Datenschutz ist Chefsache!

Leitfaden für kleine und mittlere Unternehmen

SACHSEN-ANHALT

Landesbeauftragter
für den Datenschutz

Datenschutz ist Chefsache! – Leitfaden für kleine und mittlere Unternehmen

Auflage: 2. Auflage, Dezember 2021
Herausgeber: Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt

Inhalt

1 Ziele und sachlicher Anwendungsbereich des Datenschutzes 9
2 Wichtige Begriffsbestimmungen 10
3 Grundsätze der Verarbeitung 17
4 Datenschutzmanagement..... 20
5 Rechtsgrundlagen 23
6 Betroffenenrechte 31
7 Sicherheit der Verarbeitung – technische und organisatorische Maßnahmen..... 40
8 Verzeichnis der Verarbeitungstätigkeiten..... 45
9 Der betriebliche Datenschutzbeauftragte 48
10 Meldungen von Datenschutzverletzungen und Benachrichtigung an die betroffenen Personen 52
11 Auftragsverarbeitung, gemeinsame Verantwortliche 57
12 Kundendatenschutz inkl. Werbung..... 61
13 Beschäftigtendatenschutz 66
14 Verarbeitung besonderer Kategorien personenbezogener Daten 72
15 Videoüberwachung..... 76
16 Die Unternehmenshomepage..... 80
17 Übermittlung personenbezogener Daten in Länder außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraumes (EWR) 84
18 Folgen von Datenschutzverstößen und Maßnahmen der Aufsichtsbehörden..... 86

Anhang

A Fragenkatalog für KMU zur Datenschutz-Grundverordnung – Wie gut sind Sie aufgestellt? 88

Vorwort

Liebe Leserin, lieber Leser[1]!

Sie sind Unternehmer, Geschäftsführer, gehören zu den Führungskräften eines kleinen oder mittleren Unternehmens bzw. sind in sonstiger Funktion mit Fragen des Datenschutzes befasst? Dann sind Sie Ansprechpartner dieses Leitfadens.

Datenschutz ist ein komplexes Thema, welches jedes Unternehmen betrifft. Datenschutz ist Grundrechtsschutz, auf deren Einhaltung betroffene Personen zunehmend achten. Die Erfahrung in meiner Behörde zeigt, dass dem Schutz personenbezogener Daten mitunter nicht die erforderliche Aufmerksamkeit gewidmet wird. Die Folgen sind Beschwerden der betroffenen Personen, aufsichtsbehördliche Kontrollmaßnahmen oder Anweisungen bis hin zu Bußgeldverfahren.

Die Verantwortung zur Einhaltung der Vorschriften über den Datenschutz trägt im Unternehmen in letzter Instanz die Unternehmensleitung, auch wenn die Umsetzung notwendiger Maßnahmen durch eigene Beschäftigte oder Dienstleister ausgeführt wird. Der Landesbeauftragte für den Datenschutz unterstützt hierbei gern.

Zugegeben: Datenschutz kann Kosten verursachen und erfordert Manpower. Die Einhaltung datenschutzrechtlicher Vorschriften führt jedoch zu erheblichen Vorteilen. Datenschutz schafft Vertrauen bei Kunden, Geschäftspartnern und Beschäftigten. Dies bewirkt eine positive Öffentlichkeitswirkung, stärkt die Kundenbindung und trägt zur Wettbewerbsfähigkeit Ihres Unternehmens bei.

Dieser Leitfaden soll Ihnen als Orientierungshilfe bei der Durchführung notwendiger Maßnahmen zur Umsetzung von Datenschutz und Datensicherheit sowie zur Selbstüberprüfung dienen.

Er enthält in 18 Kapiteln grundlegende Informationen zu Fragestellungen, die in jedem kleinen und mittleren Unternehmen relevant sein können. In den jeweiligen Kapiteln befinden sich Hinweise zu vertiefenden, mitunter sehr ausführlichen Quellen, hilfreichen Formularen,

[1] Genderhinweis: Aus Gründen der besseren Lesbarkeit wird in der Folge auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Vorlagen usw., die sich alle auf der Homepage des Landesbeauftragten befinden. Die Hinweise erfolgen in Form von schreibbaren Kurzlinks. Dieser Leitfaden kann damit als Druck- und als Onlineversion als konkrete Arbeitshilfe genutzt werden. Die Onlineversion ist abrufbar unter https://lsaurl.de/ChefsacheDS.

Im Anhang befindet sich ein Fragenkatalog, der Ihnen die Möglichkeit gibt, zu prüfen, wie der Datenschutz in Ihrem Unternehmen aufgestellt ist. Die Fragen geben Ihnen zugleich Anhaltspunkte, worauf die Aufsichtsbehörde bei Prüfungen regelmäßig besonderen Wert legt.

Albert Cohaus
Vertreter im Amt

Abkürzungsverzeichnis

Abs.	Absatz
AO	Abgabenordnung
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
DSAG LSA	Gesetz zur Ausfüllung der Verordnung (EU) 2016/679 und zur Anpassung des allgemeinen Datenschutzrechts in Sachsen-Anhalt
DS-GVO	VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Daten-schutz-Grundverordnung)
ErwGr	Erwägungsgrund
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
GRCh	Charta der Grundrechte der Europäischen Union
inkl.	inklusive
IT	Informationstechnik
i. V. m.	in Verbindung mit
KMU	kleine und mittlere Unternehmen
lit.	Litera
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TTDSG	Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutzgesetz)
u. a.	unter anderem

UWG	Gesetz gegen den unlauteren Wettbewerb
z. B.	zum Beispiel

Dieser Leitfaden enthält Bezugnahmen und Zitate aus den Kurzpapieren der Datenschutzkonferenz. Quellenvermerk: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz). Datenlizenz Deutschland – Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – Version 2.0 (www.govdata.de/dl-de/by-2-0).

Datenlizenz

Jede Nutzung dieses Leitfadens ist ohne Einschränkungen oder Bedingungen zulässig. Die bereitgestellten Daten und Metadaten dürfen für die kommerzielle und nicht kommerzielle Nutzung insbesondere

- vervielfältigt, ausgedruckt, präsentiert, verändert, bearbeitet sowie an Dritte übermittelt werden;
- mit eigenen Daten und Daten Anderer zusammengeführt und zu selbstständigen neuen Datensätzen verbunden werden;

in interne und externe Geschäftsprozesse, Produkte und Anwendungen in öffentlichen und nicht öffentlichen elektronischen Netzwerken eingebunden werden.

1 Ziele und sachlicher Anwendungsbereich des Datenschutzes

Datenschutz, insbesondere die DS-GVO, dient dem Ziel, die Grundrechte und Grundfreiheiten und insbesondere die Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zu schützen (zum Begriff des personenbezogenen Datums siehe Kapitel 2). Es gewährleistet jeder natürlichen Person das Recht, über Preisgabe und Verwendung ihrer persönlichen Daten grundsätzlich selbst zu entscheiden. Zudem soll der freie Verkehr personenbezogener Daten zwischen den Mitgliedstaaten der Europäischen Union gewährleistet werden, (Art. 1 DS-GVO).

Das bedeutet, dass bei Fragen, ob und inwieweit in den konkreten Fällen personenbezogene Daten verarbeitet werden dürfen, eine Abwägung unter Wahrung des Verhältnismäßigkeitsprinzips durchzuführen ist. Dies bezieht sich auch auf zu berücksichtigende Sicherheitsmaßnahmen. Dabei ist das Recht auf Datenschutz insbesondere mit der Freiheit der Kommunikation und der Meinungsäußerung, der Informationsfreiheit, der unternehmerischen Freiheit, der Achtung des Privat- und Familienlebens sowie der Unverletzlichkeit der Wohnung in Einklang zu bringen.

Allerdings unterfallen nicht alle Arten von Daten und nicht jede Form des Umgangs mit Daten der DS-GVO oder dem BDSG. Die DS-GVO ist nur anwendbar, wenn personenbezogene Daten mindestens teilweise automatisiert oder in einem nach mindestens zwei Merkmalen recherchefähigen Aktensystem („Dateisystem“) verarbeitet werden (Art. 2 Abs. 1 DS-GVO, § 1 Abs. 1 Satz 2 BDSG). Ein recherchefähiges Aktensystem liegt z. B. schon dann vor, wenn in einem Ordner die Bestellungen der Kunden alphabetisch nach deren Namen geordnet werden.

Die DS-GVO ist nicht anzuwenden, wenn personenbezogene Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten verarbeitet werden (Art. 2 Abs. 2 lit. c DS-GVO, § 1 Abs. 1 Satz 2 BDSG). So kann eine elektronisch geführte Liste von Privatkontakten ausschließlich persönlichen Tätigkeiten dienen. Hinsichtlich einer Verarbeitung personenbezogener Daten, die neben persönlichen auch unternehmerischen Tätigkeiten dient, z. B.

eine Liste von Kontaktdaten befreundeter Kunden, die auch geschäftlich genutzt werden soll, ist die DS-GVO in Gänze anwendbar.

Beschäftigtendaten (also z. B. Daten von Angestellten) werden vom Datenschutz auch dann erfasst, wenn sie nicht dateigebunden verarbeitet werden (§ 26 Abs. 7 BDSG). So gelten die Beschränkungen des § 26 BDSG auch für handschriftliche Notizen des Arbeitgebers über Beschäftigte selbst dann, wenn sie nicht zur Personalakte genommen werden sollen (Näheres zum Beschäftigtendatenschutz siehe Kapitel 13).

2 Wichtige Begriffsbestimmungen

Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen, Art. 4 Nr. 1 DS-GVO. Der Begriff ist generell weit zu verstehen, da die gesetzliche Definition ausdrücklich „alle“ Informationen einbezieht.

Zu den personenbezogenen Daten gehören Name, Anschrift, Geburtsdatum, Geschlecht, Augenfarbe, Größe und Gewicht. Außerdem zählen auch Meinungen, Motive, Wünsche, Überzeugungen und Werturteile dazu. Ebenso sind Vermögens- und Eigentumsverhältnisse sowie Vertragsbeziehungen und kundenbezogene Kennziffern umfasst. E-Mail-Adressen sind dann personenbezogen, wenn sie eindeutige Identifizierungsmerkmale, z. B. Teile des Namens, enthalten. Darüber hinaus können auch bestimmte Prognosen personenbezogene Daten sein, z. B. die Prognose hinsichtlich der Fähigkeit und des Willens, einen zukünftigen Kredit zurückzuzahlen (Bonität).

Die Form der Informationen spielt keine Rolle. Grundsätzlich sind alle Informationen umfasst, egal ob es sich um Sprache, Schrift, Zeichen, Bild oder Ton handelt.

Eine Person ist „identifiziert“, wenn sie durch vorhandene Informationen eindeutig erkennbar ist, ohne dass weitere Informationen erforderlich sind. Ein solcher Fall ist z. B. gegeben, wenn persönliche Identifikationsmerkmale (Name, Anschrift, Geburtsdatum) angegeben werden.

Müssen vorhandene Informationen erst mit anderen Daten verknüpft werden, um eine Person eindeutig bestimmen zu können, ist die Person „identifizierbar“ (vgl. Art. 4 Nr. 1 DS-GVO).

Prinzipiell sind insoweit alle Mittel zu berücksichtigen, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren (vgl. ErwGr 26 DS-GVO). Der Personenbezug besteht bereits zu dem Zeitpunkt, ab dem die Identifizierung sehr wahrscheinlich ist.

Eine Telefonnummer stellt z. B. häufig schon ein personenbezogenes Datum dar, bevor sie mit Hilfe eines Telefonverzeichnisses einer Person zugeordnet wird. Ebenso sind z. B. Videoaufzeichnungen von Personen (bei ausreichender Bildauflösung) bereits im Zeitpunkt der Aufnahme personenbezogene Daten und nicht erst ab dem Zeitpunkt der tatsächlichen Identifizierung einer Person.

Verarbeitung

Der Begriff der Verarbeitung wird in Art. 4 Nr. 2 DS-GVO gesetzlich definiert. Dabei werden verschiedene Verarbeitungsschritte ausdrücklich genannt: Das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung personenbezogener Daten.

Nicht jede datenschutzrechtliche Beurteilung erfordert eine exakte Abgrenzung der einzelnen Schritte. Andererseits ist es denkbar, dass datenschutzrechtliche Verantwortlichkeiten sich je nach Verarbeitungsschritt ändern können. Außerdem knüpfen gesetzliche Regelungen zum Teil an bestimmte Verarbeitungsschritte an. Z. B. stellt Art. 13 DS-GVO ausdrücklich auf die Erhebung ab („zum Zeitpunkt der Erhebung“).

Erheben ist das aktive Beschaffen von personenbezogenen Daten, durch welches die Daten erstmals in den Verfügungsbereich des Verantwortlichen gelangen und der Verantwortliche die Möglichkeit zur Kenntnisnahme hat. Ob tatsächlich Kenntnis vom Inhalt der Daten genommen wird, ist unerheblich.

Ein Erheben liegt z. B. vor, wenn der Verantwortliche Daten über ein von ihm zur Verfügung gestelltes Kontaktformular entgegennimmt. Gelangen Daten ohne jedes eigene Zutun in den Verfügungsbereich des Verantwortlichen, sind sie alleine dadurch noch nicht erhoben. Letzteres kann z. B. vorliegen bei der unaufgeforderten Zusendung eines Angebotes. Wird dieses Angebot allerdings elektronisch oder in Papierform weiterverarbeitet z. B. durch Aufnahme in eine Akte, liegt eine Erhebung und zusätzlich gegebenenfalls eine Speicherung, Nutzung oder sonstige Verarbeitung vor.

Erfasst werden personenbezogene Daten dann, wenn sie in irgendeiner Form verkörpert oder fixiert werden. Dies kann z. B. durch aufschreiben, filmen oder kopieren erfolgen.

Erheben und Erfassen sind häufig mit einer Speicherung (siehe unten) verbunden. Notwendig ist ein solcher Zusammenhang aber nicht.

Die Organisation und das Ordnen von Daten sind Vorgänge, bei denen Strukturen oder Sortiermerkmale so verändert werden, dass die Möglichkeiten zur Auffindung und Auswertung der Daten vereinfacht oder verbessert werden (sollen). Der Informationsgehalt der Daten selbst wird hierbei nicht verändert. Z. B. könnten Daten in einer Datei gespeichert werden, in der nach bestimmten Kriterien recherchiert werden kann. Der Begriff „Ordnen“ soll – als Unterfall der „Organisation“ – klarstellen, dass auch unsortierte Daten durch Aufbereitung („Ordnen“) unter die DS-GVO fallen können.

Speicherung ist die Aufbewahrung personenbezogener Daten in verkörperter Form „auf“ einem „lesbaren“ Datenträger zur Weiterverarbeitung. Datenträger sind z. B. Festplatten, USB-Sticks, Server und auch nichtelektronische Datenträger wie Notizblock, Karteikasten oder eine Sammlung von Aktenordnern. Der Begriff der Speicherung ist technologieneutral. Auf Eigentum, Besitz oder Verfügungsgewalt an bzw. über den Datenträger kommt es nicht an. Entscheidend ist die Zugriffsmöglichkeit. Deshalb gelten auch Daten in einer Cloud als „gespeichert“.

Die Unterscheidung von „Erfassen“ und „Speicherung“ ist manchmal nicht vollständig möglich, in aller Regel für eine datenschutzrechtliche Beurteilung in entsprechenden Fällen aber auch nicht notwendig.

Veränderung ist eine Umgestaltung – in der Regel gespeicherter – personenbezogener Daten, durch die deren Informationsgehalt geändert wird. Die Anpassung ist – als Unterfall der Veränderung – eine Änderung von Daten, die sich inhaltlich an einem anderen, vorgegebenen Datum orientiert. Ein typischer Fall der „Anpassung“ ist z. B. die Aktualisierung von Einkommensdaten oder einer Anschrift.

Unter Auslesen versteht man die Zurückgewinnung von Informationen aus gespeicherten personenbezogenen Daten. Man könnte hier auch vom Zugänglichmachen zur weiteren Verarbeitung sprechen.

Abfragen ist ein Unterfall des Auslesens. Beim Auslesen werden die Informationen mit Hilfe von Suchroutinen aus den gespeicherten Daten gewonnen, z. B. durch die Eingabe eines Stichworts zur Suche.

Die Verwendung erfasst als „Auffangtatbestand“ jede Nutzung personenbezogener Daten, die nicht schon ausdrücklich in Art. 4 Nr. 2 DS-GVO genannt ist.

Eine Offenlegung durch Übermittlung personenbezogener Daten ist die Mitteilung der Daten an einen individuell bestimmten Adressaten. Die Art und Weise der Übermittlung spielt keine Rolle (z. B. schriftlich, elektronisch oder durch Übergabe eines Datenträgers). Der Adressat muss „Empfänger“ im Sinne von Art. 4 Nr. 9 DS-GVO sein (siehe unten). Werden Daten im Internet zum Abruf bereitgehalten, liegt ohne Abruf des jeweiligen Nutzers noch keine Übermittlung vor.

Eine Verbreitung liegt vor, wenn personenbezogene Daten einem unbestimmten Adressatenkreis mitgeteilt werden (z. B. Übertragung der Daten im TV, im Rundfunk oder durch Zeitungen). Man könnte hier auch von „Veröffentlichung“ sprechen, sofern die Daten die Adressaten auch erreichen.

Werden personenbezogene Daten einem Adressaten anders zugänglich gemacht als durch eine Übermittlung oder eine Verbreitung liegt das Merkmal der „anderen Form der Bereitstellung“ vor. Hierunter fallen z. B. Fälle des Bereithaltens personenbezogener Daten zum Abruf im Internet.

Unter dem Abgleich personenbezogener Daten versteht man die Prüfung, ob die Daten in mehreren Systemen vorhanden sind bzw. ob

mehrere Daten ganz oder teilweise übereinstimmen. Dies könnte man auch mit dem Begriff „Vergleich“ bezeichnen.

Verknüpfung bezeichnet die Zusammenführung personenbezogener Daten. Dies sind z. B. Fälle, in denen ein Datensatz zu einem anderen hinzugespeichert wird oder in denen einem Datensatz ein Hinweis auf einen anderen Datensatz beigefügt wird. Verknüpfung von personenbezogenen Daten werden oft vorgenommen, um z. B. Werbung möglichst individuell auf den Empfänger abzustimmen.

Art. 4 Nr. 3 DS-GVO definiert die Einschränkung der Verarbeitung (siehe auch Kapitel 6 zu Art. 18 DS-GVO) als „Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken“. Die Daten bleiben gespeichert, Verarbeitungen werden aber durch technische und organisatorische Maßnahmen für bestimmte Zwecke ausgeschlossen. Dies kann durch eine von anderen Daten getrennte Aufbewahrung oder durch eine Markierung – deren Beachtung sichergestellt ist – erfolgen.

Das Löschen (siehe auch Kapitel 6 zum Recht auf Löschung) personenbezogener Daten bedeutet die Entfernung von allen Datenträgern. Es muss ein Zustand hergestellt werden, in dem die Daten nicht mehr mit verhältnismäßigem Aufwand ausgelesen werden können. Die Datenträger selbst bleiben funktionstüchtig.

Bei der Vernichtung personenbezogener Daten werden die Datenträger selbst zerstört, sodass ein Auslesen nicht mehr möglich ist. Ein typischer Fall ist z. B. das Schreddern von Papierakten. Die Vernichtung ist ein Unterfall der Löschung.

Automatisierte Verarbeitung

Die „automatisierte Verarbeitung“ wird in der DS-GVO und auch im BDSG (n. F.) nicht definiert. Der Begriff ist technikneutral und weit gefasst zu verstehen. Ihm unterfallen sämtliche heute gebräuchlichen Verarbeitungen personenbezogener Daten unter Verwendung von Informationstechnik. Es genügt eine teilweise automatisierte Verarbeitung, also bereits die Unterstützung auch nur eines Schrittes der gesamten Verarbeitung durch Informationstechnik. Beispiele sind Aktensysteme mit automatisiertem Index, Papierakten, die mit elektronischen Akten verknüpft sind oder Datenverarbeitungen mit Computern

(z. B. auch Textverarbeitung), Servern, Smartphones, Tablets, Videokameras.

Dateisystem

Art. 4 Nr. 6 DS-GVO definiert den Begriff „Dateisystem“. Ein Dateisystem ist eine strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien geordnet und entsprechend recherchiert werden können. Der Begriff umfasst Akten und Aktensammlungen, Krankenblätter oder sonstige Karteikartensammlungen. Ordnungs- und Recherchekriterien sind vor allem Jahrgänge, Aktenzeichen oder Namen. Ungeordnete Akten oder Aktensammlungen fallen nicht unter die DS-GVO (ErwGr 15, Satz 3), es sei denn, sie sollen später in ein sortiertes Dateisystem aufgenommen werden (Art. 2 Abs. 1 DS-GVO am Ende, § 1 Abs. 1 Satz 2 BDSG: „oder gespeichert werden sollen“).

Verantwortlicher

Verantwortlicher ist, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, also bestimmt, warum die Verarbeitung erfolgt und wie dieses Ziel erreicht wird. Nach Art. 4 Nr. 7 DS-GVO können dies natürliche Personen, juristische Personen, Behörden, Einrichtungen oder andere Stellen sein. Die (personelle) Delegation an Mitarbeiter innerhalb einer Stelle führt nicht dazu, dass die Stelle selbst (z. B. die GmbH oder der Verein) von ihrer datenschutzrechtlichen Verantwortung frei wird. So trägt die GmbH weiterhin für die Verarbeitung personenbezogener Daten die Verantwortung, auch wenn hausinterne Zuständigkeiten festgelegt wurden und ein Datenschutzbeauftragter benannt worden ist.

Auftragsverarbeiter

Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO) ist, wer personenbezogene Daten ganz und gar nach Weisung des Auftraggebers verarbeitet, welcher ausschließlich über Zwecke und Mittel der Verarbeitung entscheidet. Beispiele für eine Auftragsverarbeitung sind Verarbeitung von Kundendaten durch ein Callcenter ohne wesentliche eigene Entscheidungsspielräume, Datenerfassung, Datenkonvertierung, Einscannen von Dokumenten oder Datenträgerentsorgung durch Dienstleister. Keine Auftragsverarbeitung liegt vor, wenn eigenständige

Fachleistungen erbracht werden, wie dies z. B. bei Rechtsanwälten, Steuerberatern oder Zustelldiensten (Post) der Fall ist.

Empfänger

Nach Art. 4 Nr. 9 DS-GVO ist Empfänger eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden. Es kann also jede Person oder Personenmehrheit Empfänger sein. Auch der Auftragsverarbeiter (siehe oben) ist Empfänger. Mitarbeiterinnen und Mitarbeiter innerhalb eines Unternehmens sind normalerweise keine Empfänger. Es fehlt ihnen gegenüber dem Unternehmen als Verantwortlichem (siehe oben) an der datenschutzrechtlichen Eigenständigkeit.

Die DS-GVO verwendet den Begriff des Empfängers ausdrücklich z. B. in Art. 13 Abs. 1 lit. e, Art. 14 Abs. 1 lit. e, Art. 15 Abs. 1 lit. c und in Art. 19 DS-GVO.

Dritter

Art. 4 Nr. 10 DS-GVO definiert, wer „Dritter“ ist. Grundsätzlich ist dies jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle. Allerdings schließt die Norm folgende „Rollen“ vom Begriff des Dritten aus: 1. die betroffene Person, 2. den Verantwortlichen, 3. den Auftragsverarbeiter und 4. die Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Vereinfacht ausgedrückt sind „Dritte“ Personen oder Stellen, die keinen Bezug zu den Daten oder ihrer Verarbeitung haben. Dies wird dadurch deutlich, dass die DS-GVO in Bezug auf den Dritten keine Offenlegung personenbezogener Daten als Merkmal in der Definition enthält. Überschneidungen mit dem Begriff des „Empfängers“ sind möglich.

Die Definition des „Dritten“ wird von der DS-GVO ausdrücklich aufgegriffen (z. B. in Art. 6 Abs. 1 Satz 1 lit. f, in Art. 4 Nr. 9, 13 Abs. 1 lit. d und Art. 14 Abs. 2 lit. b DS-GVO).

Einwilligung

Art. 4 Nr. 11 DS-GVO enthält insgesamt sechs Anforderungen an eine wirksame Einwilligung: Freiwilligkeit, Bestimmtheit, Informiertheit, Erteilung durch die betroffene Person, Unmissverständlichkeit und Einwilligungsfähigkeit („Abgabe“). Die wichtigsten Punkte hierzu werden bei den Rechtsgrundlagen (siehe auch Kapitel 5) erläutert.

In Art. 4 DS-GVO befinden sich weitere wichtige Begriffsbestimmungen.

3 Grundsätze der Verarbeitung

Die Grundsätze der Verarbeitung personenbezogener Daten stellen die Grundbedingungen jeder Datenverarbeitung dar. Sie werden durch Einzelvorschriften der DS-GVO konkretisiert. Obwohl sie in Art. 5 Abs. 1 DS-GVO sehr abstrakt formuliert sind, entfalten sie eine Bindungswirkung und sind einzuhalten. Verstöße allein gegen die Grundsätze können aufsichtsbehördliche Maßnahmen, z. B. Bußgelder nach sich ziehen.

Der Verantwortliche muss die Einhaltung der Grundsätze gewährleisten und insbesondere auch nachweisen können. Zwar ist die Form des Nachweises nicht durch die DS-GVO festgelegt, es empfiehlt sich aber eine schriftliche oder elektronische Dokumentation. Zum Nachweis dienen auch die Dokumentationspflichten der DS-GVO, insbesondere das Verzeichnis von Verarbeitungstätigkeiten (siehe Kapitel 8), welches schriftlich oder in einem elektronischen Format zu führen ist.

Die Grundsätze im Einzelnen:

Der Grundsatz der Rechtmäßigkeit verlangt, dass für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage erforderlich ist. Dieser Grundsatz wird insbesondere durch Art. 6 und 9 konkretisiert (siehe Kapitel 5). Eine Rechtsgrundlage kann sich darüber hinaus aus dem nationalen Recht ergeben, wenn dies durch eine Öffnungsklausel der DS-GVO ermöglicht wird. Von der Öffnungsklausel des Art. 88 DS-GVO wurde z. B. durch § 26 BDSG Gebrauch gemacht.

Die Verarbeitung nach Treu und Glauben verlangt eine faire und offene Verarbeitung, die frei ist von Täuschungen. Davon werden Situationen erfasst, bei denen betroffene Personen durch die Verarbeitung ihrer Daten Nachteile erleiden, weil im Verhältnis zum Verantwortlichen kein Kräftegleichgewicht besteht. Treu und Glauben dürfte als Auffangtatbestand zu verstehen sein für die Fälle, in denen andere Grundsätze nicht greifen.

Dem Grundsatz der Transparenz liegt der Gedanke zugrunde, dass ohne hinreichende Informationen der betroffenen Personen der Datenschutz ins Leere laufen würde, weil ihr Verstöße nicht bekannt würden und sie ihre Betroffenenrechte nicht geltend machen könnte. Schon nach Art. 8 Abs. 2 der Grundrechtscharta der Europäischen Union hat jede Person das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Der Grundsatz wird insbesondere durch die Vorschriften zu den Informationspflichten (Art. 12-14 DS-GVO) und zum Auskunftsrecht (Art. 12, 15 DS-GVO) konkretisiert.

Nach dem Grundsatz der Zweckbindung dürfen personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke (z. B. Vertragserfüllung) erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Der Zweck der Verarbeitung ist daher entscheidend für die Zulässigkeit der Verarbeitung. Wann eine Zweckänderung im Einzelfall zulässig ist, regelt Art. 6 Abs. 4 DmS-GVO (siehe Kapitel 5).

Das Gebot der Datenminimierung verlangt, dass die Verarbeitung personenbezogener Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke notwendige Maß beschränkt ist. Die Datenminimierung wirkt sich auf alle Einzelschritte der Verarbeitung aus. Personenbezogene Daten dürfen danach nur dem festgelegten Zweck entsprechend z. B. erhoben, gespeichert, verändert, ausgelesen, abgefragt oder auch an Dritte übermittelt werden. Unternehmensintern dürfen nur die Beschäftigten personenbezogene Daten verarbeiten, für die dies zu ihrer Aufgabenerfüllung erforderlich ist. Im Rahmen der Verteilung der Aufgaben innerhalb des Unternehmens sollte geprüft werden, inwieweit die Anzahl dieser Beschäftigten begrenzt werden kann. Es sollten Rollenkonzepte für die Nutzung der elektronischen

Medien erstellt und ansonsten Zugangskriterien erstellt werden (z. B. Wer muss unbedingt Zugang zu Personalakten haben?).

Nach dem Grundsatz der Richtigkeit müssen personenbezogene Daten richtig verarbeitet werden und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Die betroffene Person kann nach Art. 16 DS-GVO die Berichtigung oder auch die Löschung ihrer Daten verlangen.

Die Speicherbegrenzung erfordert, dass die Identifizierung betroffener Personen nur so lange möglich ist, wie es für die Zwecke, für die personenbezogene Daten verarbeitet werden, erforderlich ist. Um dies sicherzustellen, sollten Unternehmen Fristen für die Löschung und eine regelmäßige Überprüfung vorsehen.

Im Rahmen der Sicherheit der Verarbeitung verlangt namentlich die Gewährleistung der Integrität und Vertraulichkeit Schutzmaßnahmen. Personenbezogene Daten sind insbesondere vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung zu schützen. Dieser Schutz ist durch geeignete technische und organisatorische Maßnahmen zu gewährleisten. Der Grundsatz wird insbesondere durch die Art. 25 und 32 DS-GVO (siehe dazu Kapitel 7) aber auch die Melde- und Benachrichtigungspflichten der Art. 33 und 34 DS-GVO (siehe dazu Kapitel 10) konkretisiert.

Geschäftsleitungen sollten Verfahren implementieren, bei denen in angemessenen Zeitabständen die Einhaltung der Grundsätze und die entsprechenden Nachweise geprüft werden. Die ist insbesondere dann erforderlich, wenn sich die Verarbeitung personenbezogener Daten oder auch nur die technischen und organisatorischen Maßnahmen verändern. Eine Prüfung ist auch dann angezeigt, wenn im Laufe der Zeit Fehler erkannt werden oder aufgrund sich fortentwickelnder Technik neue Sicherheitsmaßnahmen erforderlich werden.

4 Datenschutzmanagement

Datenschutz als Querschnittsaufgabe betrifft unterschiedliche betriebliche Bereiche. Anwenden müssen ihn alle Mitarbeiter, die personenbezogene Daten verarbeiten. Dies können z. B. Bürokräfte, Sachbearbeiter, Kundenberater, IT-Verantwortliche oder andere Beschäftigte sein, die – untereinander abgestimmt – für eine datenschutzgerechte Verarbeitung zu sorgen haben. Da regelmäßig zeitgleich unterschiedliche betriebliche Bereiche betroffen sind und der Schutz der informationellen Selbstbestimmung ein hohes Rechtsgut ist, deren Verletzung für die betroffenen Personen erhebliche Folgen haben kann, ist der Datenschutz eine Aufgabe des Managements und damit Chefsache.

Die Unternehmensleitung trägt die Gesamtverantwortung hinsichtlich der Einhaltung datenschutzrechtlicher Vorschriften für das Unternehmen. Hervorzuheben sind folgende Aspekte:

- Die Unternehmensleitung muss die organisatorischen Voraussetzungen dafür schaffen, dass die datenschutzrechtlichen Vorgaben, insbesondere die aus der DS-GVO und dem BDSG, aber auch aus den jeweils anwendbaren Spezialgesetzen, im Unternehmen umgesetzt werden. Dies beinhaltet die Erstellung von Richtlinien, Merkblättern und Anweisungen genereller Art, bei schwierigen oder grundlegenden Sachverhalten auch Entscheidungen im Einzelfall. Eine Datenschutzrichtlinie kommt z. B. häufig für die Nutzung der IT-Infrastruktur des Unternehmens, inkl. mobiler Endgeräte, in Betracht. Darin sollten insbesondere Hinweise enthalten sein, welche einschlägigen gesetzlichen und betriebsinternen Vorschriften und welche Maßnahmen zur Minimierung von Risiken für die Datenverarbeitung einzuhalten sind (siehe dazu Kapitel 7). Soll die Nutzung der IT zu privaten Zwecken der Beschäftigten möglich sein? Hinweise auf Folgen von Verstößen können die Durchsetzung der Richtlinien fördern.
- Soweit die Datenverarbeitung mitbestimmungspflichtige Angelegenheiten betrifft, wäre der Betriebsrat zu beteiligen. Weiterhin müssen die unternehmensinternen Zuständigkeiten festgelegt werden (z. B. wer meldet Datenschutzverletzungen an die Aufsichtsbehörde, wer ist verantwortlich für das Verzeichnis von Verarbeitungstätigkeiten und wer für die Implementierung technischer

Schutzmaßnahmen, wer erfüllt die Betroffenenrechte?). In kleinen Unternehmen werden diese Aufgaben nur auf wenige Schultern verteilt werden können. Gleichwohl ist der Datenschutz auch in den kleinsten Unternehmen einzuhalten.

- Die Unternehmensleitung muss die finanziellen, sachlichen und personellen Ressourcen bereitstellen, die für die Einhaltung des Datenschutzes erforderlich sind. Dazu gehört die Bereitstellung datenschutzgerechter Technik (Art. 25, 32 DS-GVO) sowie die Schulung und Sensibilisierung der Mitarbeiter. Erforderlich ist es, die Beschäftigten, die personenbezogene Daten verarbeiten, auf die Einhaltung des Datenschutzes zu verpflichten (weitere Informationen hierzu und das Muster einer Verpflichtungserklärung finden Sie im Kurzpapier Nr. 19 der Datenschutzkonferenz unter https://lsaurl.de/Kurzpapiere). Die Unternehmensleitung muss auch sicherstellen, dass die Einhaltung des Datenschutzes angemessen überwacht wird. Dies kann in Form der Eigenkontrolle, z. B. durch interne Revisoren oder den Datenschutzbeauftragten oder durch externe Fachleute geschehen.
- Schon bei der Prozess- und Produktentwicklung bzw. der Beschaffung ist durch die Unternehmensleitung darauf hinzuwirken, wie die Datenschutzgrundsätze – etwa die Datenminimierung – eingehalten werden können. Durch Voreinstellungen in Hardware- und Software-Produkten muss gewährleistet sein, dass nur solche personenbezogenen Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind.
- Verträge, die die Verarbeitung personenbezogener Daten betreffen, müssen datenschutzgerecht gestaltet sein. Soll ein anderes Unternehmen die Verarbeitung im Auftrag übernehmen, müssen die Voraussetzungen für eine Auftragsverarbeitung erfüllt werden. Hier muss insbesondere ein Vertrag abgeschlossen werden, der die Voraussetzungen des Art. 28 Abs. 3 DS-GVO erfüllt. Legt das Unternehmen zusammen mit anderen Unternehmen die Zwecke und Ziele der Datenverarbeitung fest, muss eine Vereinbarung nach Art. 26 DS-GVO getroffen werden (näheres siehe Kapitel 11).
- Die Unternehmensleitung muss dafür Sorge tragen, dass eine Datenschutz-Folgenabschätzung (DSFA) immer dann durchgeführt wird, wenn eine Form der Verarbeitung ein hohes Risiko für die

betroffene Person zur Folge hat (Art. 35 Abs. 1 DS-GVO). Sie ist insbesondere erforderlich bei einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten, z. B. Gesundheitsdaten, oder bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche (vgl. ErwGr 84, 90-93 DS-GVO und Kurzpapier Nr. 5 der Datenschutzkonferenz, siehe https://lsaurl.de/Kurzpapiere). Eine Liste von Verarbeitungsvorgängen, für die eine DSFA durchzuführen ist, befindet sich auf der Homepage des Landesbeauftragten (siehe https://lsaurl.de/DSFAListe). Geht aus der DSFA hervor, dass die Verarbeitung ein hohes Risiko hat und trifft der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos, so muss durch die Unternehmensleitung sichergestellt werden, dass die Aufsichtsbehörde konsultiert wird (Art. 36 DS-GVO).

- Weitere Informationen enthalten die Leitlinien zur Datenschutz-Folgenabschätzung der Art.-29-Datenschutzgruppe (siehe https://lsaurl.de/GuidelinesHighRisk)[2].
- Weiterhin muss durch die Unternehmensleitung gewährleistet werden, dass die Rechte der betroffenen Personen gewahrt werden (Art. 12 bis 22 DS-GVO). Die Betroffenenrechte wurden durch die DS-GVO wesentlich erweitert (siehe Kapitel 6). Gänzlich neu sind das Recht auf Vergessenwerden und das Recht auf Datenübertragbarkeit. Ein Augenmerk sollte die Unternehmensleitung auch auf die Informationspflichten, die bereits bei der Erhebung personenbezogener Daten zu erfüllen sind, werfen.
- Es muss durch die Unternehmensleitung geprüft werden, ob ein betrieblicher Datenschutzbeauftragter zu benennen ist (siehe Kapitel 9). Falls ein solcher zu benennen ist, muss sie diesem die für die Erfüllung seiner Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen. Der Datenschutzbeauftragte ist ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden (vgl. insgesamt Art. 38 DS-GVO).

[2] Da eine Datenschutz-Folgenabschätzung in KMU nur selten erforderlich ist, haben wir auf die Aufnahme eines diesbezüglichen Kapitels verzichtet und verweisen insoweit auf die genannten Quellen.

- Schließlich obliegt es dem Unternehmen, mit der Datenschutzaufsichtsbehörde zusammenzuarbeiten, Art. 31 DS-GVO. Die Aufsichtsbehörde wird sich bei schlüssigen Beschwerden über die Datenverarbeitung oder bei anderen Anlässen, die ein Einschreiten erfordern, regelmäßig an die Unternehmensleitung wenden. Die Unternehmensleitung muss Sorge dafür tragen, dass die Aufsichtsbehörde ihre Befugnisse nach Art. 58 DS-GVO im Unternehmen ausüben kann. Diese Befugnisse ermöglichen Anordnungen zu einem aktiven Handeln wie die Bereitstellung von Informationen als auch zur Duldung, wie die Gewährung von Zugang zu den verarbeiteten personenbezogenen Daten und Geschäftsräumen einschließlich aller Datenverarbeitungsanlagen.

5 Rechtsgrundlagen

Alle in der DS-GVO genannten Schritte der Datenverarbeitung nach Art. 4 Nr. 2 (siehe Kapitel 2) erfordern eine Rechtsgrundlage.

Art. 6 Abs. 1 Satz 1 DS-GVO listet die zentralen Rechtsgrundlagen auf, aus denen sich die Rechtmäßigkeit der Verarbeitung personenbezogener Daten ergeben kann. Es besteht allerdings keine Rangfolge. Daneben gibt es auch noch andere Gesetze und Rechtsquellen, die Vorschriften zur Datenverarbeitung enthalten (z. B. BDSG, DSAG LSA, TKG, TMG, TTDSG, AO, Betriebsvereinbarungen u. a.).

Die Rechtsgrundlagen nach Art. 6 Abs. 1 Satz 1 lit. b bis f DS-GVO schließen das Kriterium der Erforderlichkeit ein. Erforderlich ist die Datenverarbeitung nur, wenn eine Aufgabe oder ein Zweck ohne Verarbeitung der personenbezogenen Daten nicht oder nicht in zumutbarer Weise erfüllt werden kann.

Einwilligung

Vor der Erteilung ihrer Einwilligung muss die betroffene Person umfassend über die Datenverarbeitung informiert worden sein. Sie muss konkret wissen, welche Daten zu welchem Zweck wie lange verarbeitet werden und wer der Verantwortliche ist. Die betroffene Person soll so die Risiken der Datenverarbeitungen abschätzen können, bevor sie eine Einwilligung erteilt. Die betroffene Person muss außerdem über

ihr Recht zum jederzeitigen Widerruf der Einwilligung in Kenntnis gesetzt werden (Art. 7 Abs. 3 Satz 3 DS-GVO).

Die Einwilligung ist nur wirksam, wenn sie freiwillig, eindeutig aktiv bestätigend und konkret bestimmt erteilt wird (siehe Art. 4 Nr. 11 DS-GVO).

Freiwillig erfolgt die Einwilligung, wenn sie ohne jeden Zwang, ohne Einschüchterung und ohne Täuschung erklärt wurde. Weitere Voraussetzung ist, dass die betroffene Person für den Fall der Verweigerung oder des Widerrufs keine Nachteile befürchten muss.

Besteht zwischen dem Verantwortlichen und der betroffenen Person ein deutliches Ungleichgewicht – wie dies z. B. im Arbeitsverhältnis oft der Fall ist – spricht eine solche Situation gegen die Freiwilligkeit einer Einwilligung.

Wird die Einwilligung in Form von Listen eingeholt – z. B. von der Belegschaft einer Filiale o. ä. – entsteht regelmäßig ein psychischer Druck zur Einwilligung, wenn die Liste für alle offen lesbar herumgereicht wird.

Die Einwilligung muss durch eine unmissverständliche Erklärung oder eine sonstige eindeutig bestätigende (aktive) Handlung erklärt werden. Eine Einwilligung durch Schweigen oder Untätigkeit ist nicht wirksam. Ein bereits vorangekreuztes Kästchen vor dem Text einer Einwilligungserklärung wird die Einwilligung unwirksam machen.

Wird die Einwilligung schriftlich erteilt, müssen die Anforderungen nach Art. 7 Abs. 2 DS-GVO beachtet werden. Die Einwilligungserklärung darf nicht einfach in andere Vertragserklärungen eingefügt sein, z. B. in allgemeine Geschäftsbedingungen. Notwendig ist vielmehr eine verständliche und klare Formulierung, sowie eine leichte Unterscheidbarkeit von anderen Vertragserklärungen oder -bedingungen.

Eine Einwilligung unter Bezugnahme auf Vertragsklauseln ist aber möglich, soweit die datenschutzrechtlichen Anforderungen an die Einwilligung gewahrt sind.

Soll in eine Verarbeitung von besonderen Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) eingewilligt werden, so muss die Einwilligung „ausdrücklich“ erfolgen. Ein Verhalten, aus dem auf die

Erteilung einer Einwilligung lediglich geschlossen werden kann („konkludentes Handeln“) scheidet hier aus.

Die Einwilligung muss sich auf einen oder mehrere konkrete Zwecke der Verarbeitung personenbezogener Daten beziehen und ausreichend konkret bestimmt sein. Der Verantwortliche darf die durch eine Einwilligung erlangten Daten nicht einfach für andere Zwecke verarbeiten. Eine Zweckänderung würde ebenfalls einer Einwilligung bedürfen.

Die Einwilligung rechtfertigt nur diejenigen Datenverarbeitungsphasen (Art. 4 Nr. 2 DS-GVO), für die sie unmissverständlich erteilt wurde. Eine pauschale Einwilligung in die Datenverarbeitung insgesamt und beliebige Verwendung wäre unwirksam.

Ist der beabsichtigte Zweck der Datenverarbeitung erreicht oder ist eine befristete Einwilligung abgelaufen, darf eine weitere Datenverarbeitung nicht mehr auf die Einwilligung gestützt werden.

Eine einmal unbefristet erteilte Einwilligung erlischt grundsätzlich nicht allein durch Zeitablauf. Um Unklarheiten über die Wirksamkeit einer Einwilligung zu vermeiden, kann es aber empfehlenswert sein, Kriterien für einen Zeitraum der Wirksamkeit festzulegen. Zu denken ist z. B. an die Zeit während eines laufenden Vertragsverhältnisses bis zu höchstens zwei Jahre ab Vertragsbeendigung.

Den Verantwortlichen trifft nach Art. 7 Abs. 1 DS-GVO eine ausdrückliche Verpflichtung, die Erteilung der Einwilligung nachweisen zu können. Es empfiehlt sich daher, schriftliche oder auf elektronischem Wege nachweisbare Einwilligungen einzuholen.

Art. 8 DS-GVO enthält besondere Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft.

Vertragsverhältnisse

Art. 6 Abs. 1 Satz 1 lit. b DS-GVO regelt die Verarbeitung zur Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen. Die von der Datenverarbeitung betroffene Person muss selbst Vertragspartei sein oder erkennbar („auf Anfrage“) werden wollen. Die Datenverarbeitung muss in diesem Zusammenhang erforderlich sein (siehe schon oben).

Hierunter sind Fälle zu fassen, in denen Vertragspflichten ohne die Datenverarbeitung nicht oder nur erheblich erschwert erfüllt werden könnten. So kann z. B. eine geschuldete Lieferung nur unter Erhebung und Speicherung der Lieferadresse erfolgen. Um einen Versandkauf abwickeln zu können bedarf es der Verarbeitung von personenbezogenen Daten wie Name, Anschrift und Zahlungsdaten. Eine Altersabfrage kann erforderlich sein, um z. B. einen Verstoß gegen das Jugendschutzgesetz (§§ 9, 12, 15 JuSchG) zu vermeiden. Umfasst ist die vertragliche Hauptleistungspflicht sowie vertragliche Nebenpflichten.

Es wird für die Abwicklung von Verträgen häufig erforderlich sein, gerade Kontaktdaten des Vertragspartners zu erheben, zu erfassen, zu speichern, zu ordnen und im Bedarfsfall zu verwenden. Nicht notwendig ist, dass die Daten sofort benötigt werden.

Vor der Vermietung von Wohnraum ist es gängige Praxis, bei Mietinteressenten und Mietinteressentinnen persönliche Angaben zu erheben, auf deren Basis eine Entscheidung über den Vertragsabschluss getroffen werden soll. Die hiermit zusammenhängenden Fragestellungen werden in der Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressentinnen (https://lsaurl.de/OHMietSelbstauskunft) dargestellt.

Die vertraglichen Leistungspflichten sind auch dann für die zulässige Datenverarbeitung maßgeblich, wenn es sich bei einem Geschäftsmodell um ein Tauschgeschäft „Dienstleistung gegen Daten“ handelt, weil z. B. eine Leistung „kostenlos“ im Austausch gegen personenbezogene Daten erbracht wird (Suchdienst, Netzwerk, Informationsdienst usw.). Nicht erforderlich ist es hier in der Regel, pauschal alle verfügbaren Daten eines Nutzers auszuwerten, um optimierte Werbung anbieten zu können. Möglicherweise kommt dann aber eine Einwilligung als Rechtsgrundlage in Betracht.

Unter die Durchführung vorvertraglicher Maßnahmen fällt z. B. die Erstellung von Angeboten für Werk-, Werklieferungs-, Dienst- oder Reiseverträgen auf Anfrage. Der Vertrag muss nicht notwendig zustande kommen. Mit Erledigung entfallen Zweck und Erforderlichkeit der Verarbeitung für die Zukunft. Allerdings muss sich eine vorvertragliche Maßnahme auf das Entstehen eines konkreten Vertragsverhältnisses

beziehen. Eine vorsorgliche Datenverarbeitung auf Initiative des Verantwortlichen fällt nicht in diesen Bereich.

Erfüllung einer rechtlichen Verpflichtung

In Deutschland existieren zahlreiche gesetzliche Verpflichtungen zur Verarbeitung personenbezogener Daten. Die Rechtsgrundlage bildet Art. 6 Abs. 1 Satz 1 lit. c DS-GVO in Verbindung mit der jeweiligen speziellen Vorschrift.

Beispielhaft können §§ 11, 11a, 14 GewO; §§ 13 Abs. 4 Satz 1; 28 Abs. 1, 6 HwO; § 22 GastG genannt werden. Aber auch Regelungen des Arbeitsrechts (§§ 34, 88 BBiG), des Sozialrechts (§§ 28a, 23a SGB IV; §§ 199 ff. SGB V; §§ 190 ff. SGB VI; § 27 Abs. 2 KVLG 1989) und des Melderechts (§§ 30 Abs. 4, 32 Abs. 1 Satz 3, Abs. 2 BMG) u. v. a. fallen in diesen Bereich.

Lebenswichtige Interessen

Art. 6 Abs. 1 Satz 1 lit. d DS-GVO erlaubt die Verarbeitung personenbezogener Daten zum Schutz lebenswichtiger Interessen von natürlichen Personen. Allerdings soll diese Rechtsgrundlage nur zur Anwendung kommen, wenn offensichtlich nicht auf eine andere Rechtsgrundlage zurückgegriffen werden kann (ErwGr 46 Satz 2 DS-GVO). In derartigen Fällen wird Art. 9 DS-GVO ebenfalls zu beachten sein.

Öffentliche Gewalt/öffentliches Interesse

Nach Art. 6 Abs. 1 Satz 1 lit. e DS-GVO kann die Datenverarbeitung zur Aufgabenerfüllung in Ausübung öffentlicher Gewalt oder im öffentlichen Interesse rechtmäßig sein. Diese Rechtsgrundlage bedarf hier keiner näheren Darstellung. Auf diese Vorschrift können sich Unternehmen berufen, soweit sie hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen (z. B. Bezirksschornsteinfeger; Kfz-Werkstätten, die mit der Durchführung von Abgasuntersuchungen beliehen wurden).

Interessenabwägung

Nach Art. 6 Abs. 1 lit. f DS-GVO können die Interessen des für die Verarbeitung Verantwortlichen oder Dritter eine Verarbeitung personenbezogener Daten rechtfertigen. Dies setzt voraus, dass sich der

Verantwortliche oder der Dritte auf berechtigte Interessen berufen kann und dass die Datenverarbeitung zur Wahrung dieser berechtigten Interessen erforderlich ist. Als weitere Voraussetzung dürfen die Interessen oder Grundrechte der betroffenen Personen nicht überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Erweist sich die Verarbeitung als zur Wahrung der berechtigten Interessen erforderlich, sind die für beide Seiten bestimmten Interessen zu gewichten. Der Verantwortliche kann alle denkbaren wirtschaftlichen, ideellen oder rechtlichen Interessen – auch eines Dritten – in die Interessenabwägung einbringen.

Der Verantwortliche muss aber vor der Verarbeitung entgegenstehende Interessen prüfen und gewichten. Jede Person, deren personenbezogene Daten zur Wahrung der berechtigten Interessen des Verantwortlichen oder des Dritten verarbeitet werden, kann sich auf das Recht zum Schutz der sie betreffenden personenbezogenen Daten berufen (Art. 8 GRCh). Beeinträchtigungen dieses Rechts müssen grundsätzlich nicht hingenommen werden. Es obliegt den betroffenen Personen darüber zu bestimmen, was mit ihren personenbezogenen Daten geschieht. Zugunsten der betroffenen Personen sind hier die Daten, die missbrauchsanfällig sind, z. B. Kontodaten, besonders zu gewichten.

Stützen Verantwortliche die Verarbeitung personenbezogener Daten auf Art. 6 Abs. 1 Satz 1 lit. f DS-GVO, kommt es oft vor, dass veröffentlichte Daten – wie z. B. die im Internet zu findende E-Mail-Adresse einer Person – als ohne Weiteres nutzbar angesehen werden. Eine solche Bewertung ist datenschutzrechtlich aber nicht haltbar. Wer seine personenbezogenen Daten veröffentlicht, verzichtet damit nicht pauschal auf datenschutzrechtliche Anforderungen zur Nutzung seiner Daten. Auch in diesen Fällen ist eine sorgfältige Interessenabwägung erforderlich.

Als Kriterien sind nach ErwGr 47 DS-GVO bei einer Abwägung insbesondere zu berücksichtigen, was die betroffene Person nach ihrem Verhältnis zu dem Verantwortlichen (z. B. Kundenbeziehung) vernünftigerweise erwarten durfte und in welchem Ausmaß sie die Verarbeitung von Anfang an erkennen konnte („Absehbarkeit“).

Ein häufiger Anwendungsfall von Art. 6 Abs. 1 Satz 1 lit. f DS-GVO ist die Beurteilung der Zulässigkeit einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung, sofern die Datenverarbeitung hier nicht aufgrund einer Einwilligung der betroffenen Person erfolgt.

Anders als häufig angenommen, ergibt sich die Zulässigkeit der Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung allerdings nicht alleine aus dem ErwGr 47 Satz 7 DS-GVO. Dieser bezeichnet Direktwerbung als ein mögliches berechtigtes Interesse, wägt dieses Interesse aber nicht gegen die Interessen der betroffenen Personen ab. Die eigentliche Abwägung muss durch den Verantwortlichen im konkreten Einzelfall erfolgen (siehe Kapitel 12).

Weitere berechtigte Interessen im Sinne von Art. 6 Abs. 1 Satz 1 lit. f DS-GVO können auf Seiten des Verantwortlichen z. B. die Betrugsprävention (siehe ErwGr 47 Satz 6 DS-GVO) oder die Verbesserung der IT-Sicherheit sein (ErwGr 49 DS-GVO).

Darüber hinaus sind z. B. die Einholung von Bonitätsauskünften bei einer Auskunftei, die Veröffentlichungen von Bildern, die Datenverarbeitung durch ein Bewertungsportal und der Einsatz von Technik zur Videoüberwachung regelmäßig nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zu beurteilen.

Es ist nachdrücklich zu empfehlen, die Interessenabwägung nicht als Ersatz für eine fehlende oder widerrufene Einwilligung zu verwenden. Allzu groß ist das Risiko, das betroffene Personen davon ausgehen, ihre Daten werden nur im Rahmen ihrer erteilten Einwilligung verarbeitet. Dies könnte die Datenverarbeitung intransparent werden lassen und dazu führen, dass Interessen des Verantwortlichen zurücktreten müssen. Dann wäre Art. 6 Abs. 1 Satz 1 lit. f DS-GVO in derartigen Fällen keine tragfähige Rechtsgrundlage mehr. Ein anderes rechtliches Problem könnte die Frage nach der Wirksamkeit der Einwilligung sein. Werden Betroffene darüber informiert, dass ihre Daten „sowieso“ verarbeitet werden, sei es auf Grundlage einer Einwilligung oder jedenfalls auf Grundlage einer Interessenabwägung, kann dies eine Einwilligung unwirksam machen, da es an der erforderlichen Freiwilligkeit fehlt. Außerdem sollten Verantwortliche bedenken, dass eine

Einwilligung jederzeit frei widerrufbar ist, also als Rechtsgrundlage in konkreten Fällen durchaus nicht „in Stein gemeißelt“ ist.

Zweckänderung

Eine Weiterverarbeitung von personenbezogenen Daten zu anderen als den ursprünglich festgelegten Zwecken kann nach Art. 6 Abs. 4 DS-GVO zulässig sein, wenn eine entsprechende Einwilligung vorliegt, eine Rechtsgrundlage zum Schutz der Ziele aus Art. 23 Abs. 1 DS-GVO besteht oder soweit die neuen und die ursprünglichen Zwecke gem. Art. 6 Abs. 4 lit. a bis e DS-GVO miteinander vereinbar sind. Um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit dem ursprünglichen Zweck vereinbar ist, sind insbesondere folgende Umstände zu berücksichtigen:

- jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
- der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
- die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gem. Art. 9 DS-GVO verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DS-GVO verarbeitet werden,
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
- das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Eine Vereinbarkeit mit dem ursprünglichen Zweck ist z. B. regelmäßig anzunehmen bei der Verarbeitung von personenbezogenen Daten zu Kontrollzwecken und Rechnungsprüfungen. Die Ausnutzung des kommerziellen Wertes personenbezogener Daten mit Hilfe einer Profilbildung hat mit dem ursprünglichen Zweck der Vertragserfüllung nichts zu tun.

Die betroffene Person ist vor der zweckändernden Weiterverarbeitung zu informieren (siehe Art. 13 Abs. 4, Art. 14 Abs. 4 DS-GVO).

Art. 6 Abs. 4 DS-GVO rechtfertigt aber nicht die Datenverarbeitung selbst, sondern lediglich eine Zweckänderung der Datenverarbeitung. Für die Datenverarbeitung an sich bedarf es nach wie vor einer Rechtsgrundlage aus Art. 6 Abs. 1 DS-GVO.

6 Betroffenenrechte

Ein ganz wesentlicher Teil der DS-GVO ist Kapitel 3, das grundlegende Pflichten der Verantwortlichen und Rechte der betroffenen Personen regelt. Dazu gehören die

- die Pflicht, bestimmte Informationen im Zusammenhang mit der Verarbeitung personenbezogener Daten mitzuteilen bzw. bereitzustellen (Art. 13, 14 DS-GVO)

und die Rechte auf

- Auskunft (Art. 15 DS-GVO),
- Berichtigung (Art. 16 DS-GVO),
- Löschung (Art. 17 DS-GVO),
- Einschränkung der Verarbeitung (Art. 18 DS-GVO),
- Datenübertragbarkeit (Art. 20 DS-GVO),
- Widerspruch (Art. 21 DS-GVO) und
- die Rechte bei automatisierten Entscheidungen (Art. 22 DS-GVO).

Darüber hinaus normiert die DS-GVO auch die Rechte auf

- Widerruf der Einwilligung (Art. 7 Abs. 3 DS-GVO),
- Beschwerde bei einer Datenschutzaufsichtsbehörde (Art. 77 DS-GVO),
- wirksamen gerichtlichen Rechtsbehelf (Art. 79 DS-GVO) und
- Schadenersatz (Art. 82 DS-GVO)

„Betroffene Personen“ sind die identifizierten oder identifizierbaren Personen, auf die sich verarbeitete Daten (Informationen) beziehen. Dazu gehören nicht nur die Kunden, sondern z. B. auch Geschäftspartner, Beschäftigte, Mitglieder, Homepagebesucher, Personen, die von einer Videokamera des Verantwortlichen erfasst wurden.

Der Verantwortliche hat den betroffenen Personen die Ausübung ihrer Rechte zu erleichtern (Art. 12 Abs. 2 DS-GVO, ErwGr 59 DS-GVO). Jegliche Einflussnahme auf die Betroffenen, von der Geltendmachung ihrer Rechte abzusehen, verbietet sich. Es empfiehlt sich, für die Anträge, die besonders häufig eingehen, z. B. insbesondere für Auskunftsverlangen nach Art. 15 DS-GVO, jeweils einen standardisierten Prozess einzuführen und hierfür ggf. Formulare oder sogar IT-gestützte Funktionen für die Betroffenen und Bearbeiter beim Verantwortlichen bereitzustellen.

Geht ein Antrag einer Person ein und hat der Verantwortliche begründete Zweifel an der Identität, so kann und sollte er die notwendigen zusätzlichen Informationen anfordern, um die Identität der betroffenen Person zu überprüfen (Art. 12 Abs. 6 DS-GVO, ErwGr 64 DS-GVO). Stellt z. B. eine Person den Antrag per E-Mail und die E-Mail-Adresse ist dem Verantwortlichen bisher unbekannt, kann an die bisher bekannte E-Mail-Adresse oder einen bekannten anderen Kontaktweg bei der betroffenen Person nachgefragt werden, ob der Antrag tatsächlich von ihr stammt. Eine Kopie eines Ausweisdokuments anzufordern ist häufig nicht erforderlich bzw. auch angesichts § 20 Abs. 2 PAuswG in der Regel unzulässig. Die Antwort des Verantwortlichen sollte stets über einen Kontaktweg erfolgen, der nach gesicherter Erkenntnis zu der betroffenen Person führt.

Alle Informationen und Mitteilungen hat der Verantwortliche den betroffenen Personen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache und grundsätzlich unentgeltlich zu übermitteln (Art. 12 Abs. 1 und 5 DS-GVO).

Auf Anträge nach Art. 15 bis 22 DS-GVO muss der Verantwortliche zudem fristgerecht antworten. Er hat der betroffenen Person unverzüglich, spätestens aber innerhalb eines Monats nach Eingang, mitzuteilen, was aufgrund ihres Antrages veranlasst wurde; ggf. ist zumindest eine Zwischennachricht zu erteilen (Art. 12 Abs. 3 DS-GVO). Auch wenn z. B. der Verantwortliche gar keine Daten über die betroffene Person verarbeitet, muss ihr dieser Umstand beauskunftet werden (Art. 15 Abs. 1 1. Halbsatz DS-GVO). Wird der Verantwortliche auf einen Antrag einer betroffenen Person nicht tätig, ist die Person gleichermaßen fristgerecht über die Gründe dafür zu unterrichten

sowie über die Möglichkeit, Beschwerde bei einer Aufsichtsbehörde oder einen gerichtlichen Rechtsbehelf einzulegen (Art. 12 Abs. 4 DS-GVO).

Informationspflichten

Jeder Verantwortliche, der im Geltungsbereich der DS-GVO personenbezogene Daten verarbeitet, muss zunächst die betroffenen Personen unaufgefordert und proaktiv über die Datenverarbeitungen und die Betroffenenrechte informieren. Art. 13 und 14 DS-GVO enthalten den Katalog der Informationen, die bereitgestellt werden müssen. Dazu zählen Name und Kontaktdaten des Verantwortlichen und ggf. die Kontaktdaten des Datenschutzbeauftragten, die Verarbeitungszwecke und Rechtsgrundlagen, die berechtigten Interessen des Verantwortlichen, die Datenkategorien, die Herkunft und mögliche Empfänger der Daten, ggf. Übermittlungen in Drittländer, die Verarbeitungsdauer bzw. Löschfristen, ggf. weitere Informationen bei einer automatisierten Entscheidungsfindung sowie umfassende Hinweise auf die Betroffenenrechte.

Werden personenbezogene Daten bei der betroffenen Person erhoben, sind die Informationen zum Zeitpunkt der Erhebung der Daten zur Verfügung zu stellen (Art. 13 Abs. 1 DS-GVO), bei Dritterhebungen regelt Art. 14 Abs. 3 DS-GVO den Zeitpunkt, in der Regel spätestens binnen eines Monats nach der Erhebung.

Die Informationen können dem Betroffenen als Ausdruck ausgehändigt oder übersandt werden. Möglich ist auch ein Aushang in den Geschäftsräumen des Verantwortlichen, wenn der Kontakt zu den Betroffenen in der Regel dort persönlich stattfindet. Der Aushang muss sich dann an einer Stelle befinden, an der sich üblicherweise alle Betroffenen aufhalten. Ergänzend sollte dann eine ausgedruckte Ausgabe, ein Flyer oder Merkblatt ausgelegt werden, damit die Betroffenen die Informationen auch mitnehmen und sich später in Ruhe damit auseinandersetzen können.

Die Informationen können auch elektronisch, u. a. auf einer Webseite, zur Verfügung gestellt werden (Art. 12 Abs. 1 DS-GVO, ErwGr 58 DS-GVO). In Anbetracht der Menge an Informationen, die der betroffenen Person zur Verfügung zu stellen sind, können die Informationen auf

mehreren Ebenen erfolgen. So sollte auf der ersten Ebene (z. B. einem Schreiben an einen neuen Kunden) auf die Verarbeitungszwecke, die Identität des Verantwortlichen (regelmäßig bereits im Briefkopf enthalten), die Rechtsgrundlage der Verarbeitung, ein Hinweis auf die Existenz der Betroffenenrechte, die wichtigsten Auswirkungen der Verarbeitung, die Kontaktdaten des Datenschutzbeauftragten und auf die Fundstelle, unter der die gesamten Informationen nach Art. 13 bzw. Art. 14 DS-GVO aufzufinden sind, hingewiesen werden. Die Fundstelle kann z. B. ein Link sein, der auf die Webseite hinweist, unter der die gesamten Informationen zu finden sind. Allerdings sollten zumutbare Möglichkeiten genutzt werden, einen Medienbruch zu vermeiden, denn nicht alle betroffenen Personen können jederzeit Informationen aus dem Internet abrufen. Eine Veröffentlichung auf der Homepage des Verantwortlichen kann gleichwohl das Informationsangebot ergänzen. Dabei müssen die elektronisch verfügbaren Informationen leicht auffindbar sein; hier können Bildsymbole oder QR-Codes helfen.

Auf der Homepage sind stets die nach Art. 13 DS-GVO notwendigen Informationen bezüglich der Datenverarbeitungen zu veröffentlichen, die mittels der Homepage selbst durchgeführt werden. Diese werden häufig „Datenschutzerklärung“ genannt und dürfen auf keiner Internetseite fehlen, denn heutzutage werden auf fast allen Internetseiten aus Gründen der IT-Sicherheit zumindest die IP-Adressen der Besucher protokolliert. Dazu kommen häufig Kontaktformulare oder andere Funktionen, z. B. Cookies, mit denen personenbezogene Daten verarbeitet werden. Auch diese Datenschutzerklärung muss leicht auffindbar sein (Näheres siehe Kapitel 16).

Hilfreich zur Erfüllung der Informationspflichten kann die Nutzung eines Tools sein, welches der Landesbeauftragte für den Datenschutz Baden-Württemberg unter https://www.baden-wuerttemberg.datenschutz.de/ds-gvo.clever/ zur Verfügung stellt.

Weitere Informationen, auch zu den Ausnahmen von der Informationspflicht, sind dem Kurzpapier Nr. 10 der Datenschutzkonferenz zu entnehmen, abrufbar unter https://lsaurl.de/Kurzpapiere. Einen Vordruck für die Erfüllung der Informationspflichten aufgrund einer Videoüberwachung, der nur mit wenigen Angaben ergänzt werden muss, finden sie unter https://lsaurl.de/VideoInfoblatt. Ausführliche Hinweise

enthalten die Leitlinien für Transparenz gem. der Verordnung 2016/679 der Artikel-29-Datenschutzgruppe, abrufbar unter https://lsaurl.de/LeitlinienTransparenz.

Recht auf Auskunft

Das Auskunftsrecht nach Art. 15 DS-GVO dient dazu, dass sich die betroffene Person einen Überblick darüber verschaffen kann, ob und inwieweit ihre Daten von einem bestimmten Verantwortlichen verarbeitet werden, damit sie daran anschließend die Rechtmäßigkeit der Datenverarbeitung überprüfen und/oder weitere Betroffenenrechte ausüben kann.

Wenn eine betroffene Person von einem Verantwortlichen Auskunft nach Art. 15 DS-GVO verlangt, ist dieser Person mitzuteilen, ob ihre personenbezogenen Daten verarbeitet werden und, wenn ja, um welche Daten und Datenkategorien es sich handelt. Im Unterschied zur Informationspflicht ist hier genau anzugeben, welche Einzeldaten verarbeitet werden. So ist z. B. die konkrete Schreibweise des verarbeiteten Namens (Maier, Meier oder Meyer), der E-Mail-Adresse, der Telefonnummer, der postalischen Anschrift etc. zu beauskunften. Dies dient der betroffenen Person als Korrektiv, woraufhin sie ggf. ihr Recht auf Berichtigung geltend machen kann. Zudem wäre eine Berichtigung sicherlich auch im Interesse des Unternehmens. Mitzuteilen sind nach dem Katalog des Art. 15 Abs. 1 DS-GVO darüber hinaus konkret bezogen auf die betroffene Person die Verarbeitungszwecke, die Herkunft und Empfänger der Daten, die Speicherdauer bzw. Löschfristen, ggf. die Garantien für Datenübermittlungen in Drittländer, weitere Informationen bei einer automatisierten Entscheidungsfindung sowie Hinweise auf weitere Betroffenenrechte.

Auf Verlangen ist der betroffenen Person auch eine Kopie ihrer Daten zur Verfügung zu stellen (Art. 15 Abs. 3 DS-GVO); dazu können ggf. auch Kopien von Unterlagen gehören, die der Verantwortliche aufbewahrt, insbesondere wenn diese Unterlagen dazu dienen können, die Rechtmäßigkeit der Datenerhebung zu überprüfen. Dies können zum Beispiel auch in Dateisystemen aufgenommene Schreiben oder Gesprächsvermerke sein, in denen der Verantwortliche persönliche Merkmale der betroffenen Person festgehalten hat (z. B. Meinungen,

Motive, Wünsche, Überzeugungen und Werturteile, finanzielle Verhältnisse, Beziehungen der betroffenen Person zu Dritten und ihrer Umwelt). Neben der Auskunft selbst ist auch die erste Datenkopie unentgeltlich zu übermitteln.

Weitere Informationen sind dem Kurzpapier Nr. 6 der Datenschutzkonferenz zu entnehmen, abrufbar unter https://lsaurl.de/Kurzpapiere. Ein Muster für eine Auskunftserteilung befindet sich unter https://lsaurl.de/MusterAuskunft.

Recht auf Widerruf der Einwilligung

Beruht die Datenverarbeitung auf einer Einwilligung der Betroffenen (z. B. bei Werbung per E-Mail oder Telefon), können die Betroffenen diese Einwilligung jederzeit widerrufen. Auf dieses Recht muss der Verantwortliche vor Abgabe der Einwilligung hingewiesen haben. Ab dem Zeitpunkt des Widerrufs muss der Verantwortliche diese Datenverarbeitung unterlassen, wenn keine andere Rechtsgrundlage dafür erfüllt ist, Art. 7 Abs. 3 DS-GVO. Durch den Widerruf wird die Verarbeitung personenbezogener Daten vor dessen Einlegung nicht berührt.

Recht auf Widerspruch

Nach Art. 21 Abs. 1 DS-GVO steht den Betroffenen ein Widerspruchsrecht bei Verarbeitungen auf Grundlage von Art. 6 Abs. 1 Satz 1 lit. e und f DS-GVO (siehe Kapitel 5) zu. Hier muss die betroffene Person Gründe vortragen, die sich aus ihrer besonderen Situation ergeben, die gegen die weitere Verarbeitung sprechen. Der Verantwortliche kann sodann prüfen, ob er eigene zwingende schutzwürdige Gründe für die weitere Verarbeitung nachweisen kann oder ob die Verarbeitung der Verteidigung von Rechtsansprüchen dient. Ist beides nicht der Fall, darf er die Daten nicht weiterverarbeiten.

Auch auf dieses Recht muss der Verantwortliche ausdrücklich hingewiesen haben (Art. 21 Abs. 4 DS-GVO).

Nach einem Widerspruch gegen Verarbeitungen zu Werbezwecken muss der Verantwortliche unverzüglich dafür Sorge tragen, dass weitere Verarbeitungen dieser Art unterbleiben (Art. 21 Abs. 2 DS-GVO; Näheres siehe Kapitel 12).

Recht auf Berichtigung

Macht eine betroffene Person geltend, dass ihre Daten bei einem Verantwortlichen unrichtig oder unvollständig sind, sind diese zu berichtigen (Art. 16 DS-GVO). Der Verantwortliche hat grundsätzlich alle Empfänger, denen die personenbezogenen Daten offengelegt wurden, über die Berichtigung zu informieren (Art. 19 DS-GVO).

Recht auf Löschung

Unter bestimmten Voraussetzungen haben Betroffene auch einen Anspruch darauf, dass der Verantwortliche ihre Daten löscht. Dies ist zum Beispiel der Fall, wenn diese nicht mehr für die Erfüllung der Geschäftszwecke des Verantwortlichen benötigt werden, wenn die Verarbeitung auf einer Einwilligung beruht und die betroffene Person diese widerrufen hat, wenn die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat und keine vorrangigen berechtigte Gründe des Verantwortlichen für eine weitere Verarbeitung vorliegen oder wenn die Daten unrechtmäßig verarbeitet wurden, (Art. 17 Abs. 1 DS-GVO).

Das Recht auf Löschung besteht u. a. nicht, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen erforderlich ist (z. B. weil handels- und steuerrechtliche Aufbewahrungspflichten bestehen, etwa für Geschäfts-/Handelsbriefe oder Buchungsbelege) oder der Verantwortliche die Daten (weiterhin) zur Verteidigung von Rechtsansprüchen benötigt, (Art. 17 Abs. 3 DS-GVO).

Der Verantwortliche hat grundsätzlich alle Empfänger, denen die personenbezogenen Daten offengelegt wurden, über die Löschung zu informieren (Art. 19 DS-GVO).

Weitere Informationen sind dem Kurzpapier Nr. 11 der Datenschutzkonferenz zu entnehmen, abrufbar unter https://lsaurl.de/Kurzpapiere.

Recht auf Einschränkung der Verarbeitung

Unter bestimmten Voraussetzungen haben Betroffene einen Anspruch darauf, dass die Verarbeitung ihrer Daten eingeschränkt wird. Dies ist zum Beispiel der Fall, wenn die betroffene Person dies anstatt einer Löschung verlangt oder solange noch geprüft wird, ob Daten unrichtig sind oder ob ein Widerspruch nach Art. 21 Abs. 1 DS-GVO

durchgreift (Art. 18 Abs. 1 DS-GVO). Wurde die Verarbeitung eingeschränkt, dürfen diese Daten nur mit Einwilligung der betroffenen Person, zur Verteidigung von Rechtsansprüchen, zum Schutz der Rechte einer anderen Person oder aus Gründen eines wichtigen öffentlichen Interesses verarbeitet werden (Art. 18 Abs. 2 DS-GVO).

Der Verantwortliche hat grundsätzlich alle Empfänger, denen die personenbezogenen Daten offengelegt wurden, über die Einschränkung der Verarbeitung zu informieren (Art. 19 DS-GVO).

Recht auf Datenübertragbarkeit

Beruht eine automatisierte Datenverarbeitung auf einer Einwilligung oder auf einem Vertrag zwischen dem Verantwortlichen und der betroffenen Person, hat die betroffene Person das Recht, die Daten, die sie selbst bereitgestellt hat, von dem Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder direkt an einen anderen Verantwortlichen übermitteln zu lassen (Art. 20 Abs. 1 und 2 DS-GVO).

Es empfiehlt sich, dass Verantwortliche, die derartige Datenverarbeitungen durchführen, frühzeitig, ggf. bereits bei der Konzeption der Datenverarbeitungssysteme, dafür Sorge tragen, dass der Export der Daten in ein strukturiertes, gängiges und maschinenlesbares Format sowie eine sichere elektronische Datenübermittlung (z. B. eine Ende-zu-Ende-verschlüsselte E-Mail) möglich ist.

Details hierzu hat die Artikel-29-Gruppe in ihren Leitlinien WP 242 rev. 01 dargestellt, die der Europäische Datenschutzausschuss bestätigt hat, abrufbar unter https://lsaurl.de/LeitlinienDatenübertragbarkeit.

Rechte bei automatisierten Entscheidungen im Einzelfall einschließlich Profiling

Die betroffene Person hat das Recht, nicht einer Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wenn diese Entscheidung ausschließlich auf einer automatisierten Verarbeitung beruht, also ohne jegliches menschliche Eingreifen (Art. 22 Abs. 1 DS-GVO, ErwGr 71 DS-GVO). Anwendungsfälle können z. B. vollautomatisierte Entscheidungen über Kredit- bzw. Versicherungsanträge oder Bewerbungen sein.

Sie sind ausnahmsweise nur dann zulässig, wenn es eine spezielle Rechtsvorschrift dafür gibt (z. B. § 37 BDSG für die Leistungserbringung nach einem Versicherungsvertrag), wenn die Entscheidung für einen Vertragsabschluss erforderlich ist oder die betroffene Person ausdrücklich eingewilligt hat. In den beiden letztgenannten Fällen muss der Verantwortliche der betroffenen Person mindestens das Recht einräumen, das Eingreifen einer Person in die Entscheidung zu erwirken, den eigenen Standpunkt darzulegen und die Entscheidung anzufechten (Art. 22 Abs. 3 DS-GVO).

Details hierzu hat die Artikel-29-Gruppe in ihren Leitlinien WP 251 rev. 01 dargestellt, die der Europäische Datenschutzausschuss bestätigt hat, abrufbar unter https://datenschutzkonferenz-online.de/edsa.html.

Recht auf Beschwerde bei einer Datenschutzaufsichtsbehörde

Nimmt eine betroffene Person an, dass eine Verarbeitung ihrer Daten gegen die DS-GVO verstößt, kann sie sich an die Datenschutzaufsichtsbehörde ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes wenden (Art. 77 DS-GVO). Die Datenschutzaufsichtsbehörde geht Beschwerden von Betroffenen nach. Hat ein Verantwortlicher die Betroffenenrechte tatsächlich nicht oder nicht vollständig erfüllt, wirkt die Aufsichtsbehörde im Rahmen ihrer Befugnisse (vgl. Art. 57, 58 DS-GVO) darauf hin, dass der Verantwortliche die noch ausstehenden notwendigen Maßnahmen ergreift (z. B. die vollständige Auskunft erteilt). Verstöße, wozu auch nicht fristgerechte Handlungen der Verantwortlichen gehören, können auch mit einer Geldbuße geahndet werden (Art. 83 Abs. 4 lit. a, Abs. 5 lit. a und b DS-GVO).

Recht auf einen wirksamen gerichtlichen Rechtsbehelf

Ist eine betroffene Person der Ansicht, dass eine Verarbeitung gegen die DS-GVO verstößt und infolgedessen die ihr aufgrund der DS-GVO zustehenden Rechte verletzt wurden, hat sie das Recht auf einen wirksamen gerichtlichen Rechtsbehelf (Art. 79 Abs. 1 DS-GVO). Dieses

Recht steht neben dem Recht auf Beschwerde bei einer Aufsichtsbehörde nach Art. 77 DS-GVO und neben einem eventuellen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelf. In Deutschland können die Betroffenen diesbezüglich die Zivilgerichte anrufen.

Recht auf Schadensersatz

Jeder Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Dieser Anspruch entfällt, wenn der Verantwortliche oder Auftragsverarbeiter nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist (Art. 82 DS-GVO).

7 Sicherheit der Verarbeitung – technische und organisatorische Maßnahmen

Grundlagen

Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine angemessene Sicherheit gewährleistet ist. Die Sicherheit der Verarbeitung gehört zu den Grundsätzen der Datenverarbeitung (Art. 5 Abs. 1 lit. f DS-GVO). Die Sicherheit der Verarbeitung verlangt Schutzmaßnahmen, die Verantwortliche ergreifen müssen, um eine unbefugte oder unerwünschte Einsichtnahme, Offenlegung, Weitergabe, Manipulation oder Zerstörung in ihrer Obhut befindlicher personenbezogenen Daten zu unterbinden. Nach Art. 32 DS-GVO sind für eine Verarbeitung personenbezogener Daten Verantwortliche – und auch von ihnen eingeschaltete Auftragsverarbeiter – verpflichtet, ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten.

Dies soll erreicht werden, indem geeignete technische und organisatorische Maßnahmen getroffen werden. Diese Maßnahmen werden zwar auch unter Berücksichtigung des Stands der Technik und der Implementierungskosten festgelegt. Vor allem richten sich die zu treffenden Maßnahmen jedoch nach Art und Umfang der Datenverarbeitung sowie deren Umstände und Zwecken. Schließlich bestimmt das

Risiko für die Rechte und Freiheiten der Betroffenen maßgeblich die Intensität und den Umfang der Maßnahmen.

Was ist ein Risiko?

Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden für natürliche Personen darstellt oder zu einem Schaden für natürliche Personen führen kann. Die Höhe eines Risikos bestimmt sich aus der Schwere des zu erwartenden Schadens bzw. der möglichen Folgeschäden und der Eintrittswahrscheinlichkeit eines schadhaften Ereignisses (siehe Kurzpapier Nr. 18 der Datenschutzkonferenz, https://lsaurl.de/Kurzpapiere).

Wann ist ein Schaden anzunehmen?

Mögliche Schäden können physischer, materieller und immaterieller Natur sein. Schäden liegen z. B. insbesondere vor, wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen wirtschaftlichen oder gesellschaftlichen Nachteilen führt. Ein Schaden kann schon dann entstanden sein, wenn die betroffene Person daran gehindert wird, die sie betreffenden personenbezogenen Daten zu kontrollieren.

Der zu erwartende Schaden steht im Zusammenhang mit der Menge, dem Umfang und der Sensibilität der Daten. Werden z. B. Daten von vielen Betroffenen unbefugt offengelegt, steigt die Wahrscheinlichkeit, dass eine Person dabei ist, die dadurch eine Schädigung erleidet. Werden von wenigen Personen sehr detaillierte Daten in großem Umfang unbefugt offengelegt, steigt das Ausmaß des Schadens, den eine einzelne Person dadurch erleiden könnte. Gleiches gilt, wenn nur wenige Daten von einzelnen Personen unbefugt offengelegt werden, die allerdings sehr sensibel oder brisant sind, insbesondere, wenn es sich dabei um besondere Kategorien personenbezogener Daten, z. B. Gesundheitsdaten (siehe dazu auch Kapitel 14), handelt.

Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit für ein schadhaftes Ereignis bestimmt sich danach, wie stark die Daten einer Bedrohung ausgesetzt sind. Eine Bedrohung ist ein Szenario, in welchem die Daten während der vorgesehenen Verarbeitung kompromittiert werden könnten, z. B. indem die Daten zerstört werden, verloren gehen, entwendet werden, einer Zweckänderung unterliegen, veröffentlich werden, unbefugt eingesehen oder unbefugt verändert werden. Daten können zum einen durch die Art, wie sie verarbeitet werden, einer Bedrohung ausgesetzt sein. Sie können aber auch durch die ihnen innewohnenden Eigenschaften besonders bedroht sein. So kann eine größere Bedrohung bestehen, wenn Daten z. B. außerhalb der Handlungssphäre des Betroffenen von mehreren Verantwortlichen und/oder Verarbeitern elektronisch verarbeitet werden, wie es in komplexen Cloudumgebungen üblich ist, bei denen mehrere Ebenen von Unterauftragnehmern und Datentransfers in Drittländer bestehen, die dem Betroffenen nicht bekannt sind. Auch kann eine größere Bedrohung daraus resultieren, dass z. B. Dritte ein potentielles Interesse an der Offenlegung der Daten haben können, wie es z. B. bei Daten zu persönlichen Verhältnissen von Personen der öffentlichen Wahrnehmung der Fall sein kann.

Risikoabschätzung

Da das Schutzniveau der Verarbeitung dem Risiko angemessen sein muss, gilt es, Letzteres abzuschätzen. Wie oben dargestellt, spielen hinsichtlich der Schädigung einer Person durch Offenlegung Ihrer Daten die Eintrittswahrscheinlichkeit und das Schadensausmaß die wesentlichen Rollen. Beide Faktoren können für sich das Gesamtrisiko erhöhen und eine angemessene Reaktion durch erhöhte Sicherheitsmaßnahmen erfordern. Dabei lässt sich das Schadensausmaß meist über eine gewissenhafte Einhaltung der Grundsätze der Verarbeitung klein halten, denn die Nichtbeachtung von Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Zweckbindung, Datenminimierung, Richtigkeit und Speicherbegrenzung kann ein höheres Schadensausmaß begünstigen.

Maßnahmen

Hauptsächlich gilt es jedoch, die Eintrittswahrscheinlichkeit eines schadhaften Ereignisses zu minimieren, indem ausreichend technische Maßnahmen umgesetzt und organisatorische Vorgaben etabliert werden, so dass eine Datenverarbeitung möglichst wenigen konkreten Bedrohungen ausgesetzt ist. Zu diesen Maßnahmen gehören u. a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sowie die Wiederherstellung der Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen nach einem technischen Zwischenfall. Außerdem muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen etabliert werden.

Vertraulichkeit

Vertraulichkeit ist hinreichend gewährleistet, wenn Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können und die Daten außerdem vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust geschützt sind. Dies kann durch Beschränkung des physischen Zutritts zu den Datenverarbeitungsanlagen und Datenspeichern (z. B. Betrieb von Alarmanlagen, Verwendung von Sicherheitsschlössern, Durchführung von Ausweis- und Personenkontrollen), durch Einschränkung des Zugangs zu Datenverarbeitungsanwendungen und -plattformen (z. B. Anmeldung durch individuelles Benutzerkonto, sichere Passwortvergabe, sichere Datenträgervernichtung) und durch Begrenzung des Zugriffs auf die Daten selbst (z. B. differenzierte Rollen- und Rechtevergabe, Datenträgerverschlüsselung, verschlüsselte Datenübertragung) erfolgen.

Integrität

Integrität ist gewährleistet, wenn Daten vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt sind, die Daten also vollständig, unverändert und unversehrt sind und bleiben. Dies kann zum einen durch kryptografische Verfahren, aber auch durch organisatorische Maßnahmen und Zugriffsab-

wehr umgesetzt werden (z. B. Einsatz von Signaturverfahren, Überwachung von Wartungsaktivitäten, Betrieb von Virenschutzlösungen, Einsatz von Firewalls).

Verfügbarkeit

Verfügbarkeit ist gewährleistet, wenn die Daten ihrem Zwecke nach jederzeit nutzbar sind. Zusätzlich muss die Fähigkeit existieren, die Verfügbarkeit und den Zugang zu den Daten bei einem physischen oder technischen Zwischenfall rasch wiederherstellen zu können (z. B. Einrichten von Datenspiegelungen, regelmäßiges Anfertigen und sichere Aufbewahrung von Datensicherungen, Vorhalten von Notfallplänen).

Belastbarkeit

Belastbarkeit (auch Resilienz) bezeichnet allgemein die Fähigkeit, beim Auftreten von Störungen oder außergewöhnlichen Belastungen die angeforderte Betriebsleistung aufrechtzuerhalten, so dass auch in Zeiten von Spitzenauslastungen oder bei unplanmäßigem Fehlverhalten kein Systemausfall befürchtet werden muss. Die hinreichende Belastbarkeit der an der Verarbeitung personenbezogener Daten beteiligten Systeme und Dienste muss dauerhaft sichergestellt sein (z. B. redundanter Betrieb von IT-Ressourcen, Schutzmaßnahmen gegen Stromausfall und Überhitzung, Auslagerung von IT-Ressourcen zu Dienstleistern, die Lastausgleich und Ressourcenskalierung anbieten).

Rechenschaftspflicht und Wirksamkeitsnachweis

Die Rechenschaftspflicht ist in Bezug auf die Sicherheit der Verarbeitung erfüllt, wenn nachgewiesen werden kann, dass angemessene Sicherheitsmaßnahmen durchgeführt wurden. Der Verantwortliche muss die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung regelmäßig überprüfen und bewerten. Außerdem muss er sofort feststellen können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, um die Aufsichtsbehörde und die betroffenen Personen umgehend unterrichten zu können (z. B. Dokumentation der vor-

handenen IT-Infrastruktur, Dokumentation getroffener Sicherheitsmaßnahmen, System- und Anwendungsprotokollierung, stichprobenartige Überprüfung der Wirksamkeit von Maßnahmen).

Zur Dokumentation getroffener Sicherheitsmaßnahmen kann die Checkliste technischer und organisatorischer Maßnahmen genutzt werden, abrufbar unter https://lsaurl.de/checktom.

Detaillierte Hinweise zur Sicherheit bei der Übermittlung personenbezogener Daten im E-Mailverkehr enthält die Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“, abrufbar unter https://lsaurl.de/OHEMail.

Wie Videokonferenzsysteme sicher genutzt werden können, ergibt sich aus der „Orientierungshilfe Videokonferenzsysteme“, abrufbar unter https://lsaurl.de/OHVideokonferenz.

8 Verzeichnis der Verarbeitungstätigkeiten

Art. 30 Abs. 1 und 2 DS-GVO legen fest, dass Verantwortliche und Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten führen müssen. Zwar enthält Art. 30 Abs. 5 DS-GVO Ausnahmen von dieser Verpflichtung, diese greifen jedoch nur, wenn personenbezogene Daten nur gelegentlich, d. h. nicht regelmäßig verarbeitet werden. Da aber wohl in nahezu jedem Unternehmen z. B. Kunden- oder Beschäftigtendaten ständig gespeichert werden, müssen diese Unternehmen das Verzeichnis von Verarbeitungstätigkeiten führen.

Es ist schon im eigenen Interesse des Unternehmens ratsam, ein vollständiges Verzeichnis von Verarbeitungstätigkeiten zu erstellen. Das Verzeichnis dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft dabei, gem. Art. 5 Abs. 2 DS-GVO nachzuweisen, dass die Vorgaben aus der DS-GVO eingehalten werden (Rechenschaftspflicht). Die Datenschutzaufsichtsbehörden lassen sich das Verzeichnis regelmäßig zu Beginn von Prüfungen nach Art. 30 Abs. 4 DS-GVO vorlegen.

In dem Verzeichnis müssen sämtliche ganz oder teilweise automatisierte Verarbeitungen personenbezogener Daten sowie Verarbeitungen personenbezogener Daten beschrieben werden, die in einem Da-

teisystem (z. B. einer geordneten Akte) gespeichert sind oder gespeichert werden sollen. Dabei sollten Beschreibungen, die den gleichen Zwecken dienen, die gleichen oder ähnliche Datenarten umfassen und auf der gleichen Rechtsgrundlage beruhen, zusammengefasst werden.

Anknüpfungspunkt des Verzeichnisses ist die Verarbeitung bzw. die Verarbeitungstätigkeit. Die einzelnen Verarbeitungstätigkeiten personenbezogener Daten des Unternehmens sollen in dem Verzeichnis nachvollzogen werden können. In KMU kommen als Verarbeitungstätigkeiten, die separat in dem Verzeichnis ausgewiesen werden sollten, z. B. folgende in Betracht:

- Kundendatenverwaltung
- Marketing
- Beschaffung/Einkauf
- Finanzbuchhaltung
- Personalverwaltung
- Lohnbuchhaltung
- Bewerbungsverfahren
- Arbeitszeiterfassung
- Videoüberwachung

Das Verzeichnis des Verantwortlichen (Art. 30 Abs. 1 DS-GVO) muss folgende Angaben beinhalten:

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls gemeinsam Verantwortlichen sowie des etwaigen Datenschutzbeauftragten;
- die Zwecke der Verarbeitung z. B. „Personalaktenführung/Stammdaten“, „Lohnabrechnung“ oder „Arbeitszeiterfassung“ für die Verarbeitungen der Beschäftigtendaten; „Beschaffung/Einkauf“ für die Verarbeitung von Lieferantendaten; „Feststellung von Diebstählen“ bei der Videoüberwachung des Warenlagers;
- die Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten z. B. für die Kategorie Beschäftigte: Adressdaten, Geburtsdatum, Bankverbindung, Steuermerkmale, Lohngruppe, Qualifikationen; z. B. für die Kategorie Kunden: Kontaktdaten, Zahlungsdaten, Bonitätsdaten;

- Kategorien von Empfängern z. B. Banken, Sozialversicherungsträger, Finanzämter, Träger der Betriebsrente … für das Verzeichnis „Lohnabrechnung“;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlandes oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien z. B. bei der Nutzung von Cloudprodukten, bei denen die Speicherung von personenbezogenen Daten außerhalb der Europäischen Union stattfindet (hier muss die Zulässigkeit der Datenübermittlung in das Drittland gesondert nach Art. 44 ff. DS-GVO geprüft werden);
- die Angaben der vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien z. B. nach den geltenden handels- und steuerrechtlichen Aufbewahrungspflichten für Personal- und Kundendaten und durch den Verantwortlichen festgelegte Löschfristen.

Das Verzeichnis beim Auftragsverarbeiter (Art. 30 Abs. 2 DS-GVO) muss folgende Angaben enthalten:

- die Namen und Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie des etwaigen Datenschutzbeauftragten;
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlandes oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien.

Beide Verzeichnisse erfordern – wenn möglich – eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DS-GVO. Die Möglichkeit einer solchen Beschreibung sollte in nahezu allen Fällen bestehen.

Das Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann (Art. 30 Abs. 3 DS-GVO).

Vordrucke für das Verzeichnis von Verarbeitungstätigkeiten für den Verantwortlichen und den Auftragsverarbeiter und weitere Erläuterungen befinden sich auf der Homepage des Landesbeauftragten unter https://lsaurl.de/VerzVerarb. Die jeweiligen ersten Seiten der Vordrucke brauchen für ein Unternehmen nur einmal ausgefüllt werden. Die folgenden beiden Seiten sind für die jeweilige Verarbeitungstätigkeit (z. B. Personalaktenführung, Beschaffung/Einkauf) gesondert auszufüllen. Weitere Hinweise zum Führen des Verzeichnisses befinden sich unter https://lsaurl.de/VerzVerarb.

Zur Dokumentation der technischen und organisatorischen Maßnahmen kann die Checkliste des Landesbeauftragten genutzt werden, abrufbar unter https://lsaurl.de/checktom.

Entwerfen sollte das Verzeichnis der Bereich, der die Verarbeitung durchführt, z. B. die Personalstelle für die Verarbeitungen, die dort stattfinden. Die durchzuführenden technischen und organisatorischen Maßnahmen sollten vom IT-Bereich dokumentiert werden. Die Entscheidung, wie dieses Verzeichnis zu führen ist, sollte aber letztlich durch die Unternehmensleitung erfolgen.

9 Der betriebliche Datenschutzbeauftragte

Der betriebliche Datenschutzbeauftragte ist ein wesentlicher Faktor zur Selbstregulierung des Datenschutzes im Unternehmen. Er ist eine interne Beratungs- und Kontrollinstanz, die die Unternehmensleitung bei der Einhaltung datenschutzrechtlicher Vorschriften unterstützen soll und damit zur Vermeidung von Unternehmensrisiken beiträgt.

Wann kann/muss ein Datenschutzbeauftragter benannt werden?

Jedes Unternehmen kann freiwillig einen Datenschutzbeauftragten benennen (Art. 37 Abs. 4 Satz 1 DS-GVO).

Verpflichtend ist die Benennung eines Datenschutzbeauftragten

- nach § 38 Abs. 1 BDSG

1. soweit in der Regel mindestens zwanzig Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind;
   Als Beschäftigte Personen zählen alle Arbeitnehmer (Voll- oder Teilzeitbeschäftigte gleichermaßen), freie Mitarbeiter, Leiharbeitnehmer, Auszubildende. Eine ständige Beschäftigung ist schon dann gegeben, wenn ein Mitarbeiter eine konkrete Aufgabe übertragen bekommen hat, deren Erledigung er sich aber nur in bestimmten Zeitabständen (z. B. einmal wöchentlich) widmen muss.
2. oder wenn Verantwortliche oder Auftragsverarbeiter einer Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DS-GVO unterliegen;
   Eine DSFA ist nur bei einem hohen Risiko erforderlich, welches z. B. bei ungeprüfter neuartiger Software angenommen werden könnte.
3. oder eine geschäftsmäßige Verarbeitung personenbezogener Daten zum Zwecke der Übermittlung, der Markt- oder Meinungsforschung stattfindet
   Unternehmen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung verarbeiten, sind z. B. Auskunfteien, Detekteien und Freizeit- oder Partnerbörsen, die z. B. Kontakt- und Interessendaten an Kunden übermitteln.

- nach Art. 37 Abs. 1 DS-GVO
  1. wenn ein Unternehmen als „Behörde“ personenbezogene Daten verarbeitet;
     Dies ist z. B. dann der Fall, wenn ein Unternehmen auf einer öffentlich-rechtlichen Grundlage mit der Wahrnehmung einer öffentlichen Aufgabe beliehen wurde. Dies trifft unter anderem auf bevollmächtigte Bezirksschornsteinfeger und Kfz-Werkstätten zu, die mit der Aufgabe der Abgasuntersuchung beliehen wurden.
  2. wenn die Kerntätigkeit aus Verarbeitungen besteht, die umfangreiche und systematische Überwachung erfordern;
     Z. B. bei verhaltensbasierter Werbung, Treueprogrammen, Überwachung von Fitness- und Gesundheitsdaten, Sicherheitsunternehmen.

3. wenn die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien nach Art. 9 DS-GVO besteht (inkl. Gesundheitsdaten);
   Eine umfangreiche Verarbeitung liegt noch nicht vor, wenn die Verarbeitung personenbezogener Daten von Patienten oder Mandanten und durch einen einzelnen Arzt oder sonstigen Angehörigen eines Gesundheitsberufs oder Rechtsanwalt erfolgt, ErwGr 91 DS-GVO am Ende.

   Die Verarbeitung personenbezogener Daten ist eine Kerntätigkeit, wenn sie einen untrennbaren Bestandteil der Tätigkeit des Verantwortlichen darstellt (z. B. Krankenhaus verarbeitet Gesundheitsdaten als Kerntätigkeit). Die Kerntätigkeit muss insoweit nicht das eigentliche Unternehmensziel (bei Krankenhäusern: Behandlung der Patienten) darstellen.

Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen (z. B. auf der Homepage des Unternehmens) und der zuständigen Aufsichtsbehörde mitzuteilen. Ein Online-Formular für die Mitteilung an die Aufsichtsbehörde befindet sich hier: https://datenschutz.sachsen-anhalt.de/service/online-formulare/.

Um für kleinere Betriebe den mit der Benennung zusammenhängenden finanziellen und organisatorischen Aufwand zu begrenzen, könnte es sich empfehlen, dass mehrere gleichartige Unternehmen denselben Datenschutzbeauftragten benennen.

Berufliche Qualifikation und Fachwissen

Voraussetzung für eine Benennung als Datenschutzbeauftragter ist, dass er aufgrund seiner Ausbildung, seines Fachwissens und seiner Berufserfahrung in der Lage ist, seine Aufgaben zu erfüllen. Dies erfordert Kenntnisse im Datenschutzrecht sowie hinsichtlich der geforderten technischen und organisatorischen Maßnahmen. Zudem muss er über die Verarbeitung personenbezogener Daten im Betrieb informiert sein. In größeren Betrieben gehört sicherlich auch die Fähigkeit dazu, koordinieren bzw. Managementaufgaben erledigen zu können. Benannt werden kann ein geeigneter Mitarbeiter des Unternehmens („interner Datenschutzbeauftragter“) oder jemand, der aufgrund eines Dienstleistungsvertrages die Aufgaben übernimmt („externer Datenschutzbeauftragter“).

Form der Benennung

Besondere Formvorschriften gibt es nicht. Aus Beweisgründen und Gründen der Rechtssicherheit empfiehlt sich eine schriftliche Benennung. Ein Muster für eine Benennung finden Sie unter https://lsaurl.de/MusterBenennung.

Stellung des Datenschutzbeauftragten, Art. 38 DS-GVO

Der Datenschutzbeauftragte ist frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden. Die Unternehmensleitung hat ihn bei seiner Aufgabenwahrnehmung zu unterstützen, indem sie erforderliche Ressourcen (Sachmittel, ggf. Personal) zur Verfügung stellt und Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen gewährt. Der Datenschutzbeauftragte ist bezüglich der Ausübung seiner Aufgaben weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Er berichtet unmittelbar der Unternehmensleitung.

Der Datenschutzbeauftragte ist bei der Erfüllung seiner Aufgaben zur Wahrung der Geheimhaltung und Vertraulichkeit verpflichtet und kann sich auf das Zeugnisverweigerungsrecht berufen (§ 6 Abs. 6 BDSG). Der Datenschutzbeauftragte kann auch andere Aufgaben und Pflichten wahrnehmen. Es ist allerdings sicherzustellen, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

Aufgaben des Datenschutzbeauftragten, Art. 39 DS-GVO

Der Datenschutzbeauftragte hat zumindest folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;
- Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für

den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
- Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gem. Art. 35 DS-GVO;
- Zusammenarbeit mit der Aufsichtsbehörde;
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gem. Art. 36 DS-GVO, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Die Aufsichtsbehörden werden sich bei vielen Fragen nicht an die Geschäftsleitung, sondern direkt an den betrieblichen Datenschutzbeauftragten wenden.

Link zur Vertiefung: Leitlinien in Bezug auf Datenschutzbeauftragte der Art.-29-Datenschutzgruppe: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

10 Meldungen von Datenschutzverletzungen und Benachrichtigung an die betroffenen Personen

Eine meldepflichtige Verletzung des Schutzes personenbezogener Daten ist nach Art. 4 Nr. 12 DS-GVO „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.“ Es reicht damit bereits eine Verletzung der Sicherheit aus. Der Eintritt eines Schadens ist nicht erforderlich.

Datenschutzverletzungen liegen regelmäßig vor, wenn Unberechtigte Kenntnis von personenbezogenen Daten erlangen oder zumindest die naheliegende Möglichkeit der Kenntnisnahme besteht. Dies kann z. B. durch den Versand von Briefen oder unverschlüsselten E-Mails an

nichtbeabsichtigte Empfänger geschehen. Auch abhanden gekommene unverschlüsselte Datenträger führen zu Datenschutzverletzungen, selbst wenn es noch keine konkreten Hinweise für eine unberechtigte Kenntnisnahme gibt. Ebenfalls stellt der Verlust der Verfügbarkeit personenbezogener Daten – z. B. durch die Verschlüsselung der Daten im Rahmen eines Cyberangriffs mittels Ransomware – regelmäßig eine Datenschutzverletzung dar, sofern kein aktuelles Backup vorhanden ist.

Die Verletzung des Schutzes personenbezogener Daten kann einen physischen, materiellen oder immateriellen Schaden für betroffene Personen nach sich ziehen. Möglich ist z. B. der Verlust der Kontrolle über die Daten, eine Diskriminierung, ein Identitätsdiebstahl oder -betrug, finanzielle Verluste, Rufschädigung oder weitere erhebliche wirtschaftliche oder gesellschaftliche Nachteile, vgl. ErwGr 85 DS-GVO. Um Folgeschäden zu vermeiden bzw. zu minimieren und Transparenz gegenüber den betroffenen Personen zu schaffen, müssen in den in Art. 33 und 34 DS-GVO benannten Fällen Meldungen an die Aufsichtsbehörde und Benachrichtigungen an die betroffenen Personen erfolgen.

Meldung an die Aufsichtsbehörde, Art. 33 DS-GVO

Die Meldung an die für das Unternehmen zuständige Aufsichtsbehörde hat im Falle einer Verletzung des Schutzes personenbezogener Daten der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, zu erfolgen. Erfolgt die Meldung an die Aufsichtsbehörde erst nach Ablauf von 72 Stunden, so ist der Meldung eine Begründung für die Verzögerung beizufügen, Art. 33 Abs. 1 DS-GVO. Der Auftragsverarbeiter hat eine bei ihm bekannt gewordene Verletzung unverzüglich an den Verantwortlichen zu melden, Art. 33 Abs. 2 DS-GVO.

Die Meldepflicht entfällt nach Art. 33 Abs. 1 Satz 1, 2. Halbsatz DS-GVO lediglich dann, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Das verantwortliche Unternehmen muss also eine Risikoprognose vornehmen. Das Risiko hat zwei Dimensionen. Erstens: die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass ein Schaden eintritt. Je höher der mögliche Schaden ist, desto geringer kann

die Eintrittswahrscheinlichkeit sein, um eine Risikoschwelle zu erreichen. Da es keine vollständig risikolose Verarbeitung gibt, wird die Formulierung „nicht zu einem Risiko“ von ihrem Zweck ausgehend als „nur zu einem sehr geringen Risiko führend“ verstanden. Besteht aufgrund der Verletzung also nur ein sehr geringes Risiko, ist die Meldung an die Aufsichtsbehörde entbehrlich. Ein solches, sehr geringes Risiko liegt z. B. vor, wenn ein fehlversandter verschlossener Brief im verschlossenen Zustand zurückgeholt wird oder ein nach dem Stand der Technik verschlüsselter Datenträger abhandengekommen ist. Zur Ermittlung des Risikos kann das Kurzpapier Nr. 18 der Datenschutzkonferenz, abrufbar unter https://lsaurl.de/Kurzpapiere, genutzt werden.

In Zweifelsfällen sollte eine Meldung erfolgen. Das Risiko, dass sich ein Unternehmen durch die Meldung an die Aufsichtsbehörde oder die Benachrichtigung der betroffenen Personen der Gefahr eines Bußgeldverfahrens aussetzt, besteht insoweit nicht, als die Meldung an die Aufsichtsbehörde und Benachrichtigung an die betroffene Person (siehe unten) in einem Bußgeldverfahren nur mit Zustimmung des Meldepflichtigen verwendet werden dürfen, § 40 Abs. 4 BDSG.

Die Meldung an die Aufsichtsbehörde enthält nach Art. 33 Abs. 3 DS-GVO zumindest folgende Informationen:

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

Soweit nicht zeitgleich alle genannten Informationen zur Verfügung gestellt werden können, z. B. weil die Aufklärung des Sachverhalts noch anhält, können die Informationen auch schrittweise bereitgestellt werden. Bereits bekannte Informationen müssen aber unverzüglich erfolgen.

Der Landesbeauftragte hat auf seiner Homepage ein Online-Formular für die Meldung von Datenschutzverletzungen bereitgestellt. Dieses Formular ist unter https://lsaurl.de/DSVerletzung abrufbar und wird verschlüsselt an den Landesbeauftragten versandt. Dieser wird anhand der Meldung prüfen, ob sein Einschreiten geboten ist. Oft werden Hinweise zu Maßnahmen zur Schadensbegrenzung und zur Abwehr zukünftiger gleichartiger Verletzungen gegeben.

Über die Meldung hinaus ist die Verletzung des Schutzes personenbezogener Daten zu dokumentieren. In der Dokumentation müssen alle im Zusammenhang mit der Verletzung stehenden Fakten, deren Auswirkungen und die ergriffenen Abwehrmaßnahmen enthalten sein. Dazu ist zu untersuchen, welche Schwachstellen zu der Datenschutzverletzung geführt haben, damit diese beseitigt werden können. Die Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen des Art. 33 DS-GVO ermöglichen.

Benachrichtigung der betroffenen Personen, Art. 34 DS-GVO

Wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, so muss das verantwortliche Unternehmen die betroffenen Personen unverzüglich benachrichtigen. Diese Benachrichtigung soll es den betroffenen Personen ermöglichen, nötige Schritte einzuleiten, um sich selbst vor den negativen Folgen der Verletzung zu schützen. Sie hat in klarer und einfacher Sprache

- die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen und

- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten sowie eine Beschreibung der von dem Verantwortlichen anlässlich der Datenschutzverletzung ergriffenen oder vorgeschlagenen Maßnahmen (Art. 34 Abs. 2 DS-GVO)

zu enthalten. Zur Ermittlung des hohen Risikos kann das genannte Kurzpapier Nr. 18 der Datenschutzkonferenz herangezogen werden. Ein hohes Risiko liegt z. B. vor, wenn Daten abgeflossen sind, denen ein hohes Missbrauchsrisiko innewohnt. Solche Daten enthalten z. B. Kopien von Ausweisdokumenten. Auch Zahlungsdaten, die für Identitätsdiebstähle oder Phishing verwendet werden und somit materielle oder immaterielle Schäden auslösen können, bergen ein hohes Missbrauchsrisiko. Ein hohes Risiko liegt auch nahe, wenn besondere Kategorien personenbezogener Daten oder detaillierte Beschäftigtendaten Unberechtigten gegenüber offengelegt wurden. Auch eine abgeflossene Telefonabrechnung führt häufig zu einem hohen Risiko. Deren Nutzung gewährt Aufschluss über das Privatleben und könnte z. B. zu Stalking führen.

Die Benachrichtigung der betroffenen Person ist gem. Art. 34 Abs. 3 DS-GVO nicht erforderlich, wenn

a. der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;
b. der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gem. Abs. 1 aller Wahrscheinlichkeit nach nicht mehr besteht;
c. die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

Aufgrund der Rechenschaftspflicht sollten die verantwortlichen Unternehmen dokumentieren und der Aufsichtsbehörde nachweisen können, dass zumindest eine der vorstehend genannten Bedingungen vorliegt. Im Falle der Nichtbenachrichtigung kann die Aufsichtsbehörde – sofern sie ein voraussichtlich hohes Risiko annimmt – zur Benachrichtigung verpflichten. Der Landesbeauftragte empfiehlt eine Benachrichtigung der betroffenen Personen auch in Situationen, in denen kein hohes Risiko vorliegt, wenn dadurch Risiken minimiert werden können.

Weitergehende Informationen mit zahlreichen Beispielen finden Sie in den Leitlinien des Europäischen Datenschutzausschusses

- für die Meldung von Verletzungen des Schutzes personenbezogener Daten gem. der Verordnung (EU) 2016/679, abrufbar unter https://lsaurl.de/GuidelinesDataBreach und den
- Leitlinien 01/2021 zu Beispielen für Datenpannenmeldungen, abrufbar unter https://lsaurl.de/EDSA12021.

11 Auftragsverarbeitung, gemeinsame Verantwortliche

Viele Unternehmen bedienen sich zur Verarbeitung personenbezogener Daten externer Dienstleister. Dies ist zulässig, soweit die Anforderungen des Datenschutzes eingehalten werden.

Verarbeitet ein Unternehmen personenbezogene Daten im Auftrag des Verantwortlichen, handelt es sich um einen „Auftragsverarbeiter“ (vgl. Art. 4 Nr. 8 DS-GVO). Der Auftragsverarbeiter ist also eine gesonderte Stelle, in der Regel ein eigenständiges Unternehmen. Um eine Auftragsverarbeitung handelt es sich aber nur dann, wenn ein Unternehmen als Verantwortlicher allein die Entscheidung über die Zwecke (z. B. Kundendatenverarbeitung, Werbung) und Mittel (Art und Weise der Verarbeitung, z. B. Versendung von Werbebriefen) der Verarbeitung personenbezogener Daten trifft. Die Entscheidung, welche technischen und organisatorischen Maßnahmen zum Schutz der Daten getroffen werden, kann beim Auftragsverarbeiter liegen.

Fälle, in denen regelmäßig eine Auftragsverarbeitung vorliegt, sind z. B.

- DV-technische Arbeiten für Lohn- und Gehaltsabrechnungen oder Finanzbuchhaltung,
- Auslagerung der E-Mail-Verwaltung oder von Datendiensten zu Webseiten,
- Prüfung oder Wartung (Fernwartung, externer Support) der Datenverarbeitungsanlagen, wenn ein Zugriff auf personenbezogene Daten nicht ausgeschlossen ist,
- Datenträgerentsorgung,
- Cloudcomputing.

Keine Auftragsverarbeitung, sondern eine Inanspruchnahme fremder Fachleistungen liegt bei einem eigenständig Verantwortlichen vor, wenn die Fachleistungen aufgrund eigener Entscheidungen des Fachdienstleisters erfolgen. Dies ist z. B. regelmäßig der Fall bei der Inanspruchnahme von

- Berufsgeheimnisträgern (Steuerberater, Rechtsanwälte, Betriebsärzte),
- Inkassobüros,
- Bankinstitute für den Geldtransfer,
- Postdienstleistungen.

Anforderungen an den Auftragsverarbeiter

Der Verantwortliche darf sich dabei nur solcher Auftragsverarbeiter bedienen, die hinreichende Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz anwenden.

Der Auftragsverarbeiter unterliegt dem Weisungs- und Kontrollrecht des Verantwortlichen. Zudem hat er eigene Pflichten. Dazu zählt u. a., dass er ein Verzeichnis von Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 2 DS-GVO führt und dem Verantwortlichen unverzüglich Datenschutzverletzungen nach Art. 33 DS-GVO meldet.

Bei Verstößen haftet der Auftragsverarbeiter, wenn er seinen Pflichten nicht nachgekommen ist oder wenn er die Anweisungen des Verantwortlichen missachtet bzw. entgegen dieser Anweisungen handelt (Art. 82 Abs. 2 DS-GVO). Auch wenn er die Daten seines Auftraggebers pflichtwidrig für eigene Zwecke verarbeitet, haftet er für Verstöße;

denn nach Art. 28 Abs. 10 DS-GVO gilt er sodann als eigener Verantwortlicher.

Vertragliche Regelungen

Art. 28 Abs. 3 DS-GVO sieht vor, dass die Verarbeitung durch einen Auftragsverarbeiter auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments erfolgt und schriftlich abzufassen ist, was aber auch in einem elektronischen Format erfolgen kann (vgl. Art. 28 Abs. 9 DS-GVO). Der Vertrag bzw. das andere Rechtsinstrument muss

- den Gegenstand und die Dauer der Verarbeitung,
- die Art und den Zweck der Verarbeitung,
- die Art der personenbezogenen Daten,
- die Kategorien betroffener Personen und
- die Pflichten und Rechte des Verantwortlichen

festlegen.

Weiter muss der Vertrag bzw. das andere Rechtsinstrument vorsehen, dass der Auftragsverarbeiter

- personenbezogene Daten auf dokumentierte Weise des Verantwortlichen verarbeitet,
- gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer anderen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DS-GVO),
- alle erforderlichen technischen und organisatorischen Maßnahmen gem. Art. 32 DS-GVO ergreift,
- bei Einsatz eines Unterauftragnehmers Art. 28 Abs. 2 und 4 DS-GVO beachtet (Information des Verantwortlichen, Pflichtenübernahme des Unterauftragnehmers),
- den Verantwortlichen bei der Wahrnehmung der in Kapitel 3 der DS-GVO genannten Rechte der betroffenen Personen (siehe Kapitel 6) und der Einhaltung der in den Art. 32 bis 36 DS-GVO genannten Pflichten unterstützt,
- die für die Nachweispflicht nötigen Unterlagen zur Verfügung stellt und

- Überprüfungen und Inspektionen des Verantwortlichen ermöglicht.

Eine Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO ist auf der Internetseite des Landesbeauftragten abrufbar unter https://lsaurl.de/MusterAV.

Standardvertragsklauseln der Europäischen Union für Verträge über eine Auftragsverarbeitung nach Art. 28 Abs. 7 DS-GVO finden Sie unter https://lsaurl.de/StandardvertragsklauselnArt28. Diese Klauseln enthalten mehrere Optionen. Sie können in Verträgen zwischen einem Verantwortlichen und einem Auftragsverarbeiter, vereinbart werden. Die Kommission prüft die praktische Anwendung dieser Klauseln im Rahmen der nach Art. 97 DS-GVO vorgesehenen Bewertung.

Unterauftragnehmer

Sofern sich der Auftragsverarbeiter eines Unterauftragnehmers als weiteren Auftragsverarbeiter bedient, bedarf dies der vorherigen Genehmigung des Verantwortlichen (vgl. Art. 28 Abs. 2 DS-GVO), die auch in elektronischer Form erfolgen kann.

Sofern eine allgemeine schriftliche Genehmigung zur Inanspruchnahme weiterer Unterauftragnehmer vereinbart wurde, hat der Auftragsverarbeiter über jegliche Änderung entsprechend zu informieren. Denn dem Verantwortlichen steht dabei ein Einspruchsrecht zu (Art. 28 Abs. 2 Satz 2 DS-GVO).

Auftragnehmer im Ausland

Befindet sich der Auftragsverarbeiter außerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraumes (EWR) sind die zusätzlichen Anforderungen des Art. 44 ff. DS-GVO zu beachten. Wichtig ist insbesondere, sicherzustellen, dass das durch die DS-GVO gewährleistete Schutzniveau für natürliche Personen nicht abgesenkt wird.

Weitere Informationen

Weitere Informationen zum Thema Auftragsverarbeitung sind im Kurzpapier Nr. 13 (abrufbar unter https://lsaurl.de/Kurzpapiere) sowie in den vom Europäischen Datenschutzausschuss veröffentlichten

Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Stand 2. September 2020) zu finden. Diese waren bis zum Redaktionsschluss dieses Leitfadens in englischer Form unter https://lsaurl.de/EDSA72020 abrufbar.

Abgrenzung zu gemeinsam Verantwortlichen

Wenn zwei oder mehrere Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, liegt ein Fall einer gemeinsamen Verantwortlichkeit im Sinne des Art. 26 DS-GVO vor. Auch gemeinsam Verantwortliche haben dazu eine Vereinbarung zu treffen. Darin sollen die gemeinsam Verantwortlichen in transparenter Form festgelegen, wer von ihnen welche Verpflichtungen gem. der DS-GVO erfüllt, insbesondere,

- wer für die Wahrnehmung der Rechte der Betroffenen zuständig ist und
- wer welchen Informationspflichten gem. Art. 13, 14 DS-GVO nachkommt.

Außerdem müssen sich darin die tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber den betroffenen Personen widerspiegeln und ggf. kann eine Anlaufstelle für die betroffenen Personen benannt werden.

Eine Formvorschrift sieht die DS-GVO hierzu nicht vor. In Bezug auf die Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) sowie in Haftungsfragen empfiehlt sich jedoch ein bindendes Dokument abzuschließen. Außerdem sieht Art. 26 Abs. 2 Satz 2 DS-GVO vor, dass das Wesentliche der Vereinbarung der betroffenen Person zur Verfügung gestellt wird. Ungeachtet dieser Vereinbarung kann die betroffene Person ihre Rechte im Rahmen der DS-GVO bei und gegenüber jedem der Verantwortlichen geltend machen.

12 Kundendatenschutz inkl. Werbung

Kundendaten sind alle personenbezogenen Daten, die im Rahmen von Geschäftsprozessen von Kunden eines Unternehmens erhoben, gespeichert, genutzt, an Dritte übermittelt oder in anderer Weise weiterverarbeitet werden. Dazu gehören insbesondere Kontaktdaten,

Vertragsdaten, Kundennummern, Bonitäts- und Bankdaten sowie je nach Geschäftsinhalt viele weitere Einzeldaten.

Verarbeitung von Kundendaten

Der Umgang mit personenbezogenen Daten der Kunden ist grundsätzlich immer dann zulässig, wenn eine Einwilligung der betroffenen Personen oder eine gesetzliche Grundlage greift (vgl. Art. 6 Abs. 1 Satz 1 lit. a bis f DS-GVO). Neben der Einwilligung ist die Verarbeitung personenbezogener Daten, die für die Erfüllung eines Vertrages oder vorvertraglicher Maßnahmen auf Anfrage der betroffenen Person erforderlich ist, aufgrund von Art. 6 Abs. 1 Satz 1 lit. b DS-GVO zulässig. Auch zur Wahrnehmung berechtigter Interessen ist eine Verarbeitung gem. Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zulässig, sofern nicht die Interessen der betroffenen Personen überwiegen. Sofern die Datenverarbeitung durch eine dieser Rechtsgrundlagen gerechtfertigt ist, sollte das Einholen einer Einwilligung unterbleiben (zur Begründung siehe Kapitel 5 unter „Interessenabwägung).

Bei vielen Geschäften des täglichen Lebens, deren Leistung und Gegenleistung sofort ohne Zuhilfenahme elektronischer Zahlungsprogramme erfüllt werden (z. B. im Lebensmittelhandel oder beim Kauf von Waren des alltäglichen Bedarfs) ist eine Verarbeitung jeglicher Kundendaten regelmäßig entbehrlich.

Wird durch den Unternehmer die Lieferung einer Ware versprochen, kann natürlich auf der Grundlage des Art. 6 Abs. 1 Satz 1 lit. b DS-GVO die Lieferadresse, ggf. auch eine Rechnungsadresse verarbeitet werden. Ein Reparaturauftrag in der Wohnung des Kunden verlangt natürlich die Wohnadresse und Angaben zum zu reparierenden Gegenstand. Die Verarbeitung von Geburtsdaten ist regelmäßig nur dann erforderlich, wenn angesichts hoher Kundenzahlen ansonsten eine Verwechslung droht. Ist eine zügige Erreichbarkeit – z. B. für Zwischenabsprachen – erforderlich, kann die Telefonnummer oder die E-Mailadresse verarbeitet werden. Für jedes einzelne Geschäft muss der Unternehmer prüfen, welche personenbezogenen Daten des Kunden für die Durchführung des Geschäfts erforderlich sind. Das Ergebnis dieser Prüfung ist abhängig vom zu erfüllenden Vertrag und kann sehr unterschiedlich ausfallen. Nicht zur Vertragserfüllung dient die Werbung. Auch das Anlegen von Kunden- und Nutzerprofilen dient

regelmäßig nicht der Vertragserfüllung. Weitere Hinweise enthalten die „Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gem. Art. 6 Abs. 1 lit. b DS-GVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen“ des Europäischen Datenschutzausschusses, abrufbar unter https://lsaurl.de/EDSA22019.

Im Rahmen der Interessenabwägung (Art. 6 Abs. 1 Satz 1 lit. f DS-GVO) ist die Verarbeitung von Kundendaten zulässig, soweit diese zur Wahrnehmung berechtigter Interessen erforderlich ist, sofern nicht die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Auch hier ist oft eine Einzelfallprüfung erforderlich. Hat der Kunde sich pflichtwidrig verhalten, können, soweit dies erforderlich ist, zur Geltendmachung von Rechtsansprüchen personenbezogene Daten z. B. an einen Rechtsanwalt übermittelt werden. Zahlt der Kunde nicht pflichtgemäß, kann ein Inkassounternehmen in Anspruch genommen werden. Gerade bei kleinen Unternehmen, die über kein eigenes Forderungsmanagement verfügen, dürfte die Beauftragung eines Inkassounternehmens den Erwartungen entsprechen. Übermittelt werden dürften z. B. Namen und Anschrift des Schuldners, der Forderungsgrund sowie die Höhe und die Fälligkeit der Forderung.

Geht der Unternehmer im Rahmen seiner Vertragserfüllung ein finanzielles Risiko ein, kann eine Bonitätsanfrage an eine Auskunftei gestellt werden. Die Gewährung eines Kredites, die Überlassung einer Mietwohnung, der Versand von Waren auf Rechnung oder die Lieferung von Leistungen ohne sofortige Bezahlung stellen ein solches Risiko dar. Bei Lieferungen gegen Vorkasse dagegen dürfen Bonitätsauskünfte i. d. R. nur bei Vorliegen einer wirksamen Einwilligung eingeholt werden.

Bei fehlender Begleichung offensichtlich begründeter und fälliger Forderungen kann geprüft werden, ob eine Einmeldung der Forderungen an eine Auskunftei zulässig ist. Eine solche Einmeldung ist z. B. gem. § 31 Abs. 2 Nr. 4 BDSG zulässig, wenn

- die Zahlung nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich angemahnt wurde,
- seit der ersten Mahnung mindestens vier Wochen vergangen sind,

- der Schuldner zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet wurde und
- die Forderung vom Schuldner nicht bestritten wurde.

Wenn einem Gläubiger mitgeteilt wird, dass die geforderte Zahlung nicht oder zumindest nicht in vollem Umfang geschuldet wird, ist bereits in vielen Fällen eine Meldung an eine Auskunftei nicht mehr zulässig. Weitere Fälle, in denen Einmeldungen fälliger Forderungen bei einer Auskunftei zulässig sind, enthält § 31 Abs. 2 Nr. 1-3 und Nr. 5 BDSG.

Liegen die Voraussetzungen des Art. 6 Abs. 1 lit. b bis f DS-GVO nicht vor, ist die Verarbeitung von Kundendaten nur im Falle einer Einwilligung zulässig (siehe dazu Kapitel 5).

Werbung

Abhängig davon, ob Bestands- oder Neukunden beworben oder ob per Briefpost, elektronisch oder telefonisch geworben werden sollen, ist eine Vielzahl von Vorschriften zu beachten.

Als Grundlage für die Beurteilung der Rechtmäßigkeit der Datenverarbeitung zum Zwecke der Direktwerbung kommt zunächst die Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO in Betracht. Liegen die Voraussetzungen dieser Vorschrift nicht vor, bedarf es einer wirksamen Einwilligung. Nach ErwGr 47 DS-GVO kann die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als ein nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO berechtigtes Interesse betrachtet werden. Im Rahmen der Abwägung sind jedoch die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere deren vernünftige Erwartungen, mit zu berücksichtigen. Dabei sind zudem die Vorschriften des § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) über unzumutbare Belästigungen zu beachten. Liegt nach diesen Vorschriften eine unzumutbare Belästigung vor, ist die entsprechende Nutzung personenbezogener Daten zu Werbezwecken nicht zulässig. Daraus ergibt sich Folgendes:

Werbung per Briefpost an eigene Bestandskunden ist grundsätzlich erlaubt, wenn die Informationspflichten erfüllt und der Zusendung der Werbung nicht widersprochen wurde.

Werbung per E-Mail, SMS und Telefax wird grundsätzlich als „unzumutbare Belästigung“ eingestuft und ist daher nur mit ausdrücklicher Einwilligung erlaubt, unabhängig ob Verbraucher (B2C) oder sonstige Marktteilnehmer (B2B) beworben werden sollen.

Eine Ausnahme besteht im Falle der E-Mail-/SMS-Werbung, wenn bei Bestandskunden

- die Kontaktdaten im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung erlangt worden sind,
- ausschließlich für eigene ähnliche Produkte geworben wird,
- sie der Verwendung nicht schon widersprochen haben und
- sie bei Erhebung und jeder Verwendung der E-Mail-Adresse auf ihr Widerspruchsrecht hingewiesen werden.

Werbung per Telefon gegenüber Verbrauchern (B2C) ist ausschließlich bei vorheriger ausdrücklicher Einwilligung zulässig. Das werbende Unternehmen hat die Einwilligung des Verbrauchers in die Telefonwerbung in angemessener Form zu dokumentieren. Der Nachweis dieser Einwilligung ist ab Erteilung der Einwilligung, sowie nach jeder Verwendung – also nach jedem Werbeanruf beim Verbraucher – fünf Jahre aufzubewahren (siehe § 7a UWG). Bei sonstigen Marktteilnehmern (B2B) kommt es darauf an, ob deren mutmaßliche Einwilligung angenommen werden kann.

Ein Sonderfall gilt bei der Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DS-GVO. Hier bedarf es bei der Verarbeitung zu werblichen Zwecken einer ausdrücklichen Einwilligung.

In diesem Zusammenhang sind insbesondere auch die Informationspflichten der Art. 13 und 14 DS-GVO von Bedeutung. Zudem muss die betroffene Person spätestens zum Zeitpunkt der ersten werblichen Ansprache ausdrücklich auf das Widerspruchsrecht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen (Art. 21 Abs. 2 und 4 DS-GVO). Bei einem Werbewiderspruch und bei Widerruf einer Einwilligung wird die Verarbeitung personenbezogener Daten zu Werbezwecken unzulässig.

Ausführliche Informationen bieten das Kurzpapier Nr. 3 (https://lsaurl.de/Kurzpapiere), die „Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO)“ der Datenschutzaufsichtsbehörden, abrufbar unter https://lsaurl.de/OHWerbung sowie das Merkblatt des Landesbeauftragten für den Datenschutz Sachsen-Anhalt „Wie geht Werbung datenschutzgerecht?“, abrufbar unter https://lsaurl.de/WasDarfWerbung.

Verarbeitung der Daten von Geschäftspartnern

Die Befugnis des Umgangs mit Kundendaten lässt sich nicht gänzlich auf den Umgang mit Daten der Geschäftspartner übertragen. Aber auch jeder weitere Gebrauch personenbezogener Daten, z. B. von dem Geschäftsführer oder den Beschäftigten der Geschäftspartner, muss von einer datenschutzrechtlichen Vorschrift gedeckt sein. Die DS-GVO gilt allerdings nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere von als juristische Person gegründeten Unternehmen. Reine Unternehmensdaten ohne Personenbezug (z. B. die E-Mailadresse Marketingabteilung@firma.de) unterliegen nicht dem Datenschutz (wohl aber eine namensbezogene E-Mailadresse wie Max.Mustermann@firma.de).

13 Beschäftigtendatenschutz

Auch die Verarbeitung von personenbezogenen Daten der Beschäftigten ist an die Vorgaben der DS-GVO gebunden, u. a. an die Grundsätze des Art. 5 DS-GVO. Sie bedarf einer Rechtsgrundlage, es gilt die Zweckbindung, die Verarbeitung der Daten muss erforderlich sein und die Daten müssen grundsätzlich vertraulich behandelt werden. Neben bereichsspezifischen Vorgaben, die Verarbeitung gebieten (z. B. Aufbewahrungspflichten nach HGB bzw. AO) und tarifrechtlichen Bestimmungen ist § 26 BDSG die zentrale Vorschrift zum Beschäftigtendatenschutz. Weitere Rechtsgrundlagen für die Verarbeitung finden sich u. a. in Art. 6 Abs. 1 lit. f DS-GVO, § 22 Abs. 1 Nr. 1 BDSG oder in der Einwilligung des Betroffenen.

Der Schutz der Beschäftigten ist weit ausgedehnt, da alle Informationen über den Beschäftigten erfasst sind, nicht nur Daten aus automatisierter oder teilautomatisierter Verarbeitung und unabhängig davon, ob sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen (§ 26 Abs. 7 BDSG). Damit unterliegen z. B. handschriftliche Notizen über Beschäftigte und Bewerber, Eintragungen in Anwesenheitslisten, Vermerke zu Beschäftigten und telefonische Übermittlungen selbst dann den Beschränkungen des § 26 Abs. 1 bis 6 BDSG, wenn sie nicht in ein Dateisystem aufgenommen werden.

Der geschützte Personenkreis ist weit gezogen, einschließlich in Leiharbeit und zu ihrer Berufsbildung Beschäftigter (§ 26 Abs. 8 BDSG). Auch im Beschäftigungsverhältnis ist es geboten, geeignete technische und organisatorische Maßnahmen zu treffen, die die Rechte und Interessen der Beschäftigten schützen, z. B. in Bezug auf den Schutz gebotener Vertraulichkeit (§ 26 Abs. 5 BDSG, siehe auch Kapitel 7).

Einwilligungen als Rechtsgrundlage

Infolge des Abhängigkeitsverhältnisses sind Einwilligungen im Beschäftigungsverhältnis nur bedingt tragfähig. Näheres ergibt sich aus den strengen Anforderungen von Art. 7 DS-GVO (einschließlich ErwGr 32, 42 und 43 DS-GVO) und § 26 Abs. 2 BDSG (siehe auch Kapitel 5). Die konkreten Umstände sind zu berücksichtigen. Zumeist dürfte die gebotene Freiwilligkeit fehlen. Sie kann aber vorliegen, z. B. wenn gleichgelagerte Interessen verfolgt werden oder für die beschäftigte Person rechtliche oder wirtschaftliche Vorteile erreicht werden (§ 26 Abs. 2 Satz 2 BDSG). Diese Regelvermutungen machen aber die Ausnahme der Einwilligung als Rechtsgrundlage deutlich. Die Einwilligung muss grundsätzlich schriftlich oder elektronisch erfolgen, die Betroffenen sind auf den Verarbeitungszweck und das Widerrufsrecht (Art. 7 Abs. 3 DS-GVO) hinzuweisen (§ 26 Abs. 2 S. 3, 4 BDSG).

§ 26 BDSG als Rechtsgrundlage

Nach § 26 Abs. 1 Satz 1 BDSG dürfen Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem

Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Die vorgesehene Verarbeitung muss für den Zweck geeignet und erforderlich (es darf kein die Betroffenen weniger belastendes Mittel gegeben sein) und insgesamt verhältnismäßig sein. Im Rahmen einer Abwägung sind jeweils die legitimen Interessen des Arbeitgebers mit dem konkreten schutzbedürftigen Interesse der Beschäftigten abzuwägen.

Bewerbungsverfahren

In Bewerbungsverfahren verschafft sich der Arbeitgeber gern ein umfassendes Bild von den Bewerbern. Zunächst ist dabei zu berücksichtigen, dass die Erhebungen grundsätzlich beim betroffenen Bewerber erfolgen sollten (Art. 5 Abs. 1 lit. a DS-GVO). Der Umfang der zu erhebenden Daten ist begrenzt. Ein Fragerecht besteht, wenn ein berechtigtes, billigenswertes und schutzwürdiges Interesse des Arbeitgebers an der Information in Bezug auf das Beschäftigungsverhältnis, d. h. die konkret vorgesehene Tätigkeit, so stark ist, dass das Bewerberinteresse am Schutz seiner Persönlichkeit dahinter zurücksteht. Daher sind grundsätzlich nur solche Fragen zulässig, die in einem sachlichen Zusammenhang mit den Pflichten des Arbeitnehmers stehen. So sind Fragen zur fachlichen Qualifikation für die angestrebte Tätigkeit zulässig. Auch können z. B. Fragen zur arbeitsplatzbezogenen gesundheitlichen Eignung zulässig sein. Laufende Straf- und Ermittlungsverfahren, die Zweifel an der Eignung und Zuverlässigkeit für den konkreten Arbeitsplatz begründen, können ebenfalls erfragt werden. An unspezifischen Fragen nach eingestellten Ermittlungsverfahren besteht dagegen grundsätzlich kein berechtigtes Interesse. Eine Umgehung der Grenzen des Fragerechts und der somit zulässigen Datenverarbeitung durch heimliche Anfragen an ehemalige Arbeitgeber bzw. durch Internetrecherche ist nicht erlaubt. Nach endgültigem Abschluss eines Bewerbungsverfahrens sind die Unterlagen nicht zum Zuge gekommener Bewerber grundsätzlich spätestens nach sechs Monaten zu löschen bzw. zurückzugeben, soweit nicht eine Einwilligung in eine Aufbewahrung für weitere Verfahren gegeben ist oder die Unterlagen für gerichtliche Verfahren benötigt werden.

Vertraulichkeit

Im laufenden Beschäftigungsverhältnis ist der Vertraulichkeit von Beschäftigtendaten besondere Beachtung zu schenken. So genießen die grundlegenden Daten zum Beschäftigungsverhältnis, die in vertraulich zu behandelnden Personalakten enthalten sind, besonderen Schutz. Private Anschriften und Telefonnummern, Bewerbungsunterlagen, Steuerunterlagen, Krankmeldungen und weitere Unterlagen der Personalverwaltung sind intern und zweckgebunden nur durch die personalverwaltenden Mitarbeiter zu verwenden. Notwendige Übermittlungen von Beschäftigtendaten sind möglich (z. B. an die den Lohn zahlende Bank). Unbedenklich ist die Bekanntgabe von Namen und betrieblicher Erreichbarkeit von Ansprechpartnern nach außen. Der Einzelfall bedarf stets einer Interessenabwägung. Im offenen Terminkalender im Betrieb kann mitgeteilt werden, wer wann erreichbar ist und wann nicht. Nicht erlaubt ist die Bekanntgabe der persönlichen Ursachen der Abwesenheit („krank“, „Arzttermin“). Die Bekanntgabe des Geburtsdatums kann der Pflege des Betriebsklimas dienen, es kommt aber häufiger vor, dass das von Beschäftigten aus vielfältigen Gründen abgelehnt wird, sodass die Zustimmung zu erfragen ist. Die Erteilung von Auskünften an Dritte (Gläubiger, Behörden) ist oft bedenklich, wenn keine spezielle Verpflichtung besteht (z. B. gem. § 57 SGB II). Die Veröffentlichung von Fotos von Mitarbeitern ist wegen des Rechts am eigenen Bild (§ 22 KunstUrhG) grundsätzlich nicht von § 26 Abs. 1 BDSG gedeckt. Ob insoweit eine Einwilligung tragfähig ist, wäre anhand der o. g. Vorgaben des Einzelfalls zu prüfen.

Überwachung der Beschäftigten

Ein kritischer Bereich ist die Überwachung der Beschäftigten. Geschützt sind „berechtigte Privatheitserwartungen“ bzw. „vernünftige Erwartungen“ der Beschäftigten (vgl. EGMR, 5. 9. 2017 – 61496/08 – (Barbulescu/Rumänien); Bundesarbeitsgericht, 31.01.2019, 2 AZR 426/18), wonach eingriffsintensive Maßnahmen nicht ohne begründeten Verdacht schwerwiegender Pflichtverletzungen, insbesondere nicht „ins Blaue hinein“ erfolgen dürfen. Weniger intensiv das Persönlichkeitsrecht tangierende Verarbeitungen können ohne durch Tatsachen begründeten Anfangsverdacht vorgenommen werden (abstrakte Maßnahmen, die nicht einzelne Beschäftigte unter Verdacht stellen).

Die Schaffung eines dauerhaften Überwachungsdrucks durch unverhältnismäßige Leistungs- und Verhaltenskontrollen ist unzulässig.

Soweit zu dokumentierende konkrete Anhaltspunkte den Verdacht konkreter Straftaten begründen, können demnach Datenerhebungen nach § 26 Abs.1 Satz 2 BDSG erfolgen. Darüber hinaus können ggf. Überwachungsmaßnahmen auf Basis von § 26 Abs. 1 Satz 1 BDSG bzw. Art. 6 Abs. 1 lit. f DS-GVO möglich sein, wenn sich aus konkreten Anhaltspunkten der Verdacht gegenüber beschäftigten Personen ergibt, dass sie eine schwerwiegende Pflichtverletzung gegenüber dem Arbeitgeber begangen haben (repressive Überwachung). Im sehr seltenen Ausnahmefall kann sogar eine heimliche Überwachung möglich sein, wenn eine notwehrähnliche Lage gegeben ist, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft wären, die Überwachungsmaßnahme geeignet und erforderlich ist, praktisch das einzig verbleibende Mittel darstellt und insgesamt nicht unverhältnismäßig ist.

Präventive Überwachungen, die von Pflichtverletzungen abhalten sollen, wie z. B. Torkontrollen, die nach Zufallsprinzip und unter Abschirmung erfolgen, sind auf Basis des § 26 Abs. 1 BDSG grundsätzlich ebenfalls möglich. Die Maßnahmen müssen zunächst für ein legitimes Kontrollinteresse geeignet sein, andere wirksame aber mildere Mittel dürfen nicht gegeben sein und auch hier muss die Maßnahme im Hinblick auf das schutzwürdige Persönlichkeitsinteresse der Beschäftigten verhältnismäßig sein. Der persönliche Schrank der Beschäftigten ist dagegen i. d. R. tabu.

Beispielhaft sei der Einsatz von GPS in betrieblichen Fahrzeugen erwähnt, der datenschutzrechtlich grundsätzlich möglich ist. Dabei sind die legitimen Anliegen des Arbeitgebers mit den schützenswerten Interessen der Beschäftigten abzuwägen. Arbeitgeberinteressen sind oft die Optimierung und Koordinierung des Fahrzeugeinsatzes oder der Schutz von Sachwerten (Verbleib bei Diebstahl). Der konkrete Zweck wäre jeweils detailliert zu bestimmen, um eine Abwägung zu ermöglichen. Demgegenüber verbietet der Schutz der Persönlichkeitsrechte der Beschäftigten einen permanenten Kontrolldruck. Ist der aktuelle Aufenthalt von Bedeutung, reicht eine Echtzeitüberwachung ohne Aufzeichnung. Ist nur das Auffinden bei Verlust vorgese-

hen, reicht es, das System erst bei Verlust einzuschalten. Bei ordnungsgemäßer betrieblicher Nutzung ist eine dauernde anlasslose Überwachung (z. B. zur Kontrolle der Einhaltung der Höchstgeschwindigkeit oder privat motivierter Umwege) grundsätzlich unzulässig. Ist ausnahmsweise ein Wegenachweis für Abrechnungen nicht anders möglich, ist zumindest eine kurze Speicherdauer vorzusehen. Eine absolute Grenze der Überwachung wäre die zugelassene private Nutzung.

Kontrolle betrieblicher Kommunikation

Auch bei der Kontrolle der betrieblichen Kommunikation sind Grenzen zu beachten. Zwar besteht grundsätzlich zu betrieblichen E-Mails im betrieblichen E-Mail-Postfach Zugang wie zum Schriftverkehr. Ist aber die private Nutzung des Postfachs gestattet oder ggf. geduldet, kann der Arbeitgeber zum Telekommunikationsdiensteanbieter werden. Die Wahrung des Telekommunikationsgeheimnisses verbietet ihm und seinen Mitarbeitern dann den Zugang zum Mailpostfach. Es empfiehlt sich daher, in Bezug auf die private Nutzung rechtzeitig klare Regelungen, ggf. im Rahmen von Betriebsvereinbarungen zu treffen (z. B. klares Verbot/Erlaubnis mit Einwilligung des Zugriffs auf betriebliche Mails). Weitere Hinweise befinden sich in der Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz (siehe https://lsaurl.de/InternetOH).

Eine Telefondatenerfassung ist grundsätzlich im Rahmen der Erforderlichkeit zulässig (Abrechnungen/Kostenkontrolle, Überblick über den Geschäftsverkehr, Missbrauchskontrolle). Ein Abhören von Telefonaten ist mit dem Recht am gesprochenen Wort grundsätzlich nicht vereinbar. Anderes kann gelten, soweit dies für Ausbildungs- bzw. Qualifizierungszwecke unerlässlich ist. Beschäftigte müssen aber wissen, dass und wann sie abgehört werden. Eine allgemeine Leistungskontrolle ist dagegen nicht zulässig.

Besondere Kategorien von personenbezogenen Daten

Im Zusammenhang mit dem Beschäftigungsverhältnis ist auch eine Verarbeitung der durch Art. 9 DS-GVO besonders geschützten Daten

besonderer Kategorien (u. a. religiöse Überzeugung, Gesundheit) zulässig (§ 26 Abs. 3 BDSG i. V. m. Art. 9 Abs. 2 lit. b, h DS-GVO; z. B. Konfession für die Steuern, Krankmeldung für die Lohnfortzahlung). Auch insoweit gilt die Verhältnismäßigkeit (z. B. biometrische Daten für den Zutritt ins Kraftwerk, nicht aber für die Zeiterfassung der Arztpraxis). Einwilligungen müssen sich ausdrücklich auf diese Daten beziehen. Einwilligungsabhängig ist z. B. die Verarbeitung von Gesundheitsdaten im Rahmen des betrieblichen Eingliederungsmanagements (§ 167 SGB IX).

Kollektivvereinbarungen

Befugnisse zur Verarbeitung von Beschäftigtendaten können sich auch aus Kollektivvereinbarungen ergeben (§ 26 Abs. 4 BDSG). Dies sind nicht nur Tarifverträge, sondern auch Betriebs- und Dienstvereinbarungen. Sie müssen nach Art. 88 Abs. 2 DS-GVO die Würde und die Grundrechte der Betroffenen wahren, wie die Betriebsparteien nach der Rechtsprechung auch bisher schon nach § 75 Abs. 2 S. 1 BetrVG verpflichtet waren, die freie Entfaltung der Persönlichkeit der im Betrieb Beschäftigten zu schützen.

14 Verarbeitung besonderer Kategorien personenbezogener Daten

Art. 9 DS-GVO enthält strenge Regelungen in Bezug auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Bei diesen besonderen Kategorien, handelt es sich um personenbezogene Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie um genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Aus genetischen Daten sind Angaben ableitbar zu ererbten oder erworbenen genetischen Eigenschaften, die wiederum Informationen über die Physiologie oder die Gesundheit liefern können, auch zu Gesundheitsprognosen. Biometrische Daten könnten vorhanden sein in Systemen zur Arbeitszeiterfassung oder zur Zugangskontrolle, z. B. mittels Fingerprint. Zu den Gesundheitsdaten gehören auch Daten,

die Rückschlüsse auf Gesundheitszustände beschreiben, wie Angaben über die Einnahme von Medikamenten, der Besuch bestimmter Fachärzte oder Kliniken oder Angaben zur Inanspruchnahme bestimmter Gesundheitsdienstleistungen, wie z. B. einer Suchtberatung. Auch die Krankmeldung („gelber Schein“) enthält Gesundheitsdaten. Der regelmäßige Besuch einer Kirche gibt häufig Aufschluss über die religiöse Überzeugung. Lichtbilder enthalten biometrische Daten, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen (z. B. Gesichtserkennung). Allerdings unterliegt nicht jede mittelbare Angabe zu besonderen Kategorien dem strengen Verarbeitungsverbot nach Art. 9 Abs. 1 DS-GVO. So ist z. B. ein bloßer Alkoholkonsum im Gegensatz zu einer Alkoholabhängigkeit kein Gesundheitsdatum, der Geburtsort keine Angabe über die rassische oder ethnische Herkunft.

Die Verarbeitung von besonderen Kategorien personenbezogener Daten erfolgt in vielen sehr unterschiedlichen Unternehmen. Fast jedes Unternehmen verarbeitet die Religionszugehörigkeit und Krankmeldungen von Beschäftigten. Gesundheitsdaten werden nicht nur von den klassischen Gesundheitsberufen verarbeitet, sondern unter Umständen auch von Anbietern von Gesundheits- bzw. Sportkursen (z. B. Jogakursen), Fitnessstudios oder Erbringern von körpernahen Dienstleistungen.

Art. 9 Abs. 1 DS-GVO untersagt die Verarbeitung dieser Kategorien von personenbezogenen Daten zunächst grundsätzlich. Ausnahmen von diesem Verarbeitungsverbot sind in Art. 9 Abs. 2 DS-GVO geregelt.

Zulässig ist die Verarbeitung dieser Datenkategorien nach Art. 9 Abs. 2 lit. a DS-GVO im Rahmen einer Einwilligung durch den Betroffenen (zur Einwilligung allgemein siehe Kapitel 5) Die Wirksamkeit einer Einwilligung zur Verarbeitung von besonderen Kategorien personenbezogener Daten verlangt zusätzlich zu den allgemeinen Voraussetzungen der Einwilligung deren Ausdrücklichkeit. Dies schließt eine stillschweigende, mutmaßliche oder vermeintlich schlüssig erklärte Einwilligung aus. Eine ausdrückliche Einwilligung ist z. B. erforderlich bei der Nutzung besonderer Kategorien personenbezogener

Daten zu Werbezwecken (z. B. bei Werbung durch Apotheken, die aufgrund der Bestellhistorie personalisiert wird).

Das Verarbeitungsverbot gilt insgesamt nicht, wenn die Verarbeitung der DS-GVO nach Art. 9 Abs. 2 lit.

a. auf einer ausdrücklichen Einwilligung beruht (siehe oben);
b. „für die Ausübung von Rechten und Pflichten aus dem Arbeits- oder Sozialrecht erforderlich ist. Solche Verarbeitungen dürfen jedoch nur dann stattfinden, wenn sie nach einer Rechtsvorschrift erforderlich sind. Davon umfasst sind auch Kollektivvereinbarungen wie Betriebsvereinbarungen. Die Rechtsvorschriften müssen geeignete Garantien für die Grundrechte und die Interessen der betroffenen Personen vorsehen (siehe auch ErwGr 52 DS-GVO);
c. zum Schutz lebenswichtiger Interessen einer Person erforderlich ist und diese körperlich oder rechtlich außerstande ist einzuwilligen;
d. auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung/Vereinigung/Organisation ohne Gewinnerzielungsabsicht erfolgt und sich ausschließlich auf aktuelle oder ehemalige Mitglieder oder auf Personen bezieht, die mit der Stelle regelmäßig Kontakte im Zusammenhang mit deren Tätigkeitszweck unterhalten, und die Daten nicht ohne Einwilligung nach außen weitergegeben werden;
e. Daten betrifft, die die betroffene Person offensichtlich öffentlich gemacht hat;
f. zur Rechtsverfolgung oder für die Aufgabenerfüllung der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist;
g. auf rechtlicher Grundlage aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist;
h. für Zwecke der Gesundheitsvorsorge, der Versorgung oder Behandlung im Gesundheits- oder Sozialbereich erforderlich ist, durch Berufsgeheimnisträger erfolgt und auf einer rechtlichen Grundlage oder aufgrund eines Vertrages mit einem Angehörigen eines Gesundheitsberufes beruht;
i. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, z. B. zur Verhinderung von Epidemien oder zur

Gewährleistung der Arzneimittelsicherheit, auf rechtlicher Grundlage erforderlich ist;

j. auf rechtlicher Grundlage für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DS-GVO erforderlich ist."[3]

Für jede der Ausnahmen des Art. 9 Abs. 2 DS-GVO muss zusätzlich eine der Bedingungen des Art. 6 Abs. 1 Satz 1 DS-GVO vorliegen (zu den Voraussetzungen des Art. 6 Abs. 1 Satz 1 DS-GVO siehe Kapitel 5).

Grundsätzlich dürfen alle in einem Unternehmen Beschäftigten besondere Kategorien personenbezogener Daten verarbeiten, soweit die Verarbeitung durch sie erforderlich ist. Unternehmen sollten die an der Verarbeitung beteiligten Beschäftigten allerdings auf ein Mindestmaß beschränken. Soweit besondere Kategorien zu den in Art. 9 Abs. 2 lit. h DS-GVO genannten Zwecken verarbeitet werden, normiert Art. 9 Abs. 3 DS-GVO spezifische Anforderungen an das verarbeitende Personal. Besondere Kategorien personenbezogener Daten dürfen nur von denjenigen verarbeitet werden, die einer besonderen Geheimhaltungspflicht (Berufsgeheimnis oder Geheimhaltungsvorschrift) unterliegen. Auftragsverarbeiter unterliegen inzwischen denselben Geheimhaltungspflichten wie die berufsmäßig tätigen Gehilfen (§ 203 Abs. 3 StGB).

Bei einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten hat der Verantwortliche gem. Art. 35 Abs. 3 lit. b DS-GVO eine Datenschutz-Folgenabschätzung durchzuführen, wenn die beabsichtigte Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge hat. Eine solche umfangreiche Verarbeitung liegt aber noch nicht vor, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt oder sonstigen Angehörigen eines Gesundheitsberufs oder Rechtsanwalt erfolgt.

Automatisierte Entscheidungen, die auf der Verarbeitung von besonderen Kategorien personenbezogener Daten beruhen, sind nur zulässig, wenn die betroffene Person ausdrücklich eingewilligt hat oder die

[3] Kurzpapier 17 der Datenschutzkonferenz, Seite 2, Lizenz siehe Seite 3

Verarbeitung auf einer speziellen Rechtsgrundlage erfolgt. Eine solche Rechtsgrundlage ist § 37 Abs. 1 Nr. 2 BDSG, wonach automatisierte Entscheidungen möglich sind, die auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruhen.

Sollte aufgrund der Sensibilität von personenbezogenen Daten besonderer Kategorien ein Risiko für die Rechte und Freiheiten der betroffenen Person hinsichtlich einer unbefugten Offenlegung oder eines unbeabsichtigten Verlusts der Daten bestehen und dieses Risiko zu einem physischen, materiellen oder immateriellen Schaden mit erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen können (siehe ErwGr 75 DS-GVO), so sind die Daten dem Risiko angemessen durch ein erhöhtes Sicherheitsniveau und damit einhergehend erweiterten technischen und organisatorischen Maßnahmen zu schützen (z. B. durch Ende-zu-Ende-Verschlüsselung, Verwendung besonders sicherer Passwörter, Datenverarbeitung im Vier-Augen-Prinzip, besondere Sensibilisierung der an den Verarbeitungsvorgängen Beteiligten – siehe auch § 22 Abs. 2 BDSG). Regelmäßig unterliegt die Verarbeitung von personenbezogenen Daten, die zugleich als Berufsgeheimnisse anzusehen sind (z. B. im Falle von Gesundheitsdaten), einem erhöhten Risiko und sollte daher besondere Aufmerksamkeit bei der Risikoabwägung und der Festlegung von Sicherheitsmaßnahmen erfahren.

Weitere Hinweise zur Verarbeitung von Gesundheitsdaten aber auch anderen besonderen Kategorien personenbezogener Daten finden Sie unter https://lsaurl.de/ArztInfo.

15 Videoüberwachung

Eine Videoüberwachung liegt vor, wenn mit Hilfe optisch-elektronischer Einrichtungen personenbezogene Daten verarbeitet werden. Für den Personenbezug reicht es aus, wenn mit Hilfe der Aufnahmen eine natürliche Person identifizierbar ist, also bereits dann, wenn Rückschlüsse auf die Person des Abgelichteten möglich sind, vgl. Art. 4 Nr. 1 DS-GVO. Eine Videoüberwachung kann erfolgen mit Hilfe von handelsüblichen Überwachungskameras, Webcams, Smartphones, Dashcams, Drohnen, Wildkameras sowie Tür- und Klingelkameras. Die Zulässigkeit der Verarbeitung personenbezogener Daten richtet sich nach den Vorschriften der DS-GVO. Dies gilt nur dann nicht,

wenn es sich um eine Datenverarbeitung zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten handelt.

Gem. Art. 6 Abs. 1 DS-GVO ist eine Datenverarbeitung nur zulässig, wenn die betroffenen Personen eingewilligt haben oder eine gesetzliche Erlaubnisnorm erfüllt ist. Eine Einwilligung kommt als Rechtsgrundlage für die Videoüberwachung kaum in Betracht, da die Erfassungsbereiche regelmäßig von einem unbestimmten Personenkreis betreten werden und diese keine Einwilligung erteilt haben. Als Erlaubnisnorm kommt regelmäßig nur Art. 6 Abs. 1 Satz 1 lit. f DS-GVO in Betracht. Danach ist eine Videoüberwachung zulässig, soweit sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Berechtigte Interessen können z. B. die Beweissicherung im Falle von Schädigungen, Vandalismus oder Diebstählen sein. Es müssen allerdings konkrete nachweisbare Tatsachen vorliegen, aus denen sich eine Gefahrenlage ergibt. Subjektive Befürchtungen reichen hier nicht aus. Eine abstrakte Gefahrenlage ist für eine Videoüberwachung nur dann ausreichend, wenn nach allgemeiner Lebenserfahrung typischerweise mit Schäden zu rechnen ist (z. B. bei Juwelieren oder im Bereich der Zapfsäulen von Tankstellen).

Die Videoüberwachung ist nur dann zulässig, wenn sie erforderlich ist. Reichen andere zumutbare Maßnahmen („mildere Mittel“) aus, um eine Gefahr zu unterbinden (z. B. Zugangssicherungen, Sicherheitsschlösser, Zäune, mitunter haben auch Attrappen von Videokameras schon eine ausreichende abschreckende Wirkung), so sind diese Maßnahmen zu bevorzugen. Soweit keine milderen Mittel greifen, ist die Videoüberwachung auf das erforderliche Maß zu beschränken. Für jede Kamera ist zu prüfen, auf welche Betriebszeiten und Erfassungsbereiche sie zu beschränken ist. Ggf. sind einzelne Erfassungsbereiche irreversibel derart zu verpixeln, dass hier keine Personen erkannt werden können. Die Aufnahmen sind zu löschen, wenn sie zur Erreichung des Zweckes (z. B. der Beweissicherung) nicht mehr er-

forderlich sind. Werden die Aufnahmen nicht für Beweis- oder ähnliche Zwecke benötigt, müssen sie regelmäßig spätestens nach 72 Stunden gelöscht werden.

Weiterhin darf eine Videoüberwachung nur dann in Betrieb genommen werden, wenn schutzwürdige Interessen derjenigen, die sich im beabsichtigten Erfassungsbereich aufhalten würden, nicht überwiegen. Das heißt, dass das verantwortliche Unternehmen prüfen muss, welche Interessen hier zu berücksichtigen sind. Beobachtungen, die die Intimsphäre betreffen, z. B. die Überwachung von Toiletten, Saunas, Duschen und Umkleidekabinen sind unzulässig – von krassen, engen Ausnahmen im speziellen Einzelfall abgesehen. Im Übrigen hängt die Videoüberwachung insbesondere davon ab, welcher Personenkreis in welcher Situation wie intensiv überwacht werden soll. So ist die Videoüberwachung in Ess- und Aufenthaltsbereichen in der Gastronomie grundsätzlich unzulässig, da sie dem Zweck des Aufenthalts – der Entspannung – entgegensteht. Ausführliche Hinweise, welche Interessen hier wie zu gewichten sind, enthält die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ der Datenschutzkonferenz unter Nr. 2.2.3, abrufbar unter https://lsaurl.de/VideoOH.

Tonaufzeichnungen können den Straftatbestand des § 201 des Strafgesetzbuches erfüllen. Audiofunktionen sollten daher unumkehrbar deaktiviert werden.

Videoüberwachung von Beschäftigten

Eine längerfristige Videoüberwachung im Arbeitsverhältnis greift erheblich in die Persönlichkeitsrechte der Beschäftigten ein und ist regelmäßig unzulässig. Ausnahmen können z. B. im Einzelhandel vorliegen, wenn durch offene Warenauslagen nachweisbar die Gefahr von Diebstählen besteht und keine milderen Mittel zur Abwehr dieser Gefahr vorliegen. Allerdings ist hier darauf zu achten, dass den Beschäftigten Rückzugsmöglichkeiten eröffnet werden und die Überwachung auf die nachweisbar gefährdeten Bereiche beschränkt wird. Dabei ist Art. 88 DS-GVO i. V. m. § 26 BDSG zu berücksichtigen. Eine Videoüberwachung zum Zwecke der Verhaltens- und Leistungskontrolle ist unzulässig.

Eine gezielte Videoüberwachung von Beschäftigten zur Aufdeckung von Straftaten ist nur nach Maßgabe des § 26 Abs. 1 Satz 2 BDSG zulässig. Danach müssen zu dokumentierende tatsächliche Anhaltspunkte – Vermutungen reichen nicht – den Verdacht begründen, dass der betroffene Beschäftigte im Beschäftigtenverhältnis eine Straftat begangen hat, die Videoüberwachung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an der Unterlassung der Videoüberwachung nicht überwiegt. Dabei kann es sich nur um eine räumlich und zeitlich eng begrenzte Überwachung handeln. Reichen andere Maßnahmen wie Kassenkontrollen, Kontrollen von gebuchten Warenrücknahmen oder die Kontrolle der Warenflüsse aus, so sind nur diese Maßnahmen zur Aufklärung zulässig. Eine verdeckte Videoüberwachung ist nur zulässig, wenn sie die einzig verbleibende Möglichkeit ist, eine Straftat aufzuklären oder zu verhindern und insgesamt nicht unverhältnismäßig ist (siehe auch § 32 Abs. 1 Nr. 4 BDSG). Die Videoüberwachung ist einzustellen, wenn der damit verfolgte Zweck erreicht worden ist oder feststeht, dass er nicht mehr erreicht werden kann.

Im Beschäftigungsverhältnis kommt eine Einwilligung in die Videoüberwachung als Rechtsgrundlage grundsätzlich nicht in Betracht. Insbesondere die notwendige Freiwilligkeit einer Einwilligung ist wegen des Abhängigkeitsverhältnisses zwischen Arbeitnehmer und Arbeitgeber regelmäßig äußerst zweifelhaft (zur Einwilligung siehe auch Kapitel 5).

Maßnahmen vor der Durchführung der Videoüberwachung

Liegen die Voraussetzungen der Videoüberwachung vor, muss der Verantwortliche in der Lage sein, die Rechtmäßigkeit der Überwachung nachzuweisen, Art. 5 Abs. 2 DS-GVO. Ein geeignetes Hilfsmittel hierzu ist das zu führende Verzeichnis von Verarbeitungstätigkeiten (siehe Kapitel 8).

Zudem ist auf die Videoüberwachung nach Art. 13, 14 DS-GVO hinzuweisen. Dies kann in zwei Schritten geschehen. Das erste Hinweisschild sollte vor Betreten des überwachten Bereiches gelesen werden können. Muster für ein solches vorgelagertes Hinweisschild und ein

vollständiges Informationsblatt finden Sie unter https://lsaurl.de/VideoInfo.

Hat die Videoüberwachung ein hohes Risiko für die überwachten Personen zur Folge, so ist eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO durchzuführen. Dies ist z. B. bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche (z. B. bei der Überwachung eines gesamten Shoppingcenters oder einer größeren Sportstätte) erforderlich.

Sofern eine rechtlich zulässige Videoüberwachung objektiv in der Lage ist, das Verhalten oder die Leistung der Beschäftigten zu überwachen oder sie der Verhütung von Arbeitsunfällen dienen soll, wäre der Betriebsrat – soweit vorhanden – nach § 87 BetrVG zu beteiligen. Hilfreich könnte in diesen Fällen eine Betriebsvereinbarung nach § 77 BetrVG sein. Ansonsten sollte die Videoüberwachung durch eine möglichst konkrete Dienstanweisung geregelt werden.

Weitere vertiefende Hinweise enthalten die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“, die auch eine übersichtliche Checkliste enthält, abrufbar unter https://lsaurl.de/VideoOH und die „Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte des Europäischen Datenschutzausschusses“, abrufbar unter https://lsaurl.de/edpbvideoguidelines.

16 Die Unternehmenshomepage

Impressum und Datenschutzerklärung

Viele Unternehmen präsentieren sich mit einer eigenen Homepage im Internet. Unabhängig davon, ob nur das Unternehmen beworben wird oder direkt Waren oder Dienstleistungen über das Internet angeboten werden, ist ein Impressum zu veröffentlichen.

Das Impressum (§ 5 Abs. 1 TMG) informiert den Nutzer der Homepage über deren Anbieter. Dazu sind unter anderem Name und Anschrift des Unternehmens, bei juristischen Personen zusätzlich die Umsatzsteueridentifikationsnummer, die Rechtsform und der Vertretungsberechtigte zu nennen. Auch Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation ermöglichen, einschließlich der Adresse der elektronischen Post, gehören

dazu. Sie sind leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten.

Werden über eine Homepage personenbezogene Daten erhoben, ist eine Datenschutzerklärung nötig (Art. 13 DS-GVO, allgemeine Ausführungen zu den Informationspflichten siehe Kapitel 6). Die Datenerhebung beginnt oft schon beim Aufruf einer Homepage, da in der Regel bereits dann personenbezogene Protokolldaten, wie z. B. die IP-Adresse des Nutzers in Server-Logdateien, gespeichert werden. Außerdem ist die Verarbeitung personenbezogener Daten durch die Verwendung von Cookies und Trackingtools, die Nutzung von Social-Media-Plugins, das Angebot von Newslettern und Kontaktformularen sowie die Bestellung und Bezahlung von Waren zu berücksichtigen. Ein eingebundener Bezahldienst kann z. B. ein Empfänger personenbezogener Daten sein. Auch darauf muss in der Datenschutzerklärung hingewiesen werden.

Die Datenschutzerklärung muss genau darüber informieren, welche konkreten personenbezogenen Daten zu welchem Zweck und wie lange gespeichert oder verwendet werden. Musterdatenschutzerklärungen aus dem Internet (z. B. sogenannte „Datenschutzgeneratoren“) können eine Hilfestellung bei der Erstellung der eigenen Datenschutzerklärung sein. Allerdings ist stets zu prüfen, inwieweit Musterdatenschutzerklärungen den Verarbeitungen personenbezogener Daten auf der eigenen Homepage entsprechen. Regelmäßig sind Anpassungen erforderlich. Helfen kann hier auch ein Tool des Landesbeauftragten für den Datenschutz Baden-Württemberg, welches er unter https://www.baden-wuerttemberg.datenschutz.de/ds-gvo.clever/ zur Verfügung stellt.

Der Inhalt der Datenschutzerklärung muss jederzeit abrufbar sein. Personenbezogene Daten dürfen auch auf der Homepage nur dann erhoben und verwendet werden, wenn dies entweder durch Gesetz ausdrücklich erlaubt ist oder der Nutzer eingewilligt hat (Art. 6 Abs. 1 Satz 1 DS-GVO).

Cookies und Trackingtools zur Webanalyse

Die Speicherung von Cookies oder der Zugriff auf Informationen, die bereits in der Endeinrichtung (PC, Tablet, Smartphone) gespeichert sind, sind zulässig, wenn der Nutzer auf der Grundlage von klaren und

umfassenden Informationen eingewilligt hat (§ 25 Abs. 1 Satz 1 TTDSG).

Die Einwilligung ist nicht erforderlich, wenn die Speicherung der Cookies oder der Zugriff auf bereits in der Endeinrichtung gespeicherte Informationen unbedingt erforderlich sind, um dem Nutzer einen ausdrücklich gewünschten Dienst zur Verfügung zu stellen oder die Kommunikation zu ermöglichen (§ 25 Abs. 2 TTDSG).

Auch die Einbindung von Trackingtools zur Analyse des Nutzerverhaltens, insbesondere, wenn dies webseitenübergreifend erfolgt und die Daten an Dritte zu deren eigenen Zwecken weitergeben werden, ist nur mit vorheriger Einwilligung der Nutzer zulässig. Das gilt sowohl für Trackingtools, die Cookies setzen als auch für das sogenannte Device Fingerprinting. Dabei werden Informationen über das vom Nutzer verwendete Gerät gesammelt (z. B. Marke, Modell, Betriebssystem, Browser, verwendete Software), um so einen eindeutigen digitalen Fingerabdruck zu speichern und wiedererkennen zu können.

Soweit Trackingtools verwendet werden, die personenbezogene Daten der Nutzer in Länder außerhalb Europas übermitteln, kann dies datenschutzrechtlich problematisch oder sogar unzulässig sein. Einige Tools übermitteln z. B. Daten für eigene Zwecke an Unternehmensserver in den USA, ohne die gesetzlichen Anforderungen nach Art. 44 ff. DS-GVO zu erfüllen. Zur Datenübermittlung in Drittstaaten allgemein siehe Kapitel 17.

Anforderungen an die Einwilligung

Eine datenschutzkonforme Einwilligung (Art. 7, 8 DS-GVO, § 25 Abs. 1 Satz 2 TTDSG) verlangt die freie Entscheidung des Nutzers auf der Grundlage von klaren und umfassenden Informationen und die technische Umsetzung dieser Entscheidung durch den Betreiber der Homepage.

So dürfen nicht bereits beim Laden der Homepage einwilligungsbedürftige Cookies gesetzt und Tools zur webseitenübergreifenden Verfolgung und Auswertung des Nutzerverhaltens geladen werden, obwohl der Nutzer noch gar keine Entscheidung getroffen hat.

Die Entscheidung des Nutzers, nur notwendige Cookies zu akzeptieren, darf anschließend nicht dazu führen, dass gleichwohl andere

Cookies gesetzt und z. B. Tools für eine webseitenübergreifende Auswertung geladen werden.

Der Nutzer muss seine Einwilligung aktiv erteilen. Voreinstellungen – wie z. B. ein bereits angekreuztes Kästchen – welche der Nutzer zur Verweigerung seiner Einwilligung abwählen muss, genügen nicht.

Der Nutzer muss alle Informationen erhalten, um die Konsequenzen seiner Einwilligung leicht bestimmen und die Funktionsweise der Cookies verstehen zu können. Weitere Details zur Einwilligung siehe Kapitel 5.

Social Plugins

Sogenannte Social Plugins wie der Gefällt-mir-Button von Facebook, der +1-Button von Google+ oder der Tweet-Button von Twitter dürfen nicht direkt in die Unternehmenshomepage eingebunden werden, da hierbei Nutzerdaten auch dann an Facebook, Google und Twitter übermittelt werden, wenn der Nutzer den Button gar nicht anklickt. Deshalb wird empfohlen, die vom c't Magazin entwickelte Shariff-Lösung einzusetzen, bei der der direkte Kontakt zwischen dem sozialen Netzwerk und dem Nutzer erst dann hergestellt wird, wenn dieser aktiv auf den jeweiligen Button klickt.

Eine weitere Möglichkeit ist die Einbindung eigener, individuell gestalteter Buttons, bei denen die Kommunikation mit den sozialen Netzwerken ein auf dem Server des Webseitenbetreibers abgelegtes Skript übernimmt. Erst wenn der Nutzer einen Button betätigt, entsteht eine direkte Verbindung und Nutzerdaten werden übertragen.

Sicherheit der Verarbeitung personenbezogener Daten auf der Homepage

Wenn personenbezogene Daten auf der Homepage verarbeitet werden (z. B. durch Kontaktformulare, Webshops oder in Diskussionsforen) sollte der unberechtigte Zugriff der Homepagebesucher auf diese Daten sicher ausgeschlossen werden, z. B. durch komplexe Passwörter. Es wäre ein eklatanter Verstoß gegen den Datenschutz, aber sicherlich auch nicht im unternehmerischen Interesse, wenn z. B. die Kundendatenbank – inklusive des Warenkorbes und der Zahlungsdaten – von jedem Homepagebesucher eingesehen werden könnte.

Externe Links

Vor der Verwendung externer Links, die auf fremde Internetangebote verweisen, sollten diese genau auf strafrechtlich relevante Inhalte geprüft und die Prüfung in regelmäßigen Abständen wiederholt werden. Außerdem sind externe Links entsprechend zu kennzeichnen, damit der Nutzer die Weiterleitung zu einem anderen Diensteanbieter erkennen kann (§ 19 Abs. 3 TTDSG).

17 Übermittlung personenbezogener Daten in Länder außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraumes (EWR)

Im Zuge der Globalisierung findet vermehrt ein rascher Austausch von Daten zwischen Unternehmen und Schwesterfirmen oder Dienstleistern mit Sitz außerhalb der EU/des EWR (zum EWR gehören neben den Mitgliedstaaten der EU Island, Liechtenstein und Norwegen) statt. So werden Kunden- oder Beschäftigtendaten durch Apps, Tools und Programme nicht nur amerikanischer Anbieter in der Cloud von US Software-Firmen gespeichert, von einem Callcenter in Indien oder im Kosovo gespeichert oder genutzt oder medizinische Tests in China analysiert.

Ein solcher Transfer von personenbezogenen Daten aus der EU/EWR in ein Drittland ist aber nur rechtskonform, wenn die Vertragsparteien ihre datenschutzrechtlichen Pflichten (Art. 5, 6, 26 oder 28 DS-GVO) erfüllen und das Drittland über ein dem EU-Recht vergleichbares Datenschutzniveau verfügt (Art. 44 DS-GVO). Für z. B. die Schweiz, dem Vereinigten Königreich, Japan und Süd-Korea bestätigte die Europäische Kommission ein solches Schutzniveau per Angemessenheitsbeschluss (Art. 45 DS-GVO), so dass ein datenexportierendes Unternehmen den Status dieses Drittlandes nicht prüfen muss. Sitzt der Vertragspartner aber in einem Drittland ohne einen solchen Angemessenheitsbeschluss, muss der Verantwortliche selbst Vorkehrungen zum Schutz der betreffenden Daten treffen. Dazu besteht die Möglichkeit, mit dem Vertragspartner EU-Standarddatenschutzklauseln (Art. 46 Abs. 1 lit. c DS-GVO) abzuschließen, die als Mustervertragstexte zur Verfügung stehen. Konzernangehörige Unternehmen

können sich verbindliche unternehmensinterne Datenschutzvorschriften (Binding Corporate Rules, Art. 46 Abs. 1 b DS-GVO) geben, die behördlich zu genehmigen sind. Es bleibt aber die Herausforderung für das Unternehmen zu prüfen, ob der Partner im Drittland seine vertraglichen Pflichten überhaupt erfüllen kann, ohne z. B. gegen Gesetze des Drittlandes zu verstoßen. Unter Umständen greifen Sicherheitsbehörden des Drittlandes auf die Daten zu, ohne dass der Partner das Unternehmen noch die betroffenen Kunden darüber informieren darf. Hier sind gegebenenfalls zusätzliche Schutzmaßnahmen erforderlich.

Sofern also personenbezogene Daten des Unternehmens von anderen Unternehmen mit Sitz außerhalb der EU/EWR gespeichert, genutzt, gelesen oder in sonstiger Weise verarbeitet werden, müssen (datenexportierende) Unternehmen eine Reihe von Prüfschritten vornehmen, die auf der Homepage des Landesbeauftragten im „Infopaket Drittstaatentransfer“ unter https://lsaurl.de/DrittstaatenTransfer näher beschrieben sind. Hier finden Sie auch die EU-Standarddatenschutzklauseln.

Ist ein Transfer von personenbezogenen Daten nach den o. g. Ausführungen nicht rechtskonform, darf er nicht vorgenommen werden bzw. ist sofort auszusetzen.

Bei der Nutzung eines Clouddienstes einer europäischen Tochter eines US-Konzerns besteht, selbst wenn der Cloud-Dienst auf einem Server im EU/EWR angeboten wird, ein Restrisiko, dass gespeicherte Daten aufgrund des CLOUD-Acts (Clarifying Lawful Overseas Use of Data Act) an den US-Mutterkonzern übermittelt und von dort US-amerikanischen Sicherheitsbehörden ausgehändigt werden. Durch rechtliche und technische Gestaltung muss der Verantwortliche daher verhindern, dass das europäische Tochterunternehmen des US-Konzerns als sein Vertragspartner Zugriff auf die Daten erhalten kann. In Frage kommt neben anderen Maßnahmen – wie z. B. der Anonymisierung der Daten – die Einbindung eines dritten (ausschließlich europäischen) Unternehmens zur Verschlüsselung und Schlüsselverwahrung (Transportverschlüsselung, Speicherungsverschlüsselung und ggf. eine abgeschirmte Verarbeitungsumgebung bei Verarbeitung von sensiblen Daten in der Cloud).

18 Folgen von Datenschutzverstößen und Maßnahmen der Aufsichtsbehörden

Verstöße gegen datenschutzrechtliche Vorschriften können zu unterschiedlichen und, gerade seit Geltung der DS-GVO, zu empfindlichen Folgen führen.

So hat jede betroffene Person nach Art. 77 DS-GVO das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt. Geht beim Landesbeauftragten eine Beschwerde ein, die schlüssig einen Datenschutzverstoß beschreibt, wird er eine Untersuchung nach Art. 58 Abs. 1 DS-GVO gegenüber dem betreffenden Unternehmen einleiten und es zunächst zum Vorwurf befragen. Weitere Untersuchungen, z. B. eine Vor-Ort-Kontrolle, hängen vom Ergebnis der Befragung ab.

Der Landesbeauftragte kann aber auch unabhängig von Beschwerden oder konkreten Verdachtsmomenten Untersuchungen bei Unternehmen durchführen. Dabei kann er unter Beachtung des Verhältnismäßigkeitsgrundsatzes z. B. Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung seiner Aufgaben notwendig sind, verlangen. Auch der Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte kann ihm zu gewähren sein. Die Aufgaben und Befugnisse der Aufsichtsbehörden sind in Art. 57 bis 59 DS-GVO zusammengefasst.

Im Falle eines festgestellten Datenschutzverstoßes sind nach Art. 58 Abs. 2 DS-GVO u. a. folgende Maßnahmen denkbar:

- Warnungen, wenn beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die DS-GVO verstoßen,
- Verwarnungen, wenn ein Verstoß bereits vorliegt,
- Anweisungen, Verarbeitungsvorgänge in Einklang mit der DS-GVO zu bringen,
- Anweisungen, die betroffene Person von einer Verletzung des Schutzes personenbezogener Daten zu benachrichtigen,
- Vorübergehende oder endgültige Beschränkungen der Verarbeitung, einschließlich eines Verbots,

- Anordnungen der Berichtigung oder Löschung personenbezogener Daten,
- Verhängungen von Geldbußen i. H. v. bis zu 20 Mio € oder 4 % des gesamten weltweit erzielten Jahresumsatzes. Die Höhe der Geldbuße muss wirksam, verhältnismäßig und abschreckend sein. Bei der Berechnung werden z. B. die Schwere des Verstoßes, der Grad der Verantwortung, die getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens, etwaige einschlägige frühere Verstöße und der Umfang der Zusammenarbeit mit der Aufsichtsbehörde zur Minderung nachteiliger Auswirkungen des Verstoßes berücksichtigt (siehe insgesamt Art. 83 DS-GVO).

Betroffene Personen können sich auch mit einem Rechtsbehelf direkt an ein Gericht wenden (Art. 79 DS-GVO). Nach Kenntnis des Landesbeauftragten wird hiervon insbesondere dann Gebrauch gemacht, wenn die Einhaltung der Betroffenenrechte gerügt wird.

Die Beschwerden bei der Aufsichtsbehörde und den Rechtsbehelf bei Gericht können betroffene Personen auch durch Interessenverbände einlegen lassen, z. B. durch die Verbraucherzentrale.

Verbände haben zudem die Möglichkeit, direkt Verbandsklage gegen ein Unternehmen einzulegen, wenn das nationale Recht dies vorsieht. § 2 Nr. 11 des deutschen Unterlassungsklagengesetzes regelt insoweit, dass Unternehmer durch Verbände auf Beseitigung und Unterlassung von bestimmten Datenverarbeitungen in Anspruch genommen werden können. Dies gilt, wenn personenbezogene Daten zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens einer Auskunftei, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben, verarbeitet oder genutzt werden.

Betroffene Personen haben zudem im Falle materieller oder immaterieller Schäden einen Anspruch auf Schadensersatz gem. Art. 82 DS-GVO gegen das verantwortliche Unternehmen oder den Auftragsverarbeiter.

A Fragenkatalog für KMU zur Datenschutz-Grundverordnung – Wie gut sind Sie aufgestellt?

1. Datenschutz ist Chefsache
   a. Als Geschäftsleitung müssen Sie sich mit den Anforderungen der DS-GVO und des BDSG befassen. Kennen Sie insbesondere die Regelungen
      - zur Rechenschaftspflicht über die Einhaltung der Grundsätze der Datenverarbeitung (Art. 5 Abs. 2 DS-GVO) und den weiteren Dokumentationspflichten;
      - zu den Informationspflichten gegenüber den Betroffenen, deren personenbezogene Daten Sie verarbeiten (Art. 12 bis 14 DS-GVO), und den weiteren Betroffenenrechten;
      - zur Meldung von Datenschutzverstößen (Art. 33 DS-GVO);
      - zur technischen und organisatorischen Sicherheit der Datenverarbeitung (Art. 32 DS-GVO)? Haben Sie klare Richtlinien erlassen, die die Verarbeitung personenbezogener Daten unternehmensintern regeln?

   b. Wer ist in Ihrem Unternehmen neben der Geschäftsleitung für Datenschutzthemen zuständig? Haben Sie einen Datenschutzbeauftragten benannt (Art. 37 DS-GVO, § 38 BDSG)?

   c. Wurden Ihre Beschäftigten über die Datenschutzregelungen informiert und auf die Beachtung der datenschutzrechtlichen Anforderungen verpflichtet?

2. Bestandsaufnahme
   a. Haben Sie alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten verarbeitet werden, in ein Verzeichnis der Verarbeitungstätigkeiten aufgenommen (Art. 30 DS-GVO)? Denken Sie hierbei insbesondere an die
      - Verarbeitung von Kundendaten,
      - Verarbeitung von Beschäftigtendaten,
      - Verarbeitung von Daten von Kindern und
      - Verarbeitung von Daten für Dritte als Auftragsverarbeiter.

   b. Wird dieses Verzeichnis aktualisiert, wenn sich die Datenverarbeitung bzw. die Voraussetzungen dafür verändern? Wer ist hierfür in Ihrem Unternehmen zuständig?

3. Zulässigkeit der Verarbeitung

   Für jede Verarbeitung personenbezogener Daten benötigen Sie eine Rechtsgrundlage. Dies kann eine gesetzliche Regelung oder eine Einwilligung der Betroffenen sein.

   a. Haben Sie für alle Verarbeitungen (siehe oben Nr. 2) eine Rechtsgrundlage (Art. 6 bis 11 DS-GVO sowie §§ 22, 24, 26 bis 28 BDSG), z. B. einen Vertrag mit der betroffenen Person oder die Interessenabwägungsklausel (Art. 6 Abs. 1 Satz 1 lit. b bzw. f DS-GVO)?

   b. Haben Sie dies dokumentiert?

   c. Entsprechen Ihre Muster für Einwilligungserklärungen für Kunden, Interessenten usw. den Anforderungen der Art. 7 und 13 DS-GVO? Denken Sie insbesondere an die Informationspflichten, auch zur jederzeitigen Widerrufbarkeit der Einwilligung, und – sofern vorhanden – auch an Drittdienste auf Ihrer Internetseite, für die es einer Einwilligung bedarf.

4. Betroffenenrechte und Informationspflichten

   a. Alle Betroffenen sind über die Verarbeitung ihrer Daten zu informieren. Dies hat insbesondere in einer transparenten, leicht zugänglichen Form sowie in einer klaren und einfachen Sprache zu erfolgen (Art. 12 DS-GVO). Wie stellen Sie diese datenschutzkonforme Information der Betroffenen über alle in Art. 13 und 14 DS-GVO genannten Punkte sicher? Denken Sie dabei, wenn vorhanden, auch an Datenverarbeitungen auf Ihrer Internetseite und an die Beschilderung für Videoüberwachungen. Besonders wichtig sind in diesem Zusammenhang folgende Informationen:

      - Kontaktdaten des Verantwortlichen und seines Datenschutzbeauftragten (falls vorhanden),
      - Zwecke und Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten,
      - Herkunft und Empfänger der Daten,
      - Dauer der Speicherung, ggf. Kriterien für die Festlegung der Speicherdauer,
      - Hinweis auf Betroffenenrechte, darunter auch das Recht auf Beschwerde bei der Aufsichtsbehörde und ggf. das Recht auf Widerruf der Einwilligung.

b. Wie stellen Sie die weiteren Betroffenenrechte sicher (Art. 15 bis 22 DS-GVO)? Denken Sie dabei insbesondere an folgende Rechte:
   - Recht auf Auskunft,
   - Recht auf Berichtigung,
   - Recht auf Widerspruch,
   - Recht auf fristgemäße Löschung der Daten,
   - Recht auf Einschränkung der Verarbeitung und
   - Recht auf Datenübertragbarkeit.

5. Personenbezogene Daten von Kindern
   a. Haben Sie, sofern Sie die Verarbeitung personenbezogener Daten von Kindern (alle Minderjährigen nach deutschem Recht) auf die Interessenabwägung stützen, deren Interessen besonders gewichtet (Art. 6 Abs. 1 Satz 1 lit. f DS-GVO)?
   b. Verarbeiten Sie auch personenbezogene Daten von Kindern, die das 16. Lebensjahr noch nicht vollendet haben, in Bezug auf Dienste der Informationsgesellschaft[4]? Wenn ja, stellen Sie in diesen Fällen sicher, dass die besonderen Anforderungen an die Einwilligung erfüllt sind (Art. 8 DS-GVO)?
6. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
   a. Welche technischen und organisatorischen Maßnahmen, die ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten (Art. 32 DS-GVO), setzen Sie oder Ihre Dienstleister ein? Haben Sie Ihre diesbezügliche Schutzbedarfsklassifizierung[5] dokumentiert?
   b. Setzen Sie Pseudonymisierungs- oder Verschlüsselungsverfahren ein? Letztere sind z. B. bei Verwendung von Online-Formularen verpflichtend.
   c. Haben Sie für die von Ihnen eingesetzten IT-Anwendungen jeweils ein dokumentiertes Rollen- und Berechtigungskonzept?

[4] Dienste der Informationsgesellschaft = jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung, z. B. Online-Verkauf von Waren, Video auf Abruf, Download eines Klingeltons, Beitritt zu sozialen Netzwerken.
[5] Schutzbedarfsklassifizierung = Bewertung des konkreten Schutzbedarfs der verarbeiteten Daten.

d. Wie stellen Sie sicher, dass bei der Neuentwicklung oder Änderung von Produkten oder Dienstleistungen Datenschutzanforderungen von Anfang an mitberücksichtigt werden (Art. 25 DS-GVO)?

7. Verträge prüfen
   a. Haben Sie Verträge mit Auftragsverarbeitern, d. h. mit Unternehmen, die in Ihrem Auftrag personenbezogene Daten verarbeiten (z. B. wenn Sie die Finanzbuchhaltung, die Wartung der EDV oder die Datenträgerentsorgung ausgelagert haben) abgeschlossen? Enthalten die Verträge die nach Art. 28 DS-GVO erforderlichen Angaben? Dokumentieren Sie Anweisungen, die Sie Ihren Auftragsverarbeitern geben?
   b. Führt Ihr Unternehmen Verarbeitungen durch, bei denen eine Übermittlung personenbezogener Daten in ein Drittland möglich ist? Dies kommt auch in Betracht bei der Nutzung von außereuropäischen Speichermöglichkeiten in einer Cloud. Bestehen für diese Verarbeitungen entsprechende zusätzliche Garantien/Vereinbarungen? Z. B. EU-Standarddatenschutzklauseln, Einzelverträge, zertifizierte Verfahren, Binding Corporate Rules. Haben Sie insbesondere bei Datenübermittlungen in die USA geprüft, ob zusätzliche Schutzmaßnahmen erforderlich sind, und diese umgesetzt?
8. Datenschutz-Folgenabschätzung
   a. Führt Ihr Unternehmen Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen durch (Art. 35 DS-GVO)? Dies gilt z. B. bei einer umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten. Eine Liste von Datenverarbeitungen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, hat die Aufsichtsbehörde gem. Art. 35 Abs. 4 DS-GVO veröffentlicht[6].
   b. Falls ja, haben Sie für die in diesen Fällen erforderliche Datenschutz-Folgenabschätzung in Ihrem Unternehmen einen Prozess eingeführt?
   c. Wer ist für diesen Prozess zuständig?

[6] So genannte Muss-Liste, siehe http://lsaurl.de/DSFAListe. Bitte beachten Sie, dass diese Liste nicht abschließend ist.

9. Meldepflichten
    a. Haben Sie in Ihrem Unternehmen einen Prozess zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde eingeführt (Art. 33 DS-GVO)?
        - Haben Sie dabei insbesondere auch die Einhaltung der Meldefrist von 72 Stunden beachtet?
        - Wer ist in Ihrem Unternehmen für die Meldung zuständig?
    b. Falls Sie einen Datenschutzbeauftragten benannt haben, denken Sie an die Veröffentlichung und Meldung der Kontaktdaten an die Aufsichtsbehörde.
10. Dokumentation
    a. Können Sie die Einhaltung aller genannten Pflichten/Anforderungen (schriftlich, elektronisch) nachweisen?
    b. Wie stellen Sie sicher, dass Ihre Dokumentation immer auf dem neuesten Stand ist?

Eigene Notizen

Die Beiträge dieses Leitfadens entsprechen dem Stand Dezember 2021. Abweichungen durch seit Veröffentlichung geänderter Rechtslage sind nicht auszuschließen.

Impressum

Herausgeber:
Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt

Leiterstr. 9, 39104 Magdeburg
PF 1947, 39009 Magdeburg

Tel. (0391) 81803-0
Fax (0391) 81803-33

https://datenschutz.sachsen-anhalt.de
poststelle@lfd.sachsen-anhalt.de

PDF-Version: https://lsaurl.de/ChefsacheDS