten), die Verarbeitung von Daten schutzbedürftiger Personen (insbesondere Kinder) oder wenn die Verarbeitung eine große Menge personenbezogener Daten und/oder eine große Anzahl von betroffenen Personen betrifft.

– Eintrittswahrscheinlichkeit und Schwere von möglichen Risiken für die betroffenen Personen im Sinne einer umfassenden Güter- und Interessenabwägung.

Beispiele: Besonders hohe Anforderungen an die zu treffenden Maßnahmen sind immer dann zu stellen, wenn Risiken folgender Art bestehen: Gefahr eines Identitätsdiebstahls oder -betrugs, eines finanziellen Verlusts, einer Rufschädigung, eines Verlusts der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Entschlüsselung einer Pseudonymisierung oder anderer erheblicher wirtschaftlicher oder gesellschaftlicher Nachteile durch die Datenverarbeitung.

- Die Überlegungen und Entscheidungen sind sorgfältig schriftlich durch das Unternehmen zu dokumentieren.

11.5 Möglichkeit des genehmigten Zertifizierungsverfahrens

- Mit Hilfe eines sogenannten genehmigten Zertifizierungsverfahrens (siehe Art. 42 DS-GVO) besteht die Möglichkeit für ein Unternehmen, die Einhaltung der Anforderungen an datenschutzfreundliche Technikgestaltung nachzuweisen.

- Wird ein Zertifikat nach Art. 42 DS-GVO erteilt, entbindet dies nicht von den oben erwähnten Pflichten. Es dient hauptsächlich der Vereinfachung der Kommunikation mit Aufsichtsbehörden, Geschäftspartnern und Betroffenen.

- Der Erwerb eines solchen Zertifikats ist nicht verpflichtend, sondern freiwillig.

Achtung: Das Unternehmen ist auch nach Erhalt des Zertifikats weiterhin für die fortlaufende Kontrolle und Umsetzung des verwendeten Datenschutzkonzepts verantwortlich.

11.6 Bearbeitung

- **Schritt 1:** Bestehende Systeme, mit denen personenbezogene Daten verarbeitet werden, sind zu identifizieren.

- **Schritt 2:** Weiter ist zu überprüfen, ob im Rahmen der datenschutzkonformen Technikgestaltung, die für die Datenverarbeitung durch das System getroffenen technischen und organisatorischen Maßnahmen die Datenschutzgrundsätze (Datenminimierung, Transparenz, Zweckbindung, Integrität und Vertraulichkeit) ordnungsgemäß abbilden. Soweit dies nicht der Fall ist, sind die hierfür notwendigen Maßnahmen im System umzusetzen. Hier kann ggf. ein etwaig in dem Unternehmen bestellter Datenschutzbeauftragter zu Rate gezogen werden.

- **Schritt 3:** Die Überlegungen und Entscheidungen zu Schritt 2 sind sorgfältig zu dokumentieren und es ist sicherzustellen, dass die Dokumentation innerhalb des Unternehmens dauerhaft verfügbar ist.

- **Schritt 4:** Sofern vorhanden, sollte mithilfe des in einem Unternehmen bestellten Datenschutzbeauftragten – vor einer möglichen Verarbeitung – überlegt werden, ob eine Zertifizierung nach Art. 42 DS-GVO machbar und sinnvoll wäre.

- **Schritt 5:** Flexible Prozesse mit variablen Intervallen sind zu etablieren, um regelmäßig die einst ausgewählten Systeme mit den getroffenen Maßnahmen auf ihre anhaltende Rechtmäßigkeit zu untersuchen.

- **Schritt 6:** Bei Bedarf sind nötige Anpassungen vorzunehmen.

Schritte 1 bis 6 gelten entsprechend bei der Planung von neuen Systemen oder Software-Lösungen.

11.7 Weitere Praktische Hinweise

Siehe die Praktischen Hinweise *Datenschutzfreundliche Voreinstellungen* und *Datenschutz-Folgenabschätzung*.

Einschlägige Hilfestellungen:

Hinweise der Datenschutzkonferenz (DSK) des Bundes und der Länder, Zertifizierung nach Art. 42 DS-GVO (Kurzpapier Nr. 9 vom 15. August 2017)

Abrufbar unter:
www.lda.bayern.de/media

12 Benennung Vertreter in der EU (Art. 27)

12.1 Überblick

Für Unternehmen außerhalb der Europäischen Union (EU), die keine Niederlassung in der EU haben, aber Daten von Personen in der EU verarbeiten, um ihnen Waren oder Dienstleistungen anzubieten oder ihr Verhalten zu beobachten, gelten insoweit die Vorschriften der DS-GVO.

Diese Unternehmen müssen in der Regel einen Vertreter in der EU benennen, der Anlaufstelle für die Aufsichtsbehörden und die betroffenen Personen in der EU ist.

12.2 Rahmenbedingungen

Die Pflicht trifft Unternehmen außerhalb der EU, die dort keine Niederlassung haben, wenn sie personenbezogene Daten von Personen in der EU verarbeiten, soweit sie:

- diesen Personen in der EU Waren oder Dienstleistungen (zumindest auch) anbieten.
  - Das Anbieten muss gezielt erfolgen; Indizien hierfür sind etwa, dass Zahlungen (auch) in EURO vorgesehen sind, (auch) EU-Versandbedingungen gelten.
  - Die Tatsache, dass der Internetauftritt des Unternehmens auch in der EU aufgerufen werden kann, oder die Verwendung einer Sprache, die sowohl in der EU als auch in dem Sitzland des Unternehmens gängig ist, sind demgegenüber keine ausreichenden Anhaltspunkte für ein gezieltes Angebot.

oder

- das Verhalten dieser Personen in der EU beobachten.
  - Diese Fallgruppe umfasst insbesondere die Überwachung der Internetaktivitäten der Personen in der EU und setzt eine gewisse Intensität voraus.
  - Gemeint ist z. B. das Setzen von Cookies zu Zwecken des Targeted Advertising oder von Social Plugins.

Die Verpflichtung zur Benennung eines Vertreters entfällt ausnahmsweise, wenn die Verarbeitung der Daten von Personen in der EU nur gelegentlich (nicht planmäßig, ohne Wiederholungsabsicht) erfolgt, es sei denn:

- Es liegt eine umfangreiche Verarbeitung von sensiblen Daten vor (abschließend: rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische oder biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung, Daten über strafrechtliche Verurteilungen und Straftaten); oder

- unter Berücksichtigung von Art, Umständen, Umfang und Zwecken der Verarbeitung entsteht voraussichtlich ein Risiko für Rechte und Freiheiten natürlicher Personen.

Als Vertreter benannt werden kann eine juristische Person (z. B. eine Konzerngesellschaft, aber auch ein extern niedergelassener Dienstleister) oder eine natürliche Person (z. B. ein Mitarbeiter einer Konzerngesellschaft). Räumlich muss der Vertreter in einem EU Mitgliedstaat niedergelassen sein, in dem sich die betroffenen Personen befinden. Soweit sich in mehr als einem EU Mitgliedstaat betroffene Personen befinden, reicht trotzdem die Benennung nur eines Vertreters in lediglich einem der Mitgliedstaaten aus, in denen sich betroffene Personen befinden.

12.3 Warum sollte dies ernst genommen werden?

- Das Unternehmen muss, zusätzlich zu den Datenschutzbestimmungen seines Heimatlandes, für die Verarbeitung von Daten von Personen in der EU europäisches Datenschutzrecht (DS-GVO) beachten und hierfür einen Vertreter in der EU schriftlich benennen.

- Auch bei Benennung eines Vertreters in der EU bleibt das Unternehmen weiterhin verantwortlich und haftbar nach der DS-GVO.

- Die Nichtbenennung eines Vertreters in der EU entgegen einer Benennungspflicht kann mit sehr hohen Geldbußen geahndet werden und zu erheblichen Reputationsschäden führen.

12.4 Praktisches Vorgehen

In der Praxis empfehlen sich im Rahmen der Benennung eines Vertreters in der EU etwa die folgenden Schritte:

- **Schritt 1:** Zunächst sollte anhand der in *Nummer 12.2* genannten Vorgaben geprüft werden, ob die Benennung eines Vertreters in der EU erforderlich ist.

- **Schritt 2:** Wenn eine Pflicht zur Benennung eines Vertreters in der EU besteht, sollte bei Unternehmensgruppen geprüft werden, ob bereits eine andere Konzerngesellschaft einen Vertreter in der EU benannt hat. Soweit dies der Fall ist, sollte geprüft werden, ob der Vertreter räumlich auch für die eigene Konzerngesellschaft als Vertreter in der EU bestellt werden kann und soll.

- **Schritt 3:** Wenn in der Unternehmensgruppe noch kein Vertreter in der EU benannt ist, aber eine Pflicht zur Benennung eines solchen für eine Konzerngesellschaft besteht, sollte anhand der in *Nummer 12.2* genannten Vorgaben ermittelt werden: Soll oder kann eine Konzerngesellschaft oder ein Mitarbeiter einer Konzerngesellschaft als Vertreter in der EU benannt werden? Kann oder soll ein externes Dienstleistungsunternehmen mit der Wahrnehmung der Aufgaben des Vertreters in der EU beauftragt werden?

- **Schritt 4:** Gegebenenfalls sind diejenigen Personen in den Benennungsprozess einzubinden, deren Unterstützung benötigt wird (z. B. Personalabteilung, IT, Legal, Datenschutzbeauftragter).

- **Schritt 5:** Gegebenenfalls ist der ausgewählte Vertreter in der EU schriftlich zu benennen. Im Benennungsschreiben sollten die Aufgaben des Vertreters beschrieben werden.

- **Schritt 6:** In jedem Fall sollte in einer schriftlichen Analyse festgehalten werden, warum ein Vertreter in der EU (nicht) benannt wurde.

- **Schritt 7:** Name und Kontaktdaten des Vertreters (Anschrift, eine ihm zugewiesene Telefonnummer und eine ihm zugewiesene E-Mail-Adresse) sollte:

  – auf der Webseite des Unternehmens veröffentlicht werden; und

  – in vorgeschriebene Informationen aufgenommen werden (bei der Datenerhebung gegenüber den davon betroffenen Personen, Verzeichnis von Verarbeitungstätigkeiten).

12.5 Weitere praktische Hinweise

Siehe praktischen Hinweis *Kontakt mit Behörden One-Stop-Shop*.

Einschlägige Hilfestellungen:

Hinweise der Datenschutzkonferenz (DSK) des Bundes und der Länder, Marktortprinzip: Regelungen für außereuropäische Unternehmen (Kurzpapier Nr. 7 vom 26. Juli 2017)

Abrufbar unter:
www.lda.bayern.de/media

13 Meldung von Verletzungen (Art. 33, 34)

13.1 Überblick

Unter der DS-GVO sind Unternehmen, die personenbezogene Daten für eigene Geschäftszwecke verarbeiten, dazu verpflichtet, Datenschutzverletzungen unverzüglich an die zuständige Aufsichtsbehörde zu melden und bei hohen Risiken die betroffenen Personen zu benachrichtigen (Art. 33 und Art. 34 DS-GVO).

Gegenüber der bisherigen Rechtslage sind die Meldepflichten bei Datenschutzverstößen unter der DS-GVO deutlich verschärft und die einzuhaltenden Fristen deutlich verkürzt worden.

13.2 Rahmenbedingungen

- Unternehmen, die personenbezogene Daten für eigene Geschäftszwecke verarbeiten (Verantwortliche), haben Datenschutzverletzungen unverzüglich an die zuständige Aufsichtsbehörde zu melden.
- Bestehen hohe Risiken für die Rechte und Freiheiten der betroffenen Personen, sind diese ebenfalls zu benachrichtigen.
- Datenschutzverletzungen sind beispielsweise der Verlust, Diebstahl sowie eine unbeabsichtigte Veröffentlichung von personenbezogenen Daten.

13.3 Warum sollte dies ernst genommen werden?

- Datenpannen und Datenlecks (Hacking, Datendiebstahl) können mit erheblichen Risiken für die betroffenen Personen einhergehen. Dies ist etwa der Fall, wenn Personalakten nach einem Einbruch oder Kreditkarteninformationen durch Datendiebstahl an Unberechtigte gelangen. Um diese Risiken zu kontrollieren, muss das Unternehmen unverzüglich (i.) die Verletzung der zuständigen Aufsichtsbehörde melden und, (ii) soweit hohe Risiken für die betroffenen Personen drohen, diese benachrichtigen.
- Verstöße gegen die gesetzlichen Melde- und Benachrichtigungspflichten können mit sehr hohen Bußen geahndet werden und zudem erhebliche Reputationsschäden zur Folge haben.
- **Achtung:** Da Meldung und Benachrichtigung sehr zeitkritisch sind, sollte bereits wenn der Verdacht einer meldepflichtigen Datenschutzverletzung vorliegt, ausnahmslos und unverzüglich der Datenschutzbeauftragte sowie die für Datenschutzverletzungen zuständige Abteilung des Unternehmens (jeweils soweit vorhanden) eingebunden werden.

13.4 Wen trifft die Pflicht zur Meldung bei der Aufsichtsbehörde und zur Benachrichtigung von betroffenen Personen?

- Die Pflicht zur Meldung von Datenschutzverletzungen an die Aufsichtsbehörde und zur Benachrichtigung von betroffenen Personen trifft jedes Unternehmen, welches als Verantwortlicher personenbezogene Daten für eigene Geschäftszwecke verarbeitet und für das die DS-GVO zwingend gilt.
- Unternehmen, die als Auftragsverarbeiter für andere Unternehmen Dienstleistungen erbringen und dabei personenbezogene Daten dieses Unternehmens verarbeiten, unterliegen weder unmittelbaren Meldepflichten gegenüber Aufsichtsbehörden, noch Benachrichtigungspflichten gegenüber Betroffenen für Datenschutzverletzungen, die die Daten ihrer Kunden betreffen. Die Auftragsverarbeiter müssen aber dem anderen Unternehmen unverzüglich melden, wenn ihnen eine solche Datenschutzverletzung bekannt wird.

Hinweis: Die vorstehende Mitteilungspflicht des Auftragsverarbeiters sollte in den Vereinbarungen über die Auftragsvereinbarung detailliert geregelt werden.

13.5 Wann ist eine Meldung an die Aufsichtsbehörde vorzunehmen?

Grundsätzlich muss ein Unternehmen jede Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde melden:

- Prinzipiell muss eine Meldung immer erfolgen, wenn personenbezogene Daten im Verantwortungsbereich eines Unternehmens verloren gehen, ungewollt verändert werden oder in die Hände Dritter gelangen. Unabhängig davon, ob die Datenschutzverletzung beabsichtigt oder unabsichtlich erfolgt, erfasst die Meldepflicht jegliche(n) unrechtmäßige(n) Verlust, Vernichtung, Veränderung, unbefugte Offenlegung von oder Zugang zu personenbezogenen Daten

oder unzulässige Datenverarbeitung von personenbezogenen Daten, die das Unternehmen verarbeitet. Umfasst sind damit nicht nur Angriffe von Dritten auf das Unternehmen, sondern auch interne Datenverluste, etwa wenn ein Mitarbeiter einen Laptop mit Kundendaten verliert oder Daten aufgrund eines Stromausfalls in einem Unternehmen zeitweilig nicht verfügbar sind.

- Lediglich ausnahmsweise ist eine Verletzung nicht zu melden, wenn diese voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der durch sie betroffenen Personen führt, wenn also tatsächlich keine Beeinträchtigungen durch die Verletzung zu erwarten sind. Dies ist etwa der Fall, wenn gestohlene Daten bereits öffentlich bekannt waren oder verschlüsselt sind und ausgeschlossen werden kann, dass diese von einem Dritten entschlüsselt werden können, oder ein Stromausfall nur wenige Minuten gedauert hat.

- Maßgebliche Faktoren, die bei der Risikoabschätzung berücksichtigt werden müssen, sind insbesondere: die Art der Verletzung, die Sensibilität und Menge der betroffenen Daten, ob anhand der Daten eine Identifizierung der betroffenen Personen möglich ist, die Schwere der möglichen Auswirkungen für die betroffenen Personen, besondere Eigenschaften der betroffenen Personen (z. B. Kinder), die Anzahl der betroffenen Personen und wie wahrscheinlich es ist, dass sich das Risiko tatsächlich realisiert.

Wichtig: Jeder Schritt und jede Überlegung, die Unternehmen im Rahmen dieser *Nummer 13.5* vornehmen, ist strikt und schriftlich zu dokumentieren. Die erstellte Dokumentation muss sorgfältig aufbewahrt werden, auch wenn im Ergebnis keine Meldung an die Aufsichtsbehörde erfolgt. Insbesondere muss die Datenschutzverletzung, ihre Ursache, die betroffenen Personen und Daten sowie alle damit in Zusammenhang stehenden Fakten, die Auswirkungen der Verletzung, die Maßnahmen, die das Unternehmen zur Abhilfe ergriffen hat und die Entscheidung, die Datenschutzverletzung (nicht) zu melden, so sorgfältig dokumentiert werden, dass die Aufsichtsbehörde nachprüfen kann, ob das Unternehmen die Verpflichtungen im Zusammenhang mit der Meldepflicht eingehalten hat.

Hinweis: Im Zweifel melden! In jedem Fall immer sorgfältig dokumentieren!

13.6 Wann müssen betroffene Personen über eine Datenschutzverletzung informiert werden?

Hinweis: Die Verpflichtung betroffene Personen über eine Datenschutzverletzung zu unterrichten, besteht zusätzlich zu der Pflicht zur Meldung bei der Aufsichtsbehörde.

Grundsätzlich muss ein Unternehmen betroffene Personen über eine Verletzung des Schutzes ihrer personenbezogenen Daten im Sinne von *Nummer 13.5* benachrichtigen, wenn die Verletzung voraussichtlich ein hohes Risiko für die betroffenen Personen zur Folge hat:

Hinweis: Die Schwelle für die Benachrichtigungspflicht ist damit gegenüber der Meldepflicht höher. Während eine Benachrichtigung nur bei einem erheblichen Risiko für die betroffene Person notwendig ist, muss die Meldung bei jedem Risiko erfolgen.

- Die Risikoabschätzung erfolgt anhand der vorstehend unter *Nummer 13.5* aufgeführten Kriterien. Ein erhebliches Risiko bestände z. B., wenn bei einem Cyber-Angriff sensible Informationen gestohlen werden. Dies sind etwa Gesundheitsdaten, Kreditkarteninformationen oder online-Zugangsdaten. Gelangt demgegenüber etwa eine E-Mail mit einer Auftragsbestätigung an den falschen Empfänger, der glaubhaft versichert, die fehlgeleitete E-Mail ohne weitere Kenntnisnahme der Daten gelöscht zu haben, wäre kein gesteigertes Risiko gegeben, so dass keine Benachrichtigungspflicht bestände. Ebenso wenig würde ein hohes Risiko vorliegen, wenn Daten der betroffenen Personen aufgrund eines Stromausfalls lediglich vorübergehend nicht verfügbar waren.

- Die betroffenen Personen müssen grundsätzlich individuell benachrichtigt werden (z. B. per SMS oder E-Mail). Die Mitteilung darf nicht im Rahmen z. B. eines regulären Newsletters erfolgen, sondern muss auf die Datenschutzverletzung beschränkt sein.

Die Verpflichtung zur Benachrichtigung der betroffenen Personen entfällt, wenn:

- das Unternehmen die Daten angemessen gesichert hat (insbesondere sie verschlüsselt hat), das Risiko sich also praktisch nicht verwirklichen kann;

- das Unternehmen nachträglich Maßnahmen ergriffen hat, sodass das Risiko wahrscheinlich nicht mehr besteht, z. B. die gestohlene Festplatte sichergestellt werden konnte, bevor der Dieb sich Zugang zu den gespeicherten Daten verschafft hat; oder

- diese einen unverhältnismäßigen Aufwand verursachen würde (z. B. wenn die Kontaktdaten der betroffenen Personen erst aufwendig recherchiert werden müssten oder die mit einer individuellen Benachrichtigung verbundenen Kosten aufgrund der Vielzahl der betroffenen Personen unverhältnismäßig wären) oder es schlichtweg nicht möglich ist, etwa weil sämtliche Kontaktdaten der betroffenen Personen bei der Datenschutzverletzung vernichtet worden sind. Allerdings muss das Unternehmen die Datenschutzverletzung in diesen Fällen öffentlich bekanntmachen, also etwa in einer Zeitungsanzeige oder über die Unternehmenswebseite. Gegebenenfalls müssen mehrere Kommunikationsmethoden kombiniert werden, um eine effektive Information sicherzustellen.

Wichtig: Auch im Rahmen dieser *Nummer 13.6* müssen Unternehmen jeden durchgeführten Schritt und jede Überlegung sorgfältig und schriftlich dokumentieren sowie die Dokumentation sorgfältig aufbewahren, auch wenn im Ergebnis keine Benachrichtigung an die betroffenen Personen erfolgt ist.

13.7 Welche Fristen sind für die Meldung und Benachrichtigung zu beachten?

Die Meldung an die Aufsichtsbehörde muss unverzüglich erfolgen und möglichst binnen höchstens 72 Stunden, nachdem dem Unternehmen die Verletzung bekannt geworden ist.

- Unklare Sachverhalte müssen unverzüglich aufgeklärt werden, um zu ermitteln, ob eine Verletzung vorliegt oder nicht. Soweit innerhalb des Zeitfensters der Sachverhalt nicht abschließend aufgeklärt werden kann oder nicht alle für die Meldung vorgeschriebenen Informationen vorliegen, muss die Meldung schrittweise erfolgen, wie in *Nummer 7* erläutert.

- Unternehmen sollten die 72-Stunden Frist nicht ausschöpfen. Soweit es nicht möglich ist, innerhalb der 72 Stunden die Meldung zu machen, muss die verspätete Meldung einen (überzeugenden!) Grund hierfür enthalten.

Das Unternehmen muss jede betroffene Person so schnell wie möglich über die Datenschutzverletzung benachrichtigen:

- Der Zeitraum von 72 Stunden, der für die Meldung an die Aufsichtsbehörden gilt, darf auch für notwendige Personen-Benachrichtigungen nur in Ausnahmefällen überschritten werden.

Je nach Ereignis kann auch eine besonders schnelle Benachrichtigung geboten sein. Deshalb kann die Benachrichtigung der betroffenen Personen zeitlich sogar noch vor einer Meldung an die Aufsichtsbehörde erfolgen, beispielsweise wenn die betroffenen Personen damit in die Lage versetzt werden können, einen drohenden Schaden abzuwehren, z. B. durch Sperrung ihrer Kontokarte oder Änderung des Passworts.

13.8 Inhalt der Meldungen

Die Meldung an die Aufsichtsbehörde muss mindestens den folgenden Inhalt haben:

- Beschreibung des konkreten Ereignisses der Datenschutzverletzung, soweit möglich unter Angabe der betroffenen Personen (nach Kategorie [nicht namentlich], also etwa: „Kunden“; „Mitarbeiter“) und Daten (nach Kategorie, also etwa „Kontaktdaten“, „Benutzername und Passwort für E-Mailkonto“) und (soweit möglich) Anzahl der betroffenen Personen;

- Angaben einer Kontaktperson (Name, Kontaktdaten) im betroffenen Unternehmen. Soweit ein Datenschutzbeauftragter benannt worden ist, ist dieser anzugeben;

- Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung; und

- Beschreibung der Maßnahmen, die das Unternehmen ergriffen hat oder vorschlägt, um dem Problem zu begegnen oder es gegebenenfalls zu beheben sowie die Folgen abzumildern.

Hinweis: Soweit nicht sämtliche der vorstehend genannten Informationen innerhalb der Frist nach *Nummer 13.7* vollständig ermittelt werden können, ist

eine schrittweise Meldung zulässig und geboten. Es ist dann zusätzlich zu erläutern, warum die Meldung noch unvollständig ist und welche Informationen fehlen. Die zu ergänzenden Angaben sind unverzüglich an die Aufsichtsbehörde nachzureichen, sobald das Unternehmen über sie verfügt.

Es ist zulässig und gegebenenfalls sinnvoll, darüber hinausgehende Angaben zu machen, wenn es das Verständnis der Aufsichtsbehörde erleichtern würde. Die Aufsichtsbehörde muss sich anhand der Angaben ein vollständiges Bild von dem Ereignis machen können.

Stellt sich im Nachhinein heraus, dass keine Datenschutzverletzung vorlag, ist die Aufsichtsbehörde auch hierüber zu informieren.

Die Mitteilung an die betroffene Person muss in klarer, leicht verständlicher Sprache erfolgen, die Art der Datenschutzverletzung beschreiben und dabei mindestens die folgenden Angaben enthalten:

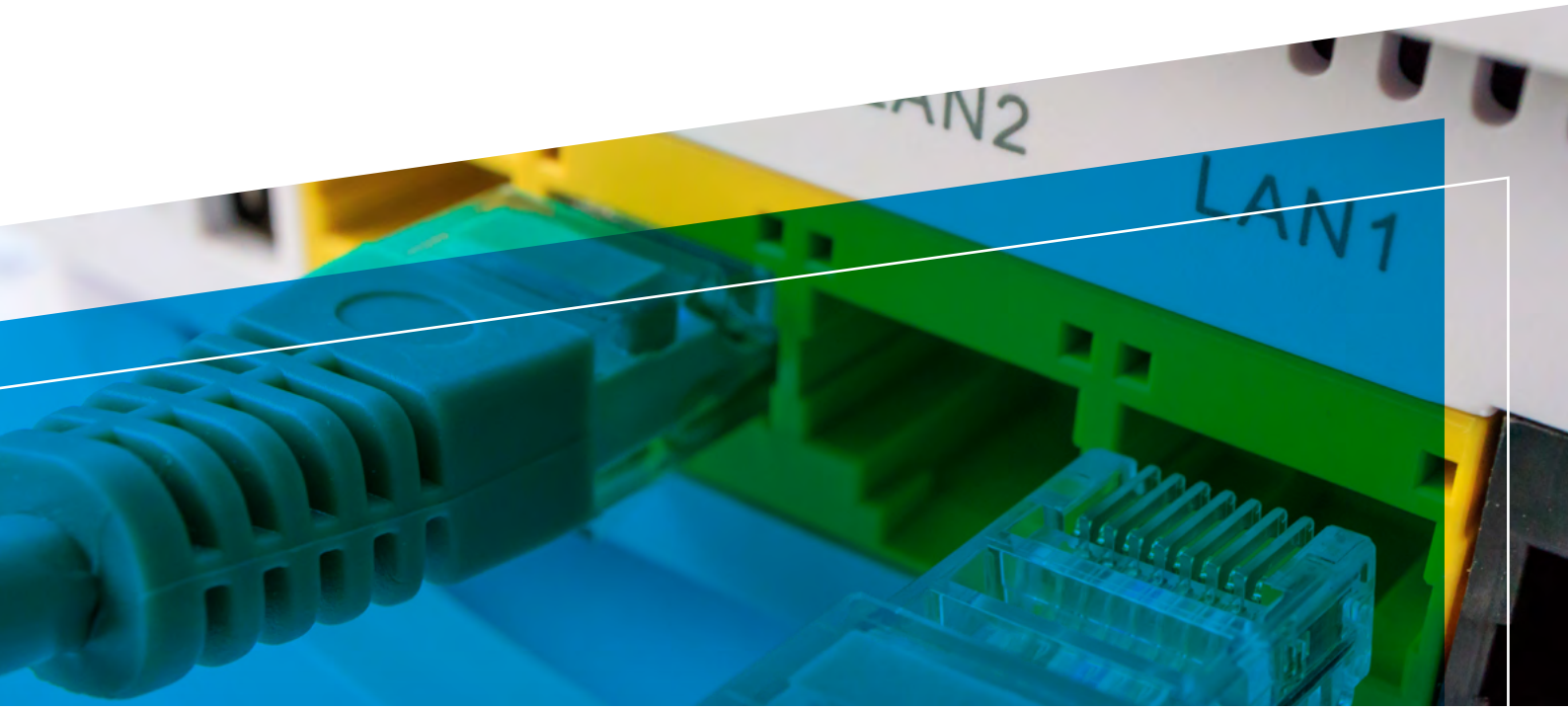
- Angaben einer Kontaktperson (Name, Kontaktdaten) im betroffenen Unternehmen. Soweit das Unternehmen einen Datenschutzbeauftragten benannt hat, ist dieser anzugeben;
- Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung; und
- Beschreibung der Maßnahmen, die das Unternehmen ergriffen hat und/oder der betroffenen Person als Reaktion auf die Datenschutzverletzung vorschlägt, um die negativen Folgen gegebenenfalls zu beheben oder diese abzumildern (z. B. Aufforderung an die betroffene Person, unverzüglich ihr Passwort zurückzusetzen).

Die einzelnen Aspekte der Benachrichtigungspflicht müssen mit den Aufsichtsbehörden abgestimmt werden. Einem Verlangen der Behörde, die betroffenen Personen zu benachrichtigen, müssen Unternehmen Folge leisten. Stellt die Aufsichtsbehörde hingegen fest, dass eine Benachrichtigung nicht erforderlich ist, besteht für das Unternehmen rechtssicher auch keine diesbezügliche Pflicht.

13.9 Bei welcher Aufsichtsbehörde muss die Meldung gemacht werden?

Die Meldung erfolgt an die für das Unternehmen zuständige Aufsichtsbehörde.

Soweit von der Verletzung Personen in mehreren Mitgliedstaaten der EU betroffen sind, ist die Meldung zentral an die federführende Aufsichtsbehörde zu machen. Dies ist prinzipiell die Aufsichtsbehörde beim Sitz der Hauptniederlassung des Unternehmens in der EU.



13.10 Bearbeitung der Meldepflicht

Zur Bearbeitung der Meldepflicht sollten Unternehmen folgende Schritte durchführen:

- **Schritt 1:** Bei einem Sicherheitsvorfall ermitteln, ob eine Datenschutzverletzung nach *Nummer 13.5* vorliegt.

- **Schritt 2:** Ist von einer Datenschutzverletzung auszugehen, ist unverzüglich der Datenschutzbeauftragte des Unternehmens (falls vorhanden) und gegebenenfalls eine für die Bearbeitung von Datenschutzverletzung zuständige Abteilung einzubinden. Daraufhin muss geprüft werden, ob die Datenschutzverletzung anhand der Vorgaben in *Nummer 13.5* wahrscheinlich ein Risiko für die betroffenen Personen birgt und ob es sich nach *Nummer 13.6* um ein hohes Risiko handelt.

- **Schritt 3:** Personen, deren Unterstützung benötigt wird (z. B. Personalabteilung, IT, Finance, Marketing, Legal), sind einzubinden.

- **Schritt 4:** Falls das Unternehmen bei seiner Untersuchung nach Schritt 2 zu dem Ergebnis kommt, dass kein Risiko für die betroffenen Personen besteht, entfallen Melde- und Benachrichtigungspflichten. Sollte das Unternehmen zu dem Ergebnis kommen, dass wahrscheinlich ein Risiko für die betroffenen Personen besteht, ist die Datenschutzverletzung unter Angabe der Informationen gemäß *Nummer 13.8* an die gemäß *Nummer 13.9* zuständige Aufsichtsbehörde zu melden. Ist davon auszugehen, dass wahrscheinlich ein hohes Risiko für die betroffenen Personen besteht, sind diese zusätzlich zu informieren, entsprechend *Nummer 13.6* unter Angabe der Informationen gemäß *Nummer 13.8*.

- **Schritt 6:** Jede der vorstehenden Überlegungen ist sorgfältig schriftlich zu dokumentieren. Es ist sicherzustellen, dass diese Dokumentation an zentraler Stelle im Unternehmen dauerhaft verfügbar gehalten wird.

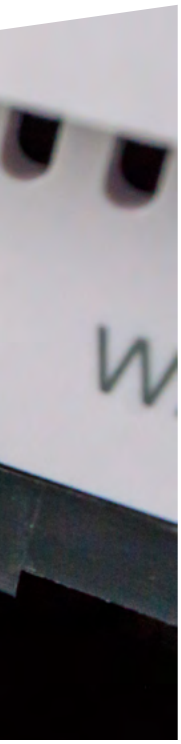
- **Schritt 7:** Unternehmen sollten im Rahmen erfolgter Meldungen eng und kooperativ mit der Aufsichtsbehörde zusammenarbeiten.

Hinweis: Soweit vorhanden sollten Mitarbeiter eines Unternehmens bei jedem Verdacht einer Datenschutzverletzung immer unverzüglich die zuständige Abteilung und/oder den Datenschutzbeauftragten kontaktieren.

Einschlägige Hilfestellungen:

Bayerisches Landesamt für Datenschutzaufsicht, Umgang mit Datenpannen – Art. 33 und 34 DS-GVO (Stand: 19. Juli 2016)

Abrufbar unter:
www.lda.bayern.de/media



Datenschutz-Folgenabschätzung (Art. 35)

Die alte Vorabkontrolle in neuen Gewändern – hier hilft Standardisierung und Automatisierung

Datenverarbeitung
Verhältnismäßigkeit
Notwendigkeit

14

14.1 Überblick

Immer dann, wenn eine geplante Datenverarbeitung voraussichtlich hohe Risiken für die betroffenen Personen birgt, hat ein Unternehmen (der Verantwortliche) vorab die möglichen Folgen zu prüfen (Art. 35, 36 DS-GVO).

14.2 Rahmenbedingungen

- Bei Datenverarbeitungsprozessen, die hohe Risiken für die durch sie betroffenen Personen bergen können, muss ein Unternehmen bereits vor dessen Beginn eine Bewertung der Risiken und Maßnahmen durchführen, die es getroffen hat. So sollen etwaige Risiken auf ein gesetzlich vertretbares Maß beschränkt werden.

- Dabei können Verarbeitungsprozesse schon während ihrer Entwicklung im Sinne datenschutzfreundlicher Anliegen beeinflusst werden.

14.3 Warum sollte dies ernst genommen werden?

- Die DS-GVO fordert einen ausreichenden Schutz von betroffenen Personen (z. B. Kunden, Mitarbeiter) vor den Risiken, die mit der Verarbeitung ihrer Daten verbunden sind.

- Verstöße gegen die ordnungsgemäße Durchführung einer Datenschutz-Folgenabschätzung können mit sehr hohen Geldbußen geahndet werden und zu erheblichen Reputationsschäden führen.

14.4 Wen trifft die Pflicht zur Durchführung der Datenschutz-Folgenabschätzung?

- Grundsätzlich jedes Unternehmen, das personenbezogene Daten für eigene Geschäftszwecke verarbeitet (Verantwortlicher).

- Das Unternehmen darf mit der Durchführung einer Datenschutz-Folgenabschätzung zwar einen Dritten beauftragen, bleibt aber selbst für die ordnungsgemäße Durchführung verantwortlich.

- Auftragsverarbeiter (d. h. Unternehmen, die für andere Unternehmen Dienstleistungen erbringen und dabei personenbezogene Daten dieses Unternehmens verarbeiten) trifft diese Pflicht nicht.

14.5 Wann muss eine Datenschutz-Folgenabschätzung durchgeführt werden?

Eine Datenschutz-Folgenabschätzung ist zwingend dann durchzuführen, wenn ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen vorliegt. Um dies zu prüfen, bedarf es im jeweiligen Einzelfall einer Analyse des konkret geplanten Datenverarbeitungsprozesses im Hinblick auf die Schwere der möglichen Risiken und ihrer Eintrittswahrscheinlichkeit. Dabei sind Art, Umfang, Umstände und Zweck der Datenverarbeitung in die Analyse einzubeziehen.

Ein hohes Risiko ist insbesondere zu bejahen bei:

- Scoring und Profiling (siehe dazu auch die Praktischen Hinweise *Profiling* und *Automatisierte Einzelentscheidung*) (z. B. Computertests zur Bewerberauswahl);

- umfangreicher Datenverarbeitung besonders sensibler oder höchstpersönlicher Daten (z. B. zentrale Verarbeitung sämtlicher Gesundheitsdaten aller Mitarbeiter);

- einer umfangreichen systematischen Überwachung öffentlich zugänglicher Bereiche (z. B. Videoüberwachung von Verkaufsflächen);

- einer Behinderung der betroffenen Personen aufgrund der Datenverarbeitung, ihre Rechte wahrnehmen oder rechtsgeschäftliche Verbindungen eingehen zu können, insbesondere bei einer komplexen und für die betroffene Person intransparenten Datenverarbeitung (z. B. Im Rahmen einer Kreditentscheidung); oder

- dem Einsatz neuer Technologien, die neue Formen der Datenerhebung und -verarbeitung ermöglichen (z. B. „Internet der Dinge“).

Hinweis 1: Die Aufsichtsbehörden stellen Positiv- und Negativlisten zur Verfügung, für welche Verarbeitungsprozesse eine Datenschutz-Folgenabschätzung (nicht) erforderlich ist. Ist die geplante Datenverarbeitung bereits von einer solchen Liste erfasst, kann sich hieran orientiert werden.

Hinweis 2: Das Vorgehen bei der Prüfung, ob eine Datenschutz-Folgenabschätzung erforderlich ist, muss sorgfältig schriftlich dokumentiert werden. Diese Dokumentation ist dauerhaft aufzubewahren.

Hinweis 3: In Zweifelsfällen sollte eine Datenschutz-Folgenabschätzung durchgeführt werden!

14.6 Wie ist die Datenschutz-Folgenabschätzung durchzuführen?

Es gibt keine Vorgaben, wie genau eine Datenschutz-Folgenabschätzung durchzuführen ist. In jedem Fall sollten jedoch die Ergebnisse der Überlegungen zu den folgenden Punkten in einer Art Protokoll schriftlich dokumentiert werden:

- Systematische Beschreibung der geplanten Datenverarbeitungsvorgänge sowie ihrer Zwecke (Vorbereitungsphase);
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitungsvorgänge im Verhältnis zu den Zwecken (Bewertungsphase I). Zu prüfen ist insbesondere im Einzelfall, ob es alternative und datenschutzrechtlich weniger eingreifende Verarbeitungsformen gibt, durch die der Zweck der Datenverarbeitung in gleichem Maße erreicht werden kann;
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen (Bewertungsphase II). Gemeint sind Risiken bei der Datenverarbeitung, etwa im Falle von ungewolltem Datenverlust oder durch Datenmanipulation. Bei der Bewertung ist der Schutzbedarf in Abhängigkeit des prognostizierten Risikos zu bestimmen (je höher das Risiko, desto höher der Schutzbedarf);
- Zu ergreifende Abhilfemaßnahmen zur Risikobewältigung (Maßnahmenphase). In Betracht kommen insoweit Garantien gegenüber den betroffenen Personen, Sicherheitsvorkehrungen in Form von Präventivmaßnahmen sowie organisatorische Abläufe (z. B. eine Vier-Augen-Kontrolle); und
- Grundsätzlich muss der Standpunkt des Datenschutzbeauftragten (soweit vorhanden) und der betroffenen Personen (soweit diese bestimmbar sind und Geheimhaltungsinteressen dies nicht zwingend verbieten) in die Datenschutz-Folgenabschätzung einfließen. Dies ist zu dokumentieren.

Hinweis: Mehrere ähnliche Datenverarbeitungsprozesse mit ähnlich hohen Risiken erfordern nur eine einzige Datenschutz-Folgenabschätzung (z. B. Einsatzes eines Videoüberwachungssystems in mehreren Verkaufsflächen).

14.7 Praktisches Vorgehen

Bei der Prüfung, ob eine Datenschutz-Folgenabschätzung notwendig ist und bei der anschließenden Durchführung ist wie folgt vorzugehen:

- **Schritt 1:** Der Datenschutzbeauftragte muss – soweit vorhanden – informiert werden. Er ist zwingend einzubinden.
- **Schritt 2:** Prüfung gemäß obiger *Nummer 14.5*, ob eine Datenschutz-Folgenabschätzung notwendig ist (hohes Risiko für die betroffenen Personen, Datenverarbeitungsprozess auf Positivliste) oder nicht (Datenverarbeitungsprozess auf Negativliste).
- **Schritt 3:** Alle Personen, deren Unterstützung erforderlich sein könnte, sind einzubinden (z. B. Personalabteilung, IT, Marketing, Legal).
- **Schritt 4:** Sollte Schritt 2 ergeben, dass eine Datenschutz-Folgenabschätzung durchzuführen ist, muss diese unter Berücksichtigung der in *Nummer 14.6* genannten Punkte angestoßen werden. Einzelne Punkte sind ordnungsgemäß zu dokumentieren.
- **Schritt 5:** Es bietet sich an, agile Prozesse mit variablen Intervallen zu etablieren. Bei eintretenden Änderungen der Datenverarbeitung kann so festgestellt werden, ob eine erneute Datenschutz-Folgenabschätzung notwendig ist. Bei Bedarf ist die Datenschutz-Folgenabschätzung zu wiederholen.
- **Schritt 6:** Eine sorgfältige schriftliche Dokumentation der vorstehenden Schritte ist an zentraler Stelle im Unternehmen dauerhaft aufzubewahren.

- **Schritt 7:** Aus Transparenzgründen kann es ggf. sinnvoll sein, die Datenschutz-Folgenabschätzung (zumindest auszugsweise) für die von dem Datenverarbeitungsprozess betroffenen Personen zu veröffentlichen (Intranet für Mitarbeiter, Homepage für Kunden).

14.8 Weitere praktische Hinweise

Siehe die praktischen Hinweise: *Profiling*, *Automatisierte Einzelentscheidung* sowie *Datenschutz durch Technikgestaltung.*

Hinweis: Es bietet sich an, für eine effiziente Datenschutz-Folgenabschätzung einen Prozess aufzusetzen und im Unternehmen zu implementieren.

Einschlägige Hilfestellungen:

Bayerisches Landesamt für Datenschutzaufsicht, Software zur Datenschutz-Folgenabschätzung (PIA-Tool)

Die Software kann kostenlos auf der Internetseite *https://www.datenschutz-bayern.de/technik/pia-tool.html.de* heruntergeladen werden.

Beispiel für eine Positivliste der Bundesländer (hier Hamburg):

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO - nicht-öffentlicher Bereich (Stand: 19. Juli 2018)

Abrufbar unter:
www.datenschutz-hamburg.de

Datenschutzkonferenz (DSK) des Bundes und der Länder, Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO (Kurzpapier Nr. 5 vom 24. Juli 2017)

Abrufbar unter:
www.lda.bayern.de/media

15 Benennung Datenschutzbeauftragter (Art. 37)

15.1 Überblick

Jedes Unternehmen, das personenbezogene Daten verarbeitet, muss unter bestimmten Umständen einen Datenschutzbeauftragten benennen.

Auch wenn eine solche Pflicht nicht besteht, steht es dem Unternehmen frei, einen Datenschutzbeauftragten zu benennen.

15.2 Warum sollte dies ernst genommen werden?

- Der Datenschutzbeauftragte unterstützt das Unternehmen bei der Einhaltung der Bestimmungen zum Datenschutz durch sein besonderes Fachwissen.
- Die Nichtbenennung eines Datenschutzbeauftragten entgegen einer Benennungspflicht kann mit sehr hohen Bußen geahndet werden und zu erheblichen Reputationsschäden des Unternehmens führen.

15.3 Welche Aufgaben hat der Datenschutzbeauftragte?

Dem Datenschutzbeauftragten obliegen folgende Aufgaben:

- Unterrichtung und Beratung des Unternehmens, der Auftragsverarbeiter und der Beschäftigten zu Fragen des Datenschutzes;
- Überwachung der Einhaltung des Datenschutzes durch das Unternehmen;
- Beratung und Überwachung im Zusammenhang mit Datenschutz-Folgenabschätzungen;
- Sensibilisierung und Schulung der Beschäftigten zum Datenschutz; und
- Zusammenarbeit mit den Aufsichtsbehörden.

15.4 Wer muss einen Datenschutzbeauftragten benennen?

Die Pflicht zur Benennung besteht im Grundsatz für jedes Unternehmen, das personenbezogene Daten für eigene Geschäftszwecke verarbeitet (Verantwortliche), soweit es eines der Kriterien in *Nummer 15.5* erfüllt.

Darüber hinaus besteht die Pflicht auch für Unternehmen, die für andere Unternehmen Dienstleistungen erbringen und dabei personenbezogene Daten dieses Unternehmens verarbeiten (Auftragsverarbeiter), soweit der Auftragsverarbeiter dabei eines der Kriterien in *Nummer 15.6* erfüllt. Der Auftragsverarbeiter kann unabhängig davon auch für die eigene Datenverarbeitung verpflichtet sein, als Verantwortlicher einen Datenschutzbeauftragten zu bestellen, wenn insoweit die Kriterien nach *Nummer 15.6* erfüllt sind.

Mehrere Unternehmen in einer Unternehmensgruppe dürfen ein und denselben Datenschutzbeauftragten benennen, sofern dieser für jedes der Unternehmen erreichbar ist. Das setzt zumindest voraus, dass:

- seine Kontaktdaten den Mitarbeitern, externen Betroffenen (z. B. Kunden) und Aufsichtsbehörden bekannt sind;
- tatsächlich sichergestellt werden kann, dass der Datenschutzbeauftragte für Anfragen von Mitarbeitern, sonstigen Betroffenen und der jeweiligen Aufsichtsbehörde zur Verfügung steht; und
- eine Verständigung in der Sprache der Mitarbeiter und Aufsichtsbehörden gewährleistet werden kann, ggf. gemeinsam mit Hilfspersonal des Datenschutzbeauftragten.

15.5 Wann muss ein Datenschutzbeauftragter benannt werden?

Ein Datenschutzbeauftragter ist zu benennen, wenn eine der folgenden Konstellationen gegeben ist:

- In Deutschland in der Regel mindestens zehn Personen, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Dies kann schon erfüllt sein, wenn zehn Arbeitnehmer Computerarbeitsplätze mit einem E-Mail Account haben.
- Die Kerngeschäftstätigkeit einen Geschäftszweck hat, der eine Datenverarbeitung notwendig macht, welche nach Art, Umfang und/oder Zweck eine umfangreiche, regelmäßige und systematische Überwachung von Personen erforderlich macht.

- Die Überwachung muss dabei eng mit dem Geschäftszweck verbunden sein. Bei einem Dienstleistungsunternehmen, das z. B. Gehaltsabrechnung oder Sicherheitsdienste erbringt, ist der Geschäftszweck so eng mit der Überwachung von Personen verbunden, dass es einen Datenschutzbeauftragten bestellen muss. Im Gegensatz dazu stellt grundsätzlich die Gehaltsabrechnung für eigene Mitarbeiter oder der reguläre IT Betrieb nicht den Geschäftszweck eines Unternehmens dar, sodass es unter diesem Gesichtspunkt keinen Datenschutzbeauftragten bestellen muss.

- Die Kerntätigkeit in der umfangreichen Verarbeitung der nachfolgend aufgeführten besonders sensiblen Daten besteht: Rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische oder biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung oder Daten über strafrechtliche Verurteilungen und Straftaten.

- Eine Benennungspflicht dürfte eher die Ausnahme sein, käme aber etwa in Betracht, wenn umfassend Gesundheitsdaten von Mitarbeitern verarbeitet werden.

- Soweit dies nach dem lokalen Recht eines Mitgliedstaates der EU vorgeschrieben ist.

15.6 Wer kann als Datenschutzbeauftragter benannt werden?

Ein Mitarbeiter eines Unternehmens darf zum Datenschutzbeauftragten benannt werden, wenn:

- Er über das erforderliche Fachwissen verfügt, insbesondere die rechtlichen und praktischen Kenntnisse im Datenschutz hat, die in dem jeweiligen Geschäftskontext des Unternehmens erforderlich sind sowie die Organisation und Datenverarbeitung des Unternehmens kennt; und

- Kein Interessenkonflikt besteht. Ein solcher wäre aufgrund einer parallelen anderweitigen Tätigkeit im Unternehmen (was grundsätzlich erlaubt ist) denkbar, wenn er sich dann als Datenschutzbeauftragter unter Umständen selbst kontrollieren muss (etwa Leiter Recht, Leiter IT, Leiter Marketing).

Daneben besteht auch die Möglichkeit, ein externes Dienstleistungsunternehmen mit den Aufgaben des Datenschutzbeauftragten zu beauftragen und in dieser Funktion zu benennen. Dies bietet sich etwa an, um eigene interne Ressourcen besser nutzen zu können und von dem spezifischen Fachwissen des Dienstleistungsunternehmens profitieren zu können. Hier ist neben der Benennung auch der Abschluss eines Dienstleistungsvertrages notwendig.

15.7 Stellung des Datenschutzbeauftragten

Der Datenschutzbeauftragte:

- ist nicht weisungsgebunden;

- darf wegen seiner Aufgaben nicht abberufen oder benachteiligt werden;

- berichtet unmittelbar der Geschäftsleitung;

- ist hinsichtlich seiner Tätigkeit zur Verschwiegenheit verpflichtet;

- ist ordnungsgemäß und frühzeitig in alle mit dem Datenschutz zusammenhängende Fragen einzubinden; und

- ist Ansprechpartner für betroffene Personen (z. B. Mitarbeiter, Kunden) zu allen Fragen des Datenschutzes.

Das Unternehmen muss den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben unterstützen. Es muss ihm hierzu Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie erforderlichen Ressourcen geben und ihm die fachliche Fortbildung ermöglichen.

15.8 Praktisches Vorgehen

Bei der Benennung eines Datenschutzbeauftragten können die folgenden Schritte durchgeführt werden:

- **Schritt 1:** Prüfung anhand der in *Nummer 15.5* genannten Vorgaben, ob das Unternehmen als Verantwortlicher oder als Auftragsverarbeiter einen Datenschutzbeauftragten benennen muss.

- **Schritt 2:** Wenn eine Pflicht zur Benennung eines Datenschutzbeauftragten besteht: Prüfung, ob bereits ein anderes Unternehmen der Unternehmensgruppe einen Datenschutzbeauftragten benannt hat. Soweit dies der Fall ist: Prüfung anhand der Vorgaben in *Nummer 15.4*, ob dieser geeignet (erreichbar) ist und damit für das Unternehmen benannt werden kann. Klärung mit dem anderen Unternehmen und dem Datenschutzbeauftragten, ob dieser auch für das anfragende Unternehmen als Datenschutzbeauftragter benannt werden kann und soll.

- **Schritt 3:** Wenn in der Unternehmensgruppe noch kein Datenschutzbeauftragter benannt worden ist, aber eine Pflicht zur Benennung besteht: Ermittlung anhand der Kriterien in *Nummer 15.6*, welcher Mitarbeiter als Datenschutzbeauftragter benannt werden kann und soll, oder ob ein externes Dienstleistungsunternehmen mit der Wahrnehmung der Aufgaben des Datenschutzbeauftragten beauftragt werden kann und soll.

- **Schritt 4:** Einbindung derjenigen Personen, deren Unterstützung benötigt wird (z. B. Personalabteilung, IT, Marketing, Legal).

- **Schritt 5:** Abhängig von Schritten 2, 3 und 4: Schriftliche Benennung des Datenschutzbeauftragten.

- **Schritt 6:** Schriftliche Dokumentation der Analyse, warum ein Datenschutzbeauftragter (nicht) zu benennen ist.

- **Schritt 7:** Sicherstellung, dass die Kontaktdaten des Datenschutzbeauftragten (Anschrift, eine ihm zugewiesene Telefonnummer und eine ihm zugewiesene E-Mail Adresse):
  - den Mitarbeitern allgemein zur Kenntnis gebracht werden (z. B. schwarzes Brett, Intranet);
  - auf der Webseite des Unternehmens veröffentlicht werden;
  - in vorgeschriebenen Informationen aufgenommen werden (bei der Datenerhebung gegenüber den davon betroffenen Personen, Verzeichnis von Verarbeitungstätigkeiten); und
  - der für das Unternehmen zuständigen Aufsichtsbehörde mitgeteilt werden.

15.9 Einschlägige Hilfestellungen

Datenschutzkonferenz (DSK) des Bundes und der Länder, Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern (Kurzpapier Nr. 12 vom 16. Januar 2018)

Abrufbar unter:
www.lda.bayern.de/media

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Häufig gestellte Fragen zu Datenschutzbeauftragten (FAQ) (Stand: November 2018)

Hinweisblatt des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfahlen:

Abrufbar unter:
www.ldi.nrw.de

16

Kontakt mit Behörden (One-Stop-Shop) (Art. 51)

16.1 Überblick

Aufsichtsbehörden spielen bei der Überwachung und Durchsetzung des Datenschutzrechts (insbesondere Art. 51 ff. DS-GVO) eine entscheidende Rolle.

Grundsätzlich ist die Aufsichtsbehörde am Sitz der Hauptniederlassung zuständig. Bei grenzüberschreitenden Datenverarbeitungen innerhalb der EU ist nur eine federführende Aufsichtsbehörde zuständig.

16.2 Rahmenbedingungen

- Das Spektrum an Aufgaben und Befugnissen der Aufsichtsbehörden über den Datenschutz ist sehr weit und umfasst insbesondere:
  - Überwachung und Durchsetzung des Datenschutzrechts im Wege ihrer Kontroll- und Sanktionsbefugnisse;
  - Öffentlichkeitsarbeit, um über die Risiken der Datenverarbeitung zu informieren;
  - Aufklärung der Unternehmen hinsichtlich bestehender datenschutzrechtlicher Pflichten; und
  - Vereinheitlichung des Datenschutzes in Europa.
- Insbesondere unter folgenden Umständen kommen Unternehmen mit Datenschutzbehörden in Kontakt:
  - Ein etwaig zu bestellender Datenschutzbeauftragter ist bei der Aufsichtsbehörde zu registrieren.
  - Ein Datenschutzverstoß muss der zuständigen Aufsichtsbehörde gemeldet werden (siehe den „Praktischen Hinweis *Meldung von Verletzungen*“).
  - Eine Aufsichtsbehörde kontaktiert ein Unternehmen, weil sich eine betroffene Person über eine Datenverarbeitung durch dieses Unternehmen beschwert hat.
- Schwierig ist häufig die Antwort auf die Frage, welche Aufsichtsbehörde für ein Unternehmen zuständig ist:
  - Die Zuständigkeit der Aufsichtsbehörden ergibt sich aus dem Recht des Landes, in dem die Niederlassung bzw. das Unternehmen den Geschäftssitz hat. Allgemein kann man sagen: Die Aufsichtsbehörde am Geschäftssitz der Niederlassung bzw. ggf. der Hauptniederlassung eines Unternehmens, ist für die Datenverarbeitung durch die Niederlassung zuständig. Die Zuständigkeit der Aufsichtsbehörde bleibt dabei vom Grundsatz her auf das Hoheitsgebiet des Staates beschränkt. Es kann

daher vorkommen, dass eine Vielzahl von Aufsichtsbehörden für ein Unternehmen bzw. eine Unternehmensgruppe zuständig sind.

– Bei grenzüberschreitender Datenverarbeitung durch mehrere Niederlassungen eines Unternehmens in der EU gibt es eine Ausnahme zu der vorstehenden Regel: Hier ist allein die Aufsichtsbehörde am Sitz der Hauptniederlassung des Unternehmens in der EU federführend zuständig (sog. One-Stop-Shop). So soll eine einheitliche Anwendung des europäischen Datenschutzrechts gewährleistet werden.

Hinweis: Auf die Aussagen einer federführenden Aufsichtsbehörde dürfen sich alle an der internationalen Datenverarbeitung beteiligten EU-Niederlassungen des Unternehmens verlassen.

- Die Aufsichtsbehörden haben weitreichende Befugnisse. Sie können unter anderem Zugang zu den Geschäftsräumen ihres Unternehmens einschließlich aller Datenverarbeitungsanlagen verlangen, eine Datenverarbeitung einschränken oder auch vollständig untersagen und Bußgelder in empfindlicher Höhe verhängen.

Hinweis: Der ggf. in einem Unternehmen bestellte Datenschutzbeauftragte oder die Rechtsabteilung sind daher umgehend zu benachrichtigen. Es empfiehlt sich, jegliche weiteren Schritte in der Kommunikation mit der Aufsichtsbehörde gemeinsam mit diesem bzw. dieser abzustimmen!

16.3 Die zuständige Aufsichtsbehörde bei innereuropäischen, grenzüberschreitenden Datenverarbeitungen (One-Stop-Shop)

Soweit ein Unternehmen seine Hauptniederlassung in der EU hat, ist bei Vorliegen einer (innereuropäischen) grenzüberschreitenden Datenverarbeitung allein die federführende Aufsichtsbehörde am Sitz dieser Hauptniederlassung zuständig.

Eine grenzüberschreitende Datenverarbeitung liegt vor bei:

- einer Verarbeitung im Rahmen der Tätigkeit von Niederlassungen des Unternehmens in mehr als einem EU-Mitgliedstaat; oder

- einer Verarbeitung im Rahmen der Tätigkeit einer einzelnen Niederlassung des Unternehmens in der EU, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedsstaat hat oder haben kann. Zu nennen sind z. B.: unfaire Behandlungen, Diskriminierung, oder soweit Reputationsschäden drohen oder es wird eine große Menge an Daten verarbeitet.

Seine Hauptniederlassung hat ein Unternehmen typischerweise dort, wo der Sitz der Hauptverwaltung in der EU ist. Typischerweise ist das die Niederlassung, bei der die tatsächlichen und effektiven Managementtätigkeiten getroffen werden, die die Grundsatzentscheidungen der Datenverarbeitung umfassen.

Soweit aber die Entscheidungen hinsichtlich der Zwecke und Mittel der konkreten Datenverarbeitung in einer anderen Niederlassung in der EU getroffen werden und diese befugt ist, diese Entscheidungen auch in den anderen Niederlassungen umsetzen zu lassen, gilt diese Niederlassung als Hauptniederlassung.

Hinweis: Dies kann dazu führen, dass für verschiedene Verarbeitungsvorgänge verschiedene federführende Aufsichtsbehörden zuständig sind.

Hinweis: Das Konzept des One-Stop-Shop greift nur, wenn die Hauptniederlassung des Unternehmens in der EU ist. Befindet sich die Hauptniederlassung des Unternehmens außerhalb der EU, sind im Falle einer grenzüberschreitenden Datenverarbeitung jeweils die Aufsichtsbehörden der beteiligten Niederlassungen zuständig.

Neben der federführenden Aufsichtsbehörde besteht eine Zuständigkeit einer betroffenen Aufsichtsbehörde bei örtlichen Fällen, wenn:

- der Sachverhalt „nur“ mit der Niederlassung der betroffenen Aufsichtsbehörde zusammenhängt; oder
- wenn betroffene Personen „nur“ im Hoheitsgebiet der betroffenen Aufsichtsbehörde erheblich beeinträchtigt sind, etwa bei der Verarbeitung von Mitarbeiterdaten im spezifischen Beschäftigungskontext des Mitgliedsstaates.

Federführende und betroffene Aufsichtsbehörden müssen in einem solchen Fall eng zusammenarbeiten, wobei sichergestellt ist, dass im Ergebnis nur eine der beiden Aufsichtsbehörden den Fall behandeln wird.

16.4 Praktisches Vorgehen

Um die zuständige Aufsichtsbehörde für Ihr Unternehmen bzw. Ihre Niederlassung zu ermitteln, ist wie folgt vorzugehen:

- **Schritt 1:** Grundsätzlich kann (soweit vorhanden) der Datenschutzbeauftragte eines Unternehmens die Frage nach der für das in Rede stehende Unternehmen bzw. seine Niederlassung zuständigen Aufsichtsbehörde beantworten.
- **Schritt 2:** Soweit ein Unternehmen keinen Datenschutzbeauftragten bestellt hat, kann mit Hilfe allgemein zugänglicher Quellen (Informationen der Handelskammern, Internetrecherche) die zuständige Aufsichtsbehörde ermittelt werden.
- **Schritt 3:** Um festzustellen, ob bei einer grenzüberschreitenden Datenverarbeitung in der EU ggf. abweichend von der in Schritt 2 ermittelten Aufsichtsbehörde eine andere, federführende Aufsichtsbehörde zuständig ist, ist anhand von *Nummer 16.3* zu prüfen, d. h. ob im betreffenden Einzelfall eine grenzüberschreitende Datenverarbeitung in diesem Sinne vorliegt.
- **Schritt 4:** Sofern eine grenzüberschreitende Datenverarbeitung in diesem Sinne vorliegt, ist die Hauptniederlassung für die Datenverarbeitung und – entsprechend Schritt 2 oder 3 – die für diese zuständige Aufsichtsbehörde anhand von *Nummer 16.3* zu bestimmen.
- **Schritt 5:** Zu prüfen ist anhand von *Nummer 16.3*, ob im betreffenden Einzelfall ein lokaler Sachverhalt gegeben ist, so dass eine betroffene Aufsichtsbehörde zuständig ist.
- **Schritt 6:** Jegliche vorstehende Überlegung ist sorgfältig schriftlich zu dokumentieren. Dabei ist sicherzustellen, dass diese Dokumentation an zentraler Stelle des Unternehmens dauerhaft verfügbar gehalten wird.

16.5 Weitere praktische Hinweise

Siehe praktischer Hinweis *Meldung von Verletzungen*.

Einschlägige Hilfestellungen:

Bayerisches Landesamte für Datenschutzaufsicht, Der One Stop Shop (Stand: 12. Dezember 2016)

Abrufbar unter:
www.lda.bayern.de/media

Übersicht der Aufsichtsbehörden im Datenschutz für den nicht-öffentlichen Bereich:

Abrufbar unter:
www.datenschutz-bayern.de/info-quel/ds-inst/deutschland.html

Artikel-29-Datenschutzgruppe, Leitlinien für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters (Stand: 5. April 2017)

Abrufbar unter:
www.datenschutz.hessen.de

Impressum

Herausgeber
Bundesverband der Deutschen Industrie e. V.
Breite Straße 29
10178 Berlin
T.: +49 30 2028-0
www.bdi.eu

Linklaters LLP (Frankfurt am Main)
Taunusanlage 8
60329 Frankfurt am Main
www.linklaters.com

Redaktion
Dr. Daniel Pauly
Partner und Leiter Telekommunikation,
Medien, Technologie (Deutschland)
Linklaters LLP (Frankfurt am Main)

Marek Jansen
Syndikusrechtsanwalt und Referent
Recht, Wettbewerb und Verbraucherpolitik (BDI)

Konzeption
Sarah Schwake, Referentin
Abteilung Marketing, Online und Veranstaltungen

Layout
Michel Arencibia, Art Director
www.man-design.net

Druck
Das Druckteam
www.druckteam-berlin.de

Verlag
Industrie-Förderung Gesellschaft mbH, Berlin

Bildnachweis
Umschlag: © 195128860 | Scanrail | Fotolia.com
S. 4: © 115457793 | dvoinik | Fotolia.com
S. 8: © 206952130 | oatawa | Fotolia.com
S. 12: © 191945238 | monsitj | Fotolia.com
S. 16: © 189792649 | iaremenko | Fotolia.com
S. 20: © 115457785 | dvoinik | Fotolia.com
S. 21: © 159912258 | Gorodenkoff | Fotolia.com
S. 23: © 136283864 | kiri | Fotolia.com
S. 24: feXpdV001o4 | unsplash.com
S. 34: © 232435870 | terovesalainen | Fotolia.com
S. 42: © 188719057 | metelevan | Fotolia.com
S. 44: © 119913056 | Cybrain | Fotolia.com
S. 51: © 158449702 | Michail | Fotolia.com

Stand
Dezember 2018
BDI-Publikations-Nr. 0082

Der BDI in den sozialen Netzwerken

Verfolgen Sie tagesaktuell unsere Beiträge in den Sozialen Medien. Wir freuen uns über Likes, Retweets und Kommentare.

Twitter

@Der_BDI

YouTube

www.youtube.com/user/bdiberlin

Facebook

www.facebook.com/DerBDI

Newsletter

bdi.eu/media/newsletter-abo