DIN

Grit Reimann

Betrieblicher Datenschutz Schritt für Schritt – gemäß EU-Datenschutz-Grundverordnung

Lösungen zur praktischen Umsetzung

2., vollständig überarbeitete und erweiterte Auflage

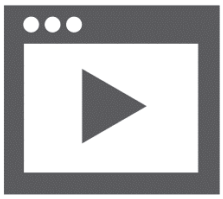
- ☑ Textbeispiele
- ☑ Musterformulare
- ☑ Checklisten

Beuth

Betrieblicher Datenschutz

Mehr zu diesem Titel

… finden Sie in der Beuth-Mediathek



Zu vielen neuen Publikationen bietet der Beuth Verlag nützliches Zusatzmaterial im Internet an, das Ihnen kostenlos bereitgestellt wird.
Art und Umfang des Zusatzmaterials – seien es Checklisten, Excel-Hilfen, Audiodateien etc. – sind jeweils abgestimmt auf die individuellen Besonderheiten der Primär-Publikationen.

Für den erstmaligen Zugriff auf die Beuth-Mediathek müssen Sie sich einmalig kostenlos registrieren. Zum Freischalten des Zusatzmaterials für diese Publikation gehen Sie bitte ins Internet unter

www.beuth-mediathek.de

und geben Sie den folgenden Media-Code in das Feld „Media-Code eingeben und registrieren“ ein:

M279815248

Sie erhalten Ihren Nutzernamen und das Passwort per E-Mail und können damit nach dem Log-in über „Meine Inhalte“ auf alle für Sie freigeschalteten Zusatzmaterialien zugreifen.

Der Media-Code muss nur bei der ersten Freischaltung der Publikation eingegeben werden. Jeder weitere Zugriff erfolgt über das Log-In.

Wir freuen uns auf Ihren Besuch in der Beuth-Mediathek.

Ihr Beuth Verlag

Hinweis: Der Media-Code wurde individuell für Sie als Erwerber dieser Publikation erzeugt und darf nicht an Dritte weitergegeben werden. Mit Zurückziehung dieses Buches wird auch der damit verbundene Media-Code ungültig.

(Leerseite)

Betrieblicher Datenschutz Schritt für Schritt – gemäß EU-Datenschutz-Grundverordnung

(Leerseite)

DIN

Grit Reimann

Betrieblicher Datenschutz Schritt für Schritt – gemäß EU-Datenschutz-Grundverordnung

Lösungen zur praktischen Umsetzung –
Textbeispiele, Musterformulare, Checklisten

2., vollständig überarbeitete und erweiterte Auflage 2018

Herausgeber:
DIN Deutsches Institut für Normung e. V.

Beuth Verlag GmbH · Berlin · Wien · Zürich

Herausgeber: DIN Deutsches Institut für Normung e. V.

Berlin · Wien · Zürich
Am DIN-Platz
Burggrafenstraße 6
10787 Berlin

Telefon: +49 30 2601-0
Telefax: +49 30 2601-1260
Internet: www.beuth.de
E-Mail: kundenservice@beuth.de

Titelbild: © iStock.com/trumzz
Satz: B & B Fachübersetzergesellschaft mbH, Berlin
Druck: COLONEL, Kraków

Gedruckt auf säurefreiem, alterungsbeständigem Papier nach DIN EN ISO 9706

ISBN 978-3-410-27981-5
ISBN (E-Book) 978-3-410-27982-2

Autorenporträt

Frau Dr. Reimann arbeitet seit vielen Jahren als externe Datenschutzbeauftragte für mittelständische Unternehmen.

Seit 1991 ist sie geschäftsführende Gesellschafterin einer Unternehmensberatung für den Aufbau von integrierten Managementsystemen in der betrieblichen Praxis. Darunter fällt auch die Beratertätigkeit als Datenschutzbeauftragte.

Regelungen im Datenschutz bezieht sie aktiv in bestehende Managementsysteme von Unternehmen ein. Sie nutzt damit das integrierte Management als methodisches Instrument für die betriebliche Einführung und Umsetzung des Datenschutzes in der Praxis. Mit der Durchführung von Datenschutzaudits deckt sie Änderungs- und Verbesserungspotenziale auf, beschreibt, welche datenschutzbezogenen Regelungen mit welchen Textbausteinen getroffen werden müssen, gibt Formblätter und Unterweisungstexte vor.

Seit mehr als 25 Jahren bringt Frau Dr. Reimann ihre methodischen Kenntnisse in der praktischen Umsetzung sowohl als Beraterin, Mediatorin, als Fachkraft für Arbeitssicherheit und Datenschutzbeauftragte sowie als Trainerin an Fachhochschulen und im eigenen Institut für Management- und Businesstraining ein. Sie arbeitet als Auditorin für verschiedene Zertifizierungsgesellschaften.

Frau Dr. Reimann war langjähriges Mitglied im Bundesverband Deutscher Unternehmensberater e. V.

Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz (in der jetzt gültigen Fassung)
BetrVG	Betriebsverfassungsgesetz
BVD	Bundesverband der Datenschutzbeauftragten Deutschlands
DSB	Datenschutzbeauftragter
DV	Datenverarbeitung
EG	Erwägungsgrund
EkStG	Einkommensteuergesetz
EU	Europäische Union
EU-DSGVO	EU-Datenschutz-Grundverordnung
EWR	Europäischer Wirtschaftsraum
MeldeG	Meldegesetz
PAuswG	Personalausweisgesetz
R & D	Research & Development
RStV	Staatsvertrag für Rundfunk und Medien
SGB	Sozialversicherungsgesetzbuch

Inhalt

(Leerseite)

1 Einleitung

Der Schutz personenbezogener Daten spielt in vielen Bereichen unseres täglichen Lebens eine große Rolle. Angaben über unsere Person werden beispielsweise zur Begründung und Aufrechterhaltung von Beschäftigungsverhältnissen, Liefer- und Leistungsbeziehungen, bei der Beantragung von Kunden- und Bonuskarten, Registrierungen bei Buchungen im Hotel, auf Reisen, in Verbänden und andernorts abgefordert. Die Verarbeitung dieser personenbezogenen Daten, deren Erfassung, Bearbeitung, Speicherung, Übermittlung und Archivierung, unterliegt datenschutzrechtlichen Regelungen. Wesentliche Belange für den Datenschutz sind auf europäischer Ebene und für alle Mitgliedstaaten verbindlich in der **EU-Datenschutz-Grundverordnung** und auf nationaler Ebene in der Bundesrepublik Deutschland vorrangig im revisionierten **Bundesdatenschutzgesetz**, im Telekommunikations- und Telemediengesetz sowie anderen Rechtsverordnungen geregelt.

Im vorliegenden Buch sollen grundlegende **Aspekte des Datenschutzes für den nicht-öffentlichen Bereich** in einfacher und verständlicher Form erläutert werden. Wesentliche Regelungen für die betriebliche Praxis werden entweder in Beispielen oder Musterlösungen dargestellt, so dass eine einfache Adaption der Texte für eigene Belange möglich wird. Diverse Situationen aus der täglichen Unternehmenspraxis werden aus datenschutzrechtlicher Sicht beleuchtet, auf Rechtskonformität bewertet und mit Optionen für Lösungen versehen.

Obwohl für den nicht-öffentlichen Bereich verfasst, sind viele der dargestellten Situationen und Muster auch für den öffentlichen Bereich oder für private Zwecke anwendbar. Beispielsweise gelten die Regelungen für die Internet-, E-Mail- und Telefonnutzung, für den Umgang mit USB-Sticks, Kopier- und Faxgeräten u. a. m. sowohl für den öffentlichen als auch nicht-öffentlichen Bereich. Weiterhin vermittelt die vorliegende Publikation wesentliche Einsichten in den Umgang mit personenbezogenen Daten auch für private Zwecke und dürfte damit im Interesse jedes Einzelnen liegen. Die Prinzipien der Datensparsamkeit und eingeschränkten Verfügbarkeit personenbezogener Daten seien hier nur stellvertretend genannt.

Der Wert dieses Buches liegt im einführenden Charakter in die Thematik und kann damit als Grundlagenwerk für den Datenschutz bezeichnet werden. Es **unterstützt die Tätigkeit des Datenschutzbeauftragten**, der über diese Publikation Anleitung für seine praktische Arbeit und die hierfür anzuwendende Methodik erhält. Der Datenschutzbeauftragte profitiert von den in der Mediathek (www.beuth-mediathek.de) zu diesem Buch geführten Mustervereinbarungen, Musterbestellurkunden, Vorlagen für datenschutzrechtliche Regelungen sowie Fallbeispielen mit Musterlösungen. Diese können ohne großen Aufwand an die eigene Situation angepasst werden. Zur besseren Übersicht sind alle Muster, Beispiele, auch Hinweise und Zitate aus den Rechtsverordnungen am Rand des Textes als solche kenntlich gemacht.

Im vorliegenden Buch werden nach der Einleitung (Kapitel 1) zunächst Aufbau und wesentliche Inhalte der EU-Datenschutz-Grundverordnung und Passagen des Bundesdatenschutzgesetzes näher beleuchtet (Kapitel 2 und 3). Die Darstellung erhebt keinen Anspruch auf Vollständigkeit. Vielmehr sollen bereits am Anfang wesentliche Grundsätze, Leitlinien und Prinzipien im Datenschutz interpretiert und damit für weitere Ausführungen verständlich und anwendbar gemacht werden. Dazu zählen die Definition personenbezogener Daten, das Recht des Betroffenen auf informationelle Selbstbestimmung, die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, die Einwilligung des Betroffenen für die Nutzung seiner Daten, Auskunftsrechte sowie die Pflichten der verantwortlichen Stelle.

Im 4. Kapitel wird explizit auf die Rolle des Datenschutzbeauftragten eingegangen. In praxisorientierter Weise und unter zur Verfügungstellung von Vorlagen und Mustertexten wird aufgezeigt, wie der Datenschutzbeauftragte seine Arbeit gestalten kann und welche Regelungen er für den betrieblichen Datenschutz aufstellen muss. Dabei steht insbesondere die Art und Weise seiner Herangehensweise an datenschutzrechtliche Belange im Fokus der Betrachtung.

Mit dieser Handlungsanleitung soll versucht werden, ausgebildeten und betrieblich bestellten Datenschutzbeauftragten mehr Sicherheit im Umgang mit den Rechtsforderungen der EU-Datenschutz-Grundverordnung und des BDSG und anderer geltender Bestimmungen zu geben und Wege aufzuzeigen, wie diese in der Praxis umgesetzt werden können.

Kapitel 5 beschäftigt sich mit den technischen und organisatorischen Anforderungen im Datenschutz. Im Wesentlichen erfolgt hier die Klarstellung der Begrifflichkeiten, mit denen in den folgenden Kapiteln betriebliche Regelungen für den Datenschutz beispielhaft dargestellt und verständlich aufbereitet werden.

In Kapitel 6 wird auf das Vorgehen bei der Datenschutzfolgeabschätzung näher eingegangen. Anhand eines Beispiels wird die Methodik zur Risikobewertung datenschutzrechtlicher Risiken (Datenschutzfolgeabschätzung) erläutert.

Den bedeutendsten Teil dieses Buches nehmen die konkreten auf die betriebliche Praxis leicht adaptierbaren Anweisungen im Datenschutz im Kapitel 7 sowie die Vertragsvorlagen für datenschutzrechtliche Vereinbarungen mit Dienstleistern in Kapitel 8 und 11 ein. Hier findet der Leser zahlreiche Beispiele aus der Praxis der Autorin, die er für seine Arbeit nutzen kann.

Weitere Abschnitte des Buches beleuchten die Auftragsverarbeitung (Kapitel 8) oder beschäftigen sich mit dem Spezialfall der Anwendung des Datenschutzes im Personalwesen (Kapitel 10). Auch hier werden Praxisbeispiele vermittelt und Vorlagen zur Adaption angeboten.

Einen nicht unerheblichen Teil der Arbeit des Datenschutzbeauftragten stellen innerbetriebliche Schulungen und Unterweisungen dar. Diesem Anspruch trägt vor allem Kapitel 12 Rechnung.

Letztlich sollen alle Aktivitäten des Datenschutzbeauftragten in einem Handbuch zusammengefasst werden (Kapitel 13). Sowohl der Aufbau der Dokumentation als auch das Vorgehen step by step werden hier beschrieben. Die Liste der Mindestregelungen für den Datenschutz kann als Leitlinie für den Datenschutzbeauftragten dienen.

Klare Grenzen sind von der Autorin des Buches hinsichtlich der technischen Umsetzung des Datenschutzes gezogen. Sie setzt vorrangig auf die Vermittlung datenschutzrechtlicher Grundsätze im Denken und Handeln, nur ansatzweise auf technische Lösungen. Hierfür existieren bereits zahlreiche Publikationsreihen am Markt, allerdings sind diese für den Einsteiger nicht selten kompliziert und schwer zu erschließen. So die Thematik des Datenschutzes und die Argumentation der Autorin richtig verstanden werden, fällt auch die Beurteilung und Auswahl der geeigneten technischen Lösung im Anschluss leicht.

Datenschutz ist ein sehr komplexes Thema. Trotz des Umfangs dieser Veröffentlichung war es nicht möglich, auf alle Aspekte des Datenschutzes einzugehen. In diesem Zusammenhang wird auf die vielfältigen Veröffentlichungen zu Spezialthemen verwiesen, u. a. durch den Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.

Das vorliegende Buch hilft dem Leser, Datenschutz in der Praxis zu regeln, diesen de facto stattfinden zu lassen und das Bewusstsein für den Datenschutz zu fördern.

2 Aufbau und wesentliche Inhalte der EU-Datenschutz-Grundverordnung (EU-DSGVO)

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 26. April 2016 (EU-DSGVO) basiert auf dem Grundrecht des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten. Mit der 1995 für alle 28 Mitgliedstaaten erlassenen europäischen Datenschutzrichtlinie wurden einheitliche Guidelines zur Umsetzung des Datenschutzes bestimmt. Alle Mitgliedstaaten veröffentlichten der europäischen Datenschutzrichtlinie folgend eigene Datenschutzgesetze. Deren praktische Umsetzung wurde jedoch auf unterschiedlichem Niveau realisiert. Mit der EU-DSGVO wird das Datenschutzrecht innerhalb der EU für den privaten und öffentlichen Bereich weitgehend vereinheitlicht. Für 500 Millionen Bürger Europas soll gleiches Recht zum Schutz der Privatsphäre gelten:

„Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden ‚Charta') sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten."

Erwägungsgrund 1, EU-DSGVO

Alle Mitgliedstaaten der EU auf ein einheitliches Vorgehen nicht nur im Grundsatz, sondern auch im Detail zu verpflichten, bedurfte etlicher Diskussionen auf inhaltlicher Ebene. Die EU-DSGVO gilt unmittelbar für jeden einzelnen Mitgliedstaat der EU. Den Mitgliedstaaten ist es grundsätzlich nicht erlaubt, die von dieser Verordnung festgeschriebenen Regelungen im Datenschutz abzuschwächen oder auch zu verstärken. Um nationale Belange dennoch berücksichtigen zu können, enthält die EU-DSGVO sogenannte Öffnungsklauseln. Diese Öffnungsklauseln erlauben es, bestimmte thematische Aspekte im Datenschutz national zu regeln. Daher spricht man im Allgemeinen von einer „Hybridlösung im Datenschutz", einem Hybrid zwischen Richtlinie und Verordnung.

Die Diskussionen um die EU-DSGVO währten mehr als 4 Jahre. Verschiedene Entwürfe der Europäischen Kommission, des Europäischen Parlaments und Rates wurden von vielen Seiten kritisiert. Auch von deutscher Seite gab es viele Einwände.

Zu den wesentlichen Kritikpunkten an den Entwürfen zur EU-DSGVO zählten:

- Bestellung von internen Datenschutzbeauftragten nur bei Unternehmen mit mehr als 250 Mitarbeitern, was eine Schwächung des Datenschutzniveaus in Deutschland und Österreich bedeutet hätte.
  - In der endgültigen Fassung der EU-DSGVO ist der verbindlich zu bestellende Datenschutzbeauftragte bei Behörden und Verantwortlichen vorgesehen, deren Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen oder in der umfangreichen Verarbeitung sensibler Daten besteht (Art. 37 Abs. 1). Gemäß Art. 37 Abs. 4 dürfen auf nationaler Ebene nun strengere Regelungen getroffen werden.
- Dokumentationspflichten nur bei Unternehmen mit mehr als 250 Mitarbeitern
  - Später wurden Dokumentationspflichten auch für kleinere Unternehmen festgelegt, sofern die Datenverarbeitung ein Risiko für die Betroffenen birgt und nicht nur gelegentlich erfolgt und die Verarbeitung sensibler Daten einschließt.
- Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) kritisierte die unkonkreten Regelungen für den Datentransfer in Drittstaaten, z. B. USA usw.

Auch nach der Verabschiedung der EU-Datenschutz-Grundverordnung blieb Kritik nicht aus, beispielsweise vom Deutschen Anwaltverein und etlichen Vertretern der Wissenschaft aus Universitäten und Hochschulen.

Unabhängig von allen Kontroversen in Europa erhoffen sich Datenschützer jenseits des europäischen Kontinents den sogenannten „California Effect", d. h. den Effekt des Nachahmens zumindest in den Grundsätzen. In den USA beispielsweise unterliegen lediglich Finanz- und Gesundheitsdaten dem Datenschutz. International agierende Konzerne sind hier die Treiber des Geschehens.

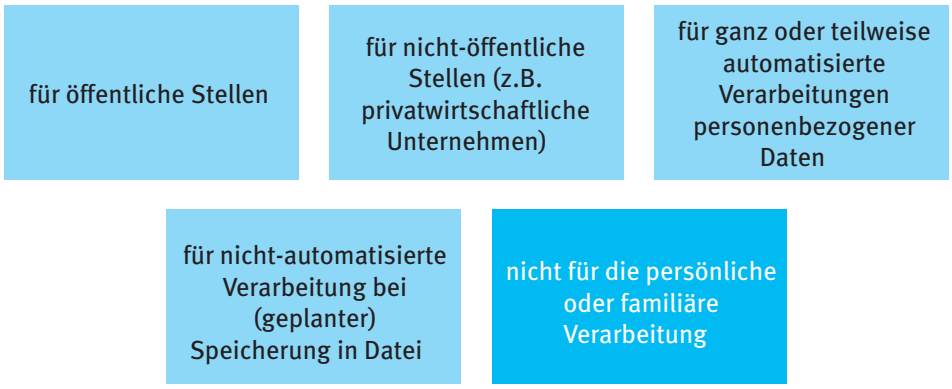
Die letzten Schritte im zeitlichen Verlauf der Vorbereitung der EU-DSGVO werden im Folgenden dargestellt:

In anderen Worten werden die Richtlinie 95/46/EG und das in Deutschland bis dato geltende „alte“ Bundesdatenschutzgesetz per Stichtag 25. Mai 2018 ungültig. Gleichzeitig läuft auch die Frist für die Meldung nationaler Umsetzungen bis 24. Mai 2018, 23.59 Uhr, aus.

Deutschland hat mit der Verabschiedung des „neuen“ Bundesdatenschutzgesetzes per 30. Juni 2017 und der Änderung des Telemedien- und Telekommunikationsgesetzes auf diese Frist rechtzeitig reagiert.

2.1 Anwendungsbereich der EU-DSGVO

Die EU-DSGVO kann auf folgende Sachverhalte angewendet werden:



Aufgrund des Risikos der Umgehung des Datenschutzes gelten die Vorschriften technologieneutral und unabhängig von jeglichem Technikzwang. Nicht der Datenschutz soll sich nach der Technik richten, sondern umgekehrt.

Weiterhin ist der Datenschutz, wie schon in der Abbildung dargestellt, sowohl auf automatisierte als auch manuelle Systeme anzuwenden.

Wenn Verarbeitungen personenbezogener Daten für private Zwecke ausgeschlossen werden, so meint die EU-DSGVO Zwecke ohne beruflichen oder wirtschaftlichen Hintergrund. Das private Tätigwerden in sozialen Netzwerken unterliegt damit nicht der EU-DSGVO. Allerdings sind die Regelungen der EU-DSGVO durch die Verantwortlichen für soziale Netzwerke oder deren Auftragsverarbeiter einzuhalten, die die Instrumente zur Verfügung stellen (EG 18). Betroffen davon sind unter anderem auch US-amerikanische Unternehmen wie Google und Facebook.

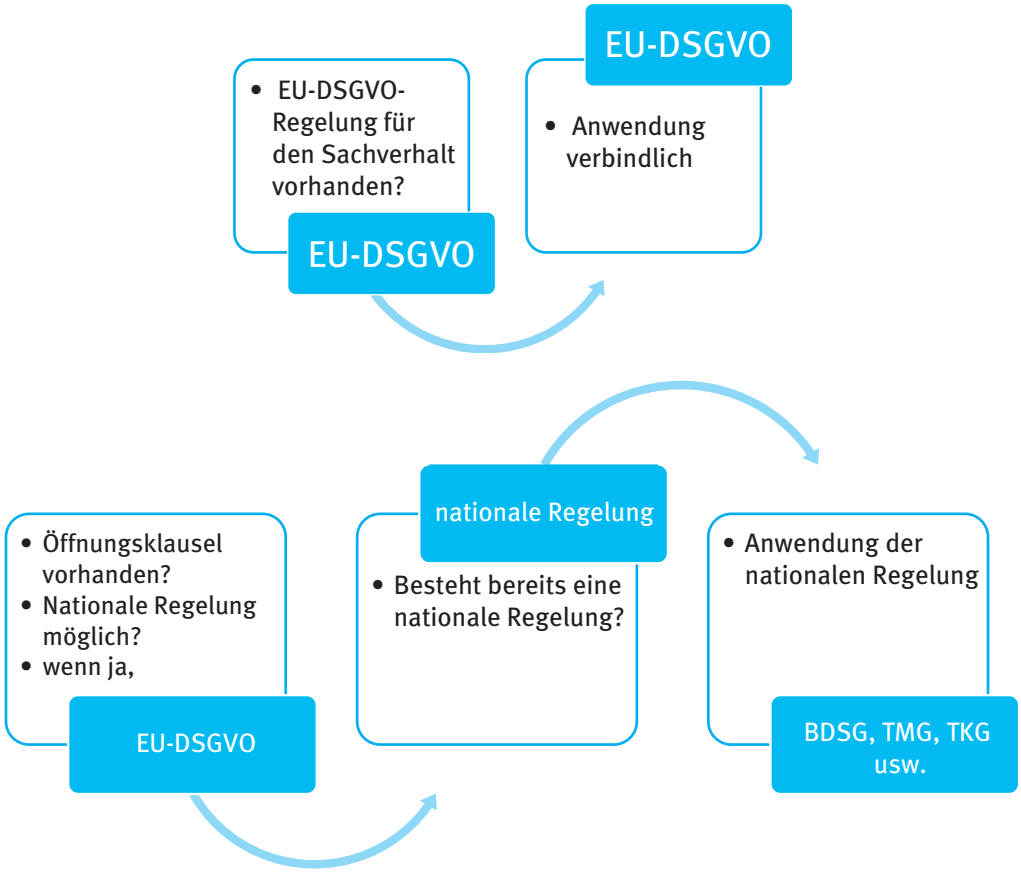
Die EU-DSGVO ist von allen Mitgliedstaaten der EU verbindlich und vorrangig anzuwenden. Sie ist nicht subsidiär, also nicht unterstützend gemeint. Sie kann durch nationales Recht flankiert werden. Die nationalen Regelungen dürfen jedoch nicht der EU-DSGVO widersprechen. In Zweifelsfällen wird das Recht durch den EuGH ausgelegt.

Um zu erkennen, welche Regelungen im Datenschutz anzuwenden sind, empfiehlt es sich, die unten abgebildete Vorgehensweise zu nutzen.

Die EU-DSGVO lässt an definierten Stellen ganz bewusst regelungsbedürftige Sachverhalte offen (Öffnungsklauseln), um dem nationalen Gesetzgeber Gestaltungsraum zu geben. Damit wird sowohl ein verbindlich einheitliches Vorgehen im Datenschutz innerhalb der EU umgesetzt als auch der Individualität und dem Freiheitsgrad der Mitglieder Rechnung getragen. Wörtlich heißt es dazu im EG 10:

„Diesbezüglich schließt diese Verordnung nicht Rechtsvorschriften aus, in denen die Umstände besonderer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.“ **EG 10, EU-DSGVO**

Zur Bestimmung, wann nationale Regelungen anwendbar sind, steht folgendes Tableau zur Verfügung.



Artikel 3 der EU-DSGVO regelt den räumlichen Anwendungsbereich der EU-DSGVO. Sie gilt für alle in der EU niedergelassenen Unternehmen (Art. 3 Abs. 1), auch wenn sie keine Verarbeitung personenbezogener Daten in der EU vornehmen. Weiterhin gilt sie für alle im EU-Raum anbietenden Unternehmen, die personenbezogene Daten von Betroffenen in der EU halten bzw. verarbeiten. Somit ist die Anwendung der EU-DSGVO bereits verpflichtend, wenn ausländische Unternehmen in der EU Offerten unterbreiten (Marktortprinzip). Dies wird im Artikel 3 Absatz 2 davon abhängig gemacht, ob das ausländische Unternehmen

- das Angebot an EU-Bürger richtet,
- eine Bestellung in einer der EU-Sprachen vorsieht,
- die Bezahlung in der Währung der EU-Bürger zulässt.

Des Weiteren ist die EU-DSGVO anzuwenden, so ein ausländisches Unternehmen das Verhalten von betroffenen Personen in der EU beobachtet.

Damit trifft der einzuhaltende Datenschutz auch viele im EU-Raum operierende ausländische Unternehmen, die sich in ihren AGB und datenschutzrechtlichen Vorgehensweisen zwingend anpassen müssen.

Im Artikel 3 Absatz 3 wird geregelt, dass die EU-DSGVO für alle Unternehmen anzuwenden ist, sofern die Verarbeitung personenbezogener Daten durch einen nicht in der EU niedergelassenen Verantwortlichen an einem Ort erfolgt, der aufgrund des Völkerrechts dem Recht eines der Mitgliedstaaten unterliegt.

2.2 Ausschlüsse aus dem Anwendungsbereich

Wie bereits dargestellt, gilt die EU-DSGVO nicht für die Anwendung im privaten und familiären Bereich. Weiterhin gilt sie gemäß EG 14 nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristisch gegründete Unternehmen einschließlich Name, Rechtsform und Kontaktdaten der juristischen Person. Sind jedoch Kontaktdaten von Ansprechpartnern, deren private Rufnummern o. Ä. angegeben, so unterliegen diese dem Datenschutzrecht.

Mit der EU-DSGVO sollte mehr Transparenz und Rechtssicherheit für kleine und mittelständische Unternehmen geschaffen werden. Die EU-DSGVO sieht in Anrechnung der Größe vieler Unternehmen eine Ausnahmeregelung für Kleinstunternehmen im Hinblick auf die Führung von Verzeichnissen vor. Ein Kleinstunternehmen ist, wer nach Art. 2 des Anhangs Empfehlung 2003/361/EG der Kommission den dort genannten Kriterien entspricht.

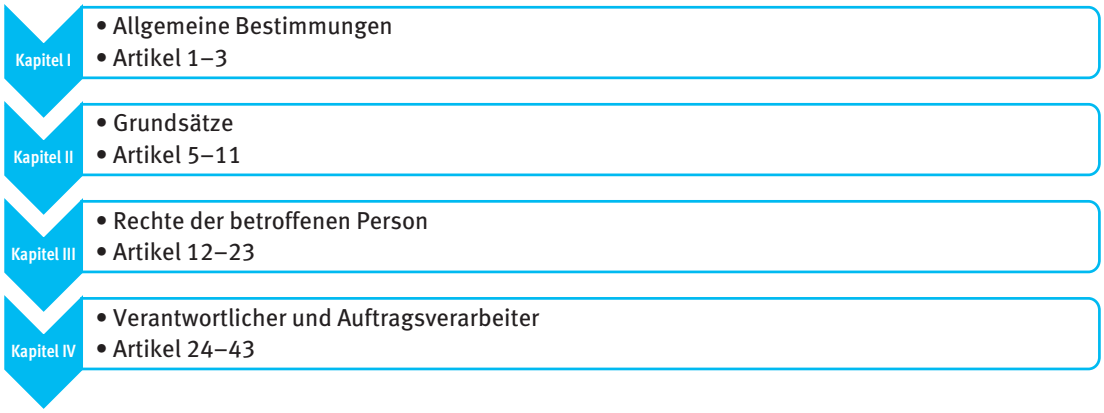
Unternehmenskategorie	Zahl der Mitarbeiter	Umsatz oder	Bilanzsumme
mittelgroß	unter 250	höchstens 50 Mio. €	höchstens 43 Mio. €
klein	unter 50	höchstens 10 Mio. €	höchstens 10 Mio. €
mikro	unter 10	höchstens 2 Mio. €	höchstens 2 Mio. €

Die EU-DSGVO gilt nicht für die Verarbeitung personenbezogener Daten Verstorbener. Hier lässt die EU-DSGVO eine Öffnung für nationale Regelungen (EG 27).

2.3 Struktur der EU-DSGVO

Die EU-DSGVO besteht aus 173 Erwägungsgründen (EG) und 99 Artikeln. Die Erwägungsgründe stellen Erläuterungen zu den einzelnen Artikeln dar, bilden Zusammenhänge ab und sind damit für die Anwendung der Artikel unerlässlich. Sie gehören zum Rechtstext und sind gleichermaßen verbindlich.

Die einzelnen Artikel der EU-DSGVO sind sachbezogen Kapiteln zugeordnet, so dass eine Auffindbarkeit von Rechtsregelungen zu bestimmten Sachthemen erleichtert wird. Hier eine Übersicht:



Kapitel V	• Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen • Artikel 44–50
Kapitel VI	• Unabhängige Aufsichtsbehörden • Artikel 51–59
Kapitel VII	• Zusammenarbeit und Kohärenz • Artikel 60–76
Kapitel VIII	• Rechtsbehelf, Haftung und Sanktionen • Artikel 77–84
Kapitel IX	• Vorschriften für besondere Verarbeitungssituationen • Artikel 85–91
Kapitel X	• Delegierte Rechtsakte und Durchführungsrechtsakte • Artikel 92–93
Kapitel XI	• Schlussbestimmungen • Artikel 94–99

2.4 Akteure im Datenschutz

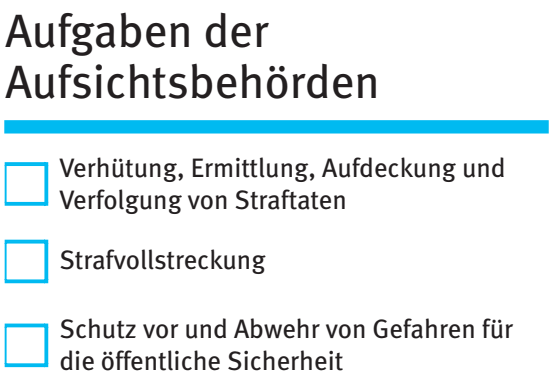
Die EU-DSGVO benennt und definiert unterschiedliche Personengruppen als Akteure im Datenschutz:

Der Verantwortliche für Datenverarbeitung personenbezogener Daten kann unter verschiedenen Bezeichnungen auftreten:

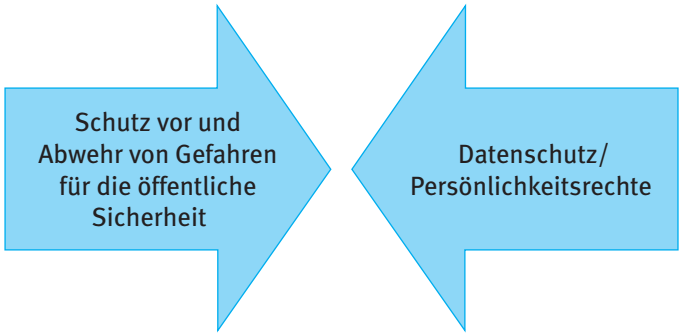
- die Hauptniederlassung
- die Niederlassung
- der (Handels-)Vertreter
- die Unternehmensgruppe (national/international)
- das Unternehmen

Sie werden durch den Inhaber oder durch die Geschäftsleitung oder den Vorstand repräsentiert.

Die Aufsichtsbehörde erfüllt im Datenschutz vorwiegend folgende Aufgaben:



Der Konflikt zwischen dem Schutz öffentlicher Interessen und dem Datenschutz ist vorprogrammiert. Auch hier bleibt von Fall zu Fall abzuwägen, welches Interesse überwiegt.



Die EU-DSGVO lässt eine Öffnungsklausel für die Verarbeitung personenbezogener Daten bei Gerichten und Justizbehörden, die einer nationalen Regelung obliegen.

2.5 Ziele der EU-Datenschutz-Grundverordnung

Der Erlass einer EU-weiten Regelung zur Verarbeitung personenbezogener Daten in Form einer Verordnung wurde aufgrund des deutlich angestiegenen Austauschs personenbezogener Daten im gewachsenen und gut funktionierenden Binnenmarkt EU notwendig. Das Unionsrecht verpflichtet die Mitgliedstaaten, immer mehr zusammenzuarbeiten und damit auch Informationen gegenseitig zugänglich zu machen. Im Erwägungsgrund (EG) 6 heißt es, dass die rasche technologische Entwicklung den Datenschutz vor neue Herausforderungen gestellt hat. Angesichts des world wide web haben die Verarbeitung und die Verarbeitungsintensität personenbezogener Daten immens zugenommen. Dem müssen datenschutzrechtliche Regelungen auf aktualisiertem Niveau folgen. Die EU-DSGVO wurde verabschiedet, um Hemmnisse im EU-Binnenmarkt abzubauen und ein gleichmäßig hohes Datenschutzniveau bei allen Mitgliedstaaten zu sichern.

Ziele der EU-DSGVO sind vor allem:

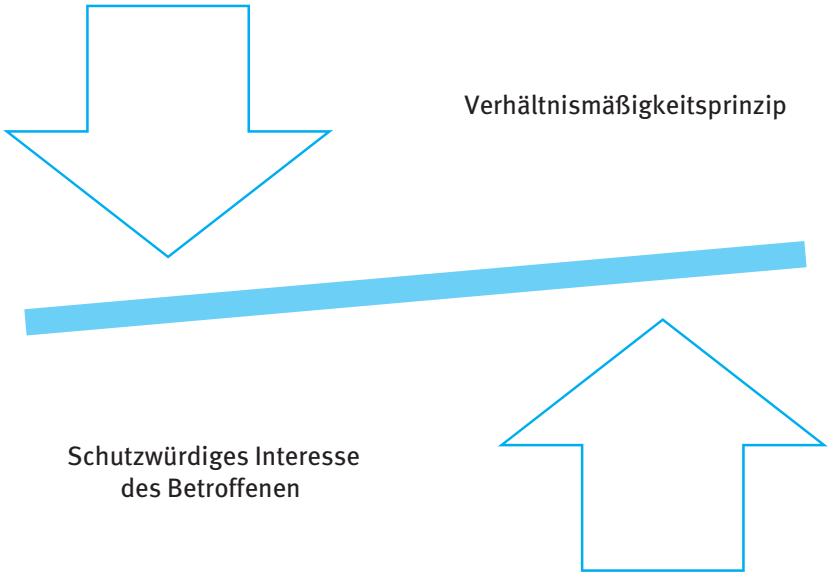
- Wahrung der Grundrechte und Grundfreiheiten
- insbesondere Wahrung des Rechts auf Schutz personenbezogener Daten ungeachtet der Staatsangehörigkeit oder des Aufenthaltsorts
- Vollendung eines Raums für
  - Freiheit
  - Sicherheit
  - Recht

- eine Wirtschaftsunion zwecks
  - wirtschaftlichen und sozialen Fortschritts
  - Stärke und Zusammenwachsens der Volkswirtschaften im Binnenmarkt EU
- freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten
- Verarbeitung personenbezogener Daten im Dienste der Menschheit

Die in der Charta verbrieften Grundrechte sind u. a.:

Der Schutz personenbezogener Daten ist indes kein uneingeschränktes Recht.

Das Recht auf Schutz personenbezogener Daten wird durch das Verhältnismäßigkeitsprinzip gebrochen. Die Verarbeitung personenbezogener Daten ist gegen andere Grundrechte abzuwägen, beispielsweise das Recht der Unversehrtheit der Person.



3 Personenbezogene Daten und ausgewählte Inhalte der EU-Datenschutz-Grundverordnung sowie des Bundesdatenschutzgesetzes (BDSG) 2018

3.1 Einführung, Aufbau und Anwendungsbereich des BDSG 2018

Der Datenschutz in Deutschland blickt auf eine mehr als 30-jährige Tradition zurück. Mit der Einführung der Datenverarbeitung in den Verwaltungen der siebziger Jahre wurden auch Diskussionen um den Datenschutz vorangetrieben. Hessen erließ dazu das erste Datenschutzgesetz 1970. Am 27. Januar 1977 folgte das erste Bundesdatenschutzgesetz (Gesetz zum Schutz vor Missbrauch personenbezogener Daten), was den Ausgangspunkt für den Erlass eigener Datenschutzgesetze auf Landesebene bildete.

Das im Jahr 2009 veröffentlichte Bundesdatenschutzgesetz geht auf die 1995 erlassene Europäische Datenschutzrichtlinie zurück, in deren Folge europäisches Recht in nationales Recht umzusetzen war. Der Erlass des Bundesdatenschutzgesetzes erfolgte erst sehr spät zum 23.05.2001.

In der Bundesrepublik Deutschland wird die Einhaltung des Datenschutzes über den Bundesdatenschutzbeauftragten der Bundesdatenschutzbehörde sowie über die Landesdatenschutzbeauftragten für jedes Bundesland überwacht.

Das im Jahr 2017 überarbeitete Bundesdatenschutzgesetz (BDSG) basierend auf der EU-Datenschutz-Grundverordnung tritt am 25. Mai 2018 mit derselben in Kraft. Es wird daher auch als Bundesdatenschutzgesetz (BDSG) 2018 bezeichnet. Mit der neuesten Fassung des Bundesdatenschutzgesetzes wird das Bundesdatenschutzgesetz 2009 komplett ersetzt. Es gliedert sich in 4 Teile:

- **Teil 1:** Gemeinsame Bestimmungen
  - Kapitel 1: Anwendungsbereich und Begriffsbestimmungen
  - Kapitel 2: Rechtsgrundlagen der Verarbeitung personenbezogener Daten
  - Kapitel 3: Datenschutzbeauftragte öffentlicher Stellen
  - Kapitel 4: Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
  - Kapitel 5: Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle, Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union
  - Kapitel 6: Rechtsbehelfe
- **Teil 2:** Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679
  - Kapitel 1: Rechtsgrundlagen der Verarbeitung personenbezogener Daten
  - Kapitel 2: Rechte der betroffenen Person
  - Kapitel 3: Pflichten der Verantwortlichen und Auftragsverarbeiter
  - Kapitel 4: Aufsichtsbehörde für die Datenverarbeitung durch nicht-öffentliche Stellen
  - Kapitel 5: Sanktionen
  - Kapitel 6: Rechtsbehelfe
- **Teil 3:** Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680
  - Kapitel 1: Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten
  - Kapitel 2: Rechtsgrundlagen der Verarbeitung personenbezogener Daten
  - Kapitel 3: Rechte der betroffenen Person

- Kapitel 4: Pflichten der Verantwortlichen und Auftragsverarbeiter
- Kapitel 5: Datenübermittlungen in Drittstaaten und an internationale Organisationen
- Kapitel 6: Zusammenarbeit der Aufsichtsbehörden

– **Teil 4:** Besondere Bestimmungen für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten

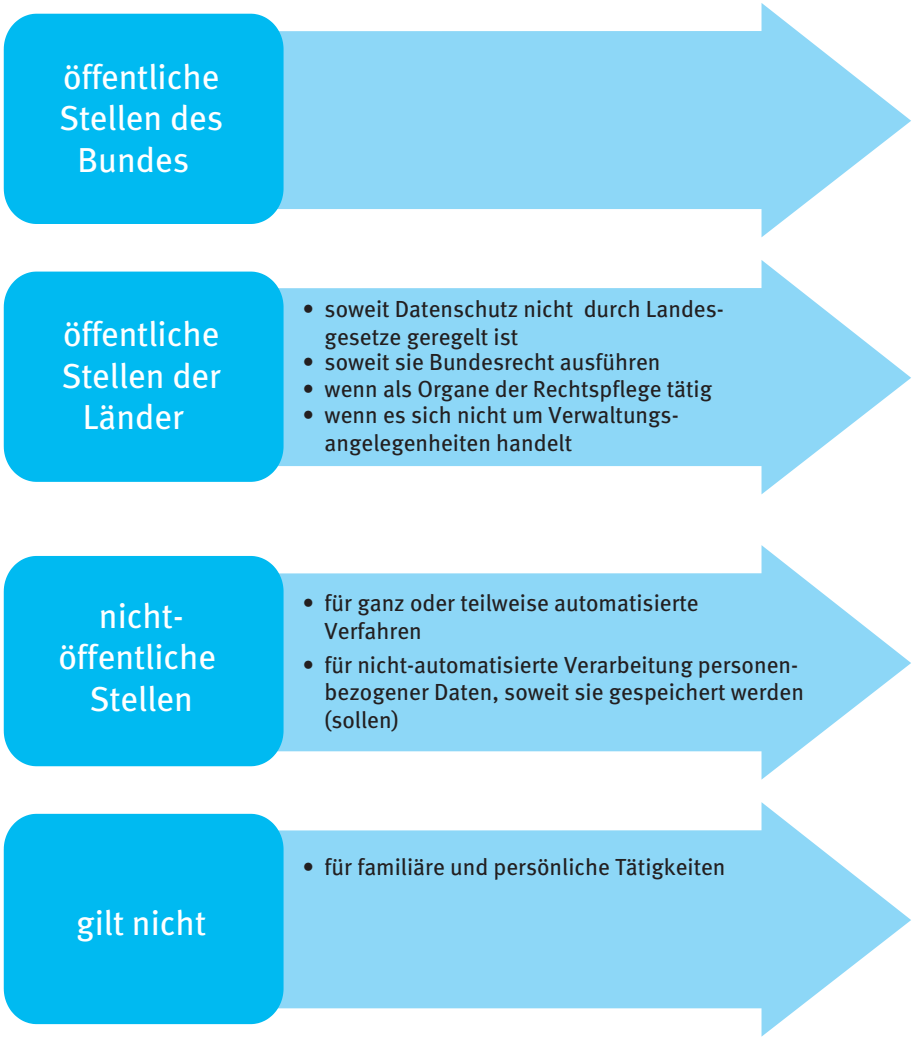
Grundsätzlich unterscheidet das BDSG zwischen einem öffentlichen Bereich (Datenverarbeitung öffentlicher Stellen) und einem nicht-öffentlichen Bereich (Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen).

In den weiteren Ausführungen dieses Buches wird **ausschließlich** auf die Datenverarbeitung **nicht-öffentlicher** Stellen eingegangen, wobei viele der hier beschriebenen und zutreffenden Regelungen im Datenschutz grundsätzlich auch für den öffentlichen Bereich Gültigkeit haben.

Auch kann aus Platzgründen nicht auf alle Belange des Datenschutzes Bezug genommen und nicht jeder Paragraph der EU-DSGVO und des BDSG 2018 im Einzelnen näher erläutert werden. Vielmehr wird der Versuch unternommen, wesentliche Zusammenhänge im Datenschutz darzustellen und Anregungen für die eigene Datenschutzpraxis zu geben mit dem Ziel der Vermeidung unbefugter Verwendung oder Weitergabe personenbezogener Daten.

Der Anwendungsbereich des neuen Bundesdatenschutzgesetzes (§ 1 BDSG) folgt den Artikeln 2 (Sachlicher Anwendungsbereich), 3 (Räumlicher Anwendungsbereich) und 90 (Geheimhaltungspflichten) der EU-DSGVO.

Das BDSG gilt für die Verarbeitung personenbezogener Daten:



Es ist nachrangig zu betrachten gegenüber:

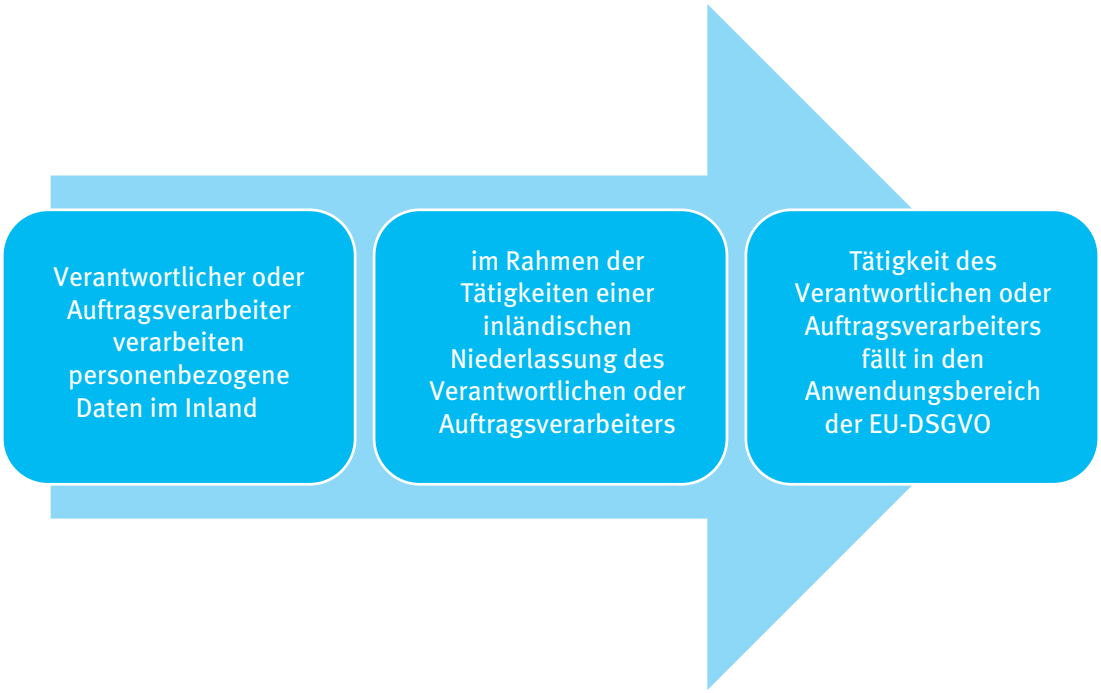
– anderen Rechtsvorschriften über den Datenschutz.

Es hat Vorrang gegenüber:

– dem Verwaltungsverfahrensgesetz.

Gesetzliche Geheimhaltungsvorschriften oder Berufs- und besondere Amtsgeheimnisse bleiben vom BDSG unberührt.

Grundsätzlich ist es anwendbar für den öffentlichen Bereich. Für den nicht-öffentlichen Bereich müssen dazu folgende Bedingungen erfüllt sein:



Weitere Besonderheiten sind:

Das BDSG gilt nicht, sofern der Sachverhalt hinreichend durch die EU-DSGVO behandelt wird (EU-Verordnung gilt unmittelbar).

Hinweis

Bei Verarbeitungen zu Zwecken Artikel 2 der Verordnung (EU) 2016/679 stehen die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und die Schweiz den Mitgliedstaaten der Europäischen Union gleich. Andere Staaten gelten als Drittstaaten (Art. 1 (6), BDSG).

Anmerkung: Artikel 2 der EU-DSGVO stellt den sachlichen Anwendungsbereich der EU-DSGVO dar.

Hinweis

Gleichstellung der Schengen-assoziierten Staaten bei Verarbeitung personenbezogener Daten zum Zwecke der Strafverfolgung und -aufklärung

Andere Staaten gelten als Drittstaaten.

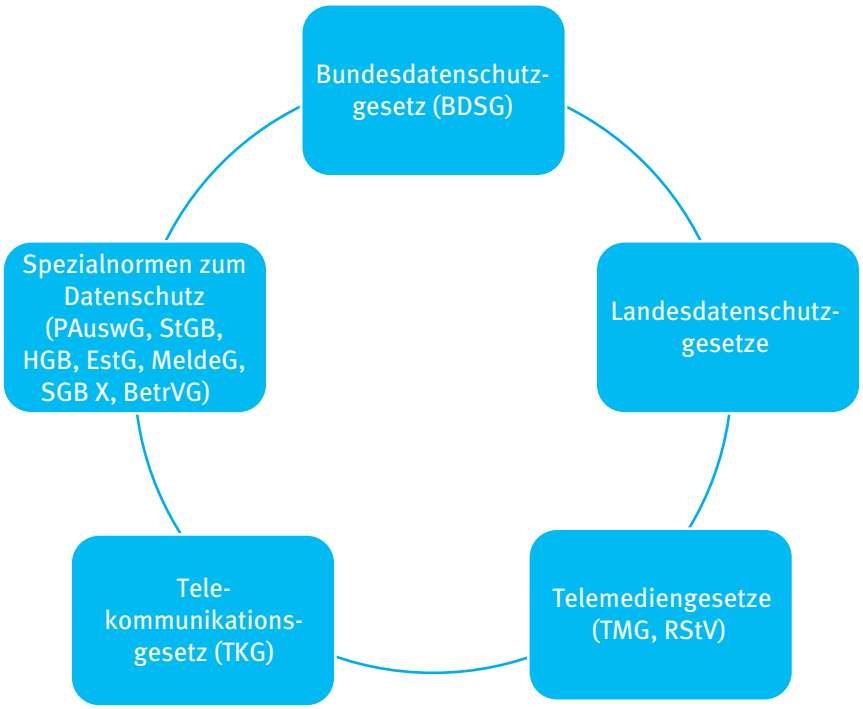
Letztlich wird das Gesetz von öffentlichen Stellen angewendet für Tätigkeiten, die nicht in den Anwendungsbereich der EU-DSGVO fallen. Dann gelten die Teile 1 und 2 des BDSG, soweit nicht in anderen Gesetzen hierzu Regelungen zu finden sind.

3.1.1 Rechtsgrundlagen des neuen Bundesdatenschutzgesetzes

Wert und Grenzen des Datenschutzes basieren u. a. auf:

- Artikel 1 und 2 des Grundgesetzes
- BVerfG-Urteil zum Schutz des Rechts auf informationelle Mitbestimmung
- EU-Datenschutz-Grundverordnung

Das Bundesdatenschutzgesetz (BDSG) regelt den Umgang mit personenbezogenen Daten in der Bundesrepublik Deutschland auf gesetzlicher Ebene. Weitere wesentliche und für den Datenschutz anzuwendende Rechtsvorschriften für den Datenschutz sind in der folgenden Übersicht dargestellt:



3.1.2 Nicht-öffentliche Stellen

Wie bereits dargestellt, gliedert sich das BDSG in zwei grundsätzliche Anwendungsbereiche auf:

- den öffentlichen Bereich und
- den nicht-öffentlichen Bereich.

Nicht-öffentliche Stellen sind alle Unternehmen, Vereine oder sonstige Vereinigungen, aber auch Niederlassungen ausländischer Unternehmen, unabhängig von der Rechtsform, die den Schutz der Daten garantieren müssen.

Letztlich sind jedoch die Beschäftigten des Unternehmens in ihrer täglichen Arbeit der Garant für die Umsetzung des Datenschutzes, sobald erforderliche datenschutzrechtliche Regelungen durch die Unternehmensleitung einmal getroffen wurden.

3.1.3 Beschäftigte nicht-öffentlicher Stellen

Unter „Beschäftigten“ fasst das BDSG folgende Personengruppen zusammen:

„(8) Beschäftige im Sinne dieses Gesetzes sind: **§ 26 BDSG**

1. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,
2. zu ihrer Berufsbildung Beschäftigte,

3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstgesetz oder dem Bundesfreiwilligendienstgesetz leisten,
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
7. Beamtinnen, Beamte, Richterinnen, Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte."

Damit erlangt das BDSG einen weit größeren Radius, als vielen bewusst ist.

3.2 Personenbezogene Daten

Personenbezogene Daten nach Definition der EU-DSGVO sind:

Art. 4 EU-DSGVO

„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;" (vgl. Merkblatt Anhang 5)

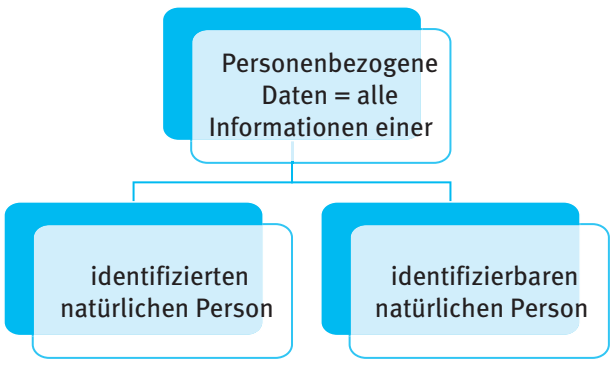
Gegenüber der Definition im „alten" Bundesdatenschutzgesetz

§ 3 (1) BDSG

„Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)."

greift die neue Definition viel weiter. Sie konkretisiert die Begrifflichkeit stärker und geht auf Aspekte der Ortung von Menschen, auf Aspekte der neuen Medien, wie der Nutzung von Online-Diensten, E-Mail und Webseiten ein.

Die nachfolgende Grafik verdeutlicht nochmals den Anwendungsbereich personenbezogener Daten:



direkt oder indirekt bestimmbar mittels Zuordnung

- zu einer Kennung (Name, Adresse, Geburtsdatum ...)
- zu einer Kennnummer (ID, Personalnummer ...)
- zu Standortdaten (Ortung mittels Mobiltelefon, Navigation ...)
- zu einer Online-Kennung (IP-Adressen, Cookie-Kennungen, die ein Gerät oder Software-Anwendungen, -Tools oder -protokolle liefern, Funkfrequenzkennungen)
- zu Merkmalen wie
  - physische
  - physiologische
  - genetische
  - psychische
  - wirtschaftliche
  - kulturelle
  - soziale Identität

Dabei ist zu beachten, dass selbst einer Pseudonymisierung unterzogene personenbezogene Daten unter Heranziehung zusätzlicher Informationen die Identität einer natürlichen Person zu erkennen geben könnten (EG 27, EU-DSGVO). In diesem Fall unterliegen selbst pseudonymisierte Daten dem Datenschutz. Zur Feststellung der Identifizierbarkeit einer natürlichen Person werden alle Mittel in Betracht gezogen, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, z. B. Aussondieren von Merkmalen zur Bestimmung einer Person. Allgemeines Ermessen bezieht sich dabei auf objektive Faktoren wie

– Kosten der Identifizierung,

– Zeitaufwand,

– verfügbare Technologie unter Berücksichtigung technologischer Entwicklungen.

Nicht unter den Datenschutz hingegen fallen anonyme Informationen (EG 27, EU-DSGVO), die so weit anonymisiert wurden, dass die betroffene Person nicht mehr identifiziert werden kann.

In der Folge trifft der Datenschutz **nicht** für die Verarbeitung anonymisierter Daten für Forschungszwecke zu.

3.2.1 Pseudonymisierung personenbezogener Informationen

Die Beschreibung des Begriffs „Pseudonymisierung“ im „alten“ BDSG sieht in ihr das Ersetzen des Namens oder anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren (§ 3 (6a), BDSG). In der Fassung der EU-DSGVO wird darüber hinausgehend definiert, dass personenbezogene Daten so weit verfremdet werden, dass nur unter Hinzuziehung zusätzlicher Informationen eine Identifikation der betroffenen Person möglich ist.

Der Pseudonymisierung personenbezogener Informationen wird in der EU-DSGVO Raum gegeben. In der Pseudonymisierung sehen die Verordnungsgeber ein probates Mittel zur Senkung des Risikos der Bestimmbarkeit natürlicher Personen, nicht ein prioritäres. Denn andererseits sollen andere oder weitere Mittel zur Durchsetzung des Datenschutzes nicht benachteiligt werden.

Pseudonymisierungen lassen allgemeine Analysen zu, die häufig in der betrieblichen Praxis zur Auswertung von Daten und Ableitung von Maßnahmen unabdingbar sind. Soweit der Verantwortliche für die Verarbeitung die entsprechenden technischen und organisatorischen Maßnahmen zur Einhaltung der Anforderungen der EU-DSGVO und des BDSG 2018 getroffen hat, kann die Verarbeitung der pseudonymisierten Informationen auch bei ihm stattfinden, vorausgesetzt, die zur Identifizierung einer natürlichen Person vorhandenen Zusatzinformationen werden getrennt gehalten und verarbeitet. Alle Personen, die befugt sind, Einsicht in die Identität der Personen zu nehmen, müssen namentlich dem Verarbeiter bekannt und dokumentiert sein.

3.2.2 Gesundheitsbezogene personenbezogene Daten

Zu den gesundheitsbezogenen Daten zählen alle Daten, die sich auf den Gesundheitszustand einer betroffenen Person beziehen, nämlich

Informationen über den

- früheren
- gegenwärtigen und
- künftigen

körperlichen und geistigen Gesundheitszustand.

Dies betrifft auch Informationen über die natürliche Person im Zuge der Anmeldung und Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates.

Im Einzelnen unterliegen dabei dem Datenschutz (EG 35, EU-DSGVO):

Unabhängig von der Herkunft der Daten (Arzt, Angehöriger eines Gesundheitsberufs, Krankenhaus, Medizinprodukt, In-vitro-Diagnostikum)		
Nummern, Symbole, Kennzeichen zur Identifizierung einer natürlichen Person (z. B. Patientennummer)	Informationen von der Prüfung oder Untersuchung eines Körperteils, einer körpereigenen Substanz, aus genetischen Daten oder biologischen Proben stammend	Informationen über Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen, physiologischen oder biomedizinischen Zustand

3.2.3 Personenbezogene Daten von Kindern

Auf das Recht des Kindes wird in der EU-DSGVO und in der Folge auch im BDSG 2018 besonderes Augenmerk gerichtet. Sie können Risiken, Folgen und Garantien nicht abschätzen und sind sich ihrer Rechte nicht ausreichend bewusst. Besonderer Schutz gilt daher

der Verwendung von personenbezogenen Daten von Kindern

- zu Werbezwecken,
- für die Erstellung von Persönlichkeits- oder Nutzerprofilen,

der Erhebung personenbezogener Daten von Kindern

- bei der Nutzung von Diensten.

3.2.4 Besondere Kategorien personenbezogener Daten

Unter besonderen Kategorien personenbezogener Daten versteht die EU-DSGVO in Art. 9

Art. 9 EU-DSGVO

„Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person …“

Die Verarbeitung dieser Daten ist untersagt. Ausnahmen davon sind im Art. 9 EU-DSGVO näher geregelt.

3.3 Wichtige Definitionen

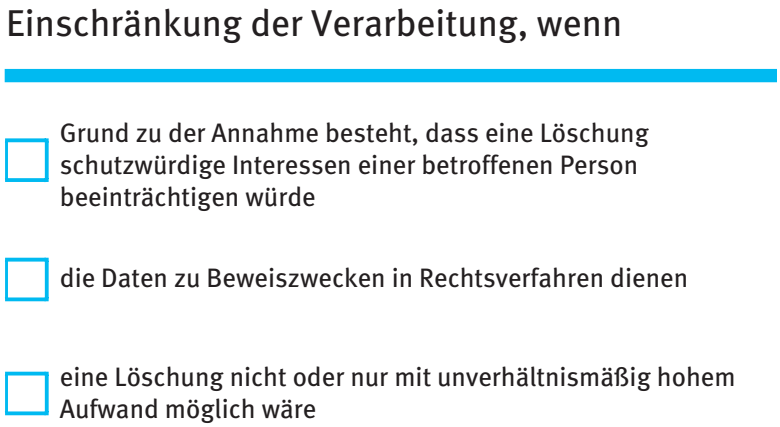
Zur Klärung, wie bestimmte Termini im Datenschutzrecht verwendet werden können, werden im Art. 4 EU-DSGVO Begriffsbestimmungen vorgenommen. Danach bezeichnet der Ausdruck

– **Verarbeitung:**

– **Einschränkung der Verarbeitung:**

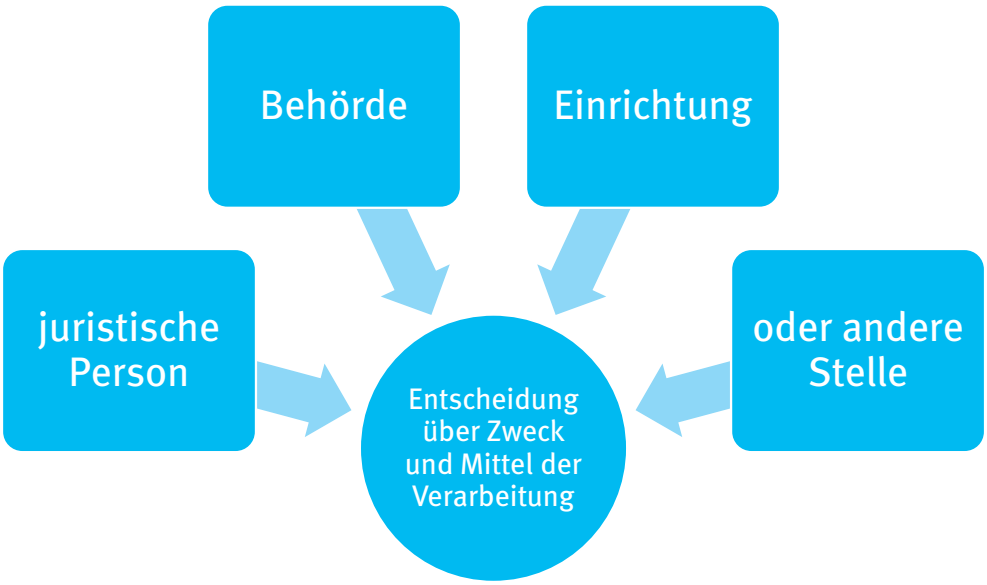
„die Markierung gespeicherter personenbezogener Daten mit dem Ziel der künftigen Einschränkung der Verarbeitung“

Nähere Erläuterungen dazu findet der Leser im Abschnitt „Recht auf Berichtigung, Ergänzung und Löschung personenbezogener Daten“ sowie im Anhang zu diesem Buch.



(vgl. Anhang 8 und 14)

– **Verantwortlicher:**



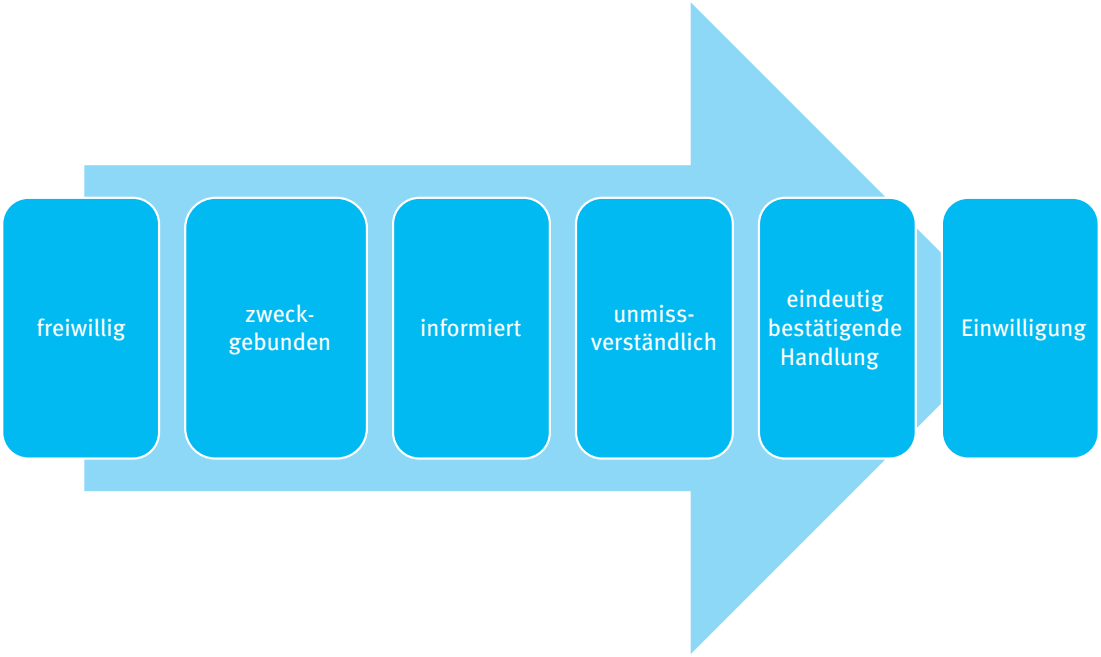
Nähere Erläuterungen dazu siehe Kapitel 4.1.1.

– **Auftragsverarbeiter:**

Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen (juristische Person, Behörde, Einrichtung oder andere Stelle), die Verantwortung für die ordnungsgemäße Verarbeitung verbleibt beim Verantwortlichen

Nähere Erläuterungen dazu siehe Kapitel 8.

– **Einwilligung:**



Im Unterschied zum „alten" BDSG bedarf es hier einer bestätigenden, d. h. eindeutig bejahenden Reaktion des Betroffenen zur Einwilligung. Nicht: „So Sie kein Mitschneiden dieses Telefonats zu Qualitätssicherungsgründen wünschen, drücken Sie 1", sondern genau anders herum.

„So Sie einer Aufnahme zu Qualitätssicherungsgründen zustimmen, drücken Sie 1".

Die Einwilligung muss bewusst hervorgehoben werden.

– **Verletzung des Schutzes personenbezogener Daten:**

Verletzung der Sicherheit, welche unbewusst oder unrechtmäßig

- zur Vernichtung,
- zum Verlust,
- zur Veränderung,
- zur unbefugten Offenlegung von,
- zum unbefugten Zugang zu

personenbezogenen Daten führt.

Nähere Erläuterungen dazu findet der Leser unter „Rechtmäßigkeit der Einwilligung" (Kapitel 3.7).

3.4 Informationelle Selbstbestimmung und Rechtmäßigkeit der Verarbeitung personenbezogener Daten

Jede natürliche Person hat das Recht auf Schutz personenbezogener Daten und auf Mitbestimmung bei der automatisierten Verarbeitung oder Strukturierung von Angaben über die Person. Folglich gilt der Datenschutz nicht für juristische Personen, wie z. B. Aktiengesellschaften, Gesellschaften mit beschränkter Haftung u. Ä.

Datenschutz dient somit dem Persönlichkeitsschutz. Der Bereich der privaten Lebensführung soll dem Zugriff staatlicher und privater datenverarbeitender Stellen bewusst entzogen werden.

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten ist gemäß Art. 6 EU-DSGVO an folgende Bedingungen geknüpft:

Einwilligungserklärung des Betroffenen	• für einen bestimmten Zweck • für mehrere bestimmte Zwecke
Verarbeitung für die Erfüllung eines Vertrags	• Vertragspartei muss die betreffende Person sein • auf Anfrage des Betroffenen für vorvertragliche Maßnahmen erforderlich
Erfüllung rechtlicher Verpflichtungen*	• Erfüllung rechtlicher Verpflichtungen des Betroffenen
erforderliche Verarbeitung zur Erfüllung lebenswichtiger Interessen	• zum Schutz des Betroffenen oder anderer natürlicher Personen
zur Wahrnehmung einer Aufgabe öffentlichen Interesses oder in Ausübung öffentlicher Gewalt*	• Zweck muss in der Rechtsgrundlage festgelegt sein oder • für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt
Erforderlichkeit der Verarbeitung zur Wahrung eines berechtigten Interesses des Verantwortlichen oder eines Dritten	• Abwägungsgrundsatz zwischen berechtigtem Interesse und Interessen, Grundrechten und Grundfreiheiten der betroffenen Person • insbesondere bei Kindern • gilt nicht für die von Behörden vorgenommene Verarbeitung zur Erfüllung ihrer Aufgaben

* Die Rechtsgrundlage wird entweder durch
- Unionsrecht oder
- das Recht der Mitgliedstaaten

festgelegt.

An dieser Stelle wird bewusst den Mitgliedstaaten die Möglichkeit eröffnet, eigene Rechtsgrundlagen auszugestalten, z. B. hinsichtlich

- allgemeiner Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen
- der Arten personenbezogener Daten
- der betroffenen Personen
- der Einrichtungen, an die personenbezogene Daten offengelegt werden sollen/können
- der Zwecke der Offenlegung
- der Zweckbindung
- der Speicherdauer
- der anzuwendenden Verarbeitungsvorgänge und -verfahren
- der Gewährleistung der Verarbeitung personenbezogener Daten nach Treu und Glauben

Eine Checkliste zur Feststellung, ob eine Verarbeitung personenbezogener Daten rechtmäßig erfolgt oder nicht, ist im Anhang zu diesem Buch enthalten (siehe Anhang 6).

3.5 Grundsätze des Datenschutzes

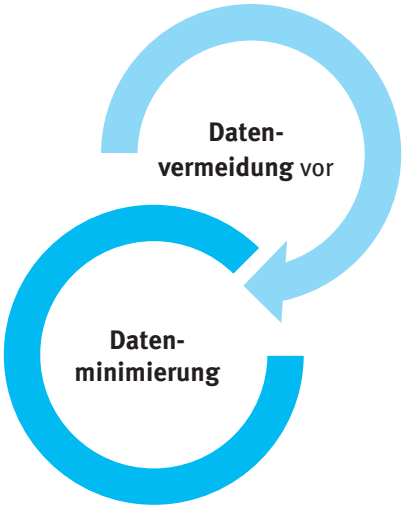
Die Legitimität der Erhebung und Verarbeitung personenbezogener Daten folgt sogenannten Grundsätzen der Verarbeitung. Sie sind im Artikel 5 der EU-DSGVO beschrieben:

Tabelle 1: Grundsätze der Verarbeitung personenbezogener Daten gemäß Art. 5 EU-DSGVO

Grundsatz	Interpretation	EG
Rechtmäßigkeit	Rechtmäßigkeit durch Einwilligung oder eine andere zulässige Rechtsgrundlage der EU oder eines Mitgliedstaates (Rechtspflicht, Vertrag, Vorvertrag) zum Schutz lebenswichtiger Interessen des Betroffenen oder einer anderen natürlichen Person im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt	40, 42, 44, 45, 46, 47
Treu und Glauben	Verlässlichkeit, Redlichkeit, Anstand	Art. 5 Abs. 1a
Transparenz	Gewährleitung von Nachvollziehbarkeit Festlegung von Löschfristen oder regelmäßige (definierte Zeiträume) Überprüfung auf Löschbarkeit umfangreiche Information des Betroffenen über die Verarbeitung	39, 42, 58, 60, Art. 5 Abs. 2, Art. 12
Zweckbindung	festgelegte, legitime und eindeutige Zwecke	39
Datenminimierung	Beschränkung der Verarbeitung auf das dem Zweck entsprechende notwendige Maß	39
Richtigkeit	Daten sind aktuell und zutreffend	Art. 5 Abs. 1 d
Speicherbegrenzung	nach Wegfall des Zwecks Löschung	Art. 5 Abs. 1 d
Integrität und Vertraulichkeit	Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, vor Verlust oder Beschädigung	Art. 5 Abs. 1 f
Nachweisbarkeit der Einhaltung getroffener Datenschutzmaßnahmen	Rechenschaftspflicht über Einhaltung der Datenschutzmaßnahmen	Art. 5 Abs. 2

Zur weiteren Erläuterung der Verarbeitung nach Treu und Glauben ist auszuführen, dass hierunter im EG 39 EU-DSGVO vor allem die Transparenz der Verarbeitung zu verstehen ist. Der Betroffene soll wissen, welche personenbezogenen Daten von ihm erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden. Des Weiteren soll ihm bekannt gemacht werden, in welchem Umfang seine Daten jetzt oder auch noch später verarbeitet werden.

Auf den Grundsatz der Datenminimierung soll an dieser Stelle näher eingegangen werden. Es versteht sich von selbst, dass nicht erhobene personenbezogene Daten selbstverständlich auch nicht geschützt werden müssen. Wer vorher bedenkt, welche personenbezogenen Daten wirklich unerlässlich für die Erfüllung einer Arbeitsaufgabe sind, trägt am besten zum Datenschutz bei. Denn häufig sind die Löschrechte der betroffenen Personen nur eingeschränkt technisch umsetzbar oder bedeuten einen unverhältnismäßig hohen Aufwand. Der Grundsatz der Datenvermeidung, Datensparsamkeit und Datenminimierung ist daher von praktischer Bedeutung. In einem Merkblatt zur Datenminimierung sind Hinweise für die praktische Umsetzung dieser Forderung gegeben. Die Handlungsanleitung geht in der Rangfolge der Vermeidung personenbezogener Daten, der Datenminimierung und Pseudonymisierung vor:



Der Grundsatz der Datenminimierung ist bereits vor Erhebung der personenbezogenen Daten anzuwenden. Ist eine Verarbeitungsstruktur einmal vorhanden, wird sie auch genutzt. Sie automatisiert sich quasi. Die Reduktion der Datenquantität und auch, so möglich, der Datenqualität ist daher der Schlüssel für einen guten Datenschutz in der Praxis (vgl. Anhang 4).

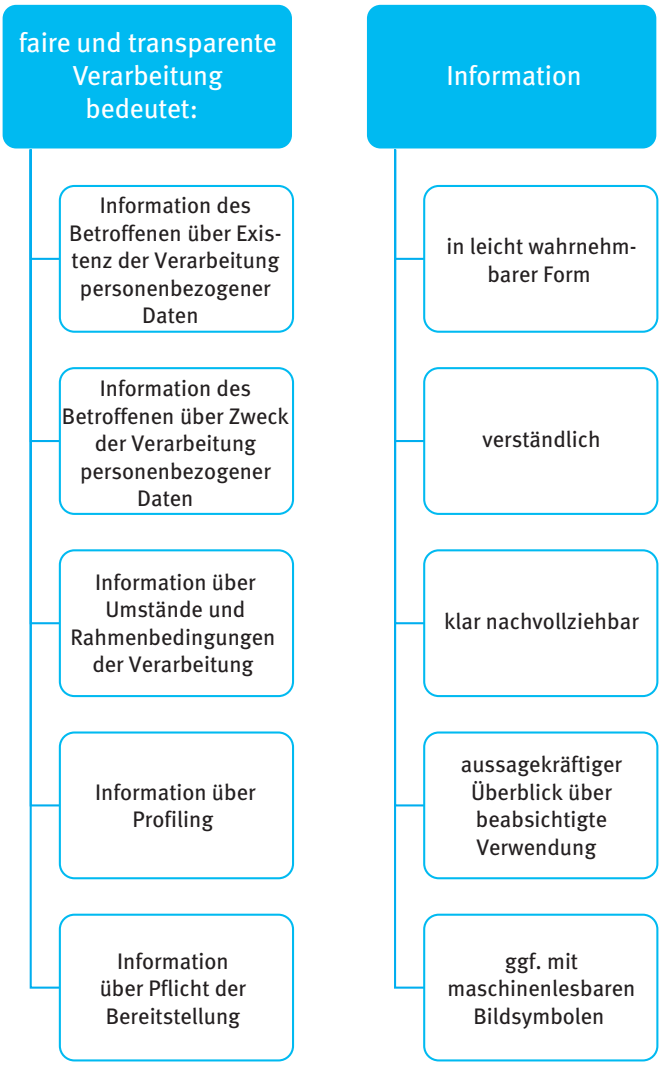
Der Grundsatz der Datenminimierung stellt auch einen Appell an die Verantwortlichen für die Verarbeitung personenbezogener Daten dar, jene technischen Systeme bzw. softwaretechnischen Lösungen zu wählen, die mit möglichst wenig personenbezogenen Daten auskommen.

Für die praktische Umsetzung der Datenminimierung wurde ein Merkblatt entwickelt. Das Merkblatt kann entweder als Aushang oder auch zur Sensibilisierung der für die Verarbeitung personenbezogener Daten verantwortlichen Mitarbeiter dienen, siehe Merkblatt „Grundsätze des Datenschutzes“, Merkblatt „Datenminimierung“.

3.6 Informationspflichten zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten

Gemäß EG 39 EU-DSGVO bestehen Informationspflichten zur Verarbeitung personenbezogener Daten gegenüber dem Betroffenen. Diese Informationen zur Verarbeitung der personenbezogenen Daten müssen

- vollständig und
- dem Betroffenen leicht zugänglich sowie
- in verständlicher und klarer Sprache abgefasst sein.



Die Informationen müssen insbesondere den Verantwortlichen für die Verarbeitung namentlich ausweisen. Sie müssen den Zweck der Verarbeitung benennen.

Grundsätzlich wird dem Betroffenen das Recht eingeräumt, eine Auskunft oder eine Bestätigung zu erhalten, welche personenbezogenen Daten verarbeitet werden, vgl. hierzu Checkliste zu Auskunftsrechten des Betroffenen.

Konkrete Informationspflichten gegenüber dem Betroffenen bestehen darüber hinaus zu

- Aufklärung über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten
- Aufklärung, wie der Betroffene seine Rechte geltend machen kann
- Eindeutigkeit und Rechtmäßigkeit des Zweckes, für den personenbezogene Daten erhoben werden
- Angemessenheit und Erheblichkeit der erhobenen personenbezogenen Daten im Hinblick auf den Zweck
- Beschränkung des Umfangs erhobener personenbezogener Daten auf das notwendige Mindestmaß (Datenminimierung/Datensparsamkeit)
- Beschränkung der Speicherfrist auf das zulässige Minimum
- Festlegung der Frist, in welcher die Löschbarkeit der Daten überprüft wird
- Zumutbarkeit der Verarbeitung personenbezogener Daten in Abgrenzung zur Erfüllung des Zwecks mit anderen möglichen Mitteln
- Verankerung des Rechts auf Berichtigung, Änderung, Löschung falscher Daten
- Garantie für die Gewährleistung der sicheren Verarbeitung personenbezogener Daten
- Garantie der Begrenzung des Zugangs zu Daten und EDV-Technik durch Unbefugte.

Hinweis

Zu betonen bleibt, dass der Zweck der Verarbeitung personenbezogener Daten vor der Erhebung feststehen muss. Eine vorratsmäßige Erhebung personenbezogener Daten auf einen künftig sich eventuell eröffnenden Verwendungszweck ist nicht möglich.

Die EU-DSGVO und das BDSG 2018 regeln die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für geschäftliche Zwecke, ausgenommen sind rein private oder familiäre Zweckbestimmungen.

Hinweis

Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen.

Vor neuen Arten von Erhebungen ist die Zulässigkeit des Verarbeitungszwecks personenbezogener Daten durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. Gleichzeitig hat der für die Verarbeitung Verantwortliche vor der Erhebung bzw. Verarbeitung von Daten schriftlich festzulegen, ob und in welcher Art und Weise der gesetzlichen Informationspflicht des Betroffenen zu genügen ist.

Aus dem EG 39 EU-DSGVO abgeleitet entstehen Informationspflichten hinsichtlich der Verarbeitung personenbezogener Daten gegenüber

1) Kunden,
2) Lieferanten und Dienstleistern,
3) Beschäftigten gemäß Definition,
4) Kooperationspartnern u. a.,

soweit personenbezogene Daten erhoben bzw. verarbeitet werden sollen.

Die Information hat schriftlich und initiativ zu erfolgen. Sie muss vor der Erhebung der personenbezogenen Daten erfolgen.

Bei bestehenden Kunden- und Lieferantenbeziehungen oder Beschäftigungsverhältnissen muss eine Aufklärung im Nachhinein erfolgen, ebenso aktiv, schriftlich und in leicht verständlicher Form (Stichwort: Transparenz).

Im Anhang zum Buch sind Checklisten für die Umsetzung der Informationspflichten angeführt (Anhang 1). Sie sollen dem Leser helfen, der Informations- und Aufklärungspflicht vollständig gerecht zu werden.

3.7 Rechtmäßigkeit der Einwilligung

Vorausgesetzt, die Anforderungen an die Rechtmäßigkeit der Verarbeitung personenbezogener Daten nach Artikel 47 des BDSG sind erfüllt und die Verarbeitung kann aufgrund einer Rechtsvorschrift auf der Grundlage einer Einwilligung erfolgen, muss der Verantwortliche die Einwilligung des Betroffenen nachweisen können (Artikel 7 Abs. 1 EU-DSGVO). Sie muss daher in schriftlicher oder elektronischer Form unter aktiver Einwilligung des Betroffenen erfolgen.

Sie muss klar und verständlich und in einfacher Sprache gefasst sein, um zu vermeiden, dass die betroffene Person Einwilligungen für die Verarbeitung personenbezogener Daten tätigt, die sie so nicht gewollt hat. Der Text muss so verständlich formuliert werden, dass die betroffene Person die Folgen der Verarbeitung der betreffenden personenbezogenen Daten abschätzen kann. Für Kinder können auch Icons verwendet werden.

Auf freiwillige Angaben, die über den Zweck der Verarbeitung hinausgehen, ist explizit hinzuweisen, z. B. „*“ für „freiwillige Angaben“. D. h. es wird zwischen Pflicht- und optionalen Angaben des Betroffenen unterschieden.

Bei der Einwilligung zum Empfang von Newslettern hat sich gerichtlich bereits das Double-opt-in-Verfahren durchgesetzt. Das bedeutet konkret:

- E-Mail mit Verweis auf E-Mail-Verfahren, die den Inhalt der Werbeeinwilligung enthält
- Bestätigungslink mit direkter Ansprache
- durch Aufrufen des Bestätigungslinks wird erst die erste Lieferung ausgelöst.

Dies entspricht der aktiven Form der Bestätigung, da der Betroffene aktiv tätig werden muss.

In Erklärungen, die auch noch andere Sachverhalte betreffen, ist die Einwilligungserklärung separat von anderen Inhalten hervorzuheben und zu zeichnen. Es besteht ein Kopplungsverbot, d. h. der Betroffene darf nicht mit der Unterzeichnung eines Vertrags beispielsweise gezwungen sein, gleichermaßen bestimmte personenbezogene Daten von ihm preiszugeben, die nichts mit der Vertragserfüllung zu tun haben. Folglich gibt es eine Unterschriftenzeile für den Vertrag und eine separate Unterschriftenzeile für die Einwilligung zur Verarbeitung personenbezogener Daten.

Die Einwilligung kann von der betroffenen Person jederzeit widerrufen werden. Ein Hinweis darauf ist im Text der Einwilligungserklärung vorzuhalten. In der Einwilligungserklärung muss zudem der Zweck der Verarbeitung benannt sein. Dieser Zweck kann nicht pauschal formuliert werden. Um zu vermeiden, dass personenbezogene Daten quasi auf Vorrat erhoben werden, ist der Zweck der Verarbeitung stets sehr konkret und möglichst fallbezogen zu halten. Somit können einmal gegebene personenbezogene Daten nicht einfach auf andere Zwecke übertragen und ggf. missbraucht werden. Eine frühzeitige Löschung der personenbezogenen Daten nach Erledigung der Angelegenheit ist empfehlenswert, soweit hier nicht rechtliche Aufbewahrungspflichten entgegenstehen.

Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, muss die Einwilligungserklärung auch konkret auf diese Daten bezogen sein.

3.7.1 Wirksamkeit der Einwilligung des Betroffenen, § 51 BDSG

Die Wirksamkeit einer Einwilligung hängt maßgeblich von der Freiwilligkeit ab. An diesem Punkt haben sich etliche Rechtsstreitigkeiten entzündet. Die Freiwilligkeit der Einwilligung ist bei abhängig Beschäftigten immer in Frage zu stellen und bemisst sich am konkreten Fall und der Angemessenheit bezüglich der Herausgabe personenbezogener Daten.

Die Einwilligung des Betroffenen setzt zudem dessen ausreichende Kenntnis bzw. Information über den Erhebungs-, Nutzungs- und Verarbeitungszweck und die spätere Verwendung personenbezogener Daten voraus. Die betroffene Person muss auch über die Folgen der Nicht-Einwilligung belehrt werden.

Grundregeln für eine ordnungsgemäße Einwilligung sind:

- Wahl der Schriftform
- optische Hervorhebung der Einwilligung in Texten (z. B. Vertragstexten)
- ausdrückliches Hervorheben besonderer personenbezogener Daten, z. B. von sensiblen Daten
- absolute Datensparsamkeit, d. h. nur Einwilligung für die unbedingt notwendigen personenbezogenen Daten.

Unter **besonderen Kategorien personenbezogener Daten** werden vor allem Angaben über

- rassische, ethnische Herkunft
- politische Meinungen
- religiöse oder philosophische Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit oder Sexualleben

verstanden. Die Einwilligungserklärung muss konkret auf die zu verarbeitenden personenbezogenen Daten ausgerichtet sein (§ 51 (5)).

Hinweis

Einwilligung in elektronischer Form

- bewusste und eindeutige Erklärung der Einwilligung des Betroffenen
- Protokollierung der Einwilligung
- jederzeitige Abrufbarkeit des Inhalts der Einwilligung
- jederzeitige Widerrufsmöglichkeit als Bestandteil der Einwilligungserklärung
- möglichst Double-opt-in-Verfahren nutzen

Hinweis

Einwilligung per Telefon

- aktive Einwilligung am Telefon („Wenn Sie damit einverstanden sind, drücken Sie 1“)
- Inhalt der Einwilligung nachträglich schriftlich zusenden
- Hinweis auf jederzeitigen Widerruf der Einwilligung (durch Rückruf des Kunden möglich)

Die bisherigen Einwilligungserklärungen sollen ihre Gültigkeit gemäß EG 171 EU-DSGVO nicht verlieren. Aufgrund der hohen Sanktionen in diesem Bereich erscheint es jedoch sinnvoll, diese Einwilligungserklärungen nochmals zu überprüfen und für die Zukunft neu abzuschließen.

Eine Verarbeitung der erhobenen personenbezogenen Daten darf nur auf Weisung des Verantwortlichen erfolgen (§ 52 BDSG). Damit soll die unbefugte Verarbeitung unterbunden werden. Die zugangsberechtigten Mitarbeiter eines Bereichs können daher nur mit Weisung des Vorgesetzten bzw. des für die Verarbeitung Verantwortlichen tätig werden. Sie sind überdies auf das Datengeheimnis zu verpflichten, welches ihnen untersagt, personenbezogene Daten unbefugt zu verarbeiten. Die Verpflichtung auf das Datengeheimnis wird mit Aufnahme der Tätigkeit unterzeichnet und muss auch dann noch befolgt werden, wenn das Beschäftigungsverhältnis bereits geendet hat (§ 53 BDSG).

3.8 Datengeheimnis

Im BDSG § 53 wird das Datengeheimnis geregelt. Personenbezogene Daten dürfen nicht unbefugt durch mit der Datenverarbeitung personenbezogener Daten befasste Personen verarbeitet werden.

Hinweis

Verpflichtung aller mit der Datenverarbeitung personenbezogener Personen auf das Datengeheimnis:

- schriftlich
- mit dem Hinweis, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht

3.9 Rechte der betroffenen Person

Jeder Betroffene hat das Recht auf

- Berichtigung
- Ergänzung
- Löschung
- Sperrung

von personenbezogenen Daten.

Über die Vorgehensweise zur Umsetzung der Rechte des Betroffenen auf Berichtigung, Ergänzung, Löschung und eingeschränkte Verarbeitung von personenbezogenen Daten sind eine Checkliste sowie eine Verfahrensanweisung dem Anhang zu entnehmen.

Das Gesuch setzt voraus, dass der Betroffene in Kenntnis ist, wer über ihn welche personenbezogenen Daten verarbeitet, speichert oder gespeichert hat. Auf diesbezügliche Informationspflichten wurde andernorts bereits hingewiesen.

So von der Informationspflicht abgewichen werden kann, sollte dies begründet werden und schriftlich erfolgen.

Hinweis

Schriftform für Festlegung: Die Festlegung, ob von einer Benachrichtigung abgesehen werden kann, trifft die verantwortliche Stelle in Schriftform.

Wird dem Betroffenen ein Schaden zugefügt, z. B. durch unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner Daten, ist die verantwortliche Stelle (Unternehmen) zum Schadenersatz verpflichtet.

Der Schadenersatzanspruch bezieht sich auf entstandene Schäden (z. B. Vermögenseinbußen) und immaterielle Schäden (z. B. schwere Verstöße im Hinblick auf die Verletzung des Persönlichkeitsrechts).

Vermögenseinbußen können beispielsweise bei Kreditanfragen durch unrichtige Speicherung von Arbeitsstellen, Einkünften u. Ä. entstehen.

Eine Schadenersatzpflicht entfällt dann, wenn die verantwortliche Stelle die notwendige Sorgfalt für den Sachverhalt walten ließ. Dies ist selbstverständlich durch die verantwortliche Stelle unter Beweis zu stellen. Eine Exkulpation ist bei Organisationsverschulden nicht möglich.

3.10 Auskunftsrecht des Betroffenen

Neben der Benachrichtigung des Betroffenen gemäß § 57 BDSG hat die verantwortliche Stelle dem Betroffenen Auskunft zu erteilen,

- welche Daten
- von wem

– zu welchem Zweck erhoben oder gespeichert und
– an wen übermittelt

werden.

Das Auskunftsrecht ist dem Betroffenen unentgeltlich zu gewähren. Er hat dieses Recht jederzeit und kann es auch mehrfach ausüben. Über diese Rechte ist der Betroffene ausreichend zu informieren. Eine Checkliste, in der die konkreten Auskunftspflichten gelistet sind, ist dem Anhang zu diesem Buch zu entnehmen (Anhang 2).

Die Rechte des Betroffenen auf Auskunft haben sich in den letzten Jahren zunehmend verschärft. Der Gesetzgeber legt Wert auf eine umfassende Information des Betroffenen, was mit seinen personenbezogenen Daten geschieht. Gleichzeitig verpflichtet er den Betroffenen, die Art der personenbezogenen Daten, über die er Auskunft verlangt, näher zu spezifizieren, und belässt der verantwortlichen Stelle das Recht auf Auskunftsverweigerung, soweit das Geschäftsgeheimnis das Informationsinteresse des Betroffenen überwiegt.

Die Festlegungen im BDSG gelten an dieser Stelle auch für nicht-automatisierte Dateien bzw. Daten.

Der Aufwand zur Umsetzung der Auskunftspflicht der verantwortlichen Stelle darf dem Betroffenen nicht in Rechnung gestellt werden.

Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur herausgegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse besteht und die Identität des Anfragenden zweifelsfrei feststeht. Die Verantwortung hierfür trägt die übermittelnde Stelle. Im Zweifel ist der DSB zu kontaktieren. Vgl. Checkliste zu Auskunftsrechten des Betroffenen (Anhang 7).

3.11 Löschung von Daten, § 58 BDSG

Soweit unrichtige Daten durch die verantwortliche Stelle gespeichert werden, besitzt der Betroffene das Recht auf Berichtigung. Eine Löschung der personenbezogenen Daten kann vom Betroffenen dann gefordert werden, wenn

– die Speicherung unzulässig vorgenommen wurde,
– die verarbeiteten Daten nicht mehr für die Aufgabenerfüllung notwendig sind,
– oder diese zur Erfüllung einer rechtlichen Pflicht gelöscht werden müssen.

Anstelle der Löschung tritt die Einschränkung der Verarbeitung für folgende Fälle:

Einschränkung der Verarbeitung, wenn

- ☐ Grund zu der Annahme besteht, dass eine Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigen würde
- ☐ die Daten zu Beweiszwecken in Rechtsverfahren dienen
- ☐ eine Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich wäre

Zur Präzisierung der Vorgehensweise und der Anforderungen an die Berichtigung und Löschung von Daten sind dem Anhang die Checkliste und die Verfahrensanweisung zu entnehmen (Anhang 9, 12, 13).

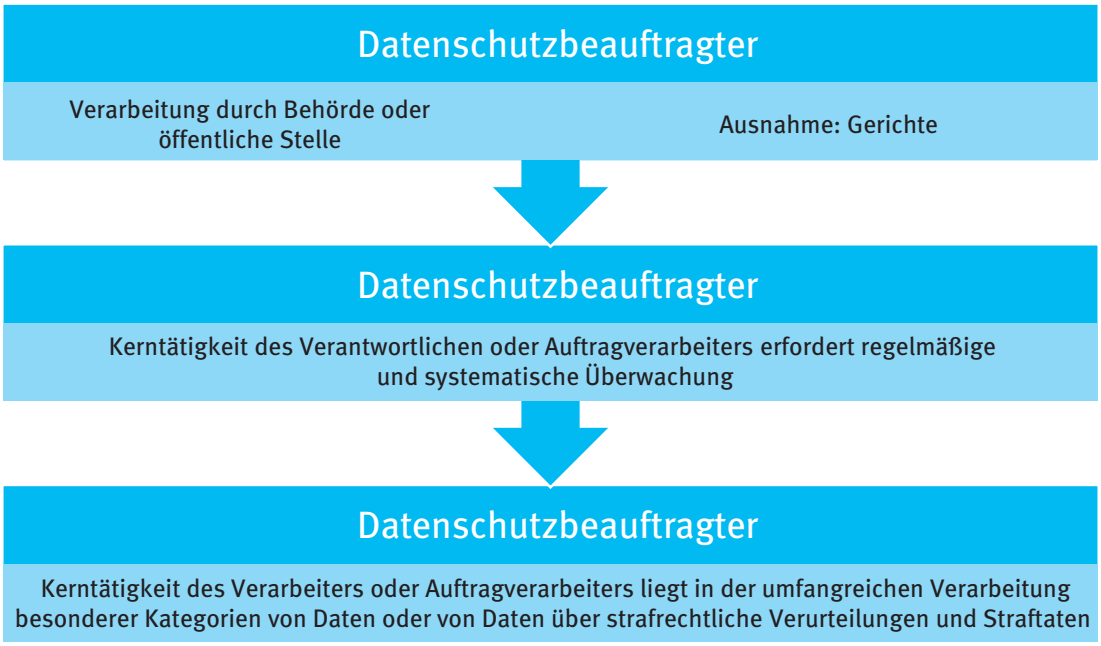
3.12 Recht auf Anrufung der oder des Bundesbeauftragten

Der betroffenen Person wird das Recht gewährt, jederzeit den oder die Bundesbeauftragte(n) zu befragen, soweit sie sich im Zweifel über die Rechtmäßigkeit des Vorgehens befindet. Der Antragsteller wird von der oder dem Bundesbeauftragten über den Stand der Beschwerde unterrichtet. Gleichzeitig wird die betroffene Person auf die Möglichkeit der Inanspruchnahme von Rechtsmitteln hingewiesen.

4 Der Datenschutzbeauftragte (DSB)

4.1 Berufung des Datenschutzbeauftragten

Die EU-Datenschutz-Grundverordnung sieht die Bestellung eines Datenschutzbeauftragten nur für besondere Kategorien von Unternehmen vor.



Weiterhin wird in der EU-DSGVO Artikel 37 ausgeführt, dass eine Unternehmensgruppe einen gemeinsamen Datenschutzbeauftragten bestellen darf. Voraussetzung ist, dass dieser Datenschutzbeauftragte leicht zu erreichen ist.

Im Artikel 37 Absatz 4 regelt die Öffnungsklausel, dass auch dann ein Datenschutzbeauftragter zu bestellen ist, wenn dies das Recht eines Mitgliedstaats vorsieht. Von dieser Einräumung hat die Bundesrepublik Gebrauch gemacht.

Das Bundesdatenschutzgesetz geht über die Forderung der EU-DSGVO hinaus und fordert den Datenschutzbeauftragen bei nicht-öffentlichen Stellen in „altbewährter Form“. Der Datenschutzbeauftragte für nicht-öffentliche Stellen ist zu bestellen, wenn

- i. d. R. mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind,
- der Verantwortliche oder Auftragsverarbeiter Verarbeitungen vornimmt, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der EU-DSGVO unterliegen,
- der Verantwortliche oder Auftragsverarbeiter personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung, der anonymisierten Übermittlung, für Zwecke der Markt- und Meinungsforschung verarbeitet.

Die letzten beiden Punkte gelten unabhängig von der mit der Verarbeitung beschäftigten Anzahl von Personen.

Im Unterschied zur EU-DSGVO sieht die Bundesrepublik Deutschland den Datenschutz vor allem in der Verantwortung des Verarbeiters oder Auftragsverarbeiters und des beratend wirkenden Datenschutzbeauftragten als Fachexperten. In vielen Unternehmen ist die Kenntnis um datenschutzrechtliche Belange häufig nur beim Datenschutzbeauftragten verankert. Es wäre wünschenswert gewesen, die Verantwortung (und natürlich auch die fachliche Qualifikation) stärker bei den Führungskräften zu verankern, die de facto täglich den Datenschutz befolgen müssen. Mit der Zentrierung auf den Datenschutzbeauftragten wird das Wissen wiederum nicht in die Breite getragen.

Soweit ein Beauftragter für Datenschutz zu bestellen ist, muss auch ein Abwesenheitsvertreter benannt werden und die Bestellung in schriftlicher Form erfolgen. Der Verantwortliche oder der Auftragsverarbeiter muss die Kontaktdaten des Datenschutzbeauftragten der zuständigen Datenschutzbehörde melden.

Bei der Ermittlung der Anzahl der Beschäftigten, die mit einer Verarbeitung personenbezogener Daten betraut sind, bleibt zu berücksichtigen, dass

- diese regelmäßigen Umgang mit personenbezogenen Daten haben müssen,
- zu den personenbezogenen Daten auch Lieferanten- und Kundendaten zählen, so sie für Personengesellschaften zutreffend sind.

Da häufig in automatisierten oder nicht-automatisierten Verfahren nicht zwischen Personen- und Kapitalgesellschaften unterschieden werden kann, gilt es, den Datenschutz auf alle Kunden- und Lieferantendateien anzuwenden. Dies vergrößert die Anzahl der mit der Verarbeitung beauftragten Beschäftigten nicht unerheblich. Somit treffen die Regelungen des Bundesdatenschutzgesetzes auch kleinere und mittlere Unternehmen, zumal in der heutigen Zeit aufgrund der umfangreichen Nutzung der IT sehr schnell die Anzahl von 10 Personen überschritten wird.

Geschieht die Erhebung, Verarbeitung und Nutzung personenbezogener Daten „ausschließlich für persönliche oder familiäre Tätigkeiten“, so sind diese vom Anwendungsbereich des BDSG ausgeschlossen. Sollten private und geschäftliche Daten nur in einer Mischform als automatisierte Daten vorliegen, so fallen diese Daten wiederum in den Geltungsbereich des BDSG.

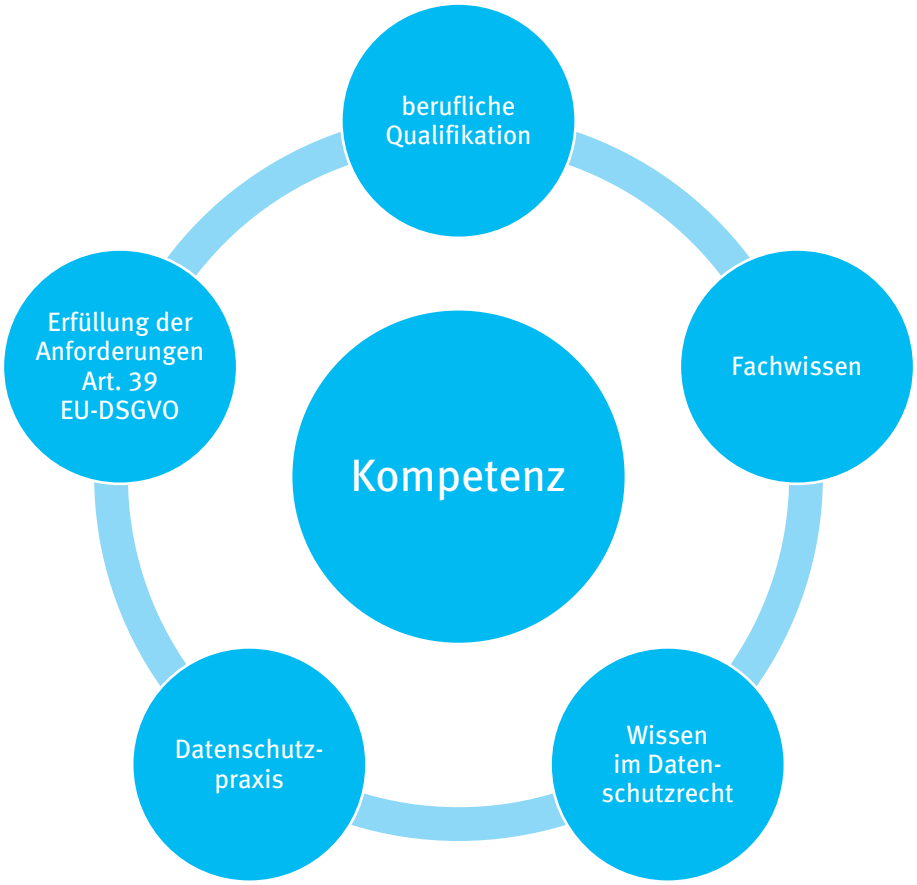
Beispiele für Unternehmen, die gemäß BDSG i. d. R. einen Datenschutzbeauftragten bestellen müssen, sind z. B.:

- Arztpraxen
- Anwaltskanzleien
- Kanzleien der Steuerberater und Wirtschaftsprüfer
- Call-Center
- Handelsbetriebe
- Industriebetriebe
- versicherungsnahe Dienstleister.

Die Auswahl des Beauftragten für Datenschutz wird von der EU-DSGVO und vom deutschen Gesetzgeber an

- dessen berufliche Qualifikation und
- den Erwerb der zur Erfüllung seiner Aufgaben notwendigen Fachkunde

geknüpft. Neu ist, dass darüber hinaus Wissen im Datenschutzrecht und in der Datenschutzpraxis verlangt wird. Der oder die Datenschutzbeauftragte muss sich in der Lage fühlen, die im Artikel 39 EU-DSGVO und § 38 BDSG genannten Aufgaben zu erfüllen.



Nach wie vor wird dem Unternehmen überlassen, das Maß der erforderlichen Fachkunde in Einklang mit dem Umfang der Datenverarbeitung und dem Schutzbedarf zu bringen. Empfehlenswert erscheint es, sowohl die für die Personenauswahl als auch für den erforderlichen Umfang der Fachkunde gewählten Argumente für wesentliche Rückfragen der Behörde oder auch für Vorfälle im Bereich des Datenschutzes in schriftlicher Form vorzuhalten.

Beispiel

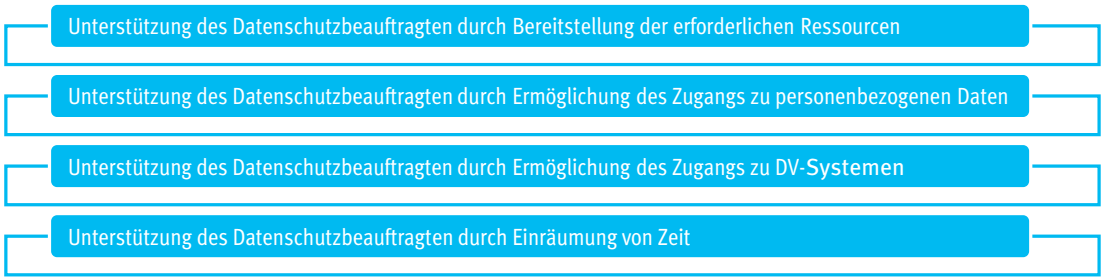
Herr/Frau xy wird als Datenschutzbeauftragte(r) benannt, weil er/sie

- über langjährige Erfahrungen im Datenschutz verfügt,
- gute Kenntnisse im Umgang mit PC-Technik und Kommunikationsmedien besitzt,
- sich ständig im Rahmen einer Mitgliedschaft in einschlägigen Verbänden weiterbildet,
- Erfahrungen bei der Unterweisung und Schulung von Mitarbeitern gesammelt hat usw.

Der Datenschutzbeauftragte kann im Unternehmen beschäftigt sein oder auch im Rahmen eines Dienstleistungsvertrags tätig werden. Als Beschäftigter kann er auch andere Aufgaben wahrnehmen. Diese dürfen jedoch keinen Interessenskonflikt zu seiner Tätigkeit als Datenschutzbeauftragter bilden.

4.1.1 Aufgaben des Verantwortlichen oder Auftragverarbeiters

Neben den Verpflichtungen des Datenschutzbeauftragten haben die Verantwortlichen für die Verarbeitung personenbezogener Daten ebenfalls Pflichten:



Diese Pflichten sind nicht selbstverständlich. Wie die Autorin aus praktischer Erfahrung weiß, wird Datenschutz eher als Stiefkind behandelt. Mittel für Weiterbildung, zeitliche Ressourcen für Schulungen der Mitarbeiter werden nicht selten nur rudimentär zur Verfügung gestellt. Es macht daher Sinn, in der folgenden Bestellung zum Datenschutzbeauftragten auch die Verpflichtungen des Verantwortlichen einzuarbeiten. Die Erfüllung der Pflichten des Verantwortlichen für die Verarbeitung zieht quasi den Rahmen, den der Datenschutzbeauftragte dann ausfüllen kann.

Die Wirksamkeit der Bestellung des innerbetrieblichen Datenschutzbeauftragten bemisst sich an der für die Wahrnehmung seiner Aufgaben eingeräumten Zeit. Ein Beauftragter für Datenschutz gilt dann als nicht bestellt, wenn der Umfang seiner notwendig zu erbringenden Leistungen nicht den bereitgestellten zeitlichen Ressourcen durch den Arbeitgeber oder Auftraggeber entspricht.

Die Bestellurkunde an sich kann in unterschiedlicher Form gefasst werden. In der Praxis existieren sowohl Beispiele für Bestellungen, die konkrete Aufgabenzuweisungen für den Beauftragten für Datenschutz beinhalten, als auch solche mit Verweisen auf Inhalte der EU-DSGVO und des BDSG.

Als Beispiel für die betriebliche Praxis kann nachstehendes Muster dienen:

Vorlage

Bestellurkunde zum Datenschutzbeauftragten

Unternehmen:	**Muster GmbH**
Wir bestellen	Herrn/Frau .....

mit Wirkung vom ..... gemäß Art. 37 ff. EU-DSGVO und § 38 BDSG (2018) zum externen/internen Datenschutzbeauftragten. In dieser Funktion ist Herr/Frau ..... der Geschäftsleitung direkt unterstellt. Ansprechpartner in Fragen des Datenschutzes ist der Geschäftsführer Herr/Frau ...

Der Beauftragte für den Datenschutz ist in Anwendung seiner Fachkunde und Ausübung seiner Tätigkeit weisungsfrei. Ihm werden alle notwendigen Ressourcen zur Verfügung gestellt und die notwendigen technischen und organisatorischen Maßnahmen zur Durchsetzung des Datenschutzes gewährt.

Ihre Aufgaben sind im Art. 37 ff. EU-DSGVO und § 38 BDSG (2018) beschrieben. Sie bestehen vor allem in:

- der Einhaltung sämtlicher einschlägiger Datenschutzvorschriften
- der beratenden und berichtenden Tätigkeit

Revision:	Änderungsdatum:	Seite: 1 von 2

– der Überwachung der Umsetzung des Datenschutzrechts im Unternehmen
– der Zuweisung von Zuständigkeiten
– der Sensibilisierung der Mitarbeiter im Umgang mit personenbezogenen Daten
– der Durchführung von Schulungen
– der Unterstützung bei der Datenschutzfolgeabschätzung
– der Zusammenarbeit mit der Datenschutzaufsicht.

In Ihrer Tätigkeit müssen Sie stets das mit den Verarbeitungsvorgängen verbundene Risiko gebührend berücksichtigen. Dabei sind Art, Umfang, die Umstände und die Zwecke der Verarbeitung heranzuziehen.

Als Beauftragter für Datenschutz sind Sie Ansprechpartner der Datenschutzaufsicht in allen datenschutzrechtlichen Fragen. In Zweifelsfällen können Sie sich jederzeit an die Datenschutzaufsicht zur Klärung von Fachfragen wenden.

Der Beauftragte für den Datenschutz verfügt über die notwendigen Fachkenntnisse, juristisches Wissen und praktisch-technische Intelligenz und Sensibilität. Er/Sie ist sich der Komplexität des Aufgabengebiets und der Verantwortung für die Umsetzung der einschlägigen Datenschutzvorschriften bewusst. Er/Sie verpflichtet sich, den Wissens- und Erfahrungsstand aktuell zu halten.

Auf die gesetzliche und vertragliche Verschwiegenheitspflicht werden Sie nochmals hingewiesen. Wir erwarten von Ihnen ein Höchstmaß an Vertraulichkeit, Achtsamkeit und Sensibilität beim Zugang bzw. Zugriff zu personenbezogenen Daten.

Für die Geschäftsleitung:

Ort, Datum, Unterschrift: _____

Ich bin mit der Bestellung zum externen/internen Datenschutzbeauftragten einverstanden.

Ort, Datum, Unterschrift: _____

Revision: Änderungsdatum: Seite: 2 von 2

Soweit es sich aufgrund organisatorischer Gegebenheiten (z. B. bei größeren Unternehmen, unselbständigen Zweigstellen) als notwendig erweist, ernennt die Geschäftsleitung neben dem DSB für die jeweilige Organisationseinheit einen Datenschutz-Koordinator. Die Bezeichnung ist willkürlich gewählt, in der Praxis finden Sie auch „Datenschutzgehilfe“ oder „Datenschutzbevollmächtigter“ dafür. Der Koordinator ist insoweit dem DSB ein fachlich zugewiesener Mitarbeiter. Er informiert den DSB über vor Ort auftretende Datenschutzfragen und setzt die betrieblichen Regelungen in der Organisationseinheit um. Er erhebt die in seinem Zuständigkeitsbereich eingesetzten datenschutzrelevanten Verfahren und gibt die Meldung an den DSB weiter.

Für Meldungen, Auskünfte etc. gegenüber den Datenschutz-Aufsichtsbehörden liegt die bearbeitende Zuständigkeit beim DSB. Die Fachabteilungen stellen die hierfür erforderlichen Informationen, Unterlagen etc. zur Verfügung. Gleiches gilt für Anfragen, Beschwerden oder Auskunftsersuchen Betroffener.

Der Datenschutzbeauftragte ist der zuständigen Aufsichtsbehörde namentlich mit seinen Kontaktdaten zu melden.

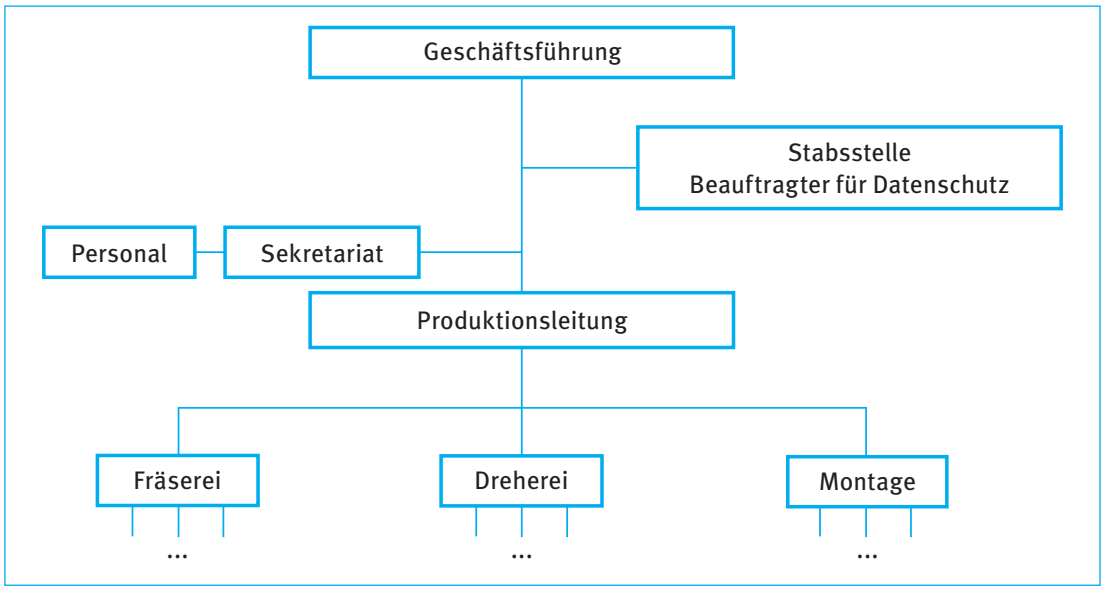
Hinweis

Meldung des Betriebsbeauftragten für Datenschutz an die Aufsichtsbehörde nicht vergessen!

4.2 Stellung des Datenschutzbeauftragten im Unternehmen

Die Stellung des Beauftragten für Datenschutz wird häufig in der Praxis nicht korrekt angegeben. Darstellungen in Organigrammen und Strukturcharts weisen den Beauftragten für Datenschutz als Unterstellungsverhältnis zu Personalabteilungen und -controlling aus. Gemäß Artikel 38 Absatz 3 der EU-DSGVO ist der Datenschutzbeauftragte weisungsfrei. Die Aufgaben des Datenschutzbeauftragten sind beratender und berichtender Natur. Der Datenschutzbeauftragte unterliegt der Verschwiegenheit und darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Seine Berichtspflicht gilt der obersten Leitungsebene. Empfehlenswert erscheint daher die Darstellung der Position des Datenschutzbeauftragten als Stabsstelle, so wie es in vielen Organisationen bereits mit Managementbeauftragten für Qualität, Umwelt und Arbeitssicherheit, Sicherheitsfachkräften und Betriebsärzten oder Beauftragten für Immissionsschutz, Gewässerschutz u. a. m. geschieht.

Beispiel



Betriebsbeauftragte für Datenschutz im nicht-öffentlichen Bereich können als interne Beauftragte oder auch externe Beauftragte berufen werden.

Eine Kündigung des betrieblichen, also internen, Beauftragten für Datenschutz kann nur nach Entbindung von seiner Tätigkeit (Abberufung) als Beauftragter für Datenschutz erfolgen, nur aus triftigem Grund. Insofern unterliegt der Beauftragte für Datenschutz einem gewissen Kündigungsschutz. Dieser Kündigungsschutz entfällt dann, wenn Tatsachen vorliegen, welche den verantwortlichen Verarbeiter zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Insofern geht das BDSG über die EU-DSGVO hinaus.

Hinweis

Eine Unternehmensgruppe kann einen gemeinsamen Datenschutzbeauftragten bestellen, soweit dieser leicht erreichbar ist.

4.3 Auswahl des Datenschutzbeauftragten

Die Tätigkeit des betrieblichen oder öffentlichen Beauftragten für Datenschutz wird als Beruf eingeordnet im Sinne von Art. 12 Abs. 1 GG. Dieser Ansicht liegt ein rechtskräftiger Beschluss des Landgerichts Ulm zum Berufsbild des betrieblichen und behördlichen Datenschutzbeauftragten vom 31. Oktober 1990 zugrunde. Auch wenn EU-DSGVO und BDSG keinen bestimmten Ausbildungsgang vorschreiben oder zu erkennen geben, sprechen doch viele der Anforderungen beider Rechtsquellen für ein Berufsbild.

An den Datenschutzbeauftragten werden hohe und vor allem komplexe Anforderungen gestellt:

- Kenntnis und Anwendung der Vorschriften der Datenschutzgesetze des Bundes und der Länder und alle anderen Vorschriften des Datenschutzrechts
- Kenntnisse über die betriebliche Organisation
- umfangreiche IT-Kenntnisse
- didaktische Fähigkeiten
- Organisationstalent
- soziale Kompetenz
- Kenntnisse und Erfahrungen in der Konfliktbewältigung
- Managementkompetenz
- Beratungskompetenz

Die Auswahl des Betriebsbeauftragten für Datenschutz sollte sehr sorgfältig erfolgen und wie bereits dargestellt schriftlich verankert werden.

Neben der Zuverlässigkeit stehen auch Fragen der Unabhängigkeit in der Betrachtung im Vordergrund. So ist es in Anbetracht des Interessenskonflikts nicht möglich, den Verantwortlichen für IT im Unternehmen gleichzeitig zum Datenschutzbeauftragten zu bestellen. Als Leiter IT kann er eine neutrale, unabhängige Sichtweise nicht mehr gewährleisten, kann die Vorgehensweisen im Datenschutz für IT-Lösungen nicht unparteilich sicherstellen, da er gleichzeitig in der Funktion des Planers, Gutachters, des Freigebers und des Ausführenden tätig wird. Gleiches gilt für den Leiter Personal oder den Leiter Rechnungswesen.

Der Betriebsbeauftragte für Datenschutz muss auf Verlangen der Aufsichtsbehörde die Nachweise für die Erfüllung seiner Aufgabe, seine Arbeitsergebnisse nachweisen. Die Aufsichtsbehörde kann bei Zweifeln an der fachlichen Qualifikation oder im Fall der Missachtung datenschutzrechtlicher Vorschriften den Datenschutzbeauftragten abberufen und ggf. strafrechtlich verfolgen.

4.4 Aus- und Weiterbildung des Datenschutzbeauftragten

Der Beauftragte für Datenschutz muss zur Erbringung seiner Leistungen fachkundig sein. Zur Aufrechterhaltung seiner Fachkunde ist der Datenschutzbeauftragte gehalten, in regelmäßigen Abständen sowie im Zuge von rechtlichen Änderungen Weiterbildungsveranstaltungen zu besuchen.

Gegenwärtig gibt es eine Vielzahl von Aus- und Weiterbildungsangeboten für DSB am Markt. Welcher Art die zu besuchenden Seminare sein müssen, ist im BDSG oder der EU-DSGVO nicht klar geregelt. Einige Anbieter stellen in ihren Aus- und Fortbildungsseminaren ein Zertifikat aus. Auch hierfür findet sich keine Aussage.

Für die Aus- und Weiterbildungskosten des Datenschutzbeauftragten muss das Unternehmen aufkommen. Externe Datenschutzbeauftragte tragen diese Kosten selbst und müssen als Grundlage für ihren Vertrag die Ausbildungsurkunde nachweisen. In jedem Fall sollte ein Unternehmen sich diesen Nachweis einfordern und zum Vertragsbestandteil erklären lassen (Holschuld).

Der Datenschutzbeauftragte kann zur Erfüllung seiner Aufgaben Hilfspersonal, Einrichtungen, Geräte und Mittel beanspruchen. Im Artikel 24 der EU-DSGVO sind die Pflichten des für die Verarbeitung Verantwortlichen klar geregelt. Sie umfassen alle notwendigen technischen und organisatorischen Maßnahmen.

Die Unterstützungspflicht des für die Verarbeitung Verantwortlichen ergibt sich aus Art. 38 Abs. 2 EU-DSGVO. Dem Datenschutzbeauftragten ist die notwendige Arbeitszeit zur Verfügung zu stellen. Er muss Zugang zu allen Informationen und DV-Anlagen haben. In der Praxis sind häufiger Unternehmen anzutreffen, die über einen formal bestellten Datenschutzbeauftragten verfügen. De facto werden jedoch häufig die Aufgaben des Beauftragten für Datenschutz nicht

betrieblich umgesetzt – zum einen aus Kapazitätsgründen, zum anderen, weil häufig die Aufgaben des Datenschutzbeauftragten nicht konkret genug bekannt oder beschrieben sind.

Nicht umsonst wurden die Sanktionen gegen unterlassene Maßnahmen im Datenschutz stark erweitert und verschärft.

4.5 Aufgaben des Datenschutzbeauftragten und betriebliche Bestellung

Der DSB ist im Wesentlichen für die Einhaltung des Datenschutzes gemäß EU-DSGVO, BDSG sowie aller anderen zutreffenden datenschutzrechtlichen Vorschriften und vor allem für die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme verantwortlich.

Die Aufgaben des DSB könnten demnach wie folgt beschrieben werden:

Aufgabenbeschreibung DSB **Vorlage**

- Der Datenschutzbeauftragte ist für die Überwachung der Einhaltung einschlägiger datenschutzrechtlicher Vorschriften, insbesondere der EU-DSGVO und des BDSG, sowie für die Überwachung der Anwendung von DV-Systemen verantwortlich.
- Er ist beratend und berichtend gegenüber der Geschäftsleitung in Fragen der Einhaltung datenschutzrechtlicher Vorschriften tätig.
- Er ist in seiner Fachkunde zum Datenschutz weisungsfrei.
- Er hat den geschäftsbezogenen Umgang mit personenbezogenen Daten zu analysieren, Schwachstellen und Lücken im Datenschutz aufzuzeigen und Lösungsvorschläge zur Gewährleistung der Einhaltung der EU-DSGVO und des BDSG und anderer geltender Vorschriften zu unterbreiten.
- Er übernimmt die Kontrolle der rechtskonformen Anwendung der Datenverarbeitungsprogramme.
- Er ist bei der Vertragsgestaltung mit externen Dienstleistern aus datenschutzrechtlicher Sicht einbezogen und bringt hier seine Fachkunde ein, insbesondere in Fällen der Auftragsverarbeitung.
- Er wirkt bei der Erarbeitung von Betriebsvereinbarungen und betrieblichen Verhaltensregeln zum Datenschutz mit.
- Er sensibilisiert alle mit der Verarbeitung von personenbezogenen Daten betrauten Personen über Schulungen und Unterweisungen.
- Bei Änderungen in DV-Verfahren übernimmt er die Prüfung vorab aus datenschutzrechtlicher Sicht vor und gibt die Verfahrensänderungen frei.
- Er unterstützt bei der Datenschutzfolgeabschätzung von automatisierten Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen.
- Er ist maßgeblich bei der Erarbeitung von Verpflichtungserklärungen auf das Datengeheimnis sowie bei der Information über Rechte des Betroffenen und die Art und Weise der Verarbeitung personenbezogener Daten von Beschäftigten, Lieferanten und Kunden beteiligt.
- Er führt Verfahrensübersichten über die Verarbeitung von personenbezogenen Daten im Unternehmen.
- Er kümmert sich um die Bearbeitung von Beschwerden und ist Ansprechpartner im Unternehmen für alle Datenschutzbelange.
- Er ist Ansprechpartner der Aufsichtsbehörde.
- Er stellt jährlich einen Arbeitsplan auf und rechnet im Jahresbericht seine Tätigkeit als DSB ab.

Revision: Änderungsdatum: Seite: 1 von 1

Aus vorgenannten Aufgabenzuweisungen ergibt sich die Beratungsfunktion des Betriebsbeauftragten für Datenschutz gegenüber der Geschäftsleitung. Diese können je nach Erfordernissen des Unternehmens erweitert werden. Sie erstreckt sich auch auf die Vereinbarungen sowie auf die Mitwirkung bei der Vertragsgestaltung mit Rechenzentren, Steuerberatern, Entsorgungsfirmen, Dienstleistern (IT, Kopierfirmen). Es ist empfehlenswert, im Vertrag mit dem internen oder externen Datenschutzbeauftragten möglichst konkret zu regeln, was im Einzelnen betriebsbezogene Pflichten des DSB auf der dargestellten Grundlage sind.

Obwohl die Aufgaben des Beauftragten für Datenschutz klar im § 38 BDSG definiert sind, mangelt es an der betrieblichen Umsetzung – wohl auch deshalb, weil viel über Datenschutz Geschriebenes das Thema zu komplex angeht und die Unternehmen bzw. den DSB nicht dort abholen, wo diese gegenwärtig stehen. Aus vielfältigen Praxiserfahrungen wird deutlich, dass die grundlegenden Regelungen zum Datenschutz, z. B. zu E-Mail, Internet, Faxbetrieb, Telefon, meist weder mündlich noch schriftlich getroffen wurden. Verfahrensverzeichnisse zum Datenschutz liegen nur in geringem Umfang in Unternehmen vor.

Im Folgenden werden grundlegende und überschaubare Anweisungen und Vereinbarungen als Mustertexte zur betrieblichen Adaption angeboten. Methodisch sollte dabei jeder Betriebsbeauftragte für Datenschutz dem Grundsatz „vom Einfachen zum Besonderen“ folgen.

4.5.1 Festlegung der Datenschutzpolitik

Ob nun als Datenschutzphilosophie, -grundsätze oder -politik bezeichnet, so ist es sinnvoll, grundlegende Werte und Grenzen im Datenschutz für das Unternehmen zwischen Unternehmensleitung und Arbeitnehmerschaft (z. B. über Betriebsräte) unter Beteiligung des Datenschutzbeauftragten festzulegen. Mit der Bekanntgabe der Datenschutzpolitik werden alle Mitarbeiter angesprochen und mit der Verbindlichkeitserklärung durch die Geschäftsleitung (Inkraftsetzung) auf die Einhaltung des Datenschutzes verpflichtet. Die Datenschutzpolitik mit wesentlichen Aussagen zu Inhalten des betrieblichen Datenschutzes sollte jedem Mitarbeiter, Leiharbeitnehmer, Besucher und Dienstleister zugänglich sein, beispielsweise durch Aushänge, als Vertragsbestandteil, auf der Internetseite des Unternehmens. Ihre Aussagekraft ist jeweils so gut, wie Belange des Datenschutzes de facto im Unternehmen auch umgesetzt werden. Auf Angemessenheit in den Aussagen in der Datenschutzpolitik sollte daher besonderer Wert gelegt werden.

Dabei gelten folgende Grundsätze:

- Die DV-Hard- und Software sind für betriebliche Aufgaben, und zwar für die jeweils vorgesehenen Zwecke zu verwenden und gegen Verlust und Manipulation zu sichern. Eine Nutzung für private Zwecke bedarf der ausdrücklichen Genehmigung.
- Jeder Mitarbeiter ist in seinem Verantwortungsbereich für die Umsetzung der Richtlinie verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden.
- Die für die Verarbeitung der eingesetzten Systeme Verantwortlichen stellen sicher, dass ihre Mitarbeiter (Benutzer) über diese Richtlinie informiert werden; das gilt auch für temporär Beschäftigte.
- Der Datenschutzbeauftragte berät bei Umsetzung der Richtlinie und prüft deren Einhaltung. Insoweit sind alle Adressaten der Richtlinie dem DSB auskunftspflichtig.

Ein Beispiel für eine Datenschutzpolitik, die je nach Art des Unternehmens adaptiert oder erweitert werden kann, zeigt nachfolgendes Muster.

Datenschutzpolitik

Vorlage

In unserem Unternehmen genießt der Datenschutz unter Einbeziehung personenbezogener und anderer vertraulicher Daten höchste Priorität.

Im Rahmen unserer Geschäftstätigkeit werden regelmäßig und unvermeidbar schutzwürdige Daten erhoben, verarbeitet, genutzt und anderen Personen zur Verfügung gestellt.

Dabei wird das Maß der Erhebung, Verarbeitung und Nutzung personenbezogener Daten unter Beachtung datenschutzrechtlicher Zulässigkeitsvoraussetzungen auf das notwendige Mindestmaß zur Aufgabenerfüllung begrenzt.

Wir arbeiten mit aktualisierten Daten. Nicht mehr benötigte Daten werden zuverlässig gelöscht. Fehlerhafte Angaben werden zeitnah berichtigt. Bei der Archivierung von Daten wird eine weitere Nutzung dieser Daten ausgeschlossen. Gesetzliche Aufbewahrungsfristen bzw. Archivierungsfristen werden eingehalten. Es werden grundsätzlich nur die zur Erfüllung rechtlicher Zwecke unbedingt notwendigen personenbezogenen Daten archiviert.

Eine Verarbeitung und Nutzung personenbezogener Daten erfolgt nur mit schriftlicher Einwilligung des Betroffenen oder ist im Geschäftsinteresse dann zulässig, wenn das schutzwürdige Interesse des Betroffenen nicht gegenüber dem Beschluss der Verarbeitung oder Nutzung überwiegt.

Unsere Mitarbeiter sind über die einschlägigen Datenschutzvorschriften belehrt. Jährlich werden sie durch den Datenschutzbeauftragten über Änderungen und Aktualisierungen im Datenschutzrecht geschult. Die Verpflichtungen der Mitarbeiter auf den Datenschutz sind aktenkundig.

Jeder Mitarbeiter ist sich dessen bewusst, dass ihm anvertraute personenbezogene Daten ausschließlich im Rahmen der Zweckbestimmung verwendet werden und gegen unberechtigten Zugriff gesichert werden müssen.

Teil unseres Verständnisses von Datenschutz ist es, dass

- ausschließlich vom Unternehmen freigegebene Softwareverfahren angewendet werden,
- keine Veränderungen an der Hard- und Software vorgenommen werden,
- keine eigene Hard- und Software eingesetzt werden darf und
- alle unternehmenseigenen Richtlinien und Maßnahmen von allen Mitarbeitern, Leiharbeitnehmern, Fremdfirmen und Besuchern

eingehalten werden.

Daten und Programme müssen vor unbefugter Einsichtnahme, vor Datendiebstahl oder -verlust zuverlässig geschützt werden. Die Mitarbeiter des Unternehmens verpflichten sich, hierfür größtmögliche Sorgfalt walten zu lassen.

Gemäß gesetzlicher Vorgabe hat jeder Beschäftigte das Recht auf Auskunft über die Verarbeitung seiner personenbezogenen Daten, seine personenbezogenen Daten einzusehen, sie ggf. berichtigen, sperren oder löschen zu lassen, soweit kein berechtigtes Interesse seitens des Unternehmens in Bezug auf diese Daten besteht.

Das Unternehmen verpflichtet sich, vor erstmaliger Verarbeitung personenbezogener Daten den Betroffenen zu informieren.

Das Unternehmen hat einen Datenschutzbeauftragten schriftlich bestellt. Zur Umsetzung datenschutzrechtlicher Forderungen im Unternehmen besitzt er gegenüber der Geschäftsleitung ein direktes Vortrags-, Empfehlungs- und Beratungsrecht. In der Anwendung seiner Fachkunde ist er weisungsfrei.

Revision:	Änderungsdatum:	Seite: 1 von 2

Zum Datenschutzbeauftragten des Unternehmens berufen wurde:

Name, Vorname

Telefon-Nr.

Fax-Nr.

E-Mail-Kontakt

(bei externen Datenschutzbeauftragten ggf. Anschrift)

Vertreter:

Name, Vorname

Telefon-Nr.

Fax-Nr.

E-Mail-Kontakt:

Der Datenschutzbeauftragte steht jedem Mitarbeiter für Fragen, Anregungen und Beschwerden jederzeit zur Verfügung. Die Vorgehensweise im Fall von Beschwerden ist in einer gesonderten Anweisung geregelt.

Ort, Datum | Geschäftsleitung

Revision: | Änderungsdatum: | Seite: 2 von 2

Die Datenschutzpolitik muss den geltenden rechtlichen Rahmenbedingungen entsprechen und sie sollte schriftlich formuliert sein. Sie bedarf letztlich einer jährlichen Überarbeitung und Anpassung an rechtliche oder sonstige Änderungen. Den Aktualisierungsbedarf zu eruieren, obliegt dem Datenschutzbeauftragten, der seine Fachkenntnis einbringen kann. Sie wird in veränderter Fassung ausschließlich durch die Geschäftsleitung genehmigt. Verstöße gegen diese Anweisung stellen Straftatbestände dar, siehe Bußgeld- und Strafvorschriften der EU-DSGVO und des BDSG. In Anhang 3 befindet sich weiterhin eine Vorlage für betriebliche Datenschutzgrundsätze.

In sicherheitskritischen Bereichen werden nur Mitarbeiter eingesetzt, deren Erfahrung und Vertrauenswürdigkeit es rechtfertigt, mit besonders sensiblen Daten umzugehen. Der Personenkreis hierfür ist schriftlich definiert. Gesonderte Verpflichtungen auf den Datenschutz sind erfolgt.

4.5.2 Jahresplan des Datenschutzbeauftragten

Um die Tätigkeit des Datenschutzbeauftragten zu planen und zu systematisieren, erscheint es empfehlenswert, zu Beginn eines Jahres einen Jahresplan aufzustellen. In diesem Plan werden nach zuvor gewichteten Schwerpunkten wesentliche Arbeitsschritte für jeweils ein Jahr festgeschrieben. Schwerpunkte der Tätigkeit können sich aus

- Ist-Analysen,
- Auditberichten,
- geänderten rechtlichen Rahmenbedingungen (z. B. Änderung im BDSG, Telekommunikations- oder Telemediengesetz),
- Diskussionen in den Medien und der Öffentlichkeit,
- Konzernanforderungen und Forderungen Dritter,
- Beschwerden und Anregungen,
- Personenwechsel, Wechsel von Dienstleistern,
- der Änderung von Hard- und Software, Netzwerken, Übermittlungswegen u. Ä. sowie

- Änderungen von Unternehmensstrukturen
- Änderung der Kategorien personenbezogener Daten
- Änderungen von Verarbeitungsverfahren
- Änderungen des Risikos bzw. Schutzniveaus bei der Verarbeitung personenbezogener Daten u. a. m.

ergeben.

Erfahrungsgemäß ist es nicht immer möglich, konkrete Termine gleich zu Beginn des Jahres abzustimmen. Daher empfiehlt es sich, eine quartalsweise Planung der Tätigkeiten des DSB vorzunehmen.

Im nachstehend aufgeführten Beispiel für eine Jahresplanung sind typische Aufgaben des DSB dargestellt. Selbstverständlich richtet sich der Plan nach den unternehmensindividuellen Problemstellungen.

Vorlage

Jahresplan des Datenschutzbeauftragten

1. Quartal

- Überprüfung der Datenschutzpolitik
- Schulung der Mitarbeiter nach Personenkreisen zu Anforderungen der EU-DSGVO und des BDSG (2018)
  - Personalwesen
  - Mitarbeiter Außendienst
  - Mitarbeiter Call-Center
  - Mitarbeiter Rechnungswesen
  - Mitarbeiter IT
  - sonstige Verwaltung
- Vorbereitung, Diskussion und Abschluss der datenschutzrechtlichen Verhaltensregeln zu
  - Informationen zur Erhebung und Verarbeitung personenbezogener Daten
  - Informationen über Rechte des Betroffenen
  - E-Mail- und Internet-Nutzung
  - Erfassung der Telefondaten
  - Nutzung privater IT-Systeme im Unternehmen
- Durchführung eines Datenschutzaudits im Bereich Personalwesen
- Aufstellung/Aktualisierung der Verfahrensübersicht im Personalwesen

2. Quartal

- Kontrolle des Maßnahmeplans vom Datenschutzaudit im Bereich Personalwesen
- Vorbereitung, Diskussion und Freigabe betrieblicher Verfahrensregelungen zu
  - Umgang mit Beschwerden
  - Umgang mit externen Anfragen
  - Erarbeitung eines Merkblatts zur Information von Kunden und Lieferanten über die Verarbeitung ihrer personenbezogenen Daten
- Durchführung eines Datenschutzaudits zu Videosystemen

– Vorbereitung, Diskussion und Abschluss von Betriebsvereinbarungen zu
  - Zeiterfassung
  - Videosystemen im Unternehmen

3. Quartal

– Überprüfung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit

usw.

Revision: Änderungsdatum: Seite: 2 von 2

4.5.3 Datenschutzaudits

Selbstverständlich stellt die Durchführung von Audits zum Thema Datenschutz keine Forderung des BDSG dar. Den Wert von internen Audits im Datenschutz erkennt der Datenschutzbeauftragte dann, wenn er Audits als systematisches Tool zur Aufdeckung von Schwachstellen in der Datenschutzorganisation nutzt. Die auch in Managementsystemen (z. B. DIN EN ISO 9001, DIN EN ISO 14001) etablierte Vorgehensweise zur Planung, Durchführung und Dokumentation interner Audits kann hier von großem Nutzen sein, wie auch der Leitfaden zur Auditierung von Managementsystemen DIN EN ISO 19011. Beispielsweise kann eine Ist-Analyse zu datenschutzrechtlichen Regelungen im Unternehmen über eine systematische Planung von Audits in einzelnen Unternehmensbereichen durchgeführt werden. Ausgangspunkt der für die in Datenschutzaudits zu untersuchenden Bereiche können entweder das Organigramm (Aufbaustruktur) oder die Prozesslandkarten des Unternehmens darstellen. Unberücksichtigt in dieser Ist-Analyse bleiben zunächst alle datenschutzrelevanten Informationen an der Schnittstelle nach außen, die später zu berücksichtigen bleiben. Ein Beispiel für die Auditplanung zeigt sowohl das zeitliche und bereichsbezogene Vorgehen als auch Soll- und Ist-Termine sowie Verantwortlichkeiten auf.

Vorlage

Auditplan für Datenschutzaudits Jahr ... (bereichsbezogen)

Unternehmensbereich/ Organisationseinheit	Auditor (Kürzel des Namens)	Januar		Februar		März		...
		Soll	Ist	Soll	Ist	Soll	Ist	
Management	DSB	X						
Call-Center	DSB							
IT-Abteilung	DSB			X				
Personalwesen	DSB							
Einkauf	DSB							
Vertrieb/Marketing	DSB							

Stand: 1.01.20..

Revision: Änderungsdatum: Seite: 1 von 1

Ein weiteres Beispiel zeigt die Planungsvariante für prozessorientierte Datenschutzaudits. Die hier aufgeführten Prozesse sind beispielhaft gewählt und müssen auf die tatsächliche Prozessorganisation des Unternehmens adaptiert werden.

Auditplan für Datenschutzaudits Jahr ... (prozessorientiert) Vorlage

Prozess	Betroffene Unternehmens-bereiche (Management, Personal usw.)	Auditor	Januar		Februar		März		...
			Soll	Ist	Soll	Ist	Soll	Ist	
Personal-rekrutierung	GL, Personal, Fachbereich	DSB	X	20.01.20..					
Bewerbungs-verfahren	GL, Personal, Fachbereich	DSB			X				
Daten-speicherung	Alle Bereiche	DSB					X		
Datenlöschung	Fachbereiche, EDV	DSB	X						
Datensicherung	EDV	GL/DSB					X		

Stand: 1.01.20..

Revision: Änderungsdatum: Seite: 1 von 1

Denkbar sind auch thematische Audits, die zu bestimmten Themenschwerpunkten durchgeführt werden. Stellvertretend seien hier folgende Themen aufgeführt:

- Audit zur Installation von Videokameras
- Audit zum Umgang mit dem Internet
- Audit zur Telefondatenerfassung
- Audit zum Umgang mit Lieferantendaten.

Diese Audits können in ähnlicher Form wie bereits abgebildet geplant werden.

Grundsätzlich gilt, dass der Auditor unabhängig von dem zu verantwortenden Bereich sein sollte. Ein Team von Auditoren, zusammengesetzt aus verschiedenen Organisationseinheiten des Unternehmens, erhöht erfahrungsgemäß den neutralen Ansatz der Auditierung.

Der prozessbezogene Auditplan stellt erhöhte Forderungen an die Unabhängigkeit der Auditoren. Prozesse können sich durch verschiedene, ja sogar durch alle Bereiche des Unternehmens ziehen. Folglich wird es schwieriger, eine unabhängige Person von der Funktion bzw. vom Prozess zu finden.

In der einschlägigen Fachliteratur findet der Leser eine Vielzahl von Checklisten und Fragelisten als Ausgangspunkt für die Auditierung. Sie sollen als interner Leitfaden dienen. Unbedingt müssen die Checklisten zuvor auf die Unternehmenssituation adaptiert werden. Wichtiger als die Auflistung von Fragen erscheint der Autorin dieses Fachbuchs die Fragetechnik eines Auditors. In der Praxis wird im Wesentlichen zwischen offenen und geschlossenen Fragen unterschieden. Während geschlossene Fragen, z. B. „Haben Sie den Datenschutz organisiert?“, sehr schnell mit der Antwort „Ja“ zum Ende einer Kommunikation führen, bieten offene Fragen, z. B. „Wie haben Sie den Datenschutz in Ihrem Bereich organisiert?“, vielfältige Möglichkeiten der Investigation durch den Auditor. Wer also etwas zum Datenschutz erfahren will, sollte sich der sogenannten „W“-Fragen bedienen, z. B.:

- Wer?
- Was?
- Wie?

– Womit?
– Wodurch?
– Wann?
– Wie häufig?
– Welche?
– Weshalb?

Lassen Sie sich in einem zweiten Schritt Belege (Nachweise) für das Gesagte zeigen. Das gesprochene Wort gilt bei guten Auditoren nicht viel. Er fragt nach „evidence", nach „Was zu beweisen wäre", wie in der Mathematik.

Als Auditor überprüfen Sie

– die Übereinstimmung des Gesagten und des Nachweises
  • mit dem BDSG und anderen rechtlichen Forderungen,
  • mit den schriftlichen betrieblichen Regelungen,
  • mit dem täglichen Handeln der Beschäftigten in der Praxis.

Daher sind die wesentlichen (zentralen) Fragen stets:

– Stimmt das, was wir tun, mit den rechtlichen Anforderungen überein?
– Stimmt das, was wir tun, mit den eventuell vorhandenen Kunden- und Forderungen Dritter (z. B. Konzernrichtlinien) überein?
– Wo haben wir diese Vorgaben dokumentiert?
– Leben wir das, was wir uns vorgenommen haben, in der Praxis?

Folgen Sie diesen Leitlinien, werden Sie sehr schnell den Wert von Datenschutzaudits erkennen.

4.5.4 Audit-Reporting

Feststellungen in Datenschutzaudits müssen dokumentiert werden. In der Praxis hat sich erwiesen, dass nur wenige Auditoren Erfahrungen mit dem Berichtswesen haben. Selbstverständlich gibt es auch hier keine direkten Vorgaben die Form betreffend. Zu den wesentlichen Inhalten der Dokumentation von internen Audits zählen:

– Datum des Audits, Beginn und Ende
– Auditor(en)
– Auditierter Bereich, Bereichsverantwortlicher
– Anwesende
– Geprüfte Fragestellungen und Dokumente sowie Aufzeichnungen
– Feststellungen
– Maßnahmeplan (vom Prozesseigner oder Leiter Bereich zu erstellen).

Die rechtlichen Grundlagen müssen hier nicht unbedingt aufgeführt werden. Sie betreffen häufig z. B.:

– die EU-DSGVO
– das BDSG (2018)
– das Telekommunikationsgesetz
– das Telemediengesetz
– landesrechtliche Regelungen

- Einzelregelungen für bestimmte Berufsgruppen
- ggf. Verbandsrichtlinien
- ggf. Konzernrichtlinien zum Datenschutz
- Berufsethos.

Die geprüften Fragestellungen und eingesehenen Dokumente und Aufzeichnungen zeigen, was konkret die Grundlage der Feststellungen bildete. Die Aufzählung der eingesehenen Dokumente und Aufzeichnungen vermeidet spätere Missverständnisse.

Feststellungen können sich in Abweichungen (Rechtsverstöße) und Empfehlungen aufgliedern. In vielen Bereichen wird jedoch zur Vereinfachung des Vorgehens keine Unterscheidung zwischen Abweichungen und Empfehlungen unternommen. Letztlich kann an der Umsetzungsfrist die Dringlichkeit der auf die getroffenen Feststellungen folgenden Maßnahmen festgestellt werden. Andere heben im Maßnahmeplan Rechtsverstöße mit einer farbigen (zumeist roten) Markierung hervor. Dies ist allein dem Gustus des DSB bzw. der betreffenden Organisation überlassen. Der Auditbericht wird vom DSB bzw. internen Auditor unterzeichnet und wird zum Ableiten von Korrektur- und Präventionsmaßnahmen dem betroffenen Bereich überlassen.

Der Maßnahmeplan wird nicht vom Auditor, sondern vom auditierten Bereich aufgestellt. Hier endet die Verantwortlichkeit des Auditors. Selbstverständlich sollte er seine Fachkenntnis gegenüber dem betroffenen Bereich einbringen und an Lösungsvorschlägen beteiligt sein. Es handelt sich hier eben um ein internes und nicht um ein Audit in einem akkreditierten Verfahren. An den Maßnahmeplan sind Forderungen hinsichtlich

- der Aufstellung der Maßnahmen,
- der zeitlichen Planung für die Umsetzung,
- der Verantwortlichkeiten für die Umsetzung der Maßnahmen- und der Umsetzungskontrolle

zu stellen.

Den Maßnahmeplan unterzeichnen die Mitarbeiter des Bereichs, die Verantwortlichkeiten im Maßnahmeplan übernommen haben. Sie leiten den Maßnahmeplan dem Auditor zwecks Überwachung zu.

Auditbericht Vorlage

Unternehmen: ...

Datum: ... Beginn: ...

Ende: ...

Auditierter Bereich: ...

Verantwortlicher des Bereichs: ...

Auditor: ...

Anwesende: ...

Geprüfte Fragestellungen und rechtliche Grundlagen: ...

...

...

...

Revision: Änderungsdatum: Seite: 1 von 2

Feststellungen: ...

...

...

...

_____

Unterschrift Auditor

Maßnahmeplan

Nr.	Maßnahme	Verantwortlich	Termin	Erledigt am: durch	Überprüft am: durch
1					
2					
3					
...					

_____

_____

_____

_____

Unterschriften Verantwortliche
für Maßnahmeumsetzung

Revision: Änderungsdatum: Seite: 2 von 2

Beispiel

Auditbericht

Unternehmen: Muster GmbH mit Sitz in ...

Datum: ... 20.. Beginn: ...

Ende: ...

Auditierter Bereich: ...

Verantwortlicher des Bereichs: ...

Auditor: ...

Anwesende: ...

Geprüfte Fragestellungen gemäß BDSG in der letzten gültigen Fassung:

§ 1	Anwendungsbereich des BDSG
§ 53	Datengeheimnis
§§ 32–36 §§ 55–59	Rechte des Betroffenen
§ 47	Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten
§ 51	Einwilligung

§ 64 Anforderungen an die Sicherheit der Datenverarbeitung
§ 26 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses
§ 71 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
§ 67 Durchführung einer Datenschutz-Folgenabschätzung
§ 70 Verzeichnis von Verarbeitungstätigkeiten

Feststellungen:

- Der neue Server für den Bereich R&D wurde erfolgreich in Betrieb genommen. Der R&D-Bereich ist nun auf einer eigenständigen Serverplattform verankert. Die Verarbeitungsverzeichnisse für Herrn XY und Herrn XY sind daraufhin neu zu erstellen.
- Der Test mit der Verschlüsselungssoftware von Muster Firma verlief negativ. Seitens Muster Firma soll nun ein neues System angeboten werden. Die Verhandlungen hierzu wurden bereits aufgenommen.
- Eine konzernweite Regelung zum Umgang mit der betrieblichen Hardware (z. B. PCs, Blackberry) wurde seitens der Konzernführung entwickelt.
- Der Test zur Wiederherstellung der Datensicherungen wurde erfolgreich durchgeführt.
- Die schriftliche Datenschutzvereinbarung zwischen Muster GmbH und Muster Firma zum Datenschutz wurde noch nicht geschlossen.
- Von der Reinigungsfirma sind die Namen all jener Personen abgefragt worden, die tatsächlich die Räume reinigen, inkl. der Vertretungen. Die polizeilichen Führungszeugnisse hierzu sind eingeholt.
- Das Meeting der Arbeitsgruppe „Datenstrukturoptimierung“ hat stattgefunden. Das Protokoll sollte nach Fertigstellung dem Datenschutzbeauftragten zugesendet werden. Zugriffsrechte sind damit auf das notwendige Maß eingeschränkt.
- Ein Notfallplan, in dem beim Ausfall bestimmter IT-Komponenten alle notwendig werdenden Notfallaktionen dokumentiert sind, liegt nicht vor. Dieser Notfallplan wird zz. ausgearbeitet.
- Es ist zu prüfen, wie bei der Nutzung von Cloud-Diensten (z. B. Microsoft 365) aus datenschutzrechtlicher Sicht zu verfahren ist.
- Die Ordner „Scanner EG“ und „Scanner OG“ auf „PCCOMMON“ sollten durch die Nutzer häufiger gelöscht werden. Es befanden sich im Überprüfungszeitpunkt z. B. Scandateien aus dem Dezember 2011 im Ordner „Scanner OG“.
- In den namentlichen Ordnern, z. B. „Müller“, „Meier“, auf dem Laufwerk „XY_Daten:“ befinden sich teilweise persönliche Daten, wie z. B. eigene Urlaubspläne. Es sollte überprüft werden, ob die betroffenen Nutzer diese Dateien löschen bzw. sperren. Des Weiteren sollte eine klare Strukturierung des Laufwerkes „XY_Daten:“ festgelegt werden, z. B. eine Sperrung von Ordnern für bestimmte Nutzer, da hier zz. alle Arten von Daten abgelegt werden. Zum internen Austausch von Daten wurde das Laufwerk „Z-Common“ zur Verfügung gestellt.

Die Verarbeitungsverzeichnisse von Frau XY, Frau XY, Frau XY und Herrn XY wurden am Tag des Datenschutzaudits aktualisiert bzw. erstellt.

_____

Unterschrift Auditor

Maßnahmeplan

Nr.	Maßnahme	Verantwortlich	Termin	Erledigt am: durch	Überprüft am: durch
1	Der neue Server für den Bereich R&D wurde erfolgreich in Betrieb genommen. Der R&D-Bereich ist nun auf einer eigenständigen Serverplattform verankert. Die Verfahrensverzeichnisse für Herrn XY, Herrn XY sind daraufhin neu zu erstellen.	DSB	Ende März 20..		
2	Der Test mit der Verschlüsselungssoftware von Muster Firma verlief negativ. Seitens Muster Firma soll nun ein neues System angeboten werden. Die Verhandlungen hierzu wurden bereits aufgenommen.	DSB	Ende Februar 20..		
3	Die schriftliche Datenschutzvereinbarung zwischen Muster GmbH und Muster Firma zum Datenschutz wurde noch nicht geschlossen.	DSB/Leiter Bereich	bis 15.02.20..		
4	Das Meeting der Arbeitsgruppe „Datenstrukturoptimierung“ hat stattgefunden. Das Protokoll sollte nach Fertigstellung dem Datenschutzbeauftragten zugesendet werden.	Leiter der Arbeitsgruppe	15.02.20..		
5	Ein Notfallplan, in dem beim Ausfall bestimmter IT-Komponenten alle notwendig werdenden Notfallaktionen dokumentiert sind, liegt nicht vor. Dieser Notfallplan wird zz. ausgearbeitet.	Leiter IT/DSB	Ende März 20..		
6	Es ist zu prüfen, wie bei der Nutzung von Cloud-Diensten (z. B. Microsoft 365) aus datenschutzrechtlicher Sicht zu verfahren ist.	DSB	31.01.20..		
7	Die Ordner „Scanner EG“ und „Scanner OG“ auf „PCCOMMON“ sollten durch die Nutzer häufiger gelöscht werden.	alle Leiter der Bereiche	31.01. 20..		
8	In den namentlichen Ordnern, z. B. „Müller“, „Meier“, auf dem Laufwerk „XY_Daten:“ befinden sich teilweise persönliche Daten, wie z. B. eigene Urlaubspläne. Es sollte überprüft werden, ob die betroffenen Nutzer diese Dateien löschen bzw. sperren. Des Weiteren sollte eine klare Strukturierung des Laufwerkes „XY_ Daten:“ festgelegt werden, z. B. eine Sperrung von Ordnern für bestimmte Nutzer, da hier zz. alle Arten von Daten abgelegt werden.	alle Leiter der Bereiche	31.01. 20..		

_____

_____

_____

_____

Unterschriften Verantwortliche
für Maßnahmeumsetzung

4.5.5 Organisation von Gesprächsrunden zum Datenschutz

Der Betriebliche Beauftragte für Datenschutz muss ein Gremium finden, in dem er über seine Tätigkeit berichtet und Lösungsvorschläge für den Datenschutz erörtern kann. Ohne dieses Gremium bleibt die Tätigkeit des Datenschutzbeauftragten häufig abgekoppelt vom Geschäftsalltag. In der Praxis haben sich gute Erfahrungen mit sogenannten Datenschutzrunden bestätigt, in denen Leiter der Bereiche mit Vertretern der Geschäftsleitung und dem DSB quartalsweise über Auffälligkeiten und Probleme im Datenschutz diskutieren. Hier werden wesentliche betriebliche Regelungen zum Datenschutz vorgestellt und freigegeben. Der DSB nutzt die Gesprächsrunden, um Änderungen im Datenschutz, Aktuelles aus der Rechtsprechung und den Medien vorzustellen. Da Themen des Datenschutzes häufig bereichsübergreifend wirksam werden, sind alle Leiter in Lösungsfindungen einbezogen. Über die Sitzungen führt der DSB Protokoll und stellt dieses im Anschluss den Beteiligten zur Verfügung.

An den Datenschutzrunden nehmen selbstverständlich auch Mitglieder des Betriebsrats teil, die ihrerseits die Rechte der Arbeitnehmer vertreten und Informationen an die Belegschaft weitergeben. Auf diese Weise findet Datenschutz nicht neben dem, sondern im Geschäftsalltag statt.

Zur Vorbereitung der Gesprächsrunden sollte eine Tagesordnung rechtzeitig an die Leiter der Organisationseinheiten verteilt werden. Darunter sollte ein Punkt „Sonstiges“ den Teilnehmern die Gelegenheit bieten, Unverstandenes oder Problemsichten zu äußern. Aus Erfahrung kann der Autor berichten, dass zahlreiche Fragen kommen, wenn einmal das Thema Datenschutz Mitarbeitern zu Bewusstsein kommt. Gleichzeitig profitiert der DSB von den Überlegungen, erhält er dann doch vielfältige Impulse für seine weitere Tätigkeit.

Die Dauer der Gesprächsrunden ist selbstverständlich abhängig von

- der Komplexität zu regelnder Fragestellungen im Datenschutz,
- dem Datenschutzniveau.

Eine Besprechungsdauer von maximal 90 Minuten hält die Autorin des Fachbuchs aus den bisherigen Erfahrungen für angemessen.

4.5.6 Überwachung und Kontrolle von Verarbeitungsverzeichnissen gemäß Art. 30 DSGVO/§ 70 BDSG

Die Organisation hat ein Verzeichnis aller Verarbeitungstätigkeiten zu führen, für die sie zuständig ist. Dabei bleibt zu berücksichtigen, dass dieses Verarbeitungsverzeichnis nur zu erstellen ist, wenn

- das Unternehmen mehr als 250 Mitarbeiter beschäftigt oder
- ein Risiko für die Rechte und Freiheiten der Betroffenen besteht und die Verarbeitung nicht nur gelegentlich erfolgt oder
- besondere Datenkategorien oder
- personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten verarbeitet werden.

Merke

Verarbeitungsverzeichnisse nicht für alle Unternehmen notwendig, sondern nur bei Vorliegen genannter Bedingungen.

Hinweis

Verfahren stellen eine Sammlung gleichwertiger Verarbeitungen dar, die über eine vom Verantwortlichen festgelegte Zweckbestimmung verbunden sind, zum Beispiel Personen oder Kundenverwaltung.

Verarbeitung stellt eine IT-Anwendung dar, beispielsweise die Personalabrechnung.

Ein **Verarbeitungsverzeichnis** ist eine Übersicht über alle Verarbeitungstätigkeiten, die der Zuständigkeit des Verantwortlichen unterliegt (Art. 30 EU-DSGVO).

Grundlage für Verarbeitungsverzeichnisse sind interne Verarbeitungsübersichten, die dem DSB von den Fachabteilungen zur Verfügung gestellt werden. Hier sind alle automatisierten Verarbeitungen aufzulisten, bei denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Darunter fallen beispielsweise SAP-Anwendungen, Excel-Listen, -Übersichten u. a. m. Die Zusammenstellung der Übersicht ist Arbeitsgrundlage für den DSB, z. B. für die Ableitung von datenschutzrechtlichen Maßnahmen, betriebsinterne Regelungen oder auch Schulungen. Sie dient gleichzeitig Dokumentationszwecken. In der Praxis hat sich jedoch vielfach herausgestellt, dass die Unterstützung der Fachabteilungen diesbezüglich gering ist. Hierfür besteht häufig weder die Wissensbasis hinsichtlich der möglichen Anforderung noch die Methodik how to do. Aus den Erfahrungen der Autorin übernimmt der DSB entweder diese Aufgabe selbst oder er muss hierfür eine Vorlage (ein Formblatt) liefern und die Fachabteilungen in der Handhabung zuvor unterweisen.

Für die Erarbeitung eines Verarbeitungverzeichnisses soll nachfolgendes Muster dienen.

Vorlage

Verarbeitungverzeichnis (Muster)

Name des Verantwortlichen:

Unternehmen: xy GmbH, Anschrift

Geschäftsführung: Name, Vorname, Telefonnummer

IT-Verantwortlicher: Name, Vorname, Telefonnummer

Datenschutzbeauftragter: Name, Vorname, Telefonnummer

Bereich/Organisationseinheit: xy

Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten (ggf. getrennt beschreiben):

Mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten beauftragte Personen:

Mitarbeiter Name, Vorname	Datenkategorie personenbezogener Daten	Empfänger der Daten	Regelfrist für Löschung

Übermittlung von Daten: ...

Übermittlung in Drittstaaten: ...

Übermittlung in eine internationale Organisation:

Technische Maßnahmen:

Revision: Änderungsdatum: Seite: 1 von 2

Organisatorische Maßnahmen:

Datum:

Fachlicher Leiter	DSB	Geschäftsführer

Revision: Änderungsdatum: Seite: 2 von 2

Nachstehende beispielhaft ausgefüllte Vorlage soll den Umgang mit Verarbeitungsverzeichnissen verdeutlichen:

Vorlage

Verarbeitungsverzeichnis

Personalbuchhaltung: Frau xy

1. Verantwortlicher der Verarbeitung personenbezogener Daten:

Muster GmbH
Straße xy
PLZ Musterort
Telefon:
Telefax:

2. Vertreten durch:

Geschäftsführer: Herr xy
Telefon:
IT-Dienstleister: Mustermann
Auftragsverarbeiter: Muster GmbH
Straße xy
PLZ Musterort
Telefon:

3. Angaben zur Person des Datenschutzbeauftragten:

Name: Herr/Frau
Firma: Mustermann GmbH
Straße xy
Musterort
Telefon:
Telefax:
E-Mail:

Vertreter:

Name:
Firma:
Kontaktdaten:

Revision: Änderungsdatum: Seite: 1 von 7

4. Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten:

Erfassen, Verarbeiten und Speichern von personenbezogenen Daten zur Erstellung der Lohn- und Gehaltsabrechnung, zum Abschluss von Arbeits-, Dienst- und Tarifverträgen.

5. Mit der Erhebung personenbezogener Daten beauftragte Personen:

Mitarbeiter (Name, Vorname)	Art der personenbezogenen Daten/ Übermittlungsweg
Geschäftsführer	Bewerbungsunterlagen, Initiativbewerbungen, Gesundheitszeugnis, Befähigungsnachweise, Personalbogen, Veränderungen persönlicher Verhältnisse, Freistellungsanträge für bezahlten Urlaub, Krankmeldungen, Reisekostenabrechnungen
Sekretärin	Bewerbungsunterlagen, Absagen, Befähigungsnachweise, Krankmeldungen
Unmittelbar Vorgesetzter	Einsicht in Bewerbungsunterlagen, Freistellungsanträge für bezahlten Urlaub
Personalbuchhalterin	Lohnsteuerkarte, Krankenkassenmitgliedschaft, Sozialversicherungsausweis, Befähigungsnachweise, Personalbogen, Veränderungen persönlicher Verhältnisse, Freistellungsanträge für bezahlten Urlaub, Krankmeldungen, Schulungsnachweise, Reisekostenabrechnungen

5a Übermittlung von Daten:

Mitarbeiter (Name, Vorname)	Datenkategorie	Empfänger der Daten	Regelfrist für die Löschung
Personalbuchhalterin	Daten für die betriebliche Altersvorsorge	ABC Consulting Deutschland GmbH über Anmeldeformular per Post	bis zum Tod des Arbeitnehmers
Personalbuchhalterin	Versicherungsmathematische Gutachten	Frau xy durch persönliche Übergabe	bis zum Tod des Arbeitnehmers
Personalbuchhalterin	Lohn- und Gehaltsabrechnungen	Arbeitnehmer über die Vorarbeiter in geschlossenen Briefumschlägen	10 Jahre
Personalbuchhalterin	Sozialversicherungsmeldungen	Krankenkassen, Rentenversicherung, BG, elektronische Datenübermittlung über Software Personalwesen	10 Jahre
Personalbuchhalterin	Lohnsteuermeldung an das Finanzamt	Finanzamt, elektronische Datenübermittlung über Software Personalwesen	10 Jahre
Personalbuchhalterin	Schwerbehindertenabgabe	Arbeitsamt, Übermittlung per Post über Herrn xy	10 Jahre

Mitarbeiter (Name, Vorname)	Datenkategorie	Empfänger der Daten	Regelfrist für die Löschung
Personalbuchhalterin	Fördermittel IHK/SAB	SAB, Übermittlung per Post über Herrn xy	10 Jahre
Personalbuchhalterin	Fördermittel Altersteilzeit	Agentur für Arbeit, Übermittlung per Post über Herrn xy	10 Jahre
Personalbuchhalterin	Ausbildungsverträge	IHK, Übermittlung per Post über Herrn xy	10 Jahre
Personalbuchhalterin	Arbeitsverträge	Arbeitnehmer, persönliche Übergabe oder Übermittlung per Post über Herrn xy	10 Jahre
Personalbuchhalterin	Anträge auf Arbeitslosengeld	Arbeitnehmer, persönliche Übergabe oder Übermittlung per Post über Herrn xy	10 Jahre

5b Übermittlung in EU-Mitgliedstaat:

Mitarbeiter (Name, Vorname)	Datenkategorie	Empfänger der Daten	Regelfrist für die Löschung
Personalbuchhalterin	Arbeitnehmerdaten bei Neueinstellung: Name, Geburtsdatum, Eintrittsdatum, Vorgesetzter, Funktion	Musterfirma Spanien, Übermittlung per E-Mail im Intranet der Musterfirma über Herrn xy	10 Jahre

Die allgemeinen Bedingungen für die Datenübermittlung in einen EU-Mitgliedstaat werden eingehalten. Keine Übermittlung in Drittstaaten oder internationale Organisationen.

Beschreibung der Daten (6–11)

6 Front-Page:

- Eigene Dateien
- Arbeitsplatz
- Netzwerkumgebung
- Internet Explorer
- HP 5550 – Druckassistent
- Lotus Notes 8.5 (passwortgeschützt)
- Sv.net 12.0 (passwortgeschützt) usw.

7 Netzwerklaufwerke:

- Groups auf „xydc01“ (H:)
- Bumkl auf „xydc01“ (U:)

7a Groups auf „xydc01“:

☐ **Anlieferung**	– kein Zugriff
☐ **Anwesenheit**	– Excel-Dateien mit Lohnabrechnungen und Anwesenheitslisten (Dateien passwortgeschützt)
☐ **Daten**	– Allgemeines: Bilder, anlagenbezogen – Datenschutz (Schulungsunterlagen) – Ersatzteilbestellungen (Excel-Dateien) – Frankreich: Bilder, anlagenbezogen – Kristallisation Korrosion: Bilder, anlagenbezogen – Materialverbrauch und Abfall: Excel-Dateien – NOC Kurse (Schulungsunterlagen des Konzerns) – Polysius (Abnahmeprotokolle) – Präsentation: Firmenpräsentation – Reporting: Schriftverkehr mit Konzernmutter (unternehmensbezogene Daten) – Richter: keine Dateien – StBG: Musterbetriebsanweisungen – Umwelt und Sicherheit: Umwelt- und Sicherheitsunterlagen mit unternehmensbezogenen Daten – Unterlagen zur Anlagensicherheit: Gesetzestexte – Versuche Kamera: anlagenbezogene Bilder – Vorlage Bestellung: keine Dateien – Vortrag Big Bag: Präsentation der B.U.S. Freiberg – XXX xy: Bilder anlagenbezogen – Zeichnungen Projekt WOII: *.DWG-Dateien, keine Möglichkeit, Dateien zu öffnen
☐ **FIBU**	kein Zugriff
☐ **Produktion**	kein Zugriff
☐ **Scan**	Anwesenheit Zugriff – keine Dateien
☐ **Silowaggons**	Excel-Tabellen mit Waggonbeladungen
☐ **Technik**	kein Zugriff usw.

7b Verzeichnis Bumkl auf „xydc01“ (U:)

☐ **Archivlohnprogramm**	Excel-Tabellen ohne personenbezogene Daten
☐ **Download**	keine Dateien
☐ **Hs_Dasi**	– Datensicherung vor Umstellung (kein Zugriff) – Elster: Backupdateien des Elsterprogramms ohne personenbezogene oder unternehmensbezogene Daten – La: *.cdb-Dateien (keine Möglichkeit, Datei zu öffnen)
☐ **Monatssicherung**	Backupdateien (kein Zugriff)

☐	**Personal**	Excel-Dateien mit Abrechnungsdaten – kennwortgeschützt
☐	**SicherungLohntaeglich**	*cdb-Dateien (keine Möglichkeit, Datei zu öffnen)
☐	**sv.net sicherung**	*svb-Dateien (keine Möglichkeit, Datei zu öffnen)
☐	**Verträge**	Word-Dateien mit Arbeitsverträgen (kennwortgeschützt)

8 Lotus Notes:

– Inbox: interner E-Mail-Verkehr

9 Ausgabemedien:

– E-Mail-Versand möglich
– Brennen von CDs möglich
– USB-Stick möglich

10 Arbeitsplatz: Eigene Dateien

Word-Dateien mit Abrechnungsdaten – kennwortgeschützt

11 Physisch vorhandene Unterlagen:

in verschließbaren Schränken:

– Personalakten je Arbeitnehmer als Hängeregister
– Lohn- und Gehaltsabrechnungen
– Lohnsteuerbescheide
– Anmeldungen, Schriftverkehr mit Krankenkassen
– Agentur für Arbeit
– Rentenversicherungen und die versicherungsmathematischen Gutachten in separat verschließbarem Schrank im Archiv
– Jährliche Leistungsnachweise der Versicherungen werden in den Personalakten aufbewahrt.
– Statistiken
– in offenen Regalen:
– Informationsmaterial

12 Technische und organisatorische Maßnahmen:

– **Zugangskontrolle**
  - Kontrollierte Schlüsselausgabe. Personenbezogen und unter Ausschluss der Schlüsselweitergabe
  - Personalbüro ist außerhalb der Dienstzeit verschlossen (Sicherheitsschloss)
  - Aufbewahrung des Schlüssels: wird mit nach Hause genommen
  - Zutrittsberechtigte: Fr. xy/Hr. xy
  - Angestellte der Reinigungsfirma
  - Regelung des Umgangs mit externen Dienstleistern (Reinigungsfirma)
  - Führungszeugnis des Dienstleisters abgefordert
  - Kein Zutritt von Unbefugten
  - Verschluss der Schränke (Sicherheitsschloss)

- **Zugriffskontrolle**
  - Determinierung der Zugangsmedien: Passwortschutz
  - Passwort wird alle 2 Monate gewechselt
  - Richtlinie „Regeln für ein gutes Passwort“ allen Mitarbeitern bekannt gegeben
  - Personalisiert durch Benutzerkonto
  - Eingerichtetes System der Kontrolle und Fortschreibung sowie Veränderungen von Zugangsberechtigungen durch xy IT
  - System des sofortigen Entzugs nicht mehr gültiger Berechtigungen
  - Sichere Aufbewahrung des Passworts gewährleistet
  - Implementierung eines Bildschirmschoners (10 Minuten)
  - Schulung der Mitarbeiter
  - Installiertes Berechtigungskonzept
  - Zugriffsnotwendigkeit auf personenbezogene Daten in Abhängigkeit der Aufgabenerfüllung wird mindestens jährlich durch DSB überprüft und protokolliert
  - Kontrolle der Übereinstimmung zwischen dem Zugriff auf physische Daten und dem Zugriff auf elektronische Daten einmal jährlich durch DSB
- **Weitergabekontrolle**
  - Prüfung der Unterscheidung beim Zugriff zwischen Lesen, Verändern, Kopieren und Löschen einmal jährlich durch DSB
- **Übertragungskontrolle**
  - Firewall installiert
  - In Anweisungen festgelegte Übermittlungswege und Datenempfänger
  - Gewährleistung der Protokollierung
  - Überprüfung der Zulässigkeiten der Übermittlung über Vorabkontrolle des DSB
  - Überwachung der Auftragsverarbeitung durch DSB
- **Speicherkontrolle/Eingabekontrolle**
  - Eingabekontrolle über vorliegende LOG-Dateien
  - Protokollierung von Systemaktionen in LOG-Dateien
  - Überprüfung der Vollständigkeit der Protokollierung
  - Prüfung, ob Utilities in die Protokollierung mit einbezogen sind
  - Überprüfung des Schutzes des Protokollierungssystems durch Manipulationen
  - Regelmäßiges Auslesen der LOG-Dateien auf Fehlermeldungen und Verstöße gegen Sicherheitsmaßnahmen
- **Auftragskontrolle**
  - Mitwirkung bei Abschluss detaillierter Verträge mit Dienstleistern durch DSB
  - Nachweis der Zuverlässigkeit der Dienstleister (Führungszeugnis)
  - Nachweis der Schulungen zum BDSG durch den Dienstleister
  - Datenschutzerklärung des Dienstleisters
  - Nennung der mit der Auftragsverarbeitung beauftragten Person
  - Abgestimmte Sicherheitsmaßnahmen mit dem Dienstleister für den technischen und organisatorischen Regelungsbereich

- **Verfügbarkeitskontrolle**
  - Regelmäßige Datensicherung
  - Erarbeitung von Notfallszenarien
  - Ausreichende Brandschutzmaßnahmen sind getroffen
  - Einheitliche Beschaffungsstrategie für IT-Komponenten
  - Einsatz nur geprüfter Fremdsoftware gewährleistet
  - Installierte Freigabeverfahren für neue Komponenten und Verfahren
  - Wartungsvertrag mit IT-Dienstleistern
  - Regelung zur privaten Nutzung von IT-Komponenten
- **Trennungskontrolle**
  - Klassifizierung der Daten in privat und dienstlich
  - Applikationskontrolle auf Datenebene durch DSB
  - Vgl. auch Regelung zur Zugriffskontrolle
- **Zuverlässigkeit und Datenintegrität**
  - Sicherstellung, dass keine Fehlfunktionen zustande kommen
  - Gewährleistung der Meldung von Fehlfunktionen
- **Benutzerkontrolle**
  - Verhinderung der Nutzung durch Unbefugte
- **Allgemeines**
  - Vierteljährliche Risikoanalyse
  - Dokumentation der Schwachstellen in To-do-list
  - Vierteljährliche Durchführung von Datenschutzaudits
  - Brennen von Daten ist möglich
  - Installation von Memory-Sticks ist möglich
  - Internetzugang und E-Mail-Verkehr sind möglich

Datum,

_____

(Leiter Fachbereich)

_____

(Datenschutzbeauftragter)

_____

(Werkleiter)

Revision: Änderungsdatum: Seite: 7 von 7

4.5.7 Aufstellen von Regelungen im Datenschutz

Welche Regelungen im Datenschutz aufzustellen sind, richtet sich nach

- der Größe des Unternehmens
- der Komplexität der Fragestellungen im Datenschutz
- der betrieblichen Praxis
- dem Bewusstseinsgrad der Beschäftigten zum betrieblichen Datenschutz.

Wesentliche Regelungen im Datenschutz sind in der „Liste der Mindestregelungen im betrieblichen Datenschutz“ aufgeführt (siehe Kapitel 14).

Neben Inhalten spielen die Struktur der Regelungen und ihre Formulierung eine nicht unwesentliche Rolle für das Verständnis der Mitarbeiter. Grundsätzlich gilt:

Merke

KISS – **K**eep **i**t **s**hort and **s**imple

Hinweis

Die Struktur der Anweisungen sollte also einfach und überschaubar sein. In etwa so:

1. Zweck	Beantwortet die Frage:	Weshalb gibt es hierfür eine Anweisung?
2. Geltungsbereich	Beantwortet die Fragen:	Für wen gilt diese Anweisung? Wer ist angesprochen?
3. Verfahren	Beantwortet die Frage:	Was soll wer wie womit tun?
4. Mitgeltende Unterlagen	Beantwortet die Frage:	Welche Dokumente stehen im Zusammenhang mit dieser Anweisung?

Bei allen Formulierungen sollte im Deutschen **das Aktiv** und **nicht das Passiv** verwendet werden.

Beispiel

Falsch:	Die Daten werden gesichert.
Hier bleibt offen:	Wer sichert die Daten? Womit werden die Daten gesichert? Wie oft werden die Daten gesichert?
Richtig:	Der Leiter des Bereichs ist für die 14-tägige Sicherung der Daten des Laufwerks xy auf einem Sicherungsband verantwortlich.

Hinweis

Gute Regelungen für den Datenschutz sind im Aktiv geschrieben und beantworten folgende Fragen, die gleichzeitig als Anleitung für den richtigen Satzaufbau dienen:

Wer tut **w**as **w**ann **w**omit **w**ozu in **w**elchen zeitlichen Abständen?

Gute Regelungen beantworten alle W-Fragen!

4.5.8 Umgang mit Hinweisen, Empfehlungen, Beschwerden

Der Datenschutzbeauftragte ist Ansprechpartner in allen datenschutzrechtlichen Fragen für alle Mitarbeiter im Unternehmen. Aus dieser Stellung resultiert auch seine Verpflichtung, Hinweise der Beschäftigten aufzunehmen, sie aus datenschutzrechtlicher Sicht zu werten, Lösungsansätze zu entwickeln und der Geschäftsleitung vorzustellen. Er wahrt die Vertrauensstellung gegenüber den Mitarbeitern insbesondere dann, wenn er über den Umgang mit Kritik oder Empfehlungen zeitnah berichtet. Eine gesetzlich festgelegte Frist zur Behandlung von Mitarbeiterbeschwerden oder Beschwerden Dritter existiert nicht. Es bleibt jeder Organisation daher selbst überlassen, einen angemessenen Zeitraum für Erwiderungen zu bestimmen. In der Praxis haben sich (je nach Schwere und Auswirkung der Kritik) ansonsten Fristen von ca. 3–7 Tagen durchgesetzt. Es handelt sich hierbei nicht um die Erledigungsfrist, sondern um die Frist zur Stellungnahme, ob und ggf. bereits wie mit dem Hinweis, der Empfehlung, der Kritik oder Beschwerde umgegangen wurde.

Das Verfahren zum Umgang mit Äußerungen der Belegschaft oder Dritter zu datenschutzrechtlichen Belangen muss klar und eindeutig definiert sein. Empfehlenswert erscheint hierzu die Beschreibung des Vorgehens im Rahmen einer Anweisung (z. B. Verfahrensanweisung). In der Anweisung „Verfahren zum Beschwerdemanagement im Datenschutz“ sind Anregungen hierfür gegeben.

Verfahren zum Beschwerdemanagement im Datenschutz

Vorlage

1 Zweck

Mit dieser Anweisung wird das Verfahren zur Einreichung von Hinweisen, Empfehlungen und Beschwerden im Datenschutz geregelt. Damit soll sichergestellt werden, dass Mitarbeiter ihr Anliegen jederzeit vorbringen und von einer unparteiischen Person gehört werden können.

2 Geltungsbereich

Der Geltungsbereich erstreckt sich auf alle Mitarbeiter der Muster GmbH.

3 Verfahren

Mitarbeiter der Muster GmbH werden über Aushang und Datenschutzschulung über Möglichkeiten der Beschwerdeführung informiert. Per Aushang am schwarzen Brett werden die Kontaktdaten des externen/internen Datenschutzbeauftragten bekannt gegeben. Der interne Datenschutzbeauftragte (DSB) agiert in datenschutzrechtlichen Belangen weisungsfrei. Als externer Berater wahrt er Unparteilichkeit und Unabhängigkeit.

Hinweise, Empfehlungen und Beschwerden können fernmündlich, schriftlich oder auch in den vereinbarten Terminen persönlich an den DSB eingereicht werden. Der DSB verpflichtet sich, die Hinweise und Beschwerden mit größtmöglicher Vertraulichkeit zu behandeln und sie erst nach Genehmigung des Beschwerdeführers offenzulegen.

Der DSB prüft die Beschwerde aus fachlicher Sicht und verpflichtet sich hiermit, dem Beschwerdeführer binnen 1 Woche eine Antwort zukommen zu lassen. Je nach Beschwerdeart kann ein Termin vor Ort zur Erörterung der Hinweise oder der Beschwerden anberaumt werden. Die Geschäftsleitung der Muster GmbH erklärt, sich offen gegenüber Hinweisen und Missständen im Datenschutz sowie im Hinblick auf die Wahrung des Datengeheimnisses zu zeigen.

Der DSB wird die Beschwerde so lang betreuen, bis eine für beide Seiten zufriedenstellende und rechtskonforme Lösung gefunden ist.

Die Beschwerden werden beim DSB gesammelt und nur nach Freigabe der Beschwerdeführer offengelegt. Die Aufbewahrungsfrist beträgt hier 3 Jahre.

Anlage

Ort, Datum

Datenschutzbeauftragter	Geschäftsführung

Anlage zum Verfahren zum Beschwerdemanagement im Datenschutz

Beschwerden zum betrieblichen Datenschutz können über die Mitarbeiter der Muster GmbH beim Datenschutzbeauftragten

Name, Vorname:

Telefon:

Telefax:

E-Mail:

Adresse:

jederzeit eingereicht werden.

Der Betroffene hat zudem das Recht auf Auskünfte über seine gespeicherten Daten.

Revision:	Änderungsdatum:	Seite: 1 von 1

4.5.9 Jahresbericht des Datenschutzbeauftragten

Aus Sicht der Autorin ist es aus der Praxis heraus empfehlenswert, über die eigene Tätigkeit als Datenschutzbeauftragter regelmäßig zu berichten. Zum einen kann die Berichtstätigkeit mit der Erstellung von Auditberichten einhergehen oder mit formlosen Berichten an die Geschäftsleitung. Zum anderen sollte das erreichte Maß in der Datenschutzorganisation einmal jährlich im Jahresrückblick in einem Jahresbericht an die Geschäftsleitung kommuniziert werden. Für die Erstellung eines Jahresberichts besteht weder Verpflichtung noch Formgebundenheit.

In der Vorlage für einen Jahresbericht werden typische Fragen gestellt und beantwortet, die dem Datenschutzbeauftragten als Leitfaden dienen. Ebenso wären vorab Äußerungen zu bestimmten Themenschwerpunkten möglich oder auch die Abrechnung der Tätigkeit nach den Punkten im Jahresplan in verbaler Form. Soweit der Bericht die Verarbeitung von Personaldaten oder Fragen der betrieblichen Organisation betrifft, wird er auch dem Betriebsrat zugänglich gemacht.

Vorlage

Jahresbericht des Datenschutzbeauftragten der Muster GmbH vom .....

Dokumentation des Status

Ist der Verantwortliche für die Verarbeitung personenbezogener Daten sich seiner Verantwortung bewusst?

.....

Wurde ein Datenschutzbeauftragter bestellt?

.....

Bestehen innerbetriebliche Regelungen, dass er rechtzeitig und ordnungsgemäß in wesentliche Datenverarbeitungen eingebunden wird?

.....

Ist der Datenschutzbeauftragte der zuständigen Behörde gemeldet worden?

.....

Ist eine zentrale Stelle bestimmt worden, die für die Datensicherheit zuständig ist?

.....

Wurden spezielle Sicherheitsrichtlinien erlassen und werden diese auf dem aktuellen Stand gehalten?

.....

Werden die Datenschutzrichtlinien kontrolliert?

.....

Sind Sanktionen bei Nichteinhaltung der Datenschutzrichtlinien vorgesehen?

.....

Entsprechen sämtliche Verarbeitungen den Grundsätzen für die rechtskonforme Verarbeitung personenbezogener Daten?

.....

Ist ein fortlaufendes Risikomanagementsystem für datenschutzrechtliche Belange installiert? Berücksichtigt dieses die Grundsätze der Anonymisierung und Pseudonymisierung?

.....

Revision: Änderungsdatum: Seite: 1 von 5

Ist das Datenschutzrisikomanagement beschrieben?

.....

Besteht ein Verarbeitungsverzeichnis aller Verarbeitungstätigkeiten bzw. ist dies erforderlich?

.....

Ist eine Prozessbeschreibung für die Datenschutz-Folgeabschätzung vorhanden?

.....

Prüfung von DV-Verfahren

Sind die Zuständigkeiten für die Systemverwaltung, Benutzerverwaltung und DV-Revision verschiedenen Personen zugeordnet?

.....

Ist die Netzwerkverwaltung in die Systemverwaltung integriert?

.....

Existiert eine Übersicht über alle Netzwerkkomponenten?

.....

Ist ein Verantwortlicher für die Durchführung der Datensicherung festgelegt?

.....

Wird bei der dezentralen Datensicherung eine regelmäßige automatische Sicherung maschinell erzwungen?

.....

Werden die Datenträger mit der Datensicherung zugriffssicher aufbewahrt?

.....

Gibt es spezielle Anwesenheitsberechtigungen für den Bereich des Serverraums?

.....

Ist die Fremdwartung von DV-Komponenten schriftlich geregelt?

.....

Existieren spezielle Sicherheitsanweisungen für die Datenerfassung, die Datensicherung, die Datenträgeraufbewahrung, die Zugangs- und Zugriffssicherungen?

.....

Wie ist die Entsorgung von Datenträgern oder personenbezogenen Daten in Papierform geregelt?

.....

Wurde mit Dienstleistern eine datenschutzrechtliche Vereinbarung getroffen, wenn sie mit personenbezogenen Daten in Berührung kommen könnten?

.....

Existiert ein schriftlicher Notfallplan, in dem beim Ausfall bestimmter IT-Komponenten alle notwendig werdenden Notfallaktionen dokumentiert sind?

.....

Existieren aufgabenbezogene Zugriffsberechtigungen?

.....

Ist sichergestellt, dass jeder Nutzer über einen eigenen Benutzercode und ein Passwort verfügt?

.....

Werden die Zugriffsrechte eines ausgeschiedenen Mitarbeiters sofort gelöscht?

.....

Ist die maschinelle Verwaltung und Pflege der Zugriffsberechtigungen geregelt?

.....

Werden sichere Passwörter verwendet?

.....

Existieren Vorgaben für ein sicheres Passwort?

.....

Wird die Einhaltung dieser Vorgaben maschinell überprüft?

.....

Ist gewährleistet, dass der Anwender nur Zugriff auf solche Funktionen und Daten erhält, die er zur Erfüllung seiner Aufgaben benötigt?

.....

Ist die Betriebssystemebene für die normalen Nutzer gesperrt?

.....

Ist die Weitergabe der Druckerzeugnisse an die Adressaten geregelt?

.....

Ist die Zuständigkeit für die Datensicherung geregelt?

.....

Ist die Art des Datensicherungsverfahrens dokumentiert?

.....

Ist festgelegt, wann welche Datensicherung zu erfolgen hat?

.....

Werden die Sicherungsdateien gegen Feuer und sonstige schädigende Einflüsse geschützt?

.....

Wird der korrekte Ablauf der Datensicherung überprüft?

.....

Wie wird überprüft, dass überhaupt eine Datensicherung stattgefunden hat (technische Funktionsfähigkeitsüberprüfung)?

.....

Werden externe Datenträger gekennzeichnet?

.....

Werden Originaldaten und Sicherungsdaten getrennt gelagert?

.....

Wird dem Nutzer der Zeitpunkt der letztmaligen Verfahrensnutzung angezeigt?

.....

Erfolgt eine Dunkelschaltung des Bildschirms bei längerer Inaktivität des Geräts?

.....

Existiert eine Strategie zur Bekämpfung von Computerviren?

.....

Ist das interne Netz durch eine Firewall vom Internet abgeschottet?

.....

Wurde die Firewall von einem Fachmann installiert?

.....

Informationspflichten

Wurden die Informationspflichten gegenüber Betroffenen (Mitarbeiter, Kunden, Lieferanten) wahrgenommen?

.....

Auftragsverarbeitung

Wurde die Rechtmäßigkeit der Auftragsverarbeitung geprüft?

.....

Dienstleister

Entsprechen die Dienstleistungsverhältnisse den Anforderungen der DSGVO und des BDSG?

.....

Innerbetriebliche Regelungen

Sind datenschutzrechtliche Regelungen im Unternehmen vorhanden und aktuell:

- Betroffenenrechte
- Beschwerdeverfahren
- Grundsätze der rechtskonformen Verarbeitung personenbezogener Daten
- E-Mail-Nutzung, Internetnutzung
- Umgang mit Ausgabemedien
- Telefondatenerfassung u. a. m.

.....

Internet/E-Mail:

Setzt der Mail-Provider entsprechend geeignete Spam-Filter ein?

.....

Ist den E-Mail-Nutzern bekannt, dass der in einer E-Mail angezeigte Absender leicht gefälscht werden kann (Identitätsdiebstahl, um Vertrauen der E-Mail-Empfänger zu erschleichen)?

.....

Werden vertrauliche Daten nur verschlüsselt per E-Mail verschickt?

.....

Werden E-Mail-Anhänge nicht ungeprüft geöffnet (Malware-Gefahr)?

.....

Sonstiges

Wurden alle Betroffenen auf das Datengeheimnis verpflichtet?

.....

Wurden alle Mitarbeiter im Datenschutz geschult?

.....

Gibt es einen Prüfplan, nach dem der DSB bestimmte Verfahren regelmäßig überprüft?

.....

Ort, Datum

Datenschutzbeauftragter

Revision: Änderungsdatum: Seite: 5 von 5

Die oben aufgeführte Frageliste kann auf die Unternehmenssituation bezogen beliebig erweitert werden.

Die Fragen sind teilweise den im WEKA-Verlag veröffentlichten Checklisten zum Datenschutz entnommen und in einen anderen Kontext gestellt worden.

4.6 Haftung des betrieblichen Datenschutzbeauftragten

Mit der zentralen Aufgabe des DSB, auf die Einhaltung der EU-DSGVO und des BDSG sowie anderer Vorschriften über den Datenschutz hinzuwirken, und der Stellung des DSB im Unternehmen verbinden sich auch Haftungsrisiken. Die beratende Funktion des DSB zieht Grundhaftungstatbestände (§ 280 und § 823 Abs. 1 BGB) nach sich. Dabei ist die o. g. wenig konkrete Formulierung und auch die recht große Aufgabenzuweisung des DSB wenig hilfreich.

Hinweis

Haftung gegenüber Verantwortlichen für Verarbeitung personenbezogener Daten (Haftungsvoraussetzungen)

- Haftung aus Vertrag (vgl. § 280 BGB u. a.):
  - **Pflichtverletzungen des betrieblichen DSB:** z. B. Falschberatung, Untätigkeit – Beweislast trägt grundsätzlich der Geschädigte!
  - **Verschulden des betrieblichen DSB:** Vorsatz Fahrlässigkeit – Beweislast: Schädiger hat Nichtverschulden zu beweisen! Das entfällt bei internen betrieblichen DSB gem. § 619 a BGB!
  - **Kausalität:** Schadenseintritt durch Pflichtverletzung – Beweislast trägt grundsätzlich der Geschädigte!
- Haftung aus § 823 Abs. 1 BGB: Beweislast durchweg beim Geschädigten!
  - Schutzgutverletzung: z. B. Verletzung des informationellen Selbstbestimmungsrechts
  - Verschulden (Vorsatz oder Fahrlässigkeit)
  - Schadenseintritt durch Verletzungshandlung (Kausalität)

[Quelle: TÜV Nord Akademie (2007): Ausbildungsunterlagen für den Datenschutzbeauftragten (TÜV)]

Im BDSG wird einerseits die unterstützende Funktion der Aufsichtsbehörden manifestiert, andererseits jedoch auch die Berechtigung der Aufsichtsbehörde, den Datenschutzbeauftragten wegen mangelnder Fachkunde oder Verstößen gegen die datenschutzrechtlichen Vorschriften abzubestellen, was eine strafrechtliche Verfolgung aufgrund

- mangelnder oder unterlassener Beratung sowie
- Falschberatung

inkludiert.

Sowohl die EU-DSGVO als auch das BDSG halten umfangreiche Sanktionen bereit, siehe Katalog der Sanktionen, je nachdem, welcher konkrete Verstoß vorliegt.

Aus der Praxis heraus gesehen gestaltete es sich bisher eher schwierig, einen internen DSB in die Haftung zu nehmen. In vielen Fällen hat das Unternehmen nicht ausreichend Zeit, Mittel und Raum

- für die Weiterbildung des DSB,
- für die Erfüllung seiner Aufgaben und
- für den Zugriff auf notwendige Datenbestände

zur Verfügung gestellt.

Gleichwohl müssen Verantwortliche nun mit weitaus höheren Strafen für Nichtstun rechnen als je zuvor.

Anders bei externen Datenschutzbeauftragten, deren Aufgaben (hoffentlich) viel konkreter geregelt und abrechenbar sind. War bereits bei Vertragsabschluss abzusehen, dass der Zeitaufwand für eine ordnungsgemäße Erfüllung der Aufgaben des DSB nicht ausreichen würde, ist hier bereits die Zuverlässigkeit des DSB in Frage zu stellen und ggf. der Haftung zu unterziehen.

4.7 Kontrolle des betrieblichen Datenschutzes durch Aufsichtsbehörden

Wesentliche Aufgabe der Aufsichtsbehörde ist die Kontrolle des Vollzugs der rechtlichen Anforderungen an den betrieblichen Datenschutz.

Grundsätzlich verfolgt die Aufsichtsbehörde dabei nachstehende Interessen:

- Wahrung des Datenschutzes bei der Verarbeitung personenbezogener Daten
- Einhaltung datenschutzrechtlicher Bestimmungen bei der Verarbeitung oder Nutzung personenbezogener Daten in und aus automatisierten Dateien
- Entfaltung von Aktivitäten bei
  - begründeter Darlegung eines Betroffenen oder bei
  - Anhaltspunkten, dass Persönlichkeitsrechte und/oder Vorschriften verletzt wurden.
- Auskünfte für Aufsichtsbehörden anderer EU-Mitgliedstaaten.

Aufsichtsbehörden können jederzeit kontrollierend tätig werden. Ihnen sind alle den Datenschutz betreffenden Regelungen, Dokumente vorzulegen und der Zugang zu allen DV-Systemen zu gewähren.

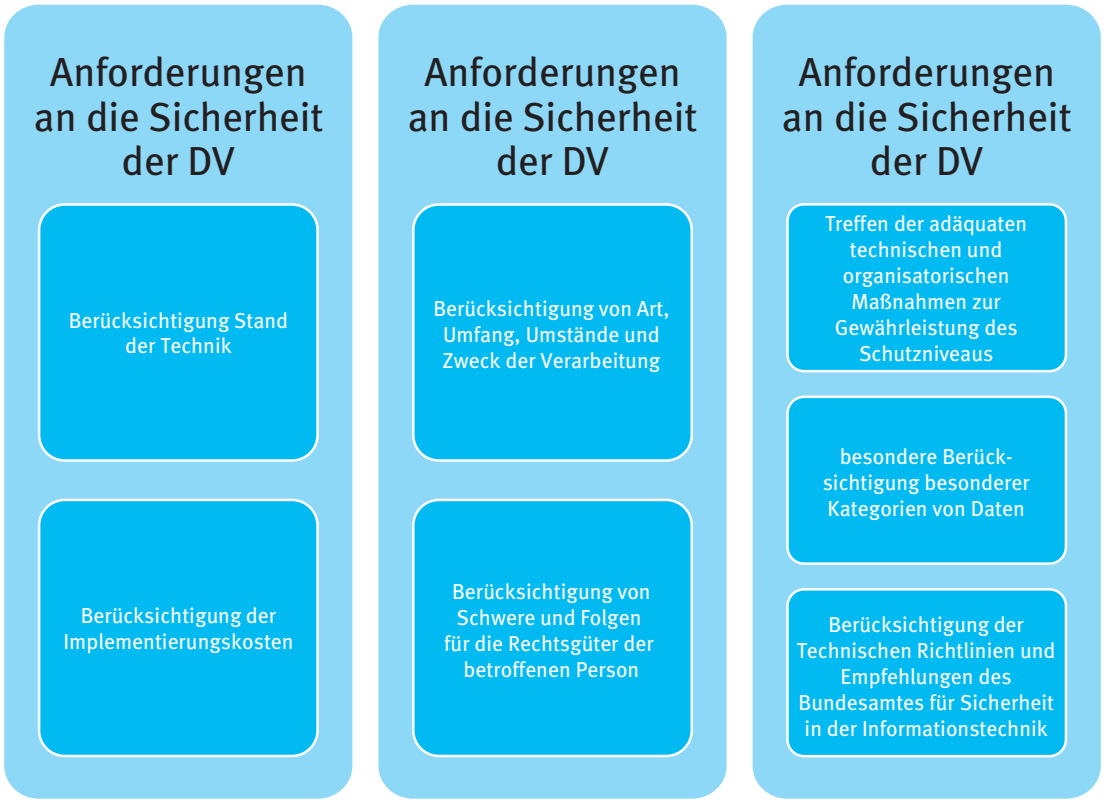
Gewinnt die Aufsichtsbehörde im Zuge ihrer Kontrollen die Ansicht, dass der DSB nicht über die erforderliche Fachkunde und Zuverlässigkeit verfügt, so kann sie ihn abberufen. Weitere Befugnisse der Aufsichtsbehörde werden u. a. in den folgenden Paragraphen des BDSG geregelt: § 38 (3), (4) und (5).

Die Zuständigkeit der Aufsichtsbehörde für Unternehmen mit mehreren Niederlassungen richtet sich nach Artikel 4 Nr. 16 der EU-DSGVO und orientiert sich damit an der Begriffsdefinition „Hauptniederlassung“. Sollten sich mehrere Aufsichtsbehörden für zuständig oder unzuständig halten, wird eine entsprechende Entscheidung getroffen, welche Aufsichtsbehörde die „federführende“ sein wird. Dies erleichtert erheblich das Vorgehen, zumal jetzt nicht mehr damit zu rechnen ist, dass unterschiedliche Entscheidungen je nach Aufsichtsbehörde getroffen werden.

5 Technische und organisatorische Maßnahmen im Datenschutz

5.1 Organisatorische Maßnahmen versus technische Maßnahmen

Im Datenschutz ist die Durchführung technischer sowie organisatorischer Maßnahmen von außerordentlicher Bedeutung. Verantwortliche und Auftragsverarbeiter haben Folgendes sicherzustellen:



Anforderungen an die Sicherheit von Datenverarbeitungen können auch die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen. Insofern greift hier das Prinzip der Datensparsamkeit. Soweit möglich ist von Anonymisierung und Pseudonymisierung Gebrauch zu machen, auch privacy-by-design und privacy-by-default genannt. Die Grundsätze sind bereits bei der Planung von Verarbeitungen zu berücksichtigen.

Hinweis

Die aufgeführten Maßnahmen sollen
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit der System und Dienste

sicherstellen und die
- Verfügbarkeit bei physischem oder technischem Zwischenfall

gewährleisten.

Technischen Maßnahmen wird automatisch der höhere Stellenwert zugeschrieben. Es herrscht das Vorrangprinzip.

Insbesondere ist den Grundsätzen des Datenschutzes durch Technik (data protection by design) und datenschutzfreundliche Voreinstellungen (data protection by default) Genüge zu tun (EU-DSGVO EG 78).

Personenbezogene Daten sind demnach zum frühestmöglichen Zeitpunkt zu anonymisieren oder pseudonymisieren, soweit dies der Verarbeitungszweck möglich macht. Voreinstellungen sollen so getroffen werden, dass nur solche personenbezogenen Daten verarbeitet werden können, die auch nur für den Verarbeitungszweck erforderlich sind.

Hinweis

Voreinstellungen sollen

- die Menge der erhobenen Daten
- den Umfang ihrer Verarbeitung
- ihre Speicherfrist
- ihre Zugänglichkeit
- ihre Übermittlung

einschränken.

Anforderungen an die Sicherheit der Datenverarbeitung werden im § 64 BDSG eindeutig formuliert. Nachstehend wird unter 5.2 eine Checkliste abgebildet, die eine Kontrolle und Überwachung der vom Gesetzgeber vorgegebenen Sicherheitsmaßnahmen gewährleisten soll.

Die Anwendung der Checkliste in der Praxis deckt oftmals viele Verstöße gegen den Datenschutz auf. Hier einige Beispiele für die Missachtung einfachster Regelungen im Datenschutz:

Beispiel 1

Ein Ordner, in dem Schriftverkehr, Datenträger, Lieferanten- und Kundenakten aufbewahrt werden, ist frei zugänglich.

Achtung: Räume, in denen Kunden- oder Lieferantenakten, d. h. personenbezogene Daten gelagert werden, müssen verschlossen sein. Dabei gilt das Prinzip der doppelten Sicherung. Dieses besteht zum einen im Verschluss des Raumes und zum anderen in der Aufbewahrung der Unterlagen in verschlossenen Schränken.

Beispiel 2

Kopierer, Drucker o. ä. Technik können nicht in Räumen aufgestellt werden, in denen ein Zugang und Zugriff durch nicht befugte Personen möglich ist, z. B. in Warte- und Seminarräumen, Vorzimmern, in denen sich Dritte ohne Beaufsichtigung Zugang zu Daten verschaffen könnten.

Beispiel 3

Zugangsrechte zu DV- oder Archivräumen sind nicht definiert. Der Schlüssel für einen Raum, in dem personenbezogene Daten aufbewahrt werden, hängt offen am Brett.

Achtung: Zugangsrechte sollten schriftlich geregelt werden. Für den Empfang oder die Verwaltung des Schlüssels sollte der Empfänger/Verwalter unterzeichnen. Eine datenschutzrechtliche Belehrung ist unerlässlich. Ein offener Zugang zu Schlüsseln sollte vermieden werden.

Beispiel 4

Auf diverse Laufwerke können alle Mitarbeiter zugreifen oder der Personenkreis, der beispielsweise auf Personaldaten zugreift, ist zu wenig eingeschränkt.

Achtung: Zugriffsrechte auf Laufwerke und Dateien sind konsequent zu regeln. Dabei ist entscheidend, dass nur jene Anzahl an Personen Zugang zu personenbezogenen Daten erhält, die für die Aufgabenerledigung unbedingt unerlässlich ist.

Beispiel 5

Scan-Verzeichnisse dienen als Zwischenspeicherung von gescannten Daten, darunter auch von personenbezogenen Daten. Diese werden häufig nicht gelöscht.

Achtung: Im allgemeinen Scan-Verzeichnis sammeln sich oft Daten an, die aus Zeitmangel nicht gelöscht werden. Bei der Auswertung der Scan-Verzeichnisse stellt sich häufig heraus, dass sich darunter viele Dateien mit personenbezogenen Daten befinden.

5.2 14 Kontrollbereiche der technisch-organisatorischen Regelungen im Datenschutz

Der Verantwortliche für die Verarbeitung personenbezogener Daten hat alle notwendigen technischen und organisatorischen Maßnahmen zu treffen, die nach der EU-DSGVO und dem BDSG erforderlich sind. Die geforderten technisch-organisatorischen Regelungen im Datenschutz basieren auf 14 Kontrollbereichen.

Diese Grundsätze werden aus Sicht der Datenschutzbehörde nicht selten vernachlässigt und bilden immer wieder Anlass für öffentliche Kritik, Datenpannen und Skandale.

Die 14 Kontrollbereiche im Datenschutz umfassen:

- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übertragungskontrolle
- Transportkontrolle
- Wiederherstellbarkeit
- Zuverlässigkeit
- Datenintegrität
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungskontrolle

Die 14 Kontrollbereiche können mithilfe einer Checkliste im Unternehmen kritisch hinterfragt werden.

Vorlage

Checkliste Anforderungen an die Sicherheit der Datenverarbeitung

Anforderung	Erfüllt?	Handlungsbedarf	Termin	Verant-wortlich	Erledigt am:
Verwehrung des Zugangs zu Verarbeitungsanlagen (Zugangskontrolle)					
Verhinderung des unbefugten Lesens, Kopierens, Veränderns, Löschens von Datenträgern (Weitergabekontrolle)					
Verhinderung von unbefugten Eingaben sowie der unbefugten Kenntnisnahme; Veränderung und Löschung personenbezogener Daten (Speicherkontrolle)					
Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen der Datenübertragung durch Unbefugte (Benutzerkontrolle)					
ausschließlicher Zugang zu von ihrer Zugangsberechtigung umfassten personenbezogenen Daten (Zugriffskontrolle)					
Gewährleistung der Überprüfung, wohin personenbezogene Daten übermittelt wurden (Übertragungskontrolle)					
Möglichkeit der nachträglichen Überprüfung, von wem personenbezogene Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (Eingabekontrolle)					
Vertraulichkeit und Integrität bei der Datenübermittlung und beim Transport der Datenträger (Transportkontrolle)					
Wiederherstellbarkeit von eingesetzten Systemen nach Störungen (Wiederherstellbarkeit)					

Anforderung	Erfüllt?	Handlungsbedarf	Termin	Verant-wortlich	Erledigt am:
Gewährleistung, dass alle Funktionen im System zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit)					
Sicherstellung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)					
Gewährleistung der Verarbeitung personenbezogener Daten im Auftrag nur entsprechend Weisung des Auftraggebers (Auftragskontrolle)					
Gewährleistung, dass personenbezogene Daten gegen Verlust und Zerstörung geschützt sind (Verfügbarkeitskontrolle)					
Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennbarkeit)					

Revision: Änderungsdatum: Seite: 2 von 2

Vgl. hierzu auch Anweisung zu „Anforderungen an die Sicherheit von DV-Anlagen“ (Anhang 15) und Checkliste (Anhang 10).

5.2.1 Zugangskontrolle

Unter Zugangskontrolle werden vor allem bauliche, technische oder organisatorische Maßnahmen verstanden, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren.

Viele Unternehmen halten die Absicherung des Serverraums für die einzig notwendige Maßnahme und selbst das ist kein Regelfall.

Gerade kleine und mittlere Betriebe, Arztpraxen, Anwaltskanzleien u. a. m. unternehmen nur wenig, um einen Schutz personenbezogener Daten zu gewährleisten. Ausweisleser, Irisscanner und Fingerabdruck (biometrische Verfahren) bieten ein weitaus höheres Schutzniveau, sind jedoch häufig nur bei großen Unternehmen oder bei Laptop-Usern (Fingerprint) in Anwendung. Auch die Einteilung der Verwaltung in verschiedene Sicherheitszonen mit unterschiedlichen erhöhten Zugangsstufen erscheint sinnvoll, ist jedoch in der Praxis kaum durchgesetzt.

Neben technischen Lösungen können an dieser Stelle organisatorische Regelungen helfen. Beispielsweise ist eine Zugangsmöglichkeit nur zu bestimmten Zeiten, in Anwesenheit einer zweiten Person oder mit Kameraüberwachung vorstellbar, auch wenn bei letzter Möglichkeit nur eine Rückverfolgbarkeit gewährleistet werden kann (Zugangsprotokollierung).

In Abhängigkeit vom zu erzielenden Schutzniveau sollen an dieser Stelle beispielhaft einige der grundlegenden Maßnahmen zur Realisierung einer Zugangskontrolle aufgeführt werden:

– klare Zuweisung der Verantwortlichkeit für die Zugangskontrolle in Kooperation mit dem DSB

- Überwachung des Betriebsgeländes durch Videosysteme
- Kontrolle des Zugangs am Gebäude (Pförtner, kontrollierte Schlüsselausgabe für Schließanlage u. a. m.)
- Kontrollgänge oder Installation von Alarmsystemen
- Sicherung eventueller Kellerzugänge
- Festlegung der Zutrittsberechtigten, auch bei Dienstleistern, personenbezogene Schlüsselausgabe unter Ausschluss der Schlüsselweitergabe
- Schulung der Mitarbeiter
- Verpflichtung der Mitarbeiter auf die Einhaltung der getroffenen Regelungen
- Regelung des Umgangs mit externen Dienstleistern und Besuchern, Praktikanten und Aushilfen
- Vermeidung von Anreizen, d. h. Einsicht in Läger für Akten oder DV-Anlagen verwehren
- Begehung von sicherheitskritischen Bereichen aus datenschutzrechtlicher Sicht nur mit Begleitperson
- Abfordern von Führungszeugnissen bei Dienstleistern
- Verschluss der Räume und Schränke (Sicherheitsschlösser/Schließanlagen)
- Regelung der Ausgabe von Zutrittsmitteln (Schlüssel, Karten usw.) und Rücknahme
- Ergreifen von Maßnahmen bei Verlust
- zeitliche Beschränkungen von Zugangssberechtigten anstelle Vergabe einer Dauerberechtigung
- Protokollierung der Zugangsberechtigungen in DV-Systemen sowie deren Kontrolle

Ein Beispiel für eine betriebliche Regelung zur Zugangskontrolle ist nachstehend aufgeführt.

Vorlage

Anweisung zur Sicherung des Serverraums

1 Zweck

Der Zugriff zum Server ist im Hinblick auf Manipulationsversuche zu erschweren, ein unerlaubter Datenzugriff auf personenbezogene Daten zu verhindern.

2 Geltungsbereich

Der Geltungsbereich erstreckt sich auf die Mitarbeiter, die Zugang zum Server haben müssen.

3 Verfahren

Der Serverraum befindet sich im Keller des Verwaltungsgebäudes am Unternehmensstandort.

Der Zugang wird durch Beschilderung eingeschränkt. Unbefugten Personen ist der Zugang nicht gestattet. Der Server befindet sich in einem elektrischen Betriebsraum mit Schaltschränken. Zugang zum Serverraum mit Schlüsselgewalt haben:

- 2 Elektriker
- Herr xy

Befugte Personen sind weiterhin:

- die Mitarbeiter von xy IT
- deren beauftragter Dienstleister: Herr x, Herr y
- der Geschäftsführer der Muster GmbH

Revision:	Änderungsdatum:	Seite: 1 von 2

Der Raum ist mit Warnschildern versehen, die darauf hinweisen, keine Rauchentwicklung entstehen zu lassen. Der Raum ist mit einem Ionisationsfeuermelder ausgerüstet, der bei Rauchentwicklung Feueralarm auslöst.

Der Serverraum ist unbedingt verschlossen zu halten.

Der Serverschrank ist nur von den EDV-Fachleuten zu öffnen. Er muss unbedingt vom Fachpersonal geschlossen gehalten werden, um einen unerlaubten Datenzugriff zu vermeiden.

4 Mitgeltende Unterlagen

Belehrung

Revision: Änderungsdatum: Seite: 2 von 2

Die Zugangskontrolle soll verhindern, dass Datenverarbeitungsanlagen von Unbefugten genutzt werden können. Sie umfasst die Art und Stärke der Zugangsmedien, die Aufbewahrung von Informationen und Medien mit Informationen sowie deren Vernichtung.

Neben dem Zugang zu PCs, Laptops, Blackberrys sind auch die Zugänge zu mobilen Endgeräten in die Betrachtung einzubeziehen. Viele dieser mobilen Endgeräte sind multifunktional einsetzbar, beispielsweise als Drucker, Kopierer und Faxgerät. Eine Zugangskontrolle in diesem Beispiel könnte über Identifikationskarten erfolgen, um eine Übermittlung von Daten von Unbefugten wirksam zu verhindern.

Daher sollten nachstehende Maßnahmen den Rahmen für eine wirksame Zugangskontrolle bilden:

- Determinierung der Zugangsmedien (Passwort, Ausweis, Identifikationskarten)
- Erstellen von Zugangsberechtigungen für Geräte und Benutzer
- Kontrolle der Zugangsberechtigungen auf Veränderungen, Fortschreibung sicherstellen
- Entzug nicht mehr gültiger Berechtigungen
- sichere Aufbewahrung der Zugangsmedien
- Implementierung von Bildschirmschonern
- Abschottung interner Netzwerke vor Angriffen (Firewall)
- Risikoanalyse durchführen
- Durchführung von Audits zur Überprüfung der Wirksamkeit der Zugangskontrolle
- Absicherung der Übertragungsleitungen.

5.2.2 Zugriffskontrolle

Oft werden Sicherheitsmaßnahmen zur Zugangs- und Zugriffskontrolle verwechselt. Im Unterschied zu den vorgenannten beiden Grundsätzen zielt die Zugriffskontrolle auf die Art und Sicherheitsstufe der Autorisierung sowie auf die Identifizierung und Verschlüsselung der Informationen. Mit der Zugriffskontrolle soll gewährleistet werden, dass ein Zugriff auf Daten nur von dazu Berechtigten erfolgt. Personenbezogene Daten dürfen bei der Verarbeitung, Nutzung und nach Speicherung nicht von Unbefugten gelesen oder kopiert, verändert oder gelöscht bzw. vernichtet werden.

Maßnahmen für Zugriffskontrollen

Folgende Maßnahmen sollten im Hinblick auf eine wirksame Zugriffskontrolle ergriffen werden:

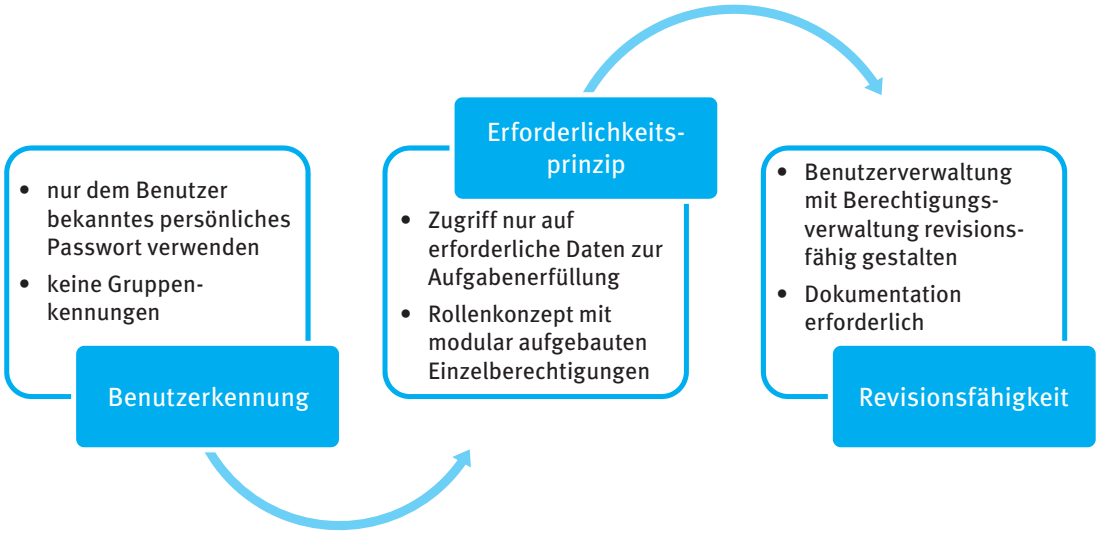
- Aufstellung von Berechtigungskonzepten
- Prüfen, welche Zugriffsnotwendigkeit in Abhängigkeit der Aufgabenerfüllung bei welchen Personen oder Personengruppen überhaupt besteht

- Herstellen der Übereinstimmung zwischen dem Zugriff auf physische Akten/Daten und dem Zugriff auf elektronische Daten, keine Erweiterung des Zugriffs im DV-Bereich
- Unterscheidung beim Zugriff zwischen Lesen, Verändern, Kopieren, Löschen (Wer darf was?)
- Dokumentation der Zugriffsberechtigungen zur Überprüfung im Nachhinein, eine Kopie sollte bei der Geschäftsleitung hinterlegt sein
- aus Sicherheitsgründen sollten die Zugriffsberechtigungen nicht allein in der EDV hinterlegt sein (z. B. Brand, Totalausfall des Systems)
- keine Einrichtung von Zugriffsrechten auf telefonischer Basis, Schrifterfordernis
- Einbindung des Datenschutzbeauftragten in den Prozess.

Bei der Aufstellung von Berechtigungskonzepten muss klar geregelt werden:

- wer (welcher Personenkreis, welche Personengruppen)
- welche Daten und Verfahren
- auf welche Art und Weise (Schreib- und Lesezugriff) nutzen darf.

Beachten Sie bei der Vergabe der Berechtigungen zum Zugriff auf DV-Systeme zusätzlich folgende Hinweise:



Verwendung von Passwörtern

Die Handhabung der Passwortvergabe, -nutzung und -änderung, insbesondere bei nicht sensiblen Daten, weicht in der Praxis häufig von den gesetzlichen Vorgaben zum Zugang und Zugriff auf personenbezogene Daten ab. Nicht selten wird auf die Vergabe von personenbezogenen Passwörtern zugunsten von Gruppenkennungen verzichtet. Eine Rückverfolgbarkeit von unerlaubten Datenzugriffen ist damit natürlich nicht mehr möglich.

Eine wesentliche Aufgabe des Datenschutzbeauftragten besteht deshalb darin, die Passwortvergabe im Unternehmen zu verifizieren.

Ein sicherer Zugangs- und Zugriffsschutz kann nur dann gewährleistet werden, wenn

- jeder Benutzer über ein eigenes Passwort verfügt,
- ein technisches System die Änderung des Passworts spätestens nach 90 Tagen fordert,
- der Benutzer das Passwort jederzeit wieder ändern kann,
- die letzte Änderung des Passworts für den Benutzer angezeigt wird und
- die Änderungshistorie systemtechnisch nachvollziehbar ist.

Das Passwort selbst muss zur Gewährung eines wirksamen Zugangs- und Zugriffsschutzes bestimmte Anforderungen erfüllen. In der Praxis hat sich gezeigt, dass viele Benutzer entweder die Namen, Geburtsdaten ihrer nächsten Verwandten oder Wörter aus ihrer unmittelbaren Arbeitsumgebung nutzen. Folglich sind diese schnell zu erraten. Gute Passwörter weisen hingegen eine Mindestlänge von 8 Zeichen auf und enthalten Ziffern oder Sonderzeichen.

Regeln für ein gutes Passwort sollten Mitarbeitern in Schulungen oder in Anweisungen bekannt gemacht werden.

Vorlage

Leitfaden für ein gutes Passwort

Ein paar Hinweise, wie ein gutes Passwort erzeugt werden könnte:

Es sollte **auf keinen Fall**:

- in einem Wörterbuch (welcher Sprache auch immer) zu finden sein
- ein Trivialkennwort wie „ABC“ sein
- den eigenen (Spitz-)Namen oder den von Familienmitgliedern enthalten
- aus (eigenen) Telefonnummern oder Geburtstagen bestehen
- den Namen der Firma beinhalten
- keinen (Nach-)namen von bekannten Persönlichkeiten, Städten, Plätzen, Gebäuden oder Firmen enthalten
- Eigennamen und beliebte fiktive Namen nutzen (Bond, Enterprise etc.)
- aus Nachbartasten bestehen wie: qwertz(y), mnbvcx oder 12345 usw.
- Rechnernamen, Benutzerkennungen oder Teile davon enthalten
- aus Abkürzungen bestehen
- rückwärts lesbar sein (reteid, reteiD, ...)
- durch Voranstellen oder Anhängen einer Zahl oder eines anderen Zeichens (dieter09, 7dieter, .dieter$, %dieter, ...) modifiziert sein.

Es **sollte**:

- 8 Zeichen enthalten
- nicht nur aus Buchstaben bestehen, sondern auch aus Sonderzeichen und/oder Zahlen
- nur höchstens zwei aufeinander folgende gleiche Zeichen beinhalten
- keine Umlaute enthalten, da die nicht auf allen Tastaturen vorhanden sind
- leicht zu merken sein, da es nicht notiert werden sollte
- dennoch möglichst kompliziert sein.

Es **könnte**:

- aus einem bewusst fehlerhaft geschriebenen Wort bestehen
- eine Zusammensetzung von Substantiven oder Wörtern sein (BahnTunnel)
- aus den Anfangsbuchstaben der Wörter eines Satzes bestehen (Ich liebe meine Arbeit – IlmA ...)
- einen Ersatz des Wortes mit Sinnbildern sein (Dach ^, Punkt .)
- ein Wort in ein anderes eingebettet sein (MHaus)

u. a. m.

Revision:	Änderungsdatum:	Seite: 1 von 1

Es existiert bereits eine große Anzahl von Programmen zum Knacken von Passwörtern. Sind diese mit Wörtern aus Wörterbüchern identisch oder nur geringfügig verändert, ist eine Identifizierung des Passworts leicht möglich. Die Programme gleichen ganze Wörterbücher ab und erkennen auch Veränderungen, wie z. B. „FuSSbaLL“ [Quelle: Probst, Thomas (2012): Passwortlisten großer Webdienste im Umlauf: Lehren für die Praxis. – Datenschutz-Berater Nr. 9, S. 195–196]. Daher wird es umso wichtiger, in Schulungen Mitarbeiter auf die korrekte Auswahl von Passwörtern hin zu sensibilisieren.

Protokollierung von Systemaktionen in Log-Dateien

Systemaktionen sollen über eine Protokollierung in sogenannten Log-Dateien rückverfolgbar gestaltet werden. Auf diese Weise ist eine Überwachung der Zugriffsberechtigungen und der Zugriffe selbst mit den unterschiedlichen Aktionen Lesen, Schreiben, Verändern, Übermitteln, Löschen möglich. Auch abnormale Systembedingungen und Verstöße gegen Sicherheitsmaßnahmen und Fehlaktionen sind damit protokolliert und auswertbar. Aus den protokollierten Fehlermeldungen, die regelmäßig einer Auswertung unterzogen werden müssen, können wertvolle Hinweise zur kontinuierlichen Verbesserung des Schutzniveaus abgeleitet werden. Sie umfassen sowohl technische als auch organisatorische Belange, die entsprechend revidiert werden. Der Datenschutzbeauftragte sollte regelmäßig mit der IT-Organisation des Unternehmens die Auswertung der Log-Dateien vornehmen und geeignete Maßnahmen mit den Verantwortlichen der Bereiche und der Geschäftsleitung abstimmen.

In automatisierten Verarbeitungssystemen haben gemäß § 78 BDSG Verantwortliche und Auftragsverarbeiter mindestens folgende Verarbeitungsvorgänge zu protokollieren:

1) Erhebung
2) Veränderung
3) Abfrage
4) Offenlegung einschließlich Übermittlung
5) Kombination und
6) Löschung.

Hinweis

Protokolle über Abfragen und Offenlegungen müssen
- die Begründung,
- das Datum,
- die Uhrzeit und
- so weit als möglich die Identität der Person, die die Daten offenlegt,
- die Identität des Empfängers der Daten

zu erkennen geben.

Zusammenfassend sind durch den Datenschutzbeauftragten folgende Sachverhalte zu prüfen:
- Möglichkeit der nachträglichen Überprüfung, welche Daten zu welcher Zeit von welcher Person eingegeben wurden
- Überprüfung der Vollständigkeit der Protokollierung
- Sicherstellung der Protokollierung des regelmäßigen Passwortwechsels
- Gewährleistung der Protokollierung von Zugriffsverletzungen
- Schutz des Protokollierungssystems gegen Manipulation
- Einbezug von Utilities in die Protokollierung
- Gewährleistung der Protokollierung von Datensicherungsaktivitäten
- Sicherstellung der Protokollierung von Datenübermittlungen

- Überwachung der Auswertungen und der abgeleiteten Korrektur- und Präventionsmaßnahmen
- Überwachung der Wirksamkeit getroffener Maßnahmen (geschlossenes Korrektursystem)
- Überprüfung, wo und wie Protokollierungen sicher aufbewahrt werden (Festplatte, Magnetbänder, CD ...)
- Überprüfung der Aufbewahrungs-/Löschfristen.

Die Aufbewahrungsdauer von Log-Dateien richtet sich nach den Löschungsregeln der Datenschutzgesetze, nach der Sensibilität der personenbezogenen Daten und nach eventuell vorgegebenen speziellen Aufbewahrungsfristen. Die allgemeinen Löschungsregeln in den Datenschutzgesetzen gehen von einer Speicherung je nach Erforderlichkeit zur Aufgabenerfüllung aus. Eine allgemein festgelegte Frist gibt es also nicht. Steht der Löschung der Log-Dateien nichts Zwingendes entgegen, so besteht sogar die Löschungspflicht.

In der Regel werden Log-Dateien nach maximal 6 Monaten gelöscht.

Hinweis

Die Protokolle über Abfragen und Offenlegungen dürfen ausschließlich zur Überprüfung der Rechtmäßigkeit

- durch den Datenschutzbeauftragten
- den Bundesbeauftragten für Datenschutz
- den Betroffenen
- zur Eigenüberwachung
- zur Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten
- für Strafverfahren

verwendet werden.

Die Protokolle müssen auf Anforderung dem Bundesbeauftragten für Datenschutz zur Verfügung gestellt werden.

Hinweis

Die Protokolldaten sind am Ende des auf deren Generierung folgenden Jahres spätestens zu löschen.

5.2.3 Transportkontrolle, Übertragungskontrolle, Speicherkontrolle

Die Kontrollmaßnahmen erstrecken sich auf die datenschutzkonforme Datenübertragung, den Datentransport sowie auf die Speicherung auf Datenträgern. Personenbezogene Daten dürfen dabei nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. Es muss geprüft und festgestellt werden können, wohin personenbezogene Daten übermittelt wurden.

Eine wesentliche Aufgabe des Datenschutzbeauftragten besteht weiterhin in der Absicherung des E-Mail-Verkehrs. Viele Informationen werden heutzutage über E-Mail kommuniziert. Nicht immer wird dabei dem Schutzbedarf personenbezogener Daten Rechnung getragen. Dies gilt auch für Dateianhänge mit personenbezogenen Daten, z. B. ein Lebenslauf als Anhang zu einem Bewerbungsschreiben. E-Mails mit personenbezogenen Daten sind beispielsweise identitätsbasiert zu verschlüsseln. Häufig wird der Aufwand für solche Verschlüsselungen nicht als angemessen empfunden.

Wesentliche Maßnahmen und Kontrollpflichten für den Datenschutzbeauftragten in diesem Kontrollbereich sind u. a.:

- Überprüfung und Überwachung der Übermittlungswege und der Datenempfänger
- Gewährleistung der Protokollierung
- Erstellen von Anweisungen, welche personenbezogenen Daten wie, auf welchem Wege übermittelt werden sollen

- Überprüfung der Zulässigkeit der Übermittlungen
- Transportregeln für Akten oder Daten erarbeiten
- Auswahl geeigneter Transportdienstleister, Überzeugen von deren Zuverlässigkeit
- Einschalten von Sicherheitsdiensten für Datentransporte
- Anforderungen an Transportbehälter festlegen
- Transportwege sichern
- Empfangsquittierung sicherstellen
- Verwendung der elektronischen Signatur
- Überprüfung der Maßnahmen zur Verhinderung unbefugter Eingabe von personenbezogenen Daten, deren unerlaubte Kenntnisnahme, Veränderung oder Löschung.

5.2.4 Eingabekontrolle

Der Kontrolle sollen Sicherheitsmaßnahmen für die ordnungsgemäße Anwendung von DV-Programmen unterliegen. Konkret ist die spätere Überprüfungsmöglichkeit zu gewährleisten, wer die personenbezogenen Daten eingegeben, verändert oder entfernt hat.

Die digitale Signatur ist eine Möglichkeit der konkreten Zuordnungsfähigkeit und damit ein probates Mittel der Eingabekontrolle.

Grundsätzlich gelten in diesem Kontrollbereich die Festlegungen zur Protokollierung, Überwachung und Auswertung von Log-Dateien wie unter Kapitel 5.2.2 beschrieben.

5.2.5 Auftragskontrolle

Hiermit sind alle Sicherheitsmaßnahmen bei der Auftragsverarbeitung oder auch bei Vergabe von Aufgaben innerhalb der DV gemeint. Die Auftragskontrolle bezieht sich auf die Überwachung der an den Dienstleister gegebenen Weisungen zur Verarbeitung personenbezogener Daten.

Die Besonderheiten der Auftragsverarbeitung werden unter Kapitel 8 „Auftragsverarbeitung“ näher beschrieben. Folgende organisatorische Maßnahmen sollten durch die verantwortliche Stelle ergriffen und vom Datenschutzbeauftragten überwacht werden:

- Nachweis der Zuverlässigkeit der mit der Auftragsverarbeitung beauftragten Dienstleister (Nachweis des Schutzkonzepts, der Schulungen der Mitarbeiter zum BDSG, der Datenschutzerklärungen)
- Abschluss detaillierter Verträge, aus denen der Zweck der Datenverarbeitung, die Kategorie der Daten und die Übermittlungswege unter Beachtung der gesetzlichen Vorgaben hervorgehen
- ggf. Nennung der mit der Auftragsverarbeitung betrauten Personen (Name, Adresse)
- in besonderen Fällen Nachweis des Führungszeugnisses
- Festlegung gemeinsam abgestimmter Sicherheitsmaßnahmen im technischen und organisatorischen Bereich
- Gewährung des Rechts, beim Dienstleister Audits durchzuführen, um sich von der korrekten Auftragsverarbeitung überzeugen zu können.

5.2.6 Verfügbarkeitskontrolle

Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust zu schützen. Maßnahmen der Verfügbarkeitskontrolle beziehen sich folglich auf

- regelmäßige Datensicherungen
- Durchführung einer Schwachstellenanalyse für den Bereich IT

- Erlass von Anweisungen und Sicherheitsrichtlinien
- Erarbeiten von Notfallszenarien
  - Brandschutzmaßnahmen
  - Notfallkonzepte
- Aufstellen von Regelungen zur Aufbewahrung von Datenträgern
- Erarbeiten von Regelungen zur privaten Nutzung von IT-Komponenten unter Sicherheitsaspekten
- Schulung der Mitarbeiter
- einheitliche Beschaffungsstrategie für IT-Komponenten
- Einsatz nur geprüfter Fremdsoftware
- Installation von Freigabeverfahren für neue Komponenten und Verfahren in der DV
- Wartung von IT-Systemen
- Anweisungen hierfür.

5.2.7 Trennungskontrolle

Das BDSG fordert mit dem Trennungsgebot die getrennte Verarbeitung von personenbezogenen Daten unter Beachtung der Zweckbindung der Verarbeitung. Durch den Verantwortlichen muss gewährleistet werden, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden.

Kern der Trennungskontrolle bildet vielmehr die Forderung, dass erhobene personenbezogene Daten im Rahmen ihrer Zweckbindung verwendet werden. Die Zweckbindung bei der Erhebung der personenbezogenen Daten setzt sich in der Datenverarbeitung und -nutzung weiterhin fort.

Eine dahingehende Konzipierung von Datenverarbeitungsprogrammen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können, ist heute kein Problem mehr.

Die Trennungskontrolle bezieht sich auch auf die Trennung privater und dienstlicher Daten, z. B. getrennte Speicherung der Daten auf dem PC, dem Laptop, dem Smartphone. Mit speziellen Regelungen ist sowohl für eine getrennte Verarbeitung als auch für eine getrennte Speicherung zu sorgen. Dem Datenschutzbeauftragten kommen diesbezüglich folgende Aufgaben im Rahmen seiner Überwachungstätigkeit zu:

- Aufstellung betrieblicher Regelungen zur getrennten Datenerhebung, -speicherung und -verarbeitung
- Klassifizierung von Daten in privat und dienstlich
- ggf. Verwendung entsprechender Applikationen (z. B. bei Blackberry)
- Applikationskontrolle auf Datenebene
- möglichst Trennung privater und dienstlicher Smartphone-Nutzung.

6 Datenschutz-Folgeabschätzung, Risikobewertung, Schutzstufenkonzept

6.1 Verhältnismäßigkeit des Maßnahmenkonzepts

Welche Maßnahmen organisatorischer oder technischer Art für den jeweiligen Kontrollbereich abzuleiten sind, richtet sich nach der einzuhaltenden Schutzstufe. Dies setzt voraus, dass eine Einstufung der verschiedenen Arten personenbezogener Daten vorgenommen und die einzelnen Verarbeitungen einer Risikobetrachtung unterzogen wurden. Im Erwägungsgrund 75 der EU-DSGVO hat der europäische Gesetzgeber einen Katalog mit Risikofaktoren veröffentlicht, mit deren Hilfe eine Einstufung der Risiken von Verarbeitungen personenbezogener Daten besser vorgenommen werden kann.

Hinweis

Eine Datenschutz-Folgeabschätzung ist vorzunehmen, wenn gemäß § 67 BDSG „eine Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge“ hat.

Der EG 75 zählt zu den Risiken für die Rechte und Freiheiten natürlicher Personen:

Der Katalog der Risikofaktoren, mithilfe derer eine Datenschutz-Folgeabschätzung vorzunehmen ist, kann der Einstufung von personenbezogenen Daten in sogenannte Schutzstufen dienen.

Schutzstufen personenbezogener Daten sind demnach:

Schutzstufe A	• frei zugängliche Daten • keine Geltendmachung berechtigter Interessen notwendig
Schutzstufe B	• Missbrauch stellt keine besondere Beeinträchtigung dar • beschränkt öffentlich zugängliche Daten, Verteiler für Unterlagen, z. B. akademischer Grad, Berufsbezeichnung, Zugehörigkeit zu einem Verein/Interessensgruppe/Berufsgruppe
Schutzstufe C – Ansehensschädigung	• durch Missbrauch Beeinträchtigung der gesellschaftlichen Stellung oder in wirtschaftlichen Verhältnissen möglich • z. B. Einkommen, Sozialleistungen, Ordnungswidrigkeiten, Grundsteuer
Schutzstufe D – Existenzschädigung	• durch Missbrauch Beschädigung der gesellschaftlichen Stellung oder der wirtschaftlichen Verhältnisse • z. B. Straffälligkeit, schwerwiegende Ordnungswidrigkeiten, psychologische Gutachten, Schulden, Pfändungen, Insolvenzen
Schutzstufe E – Frage von Leben, Tod	• Missbrauch schädigt Gesundheit, Leben, Freiheit • z. B. Daten über mögliche Opfer einer strafbaren Handlung

Hinweis

Die Datenschutz-Folgeabschätzung ist dann durchzuführen, wenn

- systematische und umfassende Bewertungen persönlicher Aspekte natürlicher Personen verarbeitet werden,
- umfangreiche Verarbeitungen besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Abs. 1 oder strafrechtliche Daten gemäß Artikel 10 stattfinden,
- öffentlich zugängliche Bereiche systematisch und umfangreich überwacht werden.

Weiterhin wird in der EU-DSGVO von der Verpflichtung für Aufsichtsbehörden gesprochen, jene Verarbeitungsvorgänge zu spezifizieren, die erhöhte Risiken für den Eigner personenbezogener Daten darstellen könnten. Die Liste ist von der Aufsichtsbehörde zu veröffentlichen. Die in der Liste aufgeführten Verarbeitungsvorgänge müssen mit Datenschutz-Folgeabschätzungen unterlegt werden.

Die Liste der relevanten Verarbeitungsvorgänge für die Datenschutz-Folgeabschätzung muss dem Ausschuss gemäß Artikel 68 gemeldet werden.

Die Aufsichtsbehörde kann auch eine Liste der nicht der Datenschutz-Folgeabschätzung unterliegenden Verarbeitungsvorgänge entwickeln. In Fällen, in denen Verarbeitungsvorgänge nicht genannt sind und die der Verantwortliche und Datenschutzbeauftragte nicht einer Datenschutz-Folgeabschätzung unterziehen würde, ist die Aufsichtsbehörde zu kontaktieren.

In der Folge daraus ergibt sich folgendes methodisches Vorgehen:

1) Prüfen der Vorlage genannter Kriterien für die Verarbeitung personenbezogener Daten
2) Prüfen, ob benannte Folgen sich bei der Verarbeitung personenbezogener Daten einstellen könnten
3) Prüfen, ob die Verarbeitungsvorgänge ggf. in der Liste der Aufsichtsbehörde enthalten sind, die eine Datenschutz-Folgeabschätzung erzwingen

4) Prüfen, ob der Verarbeitungsvorgang in der Liste der ohne Datenschutz-Folgeabschätzung zulässigen Verarbeitungen enthalten ist
5) Entscheidungsfindung, ob eine Datenschutz-Folgeabschätzung durchzuführen ist.

6.2 Folgeabschätzung und Risikobewertung im Umgang mit personenbezogenen Daten

An die Folgeabschätzung werden gemäß Artikel 35 der EU-Datenschutz-Grundverordnung folgende Anforderungen gestellt:

- systematische Beschreibung der geplanten Verarbeitungsvorgänge
- Zweck der Verarbeitung
- verfolgte berechtigte Interessen des Verarbeiters
- Bewertung der Notwendigkeit der Verarbeitung
- Bewertung der Verhältnismäßigkeit der Verarbeitung in Bezug auf den Zweck
- die Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Person gemäß Absatz 1 Artikel 35 EU-DSGVO
- geplante Abhilfemaßnahmen zur Bewältigung der Risiken einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, die den Schutz der personenbezogenen Daten sicherstellen
- die Einhaltung genehmigter Verhaltensregeln
- ggf. Einholung des Standpunkts der betroffenen Person
- Beachtung der Ermessungsgrundlage der EU-Mitgliedstaaten für die Durchführung der Datenschutz-Folgeabschätzung
- Überprüfungsrhythmus, dass das Vorgehen der Datenschutz-Folgeabschätzung entspricht oder noch entspricht
- Ergebnis der Überprüfung und eventuelle Korrekturmaßnahmen

Insofern entspricht dies einer Gliederung für eine Datenschutz-Folgeabschätzung.

Vorlage

Datenschutz-Folgeabschätzung

1 Allgemeines

Bereich:
Datum:
Verantwortlicher für die Verarbeitung:
Datenschutzbeauftragter:

Verarbeitungstätigkeit:

Beginn der Verarbeitung:
Zweck der Verarbeitung:
Art der personenbezogenen Daten:
Umfang der personenbezogenen Daten:
Berechtigtes Interesse:

Besondere Schutzbedürftigkeit gemäß Art. 9 Abs. 1 DSGVO:

Revision: Änderungsdatum: Seite: 1 von 4

Für den Zugriff berechtigte Personen:

Auftragsverarbeitung durch (falls zutreffend):

Übermittlung an:

Übermittlungsweg:

Löschfristen:

2 Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten

Grundsatz	ja	nein	Kommentar
Rechtmäßigkeit der Verarbeitung			
Verarbeitung nach Treu und Glauben			
Transparenz			
Zweckbindung (notwendig und verhältnismäßig)			
Datenminimierung			
Richtigkeit			
Speicherbegrenzung			
Integrität und Vertraulichkeit			
Anforderungen an Eignung technischer und organisatorischer Maßnahmen erfüllt			
Bestehen eigene berechtigte Interessen?			
Überwiegen Rechte der betroffenen Person die eigenen berechtigten Interessen?			
Verarbeitung zur Zweckerreichung notwendig?			
Ist die Verarbeitung verhältnismäßig? Interessensabwägung			

3 Datenschutz-Folgeabschätzung

Risikofaktoren (RF)	Nähere Erläuterung des RF	Eintrittswahrscheinlichkeit (EWS)	Tragweite der Auswirkung (TA)	Risiko* (R)	Präventionsmaßnahmen	EWS*	TA*	R**	Korrekturmaßnahmen
physischer, materieller oder immaterieller Schaden									
Diskriminierung, Identitätsdiebstahl, Identitätsbetrug									
finanzieller Verlust									
Rufschädigung									
Verlust der Vertraulichkeit der dem Berufsgeheimnis unterliegenden Daten									
Aufhebung der Pseudonymisierung									
erhebliche wirtschaftliche und gesellschaftliche Nachteile									
Hinderung an der Ausübung der Rechte des Betroffenen									
unerlaubte Verarbeitung von besonderen Kategorien personenbezogener Daten									
Bewertung persönlicher Aspekte, z. B. Arbeitsleistung, Gesundheit, wirtschaftliche Lage									
Ausspionieren des Verhaltens, des Aufenthaltsorts									
Erstellung persönlicher Profile									
unerlaubte Verarbeitung von Daten Schutzbedürftiger									
eine große Anzahl von Personen betreffend									

Skala:
EWS/TA und EWS*/TA*
1 = gering
2 = mittel
3 = hoch
R* und R** = Produkt der Faktoren

Skala Risiko gesamt:
bis 4 = gering
5–7 = mittel, Maßnahmen erforderlich
über 7 = hoch, Maßnahmen einzuleiten, zu überprüfen und ggf. Konsultation der Aufsichtsbehörde erforderlich

4 Hinnehmbares Risiko

Stellen die risikobehafteten Verarbeitungsvorgänge dennoch bezüglich
- Eintrittswahrscheinlichkeit,
- Umfang, Umstände,
- Schwere des Risikos und
- aufgrund der getroffenen Maßnahmen

ein hinnehmbares Risiko dar?

ja ☐ nein ☐

5 Hohes Risiko

Falls ein hohes Risiko die Folge wäre und keine Maßnahmen der Verringerung des Risikos getroffen wurden oder getroffen werden konnten:
- Wurde die Datenschutzbehörde vor Beginn der Verarbeitung kontaktiert?
- Wurde der Datenschutzbeauftragte einbezogen?

Existieren Ausnahmetatbestände gemäß gesetzlichen Erlaubnisnormen (Art. 35 Abs. 10 DSGVO)?

6 Zusammenfassung

Datum:

Unterschrift	Verantwortlicher	Datenschutzbeauftragter

Revision:	Änderungsdatum:	Seite: 4 von 4

Hinweis

So sich bei der Datenschutz-Folgeabschätzung herausstellt, dass die Verarbeitung personenbezogener Daten ein hohes Risiko zur Folge hat und der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, ist die Aufsichtsbehörde vorab zu konsultieren.

Mit der Feststellung der Aufsichtsbehörde, dass es sich um eine nicht rechtskonforme Verarbeitung personenbezogener Daten handeln würde, unterbreitet die Aufsichtsbehörde an den Verarbeiter/Verantwortlichen für die Verarbeitung im Zeitraster von 6–8 Wochen entsprechende Empfehlungen.

Für die Konsultation muss der Verantwortliche für die Verarbeitung die im Artikel 36 Absatz 3 der EU-DSGVO genannten Unterlagen zur Verfügung stellen.

Ähnlich der Bewertung von Sicherheitsrisiken im Lebensmittelbereich oder im Arbeitsschutz, der Bewertung von Umwelt- und Energieaspekten sind auch datenschutzrechtliche Risiken zu bewerten, um ein angemessenes Datenschutzkonzept entwickeln zu können. Die Evaluierung von Datenschutzrisiken kann auf vielfältige (und bisher nicht vorgeschriebene) Art und Weise erfolgen.

Wie bereits im Formblatt zur Datenschutz-Folgeabschätzung dargestellt, sind wesentliche Kriterien stets die Eintrittswahrscheinlichkeit einer Gefahr und die Tragweite der Auswirkung. Diese Faktoren bestimmen maßgeblich das zu ermittelnde Risiko für die in der Datenschutz-Folgeabschätzung genannten Aspekte. Selbstverständlich können hier noch weitere Faktoren angeführt werden.

Beispielsweise sind noch folgende Kriterien denkbar:

- Häufigkeit der Verarbeitung personenbezogener Daten,
- Tragweite der Auswirkung einer Fehlleitung und
- Tragweite der Auswirkung bei Verlust (Nicht-Wiederherstellbarkeit) als Spezifizierung von „Tragweite der Auswirkung“.

In unserer Vorlage wird das Produkt der Faktoren zur Ermittlung des Risikos ermittelt. Im schlimmsten Fall demnach $3 \times 3 = 9$, im besten Fall $1 \times 1 = 1$. Eine Ermittlung des Risikos über die Faktoren macht nur dann Sinn, wenn der genannte Aspekt überhaupt zutreffend ist.

Die Bewertung erfolgt doppelt, einmal vor der Präventionsmaßnahme und einmal danach. Im besten Fall kann durch die gewählte Prävention eine Minimierung der Gefahr erfolgen. In anderen Fällen bleibt das Risiko gleich, was bedeutet, dass durch die Präventionsmaßnahme der Prozess sicherer gemacht wird.

Neben dieser Vorgehensweise zur Evaluierung der Sicherheitsrisiken im datenschutzrechtlichen Bereich gibt es diverse Checklisten zur systematischen Vorgehensweise. Diese Hilfsmittel leisten auch als Grundlage für die Durchführung von internen Audits gute Dienste. Sie können in ihrer Umsetzung die Basis für ein ausgereiftes, in sich abgestimmtes unternehmensspezifisches Sicherheitskonzept bilden.

Wie bereits die Kommentare zur EU-Datenschutz-Grundverordnung und zum BDSG 2018 zeigen, herrscht viel Unsicherheit bei der Anwendung der Datenschutz-Folgeabschätzung. Bei Zweifeln, ob und inwieweit Sie eine Datenschutz-Folgeabschätzung durchführen müssen, werden Sie wirksam von der zuständigen Datenschutzbehörde unterstützt. Anfragen lohnt sich.

Davon abgesehen erlangen Sie für sich im Unternehmen als Datenschutzbeauftragter mehr Klarheit durch das systematische Vorgehen bei der Datenschutz-Folgeabschätzung. Sie können die Methodik also durchaus unabhängig von der rechtlichen Forderung auf freiwilliger Basis vornehmen. Sie erfassen und bewerten damit wesentliche Vorkehrungen für die Einhaltung der Datenschutzgrundsätze, wie das Beispiel im Anhang 11 zu zeigen vermag. Eine Verfahrensanweisung zum Thema ist im Anhang 17 geregelt.

7 Betriebliche Regelungen für den Datenschutz

7.1 Private Nutzung von Telekommunikationseinrichtungen und -systemen im Unternehmen

Grundsätzlich ist es möglich, die private Nutzung von Telekommunikationseinrichtungen und -systemen am Arbeitsplatz auszuschließen. Alle Daten wären somit Daten des Unternehmens. Allerdings existiert bei den meisten Unternehmen dazu bereits eine „geübte Praxis“. Was jahrelang geduldet wurde, kann nur noch über eine Betriebsvereinbarung, d. h. mit der Zustimmung entweder aller Arbeitnehmer oder der Arbeitnehmervertretung geändert werden.

Merke

Duldung = geübte Praxis

Des Weiteren sind die Kontrollrechte des Arbeitgebers hinsichtlich der privaten Nutzung begrenzt. Das Allgemeine Persönlichkeitsrecht lässt keine Vollkontrolle zu. Private Inhalte von Mails unterliegen dem Fernmeldegeheimnis. Der Arbeitgeber fungiert in der Rolle des Providers **(TKG § 3)** und hat das Fernmeldegeheimnis darauf hin zu garantieren. Eine Betriebsvereinbarung zum Ausschluss der privaten Nutzung von Telekommunikationseinrichtungen und -systemen im Unternehmen bliebe somit ohne wirkliche Kontrolle.

In der Praxis haben sich daher viele Unternehmen für eine begrenzte private Nutzung von Telekommunikationseinrichtungen und -systemen entschieden. Anzuwendende Rechtsvorschriften für die Nutzung von Internet, E-Mail und Telefon sind das

- Telekommunikationsgesetz (TKG)
- Telemediengesetz (TMG).

Im **§ 3** des Telekommunikationsgesetzes ist jeder ein „Diensteanbieter“, der ganz oder teilweise geschäftsmäßig

- Telekommunikationsdienste erbringt oder
- an der Erbringung solcher Dienste mitwirkt.

Der Mitarbeiter stellt im Fall der privaten Nutzung von Telekommunikationseinrichtungen und -systemen den Endnutzer, d. h. den Kunden, dar.

Pflichten des Telekommunikationsanbieters, hier der Unternehmer, ergeben sich unter anderem aus § 96 TKG Verkehrsdaten, § 88 Fernmeldegeheimnis, § 89 Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen, § 93 Informationspflichten (gegenüber den Teilnehmern), § 94 Einwilligung im elektronischen Verfahren usw.

Für die begrenzte Erlaubnis, z. B. private E-Mails zu empfangen und zu senden, muss gleichermaßen eine Vereinbarung mit den Arbeitnehmern oder der Arbeitnehmervertretung abgeschlossen werden. Dem Arbeitnehmer muss bewusst sein, dass seine zu privaten Zwecken ausgetauschten Nachrichten durch den IT-Administrator, den Provider u. a. m. ausgelesen werden können.

Erfolgt die Nutzung von Internet und E-Mail im Unternehmen für Geschäfts- und private Zwecke, so ist unabhängig von Protokollierungs- und Kontrollrechten des Arbeitgebers auch ohne Einwilligung des Mitarbeiters eine Betriebsvereinbarung zu schaffen. Der „gläserne“ Mitarbeiter ist unzulässig. Dennoch tragen beschriebene Transparenz und Grenzen in der Anwendung der Telekommunikations- und DV-Systeme wesentlich zur Umsetzung des Datenschutzes und zur Wahrung der Persönlichkeitsrechte bei. Ein Beispiel für eine Vereinbarung zur E-Mail- und Internetnutzung ist nachstehend angeführt.

Vereinbarung zur E-Mail- und Internet-Nutzung

Vorlage

1 Zweck

Diese Vereinbarung regelt die Nutzung der E-Mail, den Internet-Zugang und den Einsatz von Internet-Techniken innerhalb der xy GmbH.

2 Geltungsbereich

Diese Vereinbarung gilt für alle Mitarbeiterinnen und Mitarbeiter der xy GmbH.

3 Elektronische Post (E-Mail)

Das Mail-System dient zur Verbesserung der internen und externen Kommunikation. Die xy GmbH erlaubt die Nutzung des Mail-Systems zum Austausch kurzer privater Mitteilungen, soweit hierdurch der Betriebsablauf nicht gestört wird. Für den Umgang mit der Mail sind ausschließlich die Benutzer selbst verantwortlich, nur sie allein haben Zugriff auf ihre Mails und entscheiden über deren Löschung und Weiterverwendung im Rahmen der festgelegten Speicherkapazitäten und gesetzlichen Bestimmungen.

Arbeitgeber und Mitarbeiter stimmen in der Auffassung überein, dass die E-Mail der am wenigsten gesicherte Weg ist, Informationen per Telekommunikation zu übermitteln. Die E-Mail übernimmt die Funktion einer offenen Postkarte, soweit sie nicht verschlüsselt wird. Daher dürfen **Vorgänge mit hohem Vertraulichkeitsgrad grundsätzlich nicht** über die Mail abgewickelt werden.

Andererseits bietet die E-Mail ein hohes Maß an Praktikabilität im schnellen Austausch von Informationen.

Zur Übermittlung einer Nachricht darf nur das eigene E-Mail-Konto verwendet werden, um eine Rückverfolgbarkeit der Nachrichtenübermittlung zu gewährleisten. Letztlich haftet der Absender der E-Mail für den Inhalt und den Adressatenkreis. Die Nutzung eines fremden E-Mail-Kontos ist strikt untersagt.

Die Nutzer haben in Abwesenheitsfällen die Möglichkeit, dem Absender automatisch mitteilen zu lassen, dass die Mail vorübergehend nicht gelesen wird. Eingänge und Ausgänge der Mails werden auf dem jeweiligen Benutzerkonto (Passwortschutz) protokolliert.

Es ist aus Vertraulichkeitsgründen technisch sichergestellt, dass diese E-Mail nicht automatisch an andere mögliche Adressaten weitergeleitet wird.

Mit der Installation einer E-Mail-Adresse „info@...“ wird die Bearbeitung eingehender E-Mails, z. B. im Kundenservice, durch ein Team ermöglicht. Der Absender ist sich bei der Wahl der E-Mail-Adresse bereits bewusst, dass sich darunter keine konkrete Person „versteckt“, er sein Anliegen allgemein und an die geschäftsüblichen Gepflogenheiten angepasst gestalten muss.

Zur Erhöhung der Datensicherheit wurde für alle eingehenden und ausgehenden E-Mails ein Virenscanner installiert. Dies soll verhindern, dass mit den E-Mails Schadsoftware eingeschleppt wird.

Es werden – abgesehen vom Backup-Verfahren – keine Kopien der Mails erzeugt oder archiviert.

4 Internet-Zugang

Der Zugang zum Internet unterliegt der Erteilung der Zugangsberechtigung durch den Systemadministrator. Damit ist nur ein beschränkter (definierter) Personenkreis befugt, das Internet zu nutzen.

Den Mitarbeitern soll das Internet als Mittel zur Informationsbeschaffung dienen. Eine kurzzeitige und eingeschränkte private Nutzung des Internets wird durch die Geschäftsleitung der xy GmbH gestattet.

Der Umgang mit dem Internet muss **verantwortungsvoll** geschehen.

Der Internetzugang darf nicht für rassistische, sexuell belästigende oder diskriminierende, strafrechtlich relevante oder gegen die Systemsicherheit gerichtete Aktivitäten genutzt werden. Die Zugriffe auf externe Internetseiten werden nicht protokolliert.

Bei begründetem Verdacht auf **missbräuchliche Nutzung** des Internetzugangs darf das Protokoll nach Zustimmung der Disziplinarvorgesetzten und einer Vertretung der Personalabteilung ausgewertet werden. Alle Benutzer werden über diese Bestimmungen schriftlich informiert.

5 Schlussbestimmungen

Sollten Informationen unter Verstoß gegen diese Vereinbarung erhoben werden oder verarbeitet werden, so sind sie als Beweismittel zur Begründung personeller Maßnahmen nicht zulässig; hierauf gestützte personelle Einzelmaßnahmen sind zurückzunehmen.

6 Salvatorische Klausel

Sollte eine der zuvor geregelten Bestimmungen unwirksam sein, bleiben die übrigen Bestimmungen hiervon unberührt.

Stand:

_____

Geschäftsführung

Revision: Änderungsdatum: Seite: 2 von 2

[in Anlehnung an Horst G. A. (2012): Praxiskommentar Bundesdatenschutzgesetz, 6. Aufl., WEKA-Verlag]

Hinweis

Nach Beendigung des Arbeitsverhältnisses dürfen nur noch bestimmte Daten des Arbeitnehmers aufbewahrt (physisch) bzw. gespeichert (datentechnisch) werden. Unter Wahrung der gesetzlichen Aufbewahrungsfristen (6 oder 10 Jahre) und Interessen des Arbeitnehmers (z. B. Sozialversicherungsnachweise) sind alle anderen Daten zu löschen.

Ausgenommen davon sind auch jene Daten, die für eventuelle Rechtsstreitigkeiten vonnöten sein könnten. Weitere Ausnahmen sind unter „Rechtmäßigkeit der Verarbeitung“ aufgeführt.

Hinweis

Datensparsamkeit/Datenminimierung und Wegfall der ursprünglichen Zweckbestimmung:

Daten sind zu vernichten (zu löschen), wenn sie nicht mehr benötigt werden.

Wer kennt das nicht, dass unter dem Namen seines ehemaligen Mitarbeiters seine privaten Briefe, Fotos o. Ä. gespeichert sind. Aus Erfahrungen der Autorin kann teilweise die Personalhistorie einer ganzen Abteilung nachvollzogen werden. Diese unerlaubte Speicherung der Daten sollte u. a. Gegenstand der Überprüfungen durch den DSB sein.

7.2 Telefondatenerfassung

Mitarbeiter eines Unternehmens nutzen die zur Verfügung stehenden Kommunikationsmittel auch für kurze private Gespräche. Oft sind diese privaten Gespräche dienstlich veranlasst und betreffen private Terminverschiebungen, Mitteilungen an die Familie aufgrund von Mehrarbeit,

die Vorbereitung persönlicher Qualifizierungsmaßnahmen u. a. m. Die gewählten Telefonverbindungen werden nummerntechnisch vollständig an den Adressaten vermittelt und unterliegen der Zielnummerndokumentation, sofern diese nicht begrenzt oder ausgeschlossen wird.

Nahezu alle Telefonanlagen sind in der heutigen Zeit mit technischen Leistungsmerkmalen ausgerüstet, die ein Abspeichern, Übermitteln und Bekanntmachen personenbezogener Daten oder auf Personen beziehbarer Daten ermöglicht. Damit kann eine Auswertung vorgenommen werden, welcher Arbeitnehmer wann und mit wem wie oft und wie lang telefoniert hat. Das Ausspionieren von Beschäftigten ist gesetzlich untersagt.

Lösungen zur Entspannung dieser Situation sind u. a.:

- Einzelverbindungsnachweis um die letzten Ziffern nummerntechnisch verkürzen
- Beschränkung des Personenkreises, der die Einzelverbindungsnachweise einsehen kann
- keine Aufnahme von Telefongesprächen (Protokollierungsverbot)
- Unterbindung des unbemerkten Einschaltens in ein Telefongespräch (Abhörverbot)
- Ankündigung der Personen, die an einer Konferenzschaltung beteiligt sind.

Ein Beispiel für eine Betriebsvereinbarung zur Telefondatenerfassung soll hier abgedruckt werden:

Vorlage

Vereinbarung zur Telefondatenerfassung

1 Präambel

Die TK-Anlage der xy GmbH dient der dienstlichen und in begrenztem Umfang auch privaten Kommunikation.

Sie ist mit modernen Leistungsmerkmalen technisch und organisatorisch so konzipiert, dass das Abspeichern, Übermitteln und Bekanntmachen personenbezogener oder auf Personen beziehbarer Daten möglich wird. Die Geschäftsleitung der xy GmbH verpflichtet sich, den Umgang und die Auswertbarkeit personenbezogener Daten auf das erforderliche Mindestmaß zu beschränken.

2 Zweck

Diese Vereinbarung (Nr.) regelt die Benutzung der TK-Anlage und die Speicherung von Benutzerdaten.

3 Geltungsbereich

(1) Persönlich gilt diese Regelung für alle Mitarbeiter.

(2) Sachlich gilt diese Regelung für die TK-Anlage inkl. Auswerterechner.

(3) Räumlich gilt diese Regelung für alle Bereiche der xy GmbH, in der Telekommunikation stattfindet.

4 Erläuterungen

(1) **Dienstliche Ferngespräche** sind Gespräche, die dienstlich veranlasst sind und über den Orts- und Nahbereich hinausgehen.

Als dienstliche Ferngespräche gelten auch Privatgespräche, die über den Orts- und Nahbereich hinausgehen und dienstlich veranlasst sind. Sie werden nummerntechnisch vollständig an den Adressaten übermittelt.

Weiterhin unterliegen sie möglicherweise einer Zielnummerndokumentation. Die letzten 10 Anrufe sind mind. nummerntechnisch am Apparat abrufbar.

Ein Einzelverbuchungsnachweis ist nummerntechnisch um die letzten Ziffern verkürzt durch die Geschäftsführung einholbar. Die Gespräche werden nicht aufgenommen.

(2) **Private Ferngespräche** werden erfasst und nummernbezogen verkürzt gespeichert.

Die Verbindungsnachweise sind nummernverkürzt durch die Geschäftsleitung abrufbar.

(3) **Private Orts- und Ferngespräche** werden nicht weiterverrechnet.

(4) **Handy-Nutzung (Firmenhandy)**

Bei Nutzung von Handys kann ein Einzelgesprächsnachweis auf Nachfrage erhoben werden, der um die letzten Ziffern gekürzt ist. Zur Kostenbegrenzung kann stichprobenhaft ohne Ankündigung ein entsprechender Einzelgesprächsnachweis durch den Geschäftsführer angefordert werden.

5 Abhörverbot/Protokollierungsverbot

Abgesehen von der sachgerechten Nutzung eines Voice-Mail-Servers (Anrufbeantworter) werden Telefongespräche weder abgehört noch mitgeschnitten oder gespeichert.

Das Einschalten in Telefongespräche oder das Mithören von Telefongesprächen ohne Zustimmung der Gesprächspartner wird hiermit ausgeschlossen. Bei Konferenzschaltungen oder Mithören über Lautsprecher muss jeder Teilnehmer vor Beginn des Gespräches darüber informiert werden, wer außer ihm noch an dem Gespräch teilnimmt.

6 Datenschutz

Die mit der Handhabung von personenbezogenen Gesprächsdaten beauftragten Mitarbeiter werden über die Anforderungen des Datenschutzes unterrichtet. Alle Mitarbeiter sind zur Einhaltung dieser Betriebsvereinbarung verpflichtet.

7 Salvatorische Klausel

Sollte eine der zuvor geregelten Bestimmungen unwirksam sein, bleiben die übrigen Bestimmungen hiervon unberührt.

Stand:

_____

Geschäftsführung

Revision: Änderungsdatum: Seite: 2 von 2

7.3 Private IT im Unternehmen

Die Nutzung privater IT im Unternehmen bedarf einer besonderen Sensibilisierung der Mitarbeiter. Insbesondere sollte der DSB Mitarbeiter, die ihre eigene IT in das Unternehmen einbringen, über diesbezügliche besondere datenschutzrechtliche Risiken aufklären und mit Unterschrift bestätigen lassen.

Unabhängig davon sollte eine schriftliche Anweisung zur Nutzung privater IT im Unternehmen aufgestellt werden. **Wesentliche Punkte** dieser Regelung sind:

- Was ist zu tun bei einem Verlust der privaten Geräte mit den Daten?
- Wer kontrolliert die Daten auf diesen Geräten, der Nutzer oder das Unternehmen? (Für geschäftliche Daten ist das Unternehmen verpflichtet.)
- Wie wird eine Löschung der Daten sichergestellt?

- Wer hat Zugriff auf die Daten auf den privaten Geräten? (Schutz der geschäftlichen Daten in Gefahr! Kein Zugriff von Mitgliedern der Familie erlaubt!)
- Wie wird der Zugriff limitiert? (z. B. über Passwörter)
- Wie wird der Zugriff des Unternehmens auf seine geschäftlichen Daten auf den privaten Geräten ermöglicht? (Verantwortung des Unternehmens für Geschäftsdaten)
- Sind Kontrollmechanismen etabliert und sind eventuell neue notwendig?

Was ist zu tun, um den Datenschutz bei privater IT im Unternehmen zu gewährleisten? An dieser Stelle können nur einige wesentliche Lösungsansätze dargestellt werden. Datenschutzrechtliche Regelungen sind immer von der Situation im Einzelnen abhängig.

Hinweis

Grundsätzlich können folgende Schutzmaßnahmen zur privaten Nutzung von IT im Unternehmen ergriffen werden:

- strikte Trennung von privaten und geschäftlichen Daten auf dem Gerät
- Verschlüsselung der Daten; Zugriffsrechte limitieren
- klare Verhaltensregeln für die Nutzung aufstellen
- Löschroutinen für den Verlust des Gerätes vorbereiten.

Auch hier gilt, dass Kontrollrechte mit der Arbeitnehmervertretung abzustimmen sind.

7.4 Umgang mit USB-Sticks

In vielen geschäftlichen und privaten Situationen erleichtern USB-Sticks die Speicherung von Daten und deren Transport. Sie sind klein und handlich und erfreuen sich daher einer breiten Anwendung und großen Beliebtheit. Weiterhin unterschätzt werden die mit der Nutzung von USB-Sticks einhergehenden datenschutzrechtlichen Risiken. USB-Sticks gehören zu den größten Gefahrenquellen für den Schutz personenbezogener Daten. Eine besondere Sensibilisierung der Mitarbeiter und strikte Regelungen zum Umgang mit USB-Sticks sind daher unentbehrlich.

Vorteile der Nutzung von USB-Sticks liegen

- in der Kurzzeit-Archivierung von Daten, Sicherungskopien
- im mobilen Austausch von Daten
- in der Nutzung als Programmträger zur Installation für komplexe Betriebssysteme
- im Datentransport von A nach B.

Nachteile bestehen

- im leichten Verlust der USB-Sticks
- in der mangelnden Verschlüsselung und dem damit einhergehenden Datendiebstahl, Datenmissbrauch, Datenverlust
- im Einschleppen von Viren, z. B. bei Werbegeschenken.

Schutzmechanismen des auf dem PC installierten Betriebssystems lassen sich leicht umgehen, wenn von einem Betriebssystem über USB gebootet wird und dieses Betriebssystem unter Kontrolle eines Angreifers steht. Das Booten von USB-Medien wird durch BIOS-Versionen unterstützt.

Weiterhin entfallen heutzutage aufwändige Prozeduren für die Installation von Hard- und Software. Damit sinkt auch die Hemmschwelle, USB-Sticks einzubinden.

Die Fachpresse geht davon aus, dass jährlich 20 Millionen USB-Sticks verloren gehen. Haben Sie nicht auch schon mal einen Stick gesucht? Damit verbindet sich häufig ein Verlust auch von personenbezogenen Daten, bei denen wir nicht wissen, wer in den Besitz der Daten letztlich gelangt.

Was ist aus datenschutzrechtlicher Sicht zu tun?

Empfehlenswert erscheint die Nutzung nur vom Unternehmen zugelassener USB-Sticks. Damit wird eine Überwachung eingesetzter USB-Sticks überhaupt erst möglich. Weiterhin sind nur einige wenige PCs für die Verwendung von USB-Sticks freizugeben, bei allen anderen ist diese Funktion zu sperren.

Unentbehrlich an dieser Stelle ist die Unterweisung der Mitarbeiter, damit sie nicht von Dienstleistern, Gästen, also Externen, USB-Sticks annehmen. Mit jeder Verwendung eines externen USB-Stick (auch des privaten) steigt die Wahrscheinlichkeit des Einschleppens von Viren, gleich der Saga nach dem „Trojanischen Pferd“. Der Nutzer kann bei externen USB-Sticks nie wissen, wo dieser Stick bereits im Einsatz war.

Hinweis

Die betrieblich zugelassenen USB-Sticks sollen über Sicherheitsfunktionen abgesichert werden:

- Beschaffung von USB-Sticks mit Sicherheitsfunktionen oder Zusatzsoftware intern
- Kontrolle der beschafften USB-Sticks
- Ermöglichung einer Zugangssoftware über Passworteingabe
- Reaktivierung einer Weitergabekontrolle durch Verschlüsselungslösung
- Unterteilung zwischen privaten und geschäftlichen Daten auf dem USB-Stick – Trennungsgebot
- ggf. Integration von Datenlöschfunktionen
- Begrenzung des Nutzerkreises (Wer darf mit USB-Sticks umgehen?)
- Transport von Daten auf USB-Sticks nur von definierten Datenkategorien (Was darf auf USB-Sticks gespeichert werden?)
- Deaktivierung aller Treiber, die zur Verwaltung bestimmter USB-Sticks nicht erforderlich sind
- Virenscanner für USB-Sticks installieren
- Bootmöglichkeit von USB-Geräten im BIOS-Menü ausschalten oder
- Boot-Optionen so konfigurieren, dass USB-Geräte erst nach der System-Festplatte (oder nach Netzwerk) angesprochen werden
- Betriebliche Regelung aufstellen

[Quelle: WEKA (2012): Mängelschwerpunkte bei Datensicherheitsmaßnahmen]

Merke

Sensibilisierung der Mitarbeiter!

Vorlage

Vereinbarung zum Umgang mit USB-Sticks

1 Zweck

Der Zugriff auf mobile Datenträger ist im Hinblick auf Manipulationsversuche zu erschweren, ein unerlaubter Datenzugriff auf personenbezogene Daten zu verhindern.

2 Geltungsbereich

Der Geltungsbereich erstreckt sich auf alle Nutzer von mobilen Datenträgern.

Revision: Änderungsdatum: Seite: 1 von 2

3 Verfahren

Im Unternehmen ist eine ausreichende Anzahl von USB-Sticks mit bestimmten Sicherheitsfunktionen zugelassen. Diese USB-Sticks sind nur für einen definierten Personenkreis zugelassen. Eine Nutzung von USB-Sticks anderer Quellen und von anderen Beschäftigten ist ausdrücklich untersagt. Die Nutzung von USB-Sticks ist zudem bei allen anderen Beschäftigten außerhalb des definierten Personenkreises technisch ausgeschlossen. Eine Ausgabe der unternehmenseigenen USB-Sticks erfolgt kontrolliert und gegen Unterschrift des Mitarbeiters. Die Verwendung erfolgt passwortgeschützt. Eine Weitergabe von Passwörtern ist grundsätzlich untersagt.

Die Speicherung von Daten auf dem USB-Stick soll von Mitarbeitern getrennt nach persönlichen und geschäftlichen Daten erfolgen. Die Trennung stellt sicher, dass bei einer Datenschutzkontrolle persönliche Daten außen vor bleiben.

Mit dem USB-Stick dürfen nur folgende Datenkategorien übertragen werden:

– (betrieblich zu benennen)
– ...
– ...

Mit der Übergabe von Daten wird über eine Verschlüsselung eine Weitergabekontrolle realisiert. Mitarbeiter, denen USB-Sticks zugeordnet sind, haben alle erdenkliche Sorgfalt walten zu lassen, um einen unberechtigten Zugriff oder Verlust des Datenträgers zu verhindern. Sofern bestimmte Daten der Datenkategorie xy in falsche Hände geraten (unrechtmäßige Kenntniserlangung), ist Folgendes zu tun:

– unverzügliche Benachrichtigung des DSB

Der DSB hat folgende Aufgaben:

– unverzüglich binnen 72 Stunden die Aufsichtsbehörde informieren,
– nach Beseitigung einer Wiederholungsgefahr jeden Betroffenen informieren (soweit zumutbar),
– es sei denn, es sind keine größeren Risiken mit dem Verlust der personenbezogenen Daten absehbar.

Kritische Daten, mit denen ein hohes Risiko für den Betroffenen verbunden sein wird, sind insbesondere:

– besondere Kategorien personenbezogener Daten,
– personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
– personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder einen entsprechenden Verdacht beziehen,
– personenbezogene Daten zu Bank- oder Kreditkartenkonten.

Zur Prävention eines möglichen Datenverlustes bei besonderen Kategorien personenbezogener Daten sind folgende Punkte zu beachten:

– besondere Kategorien personenbezogener Daten möglichst nicht auf mobilen Datenträgern speichern,
– diese Daten immer verschlüsseln,
– verschlüsselte Daten können auch bei Verlust vom „Finder“ nicht zur Kenntnis genommen werden.

4 Mitgeltende Unterlagen

VA Meldungen von Verletzungen des Datenschutzes

7.5 Nutzung betrieblicher Laptops

In vielen Unternehmen wird Arbeitnehmern ein betriebliches Laptop zur Verfügung gestellt. Die Geräte sind flexibel handhabbar und praktisch überall hin mitzunehmen. Das erleichtert die Aufnahme und Verarbeitung von Daten im Wartungs- und Instandhaltungsbereich, im Vertrieb, in leitenden Positionen, in Besprechungen u. a. m. Häufig werden die Laptops auch für private Zwecke überlassen oder eine ausschließliche Verwendung zu betrieblichen Zwecken ist nicht explizit vertraglich verankert. Datenschutzrechtlich gestaltet sich dies nicht unproblematisch, müssen doch für den privaten Gebrauch die gleichen technischen und organisatorischen Sicherheitsaspekte zum Schutz personenbezogener Daten eingehalten werden wie im Unternehmen. Zudem werden die Geräte i. d. R. mit Anschlüssen für USB-Sticks, Beamer, CD-Brenner, Diskettenlaufwerk und Zugang zum Internet zur Verfügung gestellt, also mit Möglichkeiten ausgestattet, Daten extern zu speichern, sie zu übermitteln, zu veröffentlichen oder zu löschen. Eine Kontrolle der Datenverarbeitung auf Laptops gestaltet sich damit schwierig. Eine private Nutzung ist de facto nicht auszuschließen. Daher erscheint es unabdingbar, eine Überlassungsvereinbarung für die Nutzung betrieblicher Laptops aufzustellen und eine Unterweisung der Mitarbeiter vorzunehmen bzw. sie auf die Einhaltung des Datengeheimnisses (auch zu Hause) zu verpflichten.

7.5.1 Vereinbarung zur Nutzung betrieblicher Laptops

Wesentliche Inhalte einer solchen Vereinbarung sind u. a.:

- Nennung der Bezeichnung und Typisierung des betrieblichen Laptops
- Nennung aller Zusatzoptionen (Anschlüsse für USB-Sticks, CD-Brenner ...)
- Dauer der Überlassung
- Überlassung auch zu privaten Zwecken
- Widerruflichkeit der Vereinbarung
- Einräumen einer Kontrollmöglichkeit durch den DSB
- Beschreibung der technischen und organisatorischen Maßnahmen am Gerät
- Verpflichtungen des Laptop-Nutzers
- Internet- und E-Mail-Umgang
- Speicherung und Löschung von personenbezogenen Daten – Was ist zu beachten?
- Aufspielen privater Software
- Datensicherung und Abgleich der Daten mit dem Netzwerk.

7.5.2 Technische und organisatorische Maßnahmen für Laptops

Die Beschreibung der **technischen Maßnahmen** zur Sicherung des Laptops könnte sich wie folgt gestalten:

Beispiel

Das Unternehmen bietet als technische Schutzmaßnahmen für Laptops:

- Zugangscode/Passwortschutz
- Automatischer Passwortwechsel alle x Wochen
- Installation eines Bildschirmschoners
- Passwortschutz für den Zugang zum Internet, Lotus-Notes und Adressbuch
- Überprüfung von externen Ausgabemedien auf Viren
- Virenschutzprogramm

- Automatischer Update-Service
- USB-Stick „Notebook-Bodyguard“ o. Ä. (muss beim Systemstart mit dem Notebook verbunden sein, sonst ist kein Systemstart möglich, auch für die Sicherung/Speicherung von personenbezogenen Daten vorgesehen).

Organisatorische Pflichten des Users sollten u. a. nachstehende Aspekte behandeln:

Der Nutzer ist verpflichtet, regelmäßige Updates auf seinem Rechner selbst durchzuführen und für den Wechsel des Passworts sowie für die Anwendung der Regeln für ein gutes Passwort zu sorgen.

Weiterhin sollte das Unternehmen dem Nutzer des betrieblichen Laptops die Möglichkeit einer Versicherung offeriert werden.

Die übergebenen Laptops sind wie folgt über das Unternehmen versichert:

- gegen Einbruch und Diebstahl
- gegen Brand.

Speicherung personenbezogener Daten:

Die Speicherung von personenbezogenen Daten auf Laptops ist insbesondere dann problematisch, wenn sie unverschlüsselt erfolgt. Wird der Laptop gestohlen oder an einem privaten, nicht hinreichend gesicherten Anschluss mit dem Internet verbunden, ist der erforderliche Datenschutz nicht mehr gewährleistet.

Sensible oder personenbezogene Daten sollten daher nach Möglichkeit nicht auf Laptops gespeichert werden. Ist dies unumgänglich, sollte die Speicherung stets in verschlüsselter Form erfolgen.

Auf Laptops befindliche personenbezogene Daten sollten so schnell wie möglich wieder gelöscht werden.

Löschung vorhandener personenbezogener Daten:

Personenbezogene Daten müssen stets unverzüglich nach dem Wegfall des Grundes ihrer Erhebung gelöscht werden. Insbesondere ist es nicht zulässig, Daten zur späteren Verwendung „auf Vorrat“ zu speichern. Unter Löschung versteht man dabei das unwiederbringliche Tilgen von Daten. Bei elektronisch gespeicherten Daten ist dabei zu beachten, dass der Befehl „Löschen“ die Daten im Allgemeinen nur zum Überschreiben freigibt. Tatsächlich sind sie noch auf dem Speichermedium vorhanden.

Datensicherung:

Häufig werden auf dem Laptop gespeicherte Daten nicht extern gesichert.

Durch das Überspielen der auf dem Laptop befindlichen Daten auf das betriebliche Netzwerk unterliegen diese Daten dann auch einer regelmäßigen Sicherung. Sensible Daten sollten möglichst nicht auf Laptops gespeichert werden, da ein Diebstahl des Geräts und damit der Daten einer größeren Wahrscheinlichkeit unterliegt.

Abgleich der Daten mit dem Netzwerk:

Der Abgleich der Daten auf dem Laptop mit den Daten im Intranet soll regelmäßig erfolgen, mindestens alle 14 Tage, um einen Datenverlust möglichst zu vermeiden.

Beispiel

Vereinbarung zur Nutzung von betrieblichen Laptops

zwischen xy GmbH

und

Name, Vorname

Anschrift

§ 1 Überlassung zur Nutzung

Herrn/Frau _____ wird ein betriebliches Laptop (Bezeichnung, Typisierung) unentgeltlich und für den Zeitraum der Beschäftigung im Unternehmen mit Anschlüssen für USB-Stick, Beamer, mit CD-Brenner, Diskettenlaufwerk und Zugang per _____ zum Internet überlassen.

Die Überlassung geschieht vorwiegend zu betrieblichen Zwecken, der private Gebrauch ist in geringem Maße erlaubt.

Die Überlassung ist jederzeit widerruflich.

§ 2 Schutzmechanismen

Das Unternehmen bietet als technische Schutzmaßnahmen für Laptops:

- Zugangscode/Passwortschutz
- Automatischer Passwortwechsel alle _____ Wochen
- Installation eines Bildschirmschoners
- Passwortschutz für den Zugang zum Internet, Outlook und Adressbuch
- Überprüfung von externen Ausgabemedien auf Viren
- Virenschutzprogramm
- Automatischer Update-Service

§ 3 Verpflichtungen des Laptopnutzers

Der Nutzer des überlassenen Laptops verpflichtet sich zum pfleglichen Umgang mit dem Gerät. Alle Reparaturnotwendigkeiten und Beschädigungen sind unverzüglich an den Geschäftsführer oder den IT-Beauftragten zu melden.

Für eine unsachgemäße Behandlung des Geräts haftet der Nutzer.

Die übergebenen Laptops sind wie folgt über das Unternehmen versichert:

- gegen Einbruch und Diebstahl
- gegen Brand

Der Nutzer ist verpflichtet, regelmäßige Updates auf seinem Rechner selbst durchzuführen und für den Wechsel des Passworts sowie für die Anwendung der Regeln für ein gutes Passwort zu sorgen (siehe Anlage).

§ 4 Zugang zum Internet

Der Zugang zum Internet ist nur über eine gesicherte Verbindung zu wählen.

§ 5 E-Mail – Verwendung

Der Nutzer des Laptops hat dafür Sorge zu tragen, dass personenbezogene Daten nicht unverschlüsselt per E-Mail versendet werden. Die Übergabe der personenbezogenen Daten soll entweder

- per Fax nach vorheriger Information des Empfängers
- per Post
- per USB-Stick
- oder verschlüsselt per E-Mail erfolgen.

§ 6 Personenbezogene Daten

Unter den Begriff personenbezogene Daten fallen alle Einzelangaben über eine natürliche Person, soweit sie nicht ausschließlich für familiäre oder persönliche Zwecke verwendet werden. Auch bloße Adressdaten, Telefonnummern, E-Mail-Adressen, Geburtsdaten etc. unterliegen bereits diesem Begriff.

Bei Personengesellschaften, d. h. Gesellschaften bürgerlichen Rechts, Einzelunternehmen etc. sind die Angaben zum Inhaber gleichzeitig als personenbezogene Daten anzusehen. So zählen auch Kunden- und Lieferantendaten zu den personenbezogenen Daten.

§ 7 Speicherung personenbezogener Daten

Die Speicherung von personenbezogenen Daten auf Laptops ist insbesondere dann problematisch, wenn sie unverschlüsselt erfolgt. Wird der Laptop gestohlen oder an einem privaten, nicht hinreichend gesicherten Anschluss mit dem Internet verbunden, ist der erforderliche Datenschutz nicht mehr gewährleistet.

Besondere Kategorien personenbezogener Daten oder personenbezogene Daten sollten daher nach Möglichkeit nicht auf Laptops gespeichert werden. Ist dies unumgänglich, sollte die Speicherung stets in verschlüsselter Form erfolgen.

Auf Laptops befindliche personenbezogene Daten sollten so schnell wie möglich wieder gelöscht werden.

§ 8 Löschung vorhandener personenbezogener Daten

Personenbezogene Daten müssen stets unverzüglich nach dem Wegfall des Grundes ihrer Erhebung gelöscht werden. Insbesondere ist es nicht zulässig, Daten zur späteren Verwendung „auf Vorrat“ zu speichern. Unter Löschung versteht man dabei das unwiederbringliche Tilgen von Daten. Bei elektronisch gespeicherten Daten ist dabei zu beachten, dass der Befehl „Löschen“ die Daten im Allgemeinen nur zum Überschreiben freigibt. Tatsächlich sind sie noch auf dem Speichermedium vorhanden.

§ 9 Aufspielen von privater Software

Das Herunterladen von Freeware- oder Shareware-Programmen oder auch Spielen aus dem Internet ist untersagt.

Es darf nur Software aus vertrauenswürdigen Quellen eingesetzt werden.

Vor jeglicher Installation neuer Programme sollte dessen Datenträger auf einen Befall mit Schadsoftware überprüft werden. Generell sollten alle ein- und ausgehenden Datenträger einer entsprechenden Überprüfung unterzogen werden.

§ 10 Datensicherung

Daten auf den betrieblichen Laptops müssen 14-tägig gesichert werden. Hierfür ist ein Überspielen der Daten auf den stationären Rechner erforderlich. Alternativ kann über eine externe Festplatte die Datensicherung vollzogen werden. Die externe Festplatte ist der IT-Abteilung auf Anforderung zur Verfügung zu stellen.

§ 11 Salvatorische Klausel

Sollte eine dieser Bestimmungen unwirksam sein, so ist nicht die gesamte Vereinbarung hinfällig. Vielmehr tritt an die Stelle der unwirksamen Bestimmung jene, die dem verfolgten Zweck am nächsten kommt.

§ 12 Gerichtsstand

Der Gerichtsstand ist _____

Ort,

_____ _____

Anlagen:

Regeln für ein gutes Passwort

7.6 Telefax-Umgang

Der Versand von Telefaxen ebenso wie deren Sende- und Empfangsprotokolle unterliegen dem Fernmeldegeheimnis. Ein Ausdruck oder eine Kenntnisnahme durch Unbefugte ist wirksam zu verhindern. Die Einsichtnahme in Telefaxe und deren Sende- und Empfangsprotokolle ist wirksam zu regeln.

Nicht selten werden per Fax personenbezogene und darunter vor allem sensible personenbezogene Daten übermittelt. Personalabteilungen, Steuerbüros wählen gern diesen kurzen und unkomplizierten Datenübermittlungsweg.

Hinweis

Was bei einem Versenden von Faxen vorrangig zu beachten ist, wird in Folgendem deutlich:

- vor der Absendung des Telefaxes Anschlussnummer prüfen,
- bei Versand Einstellung des Datums und der Uhrzeit prüfen (für rechtliche Nachweiszwecke),
- Gleiches für Auslandsfaxe,
- prüfen, ob Anrufumleitung, -weiterschaltung besteht,
- prüfen, ob tatsächlich alle Seiten übermittelt worden sind.

Eine Übertragung von Daten, die sich auf strafbare Handlungen bezieht, auf religiöse oder politische Anschauungen oder arbeitsrechtliche Sachverhalte, ist generell per Fax untersagt. Ausnahme: Es handelt sich um äußerst eilige Informationen. Dann ist auf die persönliche Entgegennahme des Faxes durch den Empfänger zu dringen.

Faxgeräte werden in der Praxis häufig in begehbaren Räumen durch Dritte, z. B. Betriebsfremde, Mitarbeiter anderer Abteilungen, Besucher, aufgestellt. Hier können unbeobachtet Faxe mit personenbezogenen Daten ankommen, die dann Unbefugten zur Kenntnis gelangen. Beispielsweise werden bei Bildungsträgern auch Teilnahmezertifikate per Fax versendet, aufgrund von Eilbedürftigkeit ohne vorherigen Anruf beim Empfänger. Die Aufstellung der Faxgeräte sollte folglich innerhalb der Diensträume erfolgen.

7.7 Organisation des betrieblichen Postwesens

Personenbezogene Daten dürfen grundsätzlich nicht auf Postkarten oder mit E-Mails versendet werden und nur in Ausnahmefällen per Fax.

Das Versenden von Geschäftspost (außer Werbebriefen) sollte in verschlossenen Umschlägen erfolgen, auch intern. Sobald personenbezogene Daten enthalten sind, z. B. Kunden- und Lieferantendaten, Personaldaten u. a. m., ist eine Versendung per Postkarte aus datenschutzrechtlicher Sicht nicht mehr möglich.

In einigen Fällen kann selbst anhand eines geschlossenen Briefes auf den Inhalt geschlussfolgert werden. Zum Beispiel ist im Adressfeld der Absender noch erkenntlich. Behördenbriefe, Briefe von Vollstreckungsbeamten können somit von Betroffenen als Peinlichkeit empfunden werden, sobald jeder Mitarbeiter den Brief in der Hand hatte. Daher sollen auch geschlossene Briefe in Brieffächer oder diskret an den Adressaten verteilt werden und eben nicht erst durch viele Hände gehen. Diskretion und damit die Wahrung von Persönlichkeitsrechten sind ein wichtiger Bestandteil des Datenschutzes. Hilfreich erweist sich auch hier die explizite Nennung des Empfängers, z. B. zu Händen von Herr/Frau XY. Mit den Worten „persönlich/vertraulich“ wird konstatiert, dass der Brief nur vom Empfänger geöffnet werden darf und eben nicht von einem Sekretariat oder Teammitglied. Schulungen der Mitarbeiter zu diesem Thema erhöhen die oftmals in der täglichen Praxis bereits abgeschliffene Sensibilität gegenüber der Wahrung datenschutzrechtlicher Persönlichkeitsrechte.

In der betrieblichen Praxis betrifft die Versendung mit der Post in der Regel

- Gehalts-/Lohnabrechnungen
- Zertifikate

- Telefonabrechnungen (Verbindungsnachweise)
- Reiseunterlagen
- Medizinische Vorsorgenachweise
- Unfallmeldungen
- Informationen über Pfändungen
- Arbeitnehmerdarlehen
- Prämienzusagen.

Hinweis

Was bleibt beim Versand mit der Post zu beachten?

- keine Zustellung im offenen Umschlag oder per Postkarte
- keine Verwendung von Fensterbriefumschlägen, da eine Einsicht auf das Schriftgut und auf den Absender möglich ist
- bei sensiblen Daten kein Absender, da vom Absender bereits auf den Inhalt geschlossen werden könnte
- keine Verwendung von wiederverschließbaren Umschlägen (Öffnen und Schließen mehrfach möglich)
- möglichst persönliche Zustellung sicherstellen oder per Post, nicht in einem Fachsystem für eine Abholung.

7.8 Vorgehen bei externen Anfragen (z. B. Behörden)

Eine Herausgabe von personenbezogenen Daten kann auch ohne Einwilligung des Beschäftigten bei übergeordneten Interessen, z. B. bei Auskunftsersuchen oder -verlangen durch die Kriminalpolizei, möglich werden. Um festzustellen, ob die Herausgabe personenbezogener Daten erlaubt oder untersagt ist, sind zunächst der Geschäftsführer und der DSB zu informieren. Bestehen Zweifel ob der Rechtmäßigkeit des Auskunftsbegehrens ist ein Jurist oder ggf. die Datenschutzbehörde zu kontaktieren. Von telefonischen Auskünften sollte grundsätzlich abgesehen werden. Der Ablauf der Auskunfterteilung ist mit einer Anweisung zu regeln.

Vorlage

Regelung zur Bearbeitung externer Anfragen

1 Geltungsbereich

Die Muster GmbH kann im Sinne eines Auskunftsersuchens/-verlangens verpflichtet sein, zu Anfragen von Behörden (z. B. Kripo, Polizei, BGS, Zoll) im Zusammenhang mit personenbezogenen Daten Auskunft zu geben.

2 Zuständigkeiten

Diese Anfragen werden ausschließlich von der Geschäftsführung, dem Leiter Personal oder der Mitarbeiterin Rechnungswesen in Kooperation mit dem Datenschutzbeauftragten bearbeitet. Anfragen, die nicht in diesem Bereich auflaufen, sind unabhängig davon, ob diese telefonisch oder schriftlich gestellt werden, grundsätzlich an den Geschäftsführer oder Datenschutzbeauftragten weiterzuleiten.

Vor jeder Auskunfterteilung ist grundsätzlich deren Rechtmäßigkeit zu prüfen.

Bestehen Zweifel an der Auskunftspflicht, ist über den Geschäftsführer, den Leiter Personal oder die Mitarbeiterin Rechnungswesen oder den Datenschutzbeauftragten der Anwalt/Justiziar des Unternehmens einzuschalten.

Revision: Änderungsdatum: Seite: 1 von 2

3 Vorgehen

Um ein einheitliches Vorgehen aller Beteiligten bei der Bearbeitung von Anfragen sicherzustellen, ist der folgende Ablauf einzuhalten:

- Bei telefonischer Anfrage Name, Dienststelle und Telefonnummer des Anfragenden notieren.
- Fax auf Dienstpapier mit Begründung der Anfrage und möglichst detaillierten Angaben zum Vorgang erbitten. Empfänger: DSB der … bzw. o. g. Vertreter, Fax.-Nr.: …
- Faxempfänger informieren und um sofortige Benachrichtigung bei Fax-Eingang bitten.
- Klären, ob Pflicht zur Herausgabe der Daten besteht.
- Fax persönlich beim Faxempfänger abholen.
- Durch Kontrollanruf bei der auf dem Fax angegebenen Dienststelle (Zentrale/Nebenstelle) sicherstellen, dass hinter der Anfrage tatsächlich auch die angegebene Behörde steht.
- Fax bearbeiten (falls Pflicht zur Herausgabe der Daten besteht und der Kontrollanruf positiv verlief).
- Sofern zur Beantwortung von Anfragen Informationen aus anderen Bereichen einzuholen wären, sind in diesem Zusammenhang nur die für die Datenerhebung unbedingt erforderlichen Ausgangsdaten, jedoch nicht der zugrunde liegende Sachverhalt bzw. die anfordernde Stelle zu nennen.
- Abhängig von der Art der Anfrage kommen folgende Bereiche als Informationsquelle infrage:
  - Geschäftsführer
  - Personal
  - Rechnungswesen
- Die im Fachbereich erhobenen Daten sollten möglichst ausgedruckt werden.
- Alle im Zusammenhang mit der Anfrage ermittelten Informationen sind per Fax oder Einschreiben/Rückschein an die nachfragende Behörde zu übermitteln.
- Das Antwort-Fax sowie die dazugehörigen Unterlagen sind dem Geschäftsführer, dem Leiter Personal, der Mitarbeiterin Rechnungswesen oder dem Datenschutzbeauftragten zuzuleiten.

_____

Geschäftsführung

Revision: Änderungsdatum: Seite: 2 von 2

[Quelle: H&L Montagebau GmbH, Bad Dürrenberg, 2018]

7.9 Einsatz von Multifunktionsgeräten

Multifunktionsgeräte, gemeint sind Geräte, die Kopier-, Druck-, Scan- und/oder Faxfunktionen erfüllen, erfreuen sich im Verwaltungsalltag großer Beliebtheit. Ein Gerät, das (fast) alles kann. Diese Multifunktionsgeräte verfügen über eine Festplatte oder ein anderes Speichermedium, um Dokumente zwischenspeichern zu können. Je nach Speicherart, flüchtig oder nicht flüchtig, findet eine dauerhafte Speicherung der Daten statt, die relativ leicht auszulesen sind. Flüchtige Speichermedien löschen die Daten, sobald keine Versorgungsspannung mehr anliegt. Bei nichtflüchtigen Speichermedien können Daten auch nach dem Ausschalten des Gerätes noch ausgelesen werden.

Hinweis

Überprüfen Sie, welche Art von Speicher Ihr Multifunktionsgerät hat!

Teilweise werden Daten mit dem Einlesen des nächsten Dokuments gelöscht, andere wiederum erst, wenn Speicherplatz benötigt wird.

Oft werden Kopien, Ausdrucke oder Scans auch von personenbezogenen oder sensiblen Daten erstellt. Die Auslesung dieser Daten von unbefugten Personen wäre fatal.

Ein Bewusstsein über diese Art des Datendiebstahls existiert in der Praxis häufig nicht. Wie in diversen Fernsehsendungen gezeigt wurde, dauert es nur wenige Minuten, bis Daten ausgelesen werden können. Das stellt erhöhte Anforderungen an das vertraglich gebundene Wartungspersonal für Druck-, Kopier- und Scantechnik. Weiterhin sollte der Zugang zu diesen Geräten nur dem betriebseigenen Personal ermöglicht werden oder für Externe entsprechend abgekoppelte Geräte zur Verfügung gestellt werden, beispielsweise für Teilnehmer in Bildungseinrichtungen, Schulen, Universitäten.

Hinweis

Aus datenschutzrechtlicher Sicht ist es daher empfehlenswert, den Umgang mit Multifunktionsgeräten zu regeln:

- Multifunktionsgerät – analog den Endgeräten – in das Sicherheitskonzept aufnehmen
- unbefugten Zugriff von Mitarbeitern aus dem internen Netz verhindern mittels
  - sicherer Konfiguration der Datenschnittstelle
  - Sicherstellung, dass Software des Druckers nicht fehlerhaft ist

  Fragestellung: Muss das Multifunktionsgerät unbedingt im Netzwerk eingebunden werden?
- Installieren einer kleinen Firewall als Zugriffsschutz
- Zugriff auf Kopiersystem mit Passwort bzw. Smartcard
- ggf. Funktionen nur für Berechtigte freischalten
- Deaktivierung des nochmaligen Aufrufs der zuletzt gedruckten Seite
- Übertragung der Druckdaten im Netzwerk nur mit Verschlüsselung
- Verschlüsselung der Datenspeicherung auf Multifunktionsgeräten oder Überschreibung der Daten installieren
- bei Hardwarebeschaffung auf ausreichende Sicherheitsfunktionen achten.

[Quelle: WEKA (2012): Mängelschwerpunkte bei Datensicherheitsmaßnahmen]

Vorsicht ist auch bei der Rückgabe von gemieteten bzw. geleasten Geräten walten zu lassen. Die Weitergabe an den nächsten Kunden erfolgt i. d. R. ohne vorherige Löschung der Festplatte.

Ein entsprechender Passus sollte im Vertrag mit dem Anbieter für Wartungen aufgenommen werden. Der Löschnachweis sollte schriftlich erbracht werden im 2-Unterschriften-Prinzip (Zwei Unterschriften durch die Wartungsfirma!). Wenn möglich, sollte die Löschung stichprobenartig kontrolliert werden.

Zu beachten ist weiterhin, dass bei installierten Fernwartungen ein Zugriff auf den Datenbestand ebenso möglich ist. Auch hier sind vertragliche Regelungen zur Verhinderung eines Datenmissbrauchs zu treffen.

Hinweis

Bedenken Sie, dass die Verantwortung für den Datenschutz stets die Stelle trägt, die die Geräte einsetzt, d. h. das Unternehmen!

Vorlage

Sicherheitsbelehrung für die Bedienung von multifunktionalen Endgeräten

1 Zweck

Mitarbeiter sind über besondere Risiken, die mit der Arbeit mit multifunktionalen Endgeräten verbunden sind, zu belehren. Die Mitarbeiter sollen mit dieser speziellen Anweisung erneut auf die Einhaltung der notwendigen technischen und organisatorischen Maßnahmen im Zusammenhang mit dem Umgang mit multifunktionalen Endgeräten hingewiesen und sensibilisiert werden.

2 Geltungsbereich

Der Geltungsbereich erstreckt sich auf alle Mitarbeiter, die mit multifunktionalen Endgeräten umgehen.

3 Verfahren

Nochmals werden die Mitarbeiter des Unternehmens auf die besonderen Risiken im Umgang mit multifunktionalen Endgeräten hingewiesen:

- Zur Aufgabenerledigung verwenden Sie ausschließlich die vom Unternehmen freigegebenen Softwareverfahren.
- Es ist nicht zulässig, eigene Hard- oder Software einzusetzen.
- An der bereitgestellten Hardware dürfen keine Veränderungen vorgenommen werden.
- Softwareverfahren und Daten dürfen nicht verfälscht werden oder an unbefugte Dritte weitergegeben werden.
- Hard- und Software darf nicht für eigene Zwecke, insbesondere zum privaten Surfen im Internet, verwendet werden.
- Jederzeit sind die vorgegebenen Sicherheitsmaßnahmen zum Zugangs- und Zugriffsschutz einzuhalten.
- Es dürfen weiterhin keine eigenen Sicherungsdatenbestände angelegt werden.
- Auf mobilen Endgeräten dürfen personenbezogene Daten nur verschlüsselt gespeichert werden.
- Mobile Endgeräte sind stets sicher aufzubewahren.
- Berechtigten Mitarbeitern oder Fremdfirmen ist der Zugriff auf die Endgeräte zu ermöglichen, um eine Revision und Kontrolle vorzunehmen.
- Alle unternehmensspezifischen sonstigen technischen und organisatorischen Maßnahmen sind einzuhalten.

Ein Verstoß gegen diese Maßnahmen kann strafrechtlich und arbeitsrechtlich geahndet werden. Verstöße können den Ruf des Unternehmens schädigen und in besonderen Fällen sogar finanzielle Einbußen nach sich ziehen.

4 Mitgeltende Unterlagen

Alle anderen genehmigten datenschutzrechtlichen Regelungen des Betriebes.

Revision: Änderungsdatum: Seite: 1 von 1

7.10 Beschaffung von Hard- und Software

Die Beschaffung der Hard- und Software sollte auf der Grundlage eines betrieblichen Datenschutzkonzepts zentral erfolgen, um die notwendigen Sicherheitsfeatures aufeinander abstimmen zu können. Die Einbindung privater Hard- und Software ist möglichst auszuschließen oder nur unter eng kontrollierten Bedingungen herzustellen. Sie bedarf der Genehmigung durch die IT-Abteilung des Unternehmens.

In der IT-Abteilung wird ein Verzeichnis über die vorhandene Hardware geführt. Weiterhin wird eine Liste der verwendeten Software mit den dazugehörigen Lizenzen verwaltet. Es muss sichergestellt sein, dass für jeden Arbeitsplatz, der mit Software ausgestattet ist, auch eine Lizenz vorliegt. Von diesen Listen erhält der Datenschutzbeauftragte eine Kopie. Die Listen sind von der IT-Abteilung aktuell zu halten und durch den DSB stichprobenartig zu überprüfen.

Falls neue Verfahren zur Verarbeitung personenbezogener Daten eingeführt werden sollen, ist vorab der DSB zu informieren. Erst nach Freigabe durch den DSB kann eine Beschaffung erfolgen. Um diesen Prozess reibungslos gestalten zu können, ist eine enge Kooperation zwischen IT-Abteilung und DSB vonnöten.

Sollten Hardware- oder Softwarekomponenten gestohlen und damit ein Zugriff auf personenbezogene Daten wahrscheinlich werden, sind die IT-Abteilung und der DSB unverzüglich zu informieren. Der DSB leitet die Informationen an die Datenschutzbehörde des Landes weiter. Die Geschäftsführung schaltet die Polizei ein, siehe Meldeverfahren für Datenpannen (Anhang 18 und 19).

7.11 Speicherung/Sicherung von Daten

Die Speicherung von Daten sollte grundsätzlich auf hierfür zur Verfügung gestellten Netzlaufwerken erfolgen. Speicherungen auf privaten Rechnern, Laptops und mobilen Speichermedien sollten der Restriktion unterliegen und in einer Anweisung geregelt werden:

Merke

Welche Datenkategorien dürfen wo gespeichert werden?

Bei Netzwerken zeichnet gewöhnlich die DV-Abteilung für die Sicherung jener Daten verantwortlich, die auf dem Server gespeichert sind.

Eine wichtige zu klärende Frage ist, welche Daten über die DV-Abteilung zu sichern sind und welche Daten, wie z. B. E-Mails, über den Nutzer. Erfahrungsgemäß ist teilweise kein Bewusstsein bei den Mitarbeitern gegeben, dass auch sie Daten sichern müssen.

Bei Notebooks ist der Nutzer selbst für die Datensicherung zuständig. Dies wird erfahrungsgemäß jedoch nicht getan. Auch hier ergeben sich Impulse für ein wirksames Datenschutzkonzept.

Sollte ein Netzwerkzugang möglich sein (Notebook mit Netzwerkkarte), so scheint es sinnvoll, die Daten in einem festgelegten Zeitraum auf das für den Benutzer reservierte Netzlaufwerk zu überspielen. Welcher Zeitraum für die Datensicherung gewählt wird, ist abhängig von

- der Menge der erzeugten Daten,
- ihrer Redundanz,
- ihrer Bedeutung.

Die Datensicherung ist regelmäßig über Stichprobenverfahren zu testen.

Beispiel

In einem mittelständischen Unternehmen wurden Datensicherungen durchgeführt; wie sich jedoch herausstellte, waren keine Daten auf den Sicherungsbändern vorhanden. Eine technische Panne, die mit einem erheblichen Aufwand der Wiederherstellung von Daten aus anderen Quellen verbunden war.

Bei der Sicherung von Daten müssen die Aufbewahrungsfristen (in der Regel 6 und 10 Jahre) beachtet werden. Insbesondere stellt sich technisch die Frage, ob in 10 Jahren die Daten mit dem Stand der zukünftigen Technik noch auslesbar sind. Eine Löschung derartig relevanter Daten, darunter insbesondere personenbezogener Daten, ist der DV-Abteilung anzuzeigen. Nochmals sei darauf hingewiesen, dass bei der Rückgabe von IT-Komponenten zuvor alle Daten wirksam gelöscht werden müssen. Die Löschung sollte im 2-Unterschriften-Prinzip manifestiert werden.

So externe Dienstleister mit der Datensicherung beauftragt werden, sind entsprechende vertragliche Regelungen unabdingbar. Auch ist der Nachweis der Datensicherung über eine Stichprobe regelmäßig abzufordern, um Datenverlusten vorzubeugen. Im Anhang findet sich eine Anweisung zum Speichern und Scannen von Daten (Anhang 16).

7.12 Einsatz von Videosystemen

7.12.1 Videoüberwachung öffentlich zugänglicher Räume

Die Überwachung von Personen per Videokamera stellt einen gravierenden Einschnitt in die Privatsphäre des Betroffenen dar. Videoüberwachungen bedürfen daher einer besonderen Abwägung der Interessenslage. Eine Zulässigkeit der Videoüberwachung öffentlich zugänglicher Räume ergibt sich aus den Ausführungen im § 4 BDSG. Gründe für eine Zulässigkeit sind demnach:

a) – zur Aufgabenerfüllung öffentlicher Stellen,
   – zur Wahrnehmung des Hausrechts
   – zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke.

und

b) wenn keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen.

Ein besonders wichtiges schutzwürdiges Interesse besteht bei der Videoüberwachung von öffentlich zugänglichen großflächigen Einrichtungen (Plätze, Sportanlagen usw.), Fahrzeugen oder öffentlich zugänglichen großflächigen Einrichtungen des Schienen-, Schiffs- und Busverkehrs. Hier liegen Gründe vor, die im Schutz von Leib und Leben der Betroffenen liegen.

Die Videoüberwachung ist anzuzeigen (zu kennzeichnen). Der Name und die Kontaktdaten des für die Verarbeitung Verantwortlichen sind frühestmöglich bekannt zu machen. Speicherung und Verwendung der gewonnenen Bilddaten sind zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich werden oder zur Abwehr von Gefahren dienen. So Bilddaten einer Person zugeordnet werden können, muss der Betroffene informiert werden.

Die Daten unterliegen der Löschung, so der Zweck sie nicht mehr erforderlich macht.

7.12.2 Betriebliche Videoüberwachung

Der Einsatz von Videotechniken zur Überwachung von maschinellen Anlagen, Lüftungsklappen, Schornsteinen, Filtern, Tankanlagen, Gebäuden u. a. m. gehört zu einer weit verbreiteten Geschäftspraxis. Zum einen stehen die Videoüberwachungen im Zusammenhang mit der Kontrolle technischer Funktionen, zum anderen gilt es, Sachbeschädigungen und Diebstähle abzuwehren.

Mit dem Einsatz von Videosystemen sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Die Anforderungen an die Installation von Videoüberwachungen sind aus datenschutzrechtlicher Sicht entsprechend hoch. Eine Videoüberwachung ist folglich nur dann zulässig, wenn weniger einschneidende Maßnahmen nicht zum gleichen Ziel führen.

An dieser Stelle ist stets eine Interessenabwägung zwischen dem Schutzbedarf der Betroffenen und den Interessen des Arbeitgebers anzustellen. Die Gründe für die Installation betrieblicher Videokameras dürfen folglich nicht lapidar sein und keinesfalls zur Ausspionierung von Mitarbeitern geeignet sein.

Beispiel

Ein Unternehmen ist auf dem Gelände eines Chemieparks angesiedelt. Der Chemiepark ist großflächig umzäunt. Einfahrten sind nur kontrolliert über die definierten Werkstore und nach einer Anmeldung mit Personalausweis beim Werkschutz möglich. Das Areal des Unternehmens selbst ist ebenso umzäunt. Vor 2 Jahren wurde im Unternehmen in mehrere Räume eingebrochen. Es wurde eine Kaffeemaschine im Wert von 100 EURO entwendet. Der Vorfall wurde der Polizei gemeldet. Recherchen ergaben nichts. Nach 2 Jahren argumentiert der Arbeitgeber, dass er aufgrund dieses Vorfalls Videokameras an allen Zugängen zum Gebäude aufstellen möchte. Nach den Plänen werden mit den Kameras Mitarbeiter an allen Zugängen zum Gebäude gefilmt, aber auch Besucher, Fremdfirmen sowie die angrenzenden Parkplätze auf den Straßen des Chemieparks (und damit auch alle, die ihr Auto dort parken). Der Arbeitgeber plädiert auf sein Hausrecht.

Die Aufstellung der Videokameras erscheint unverhältnismäßig. Der Einbruch liegt 2 Jahre zurück. Es handelte sich um einen Bagatelldiebstahl. Es konnte überdies nicht geklärt werden, ob jemand von außen überhaupt in das Gebäude eingedrungen ist.

Die Umzäunung stellt eine ausreichende Abwehr dar. Besucher und Betriebsfremde können nur unter Registrierung an der Pforte auf das Gelände. Die Überwachung der Parkplätze steht in keinem Verhältnis zur eigentlichen Absicht des Arbeitgebers. Hier kam es weder zu Diebstählen noch zu Sachbeschädigungen. Das Kommen und Gehen der Mitarbeiter, ihr Pausenverhalten an den Zugängen zur Produktion stellen schutzwürdige Interessen der Mitarbeiter dar. Diese übersteigen das Ansinnen des Arbeitgebers in deutlichem Maße.

Allenfalls können Videokameras an den Zäumen so angebracht werden, dass sie Einbrecher aufnehmen, die über den Zaun in das Betriebsgelände eindringen wollen. Die Kameras sind so aufgestellt, dass sie jeweils an den Ecken der Umzäunung gegenläufig ausgerichtet sind. Der Winkel der Videokameras ist so festgestellt, dass eine Schwenkung in den Innenbereich des Geländes oder zu den Parkplätzen nicht möglich ist. Damit können auch keine Arbeitnehmer aufgenommen werden. Besucher oder Betriebsfremde könnten nur beim Öffnen des Tors und beim Zugang zum Gelände kurzzeitig aufgenommen werden. Ein Hinweisschild wäre für diesen Fall deutlich sichtbar anzubringen. Die verantwortliche Stelle wäre über das Firmenschild eindeutig ausgewiesen.

Daher erscheint es empfehlenswert, Pro und Kontra der Videoüberwachungsnotwendigkeit genauestens gegenüberzustellen. Der Datenschutzbeauftragte ist selbstverständlich in allen Belangen hierzu einzubeziehen.

Hinweis

Die Betrachtung des Sachverhalts, weshalb ein Videoüberwachungssystem installiert wird, sollte vom DSB dokumentiert werden.

Für den Fall der Videoüberwachung der Lüftungsklappen kam es u. a. zu folgenden Erwägungen:

Die Herangehensweise ließe sich in einer Tabelle darstellen:

Vorlage

Vergleich konventionelle und Videotechnik aus datenschutzrechtlicher Sicht

Ort/Tätigkeit	konventionelle Maßnahmen	Vorteile der Videoüberwachung	Maßnahmen zur Wahrung der informationellen Selbstbestimmung
Lüftungsklappen auf dem Hallendach 1	– nur stichprobenartige Inspektionen der Lüftungsklappen möglich – Sicherheitsrisiko bei der Besteigung des Daches	– permanente Überwachung und Datenübertragung an die Leitwarte – bei korrekter Installation keine Aufnahme über das betreffende Hallendach hinaus	– keine Speicherung von Daten – Installation in der Weise, dass außer dem Hallendach keine weiteren Bereiche aufgenommen werden.
Tankstelle	– hoher personeller Einsatz zur Rund-um-Bewachung	– permanente Überwachung und Datenübertragung an die Leitwarte	– Winkel der Überwachungskamera so einstellen, dass nur die Tankstelle, der LKW und der Fahrer, ggf. betreuendes Betriebspersonal aufgenommen werden können. – andere Bereiche mit Schwarzblende versehen – Hinweisschild anbringen – Schulung der Mitarbeiter – Betriebsvereinbarung abschließen

Revision: Änderungsdatum: Seite: 1 von 1

Gemäß dargestelltem Beispiel sind im Rahmen der Installation von Überwachungskameras folgende Überlegungen anzustellen:

- Grund für die Aufstellung von Videosystemen
- Aufnahmebereich/Schwenkradius der Kamera
- Zeitraum der Überwachung
- Videoüberwachung mit oder ohne Aufzeichnung.

Sollen Mitarbeiter potenziell mit dem Videosystem überwacht werden können, so ist die Arbeitnehmervertretung in die Pläne zur Aufstellung von Videoüberwachungen einzubeziehen. In der Regel wird hierüber unter Beteiligung des Betriebsrats eine Betriebsvereinbarung geschlossen. Sie soll das heimliche Ausspionieren von Betriebsangehörigen wirksam verhindern.

Neben der Aufnahme von Betriebsangehörigen geraten auch benachbarte Gebäude, Wohnungen, Parkplätze und öffentliche Straßen ins Visier der Kamera. Dem Anspruch auf Schwarzschaltung, d. h. auf die Ausblendung dieser Bereiche, wurde bereits mehrfach gerichtlich stattgegeben. Maßgeblich für die Urteilsfindung der Gerichte war es, dass für die Art der Wohnungsüberwachung keine erklärbare Rechtsgrundlage existiere, die den Regelungen im Grundsatz genüge.

Folglich sind technische Maßnahmen zu ergreifen, wie z. B.

- Schwenksperren
- Schwarzblendungen
- Bildübertragung ohne Speicherung.

Nachstehend sollen die grundlegenden Anforderungen an die Aufstellung von Videosystemen nochmals zusammengefasst werden:

Videoüberwachung mit dem Ziel	nur erlaubt bei
Prävention	– strikter Zweckbindung (dokumentieren) – der Ausübung des Hausrechts oder nur **mit** rechtswirksamer Einwilligung der Betroffenen – Umsetzung des Prinzips der Datensparsamkeit – datenschutzrechtlicher Vorabkontrolle – Beschränkung auf unabdingbares Maß – enger räumlicher Eingrenzung der Aufnahmen – zeitlicher Begrenzung – möglichstem Verzicht auf Speicherung – Zoom-Kontrolle – Hinweisschild installieren – Schulung/Unterweisung
Gefahrenabwehr	
Verfolgung strafrechtlicher Handlungen	

Ein Beispiel für eine Betriebsvereinbarung ist nachstehend abgebildet.

Vorlage

Betriebsvereinbarung zur Aufstellung/Installation von Videokameras im Unternehmen

zwischen

Muster GmbH

und

Betriebsrat der Muster GmbH

vertreten durch

_____

_____

Präambel

Beide Parteien stimmen überein, dass eine Videoüberwachung der Zufahrtsbereiche und des Parkplatzes unter Wahrung der Privatsphäre der Mitarbeiter, der Datensparsamkeit und der Verhältnismäßigkeit der Maßnahmen rechtlich gemäß BDSG in seiner letzten Fassung möglich ist. Sicherheitsforderungen und Datenschutz sollen sich nicht ausschließen, sondern in vertretbarer Weise miteinander gekoppelt werden.

Regelungsgegenstand

Gegenstand dieser Betriebsvereinbarung ist die Installation und Nutzung von Videosystemen innerhalb des Unternehmens.

Bei der Anfertigung von Videoaufnahmen handelt es sich um eine Erhebung, Speicherung und ggf. auch Verarbeitung personenbezogener Bilddaten, die unter das Datenschutzrecht fallen.

Revision: Änderungsdatum: Seite: 1 von 3

Zweck des Einsatzes von Videoüberwachungskameras

Um eine Zufahrtskontrolle zu ermöglichen, strafbare Handlungen effektiver zu vermeiden sowie Havarien und Sicherheitsvorfälle unverzüglich erkennen und abstellen zu können, sind im Unternehmen Videokameras aufgestellt.

Es handelt sich um folgende Videokameras:

- Videokamera zur Überwachung des Lieferverkehrs – i. d. R. werden die Straße, die Transporter, PKW, die Nummernschilder der KFZ, ggf. die Fahrer und Insassen sowie Passanten aufgezeichnet; der Schwenkbereich der Videokamera ist so eingeschränkt, dass ein Blick in die Büros der benachbarten Unternehmung explizit nicht möglich ist
- 2 Videokameras zur Überwachung des Entladevorgangs und -verkehrs – i. d. R. wird der LKW, das Nummernschild, der Fahrer aufgenommen, ggf. auch ein Mitarbeiter der Muster GmbH
- 2 Videokameras an den 3 Silos auf den Dächern zur Staubemissionsüberwachung – Aufnahme von Mitarbeitern wenig wahrscheinlich
- 1 Videokamera zur Überwachung des Ofenauslaufs am Drehrohrofen – ggf. wird ein Passant (Mitarbeiter) aufgenommen
- 1 Videokamera in der Halle zur Überwachung des Anlieferverkehrs und der Schließung der Tore – Aufnahme der dort tätigen Personen möglich

Die unter Umständen aufgezeichneten personenbezogenen Bilder werden durch Mitarbeiter in der Leitwarte überwacht und im Videosystem gespeichert. Der Personenkreis, der die Bilder auswertet, ist auf ... beschränkt.

Die Verhältnismäßigkeit der Maßnahme wurde positiv durch den DSB geprüft.

Aufzeichnungszeitraum

Das Videosystem ist täglich von ... bis ... in Betrieb.

Festlegung des Nutzungsanlasses

Die Videoaufzeichnungen werden ausgewertet, wenn Unregelmäßigkeiten stattgefunden haben.

Die Auswertung wird vom Geschäftsführer in Zusammenarbeit mit dem Betriebsrat und dem DSB angeordnet.

Aufbewahrung und Zugriff auf Videobänder

Die Videobänder werden vor Missbrauch ... aufbewahrt.

Zugriff haben:

_____

_____

Aufbewahrungsdauer

Die Videobänder werden ... Tage aufbewahrt und danach zum Überschreiben gelöscht.

Sonstiges

Müssen für Beweiszwecke Videoprints gefertigt werden, sind diese in einem Verzeichnis festzuhalten, aus dem hervorgeht, wann und zu welchem Zweck diese angefertigt wurden und wer sie erhalten hat.

Defekte Videobänder werden eingezogen und wirksam vernichtet unter Einhaltung des Datenschutzes. Die Löschung wird dokumentiert (Bandnummer, Löschdatum).

Schlussbestimmungen

Der DSB kontrolliert die Einhaltung der Datenschutzbestimmungen und der Datensicherheit.

Die Betriebsvereinbarung tritt mit … in Kraft und kann mit einer Frist von 3 Monaten beidseits schriftlich gekündigt werden. Nach Eingang der Kündigung sind unverzüglich Verhandlungen über eine neue Vereinbarung einzuleiten.

Nachträgliche Änderungen können in beiderseitigem Einvernehmen vorgenommen werden, ohne dass die restlichen Bestimmungen des Vertrages berührt werden oder der Vertrag gekündigt werden muss.

_____

Ort, Datum

Unterschriften:

_____ _____

Betriebsrat Geschäftsführer

Stand:

7.13 Vernichtung, Entsorgung von Dokumenten und Datenträgern personenbezogenen Inhalts

In den Medien wurde bereits mehrfach über Pleiten, Pech und Pannen bei der Vernichtung von Dokumenten und Datenträgern mit personenbezogenen Daten berichtet. Wollen auch Sie Opfer eines Datenskandals werden? Diese provokante Frage zeigt, wie sorglos wir häufig bei der Vernichtung von Papieren personenbezogenen Inhalts vorgehen. Das Schreddern von personenbezogenen Daten in Papierform wird häufig der Personalabteilung oder der Abteilung für die Lohn- und Gehaltsabrechnung zugeordnet. Andere Bereiche verfügen in der Regel über keinen Schredder. Ob es nun Unfallmeldungen sind, Urlaubspläne, Leistungsnachweise, Teilnahmezertifikate, vorgeschriebene Zeugnisse o. a. m., dies alles sind Dokumente personenbezogenen Inhalts. Nach wie vor werden die häufigsten Fehler bei der Vernichtung von Papierunterlagen begangen. Hier kann durch einfache organisatorische Regelungen und mit einer Sensibilisierung der Mitarbeiter Abhilfe geschaffen werden. Dennoch werden immer wieder durch Reinigungspersonal Akten mit personenbezogenen Daten im Papierkorb gefunden und an Unbefugte weitergeleitet oder von Dritten aus Abfalltonnen herausgezogen.

Die Beauftragung externer Unternehmen für eine professionelle Vernichtung/Entsorgung schützt, wie die Praxis zeigt, nicht vor bösen Überraschungen.

Das Unternehmen entledigt sich mit der Beauftragung einer externen Unternehmung seiner Verantwortung im Datenschutz nicht. Es bleibt so lange in der Haftung, wie es durch gezielte Kontrollen sich des Entsorgungsweges auch versichert. Nicht allein, dass ein schriftlicher Vertrag zur Bindung des Dienstleisters mit eng beschriebenen Pflichten vorliegen muss, sondern auch die Begehung vor Ort und das sich Überzeugen von den dem Datenschutzniveau angemessenen Gerätschaften nach DIN 66399-1[1)] spielen eine wesentliche Rolle für die Eingrenzung des Haftungsrisikos. Vorzugsweise sind entsprechende Zertifizierungen für die ordnungsgemäße Entsorgung vom Dienstleister vorzulegen.

1) DIN 66399-1:2012-10, Büro- und Datentechnik – Vernichten von Datenträgern – Teil 1: Grundlagen und Begriffe, Beuth Verlag

Bei der Entsorgung von Datenträgern ist zu beachten, dass je sensibler die personenbezogenen Daten ausfallen, sich auch die Anforderungen an die technischen und organisatorischen Maßnahmen erhöhen. Diese Botschaft richtet sich auch an die verwendeten Gerätschaften. Bereits im Jahr 1985 wurde mit dem Erscheinen von DIN 32757-2[2)] (ersetzt durch DIN 66399) zwischen 5 Sicherheitsstufen unterschieden. Die Sicherheitsstufen sind auf verschiedene Materialkategorien anzuwenden, z. B. auf Papier, SIM-Karten, Disketten, Tonbänder, Computer usw.

Im Hinblick auf die Beauftragung eines Entsorgers wird ein schriftlicher Vertrag zwischen Auftraggeber und Entsorger gefordert. Die eingesetzten Fahrzeuge für den Datentransport müssen entweder über einen Kofferaufbau oder über einen gesicherten Containeraufbau verfügen. Weiterhin wird die Vernichtung der Datenträger in möglichst einem Tag nach Eintreffen beim Entsorger verlangt.

Daher sollte der Auftraggeber sich von den Umständen der Entsorgung und der Qualifizierung des beauftragten Unternehmens gründlich überzeugen.

Hinweis

Verträge sollen

- das Recht auf unangemeldete Kontrollen
- Vertragsstrafen für den Fall der Verletzung datenschutzrechtlicher Bestimmungen
- die Beschreibung der Technik für die Vernichtung
- den Nachweis der Zertifizierung
- die Beschreibung der Transportmittel bzw. der ggf. eingesetzten Unterauftragnehmer
- Gewährleistung der Mindestsicherheitsstufe 3

enthalten.

Was die Vernichtung von magnetischen Datenträgern anbelangt, so ist DIN EN 66399 Folge zu leisten. Aufsichtsbehörden weisen immer wieder darauf hin, dass Datenträger entweder physisch vernichtet oder physikalisch gelöscht werden müssen.

Für CDs und DVDs kommen Multimedia-Schredder zur Anwendung. Festplatten, die sich nicht mehrfach überschreiben lassen, müssen entweder physikalisch oder durch ein starkes Magnetfeld irreversibel gelöscht werden. Durchbohren und Häckseln sind selbstverständlich auch möglich.

7.14 Reisedaten von Arbeitnehmern

Im Zuge der Planung von Dienstreisen werden beim Arbeitnehmer verschiedenste personenbezogene Daten erhoben. Beispielsweise betrifft dies:

- Kopien des Personalausweises oder Reisepasses
- Kreditkartendaten
- Wohnanschrift
- Geburtsdatum
- KFZ-Kennzeichen
- personenbezogene Daten eventuell Mitreisender.

Diese Daten müssen nach den gleichen Prinzipien des Datenschutzes aufbewahrt und gehalten werden wie auch andere personenbezogene Daten im Zusammenhang mit dem Arbeitsverhältnis. In der Praxis sind jedoch häufig weder die Räume noch die Schränke verschlossen, in denen Reisedaten aufbewahrt werden. Entsprechende technische und organisatorische Datenschutzmaßnahmen sind abzuleiten und unterliegen der Kontrolle durch den DSB.

2) DIN 32757-2:1985-10, Büro- und Datentechnik; Vernichten von Informationsträgern; Maschinen und Einrichtungen; Mindestangaben, Beuth Verlag

Auch ergibt sich nicht aus dem geschlossenen Arbeitsverhältnis automatisch, dass die für Reisebuchungen benötigten Angaben der Einwilligung des Beschäftigten unterliegen. Auch hier empfiehlt es sich, entsprechende Einwilligungserklärungen fallbezogen vom Arbeitnehmer einzuholen. Als praktikabel haben sich in Dienstreiseanträge integrierte Textpassagen mit Einwilligungserklärungen erwiesen.

Einverständniserklärung Vorlage

Hiermit erkläre ich mich einverstanden, dass meine personenbezogenen Daten im Rahmen der konkreten Reisemeldung den mit der Reisebuchung beauftragten Personen offengelegt und die für die Reisebuchung notwendigen Daten an Reisebüros, Fluggesellschaften, Autovermietungen, Leasinggesellschaften, der Deutschen Bahn AG und/oder anderen konkret von dieser Reisebuchung betroffenen Gesellschaften unter Wahrung der weitestgehend möglichen Datensparsamkeit und des Datenschutzes übergeben werden.

Im Unternehmen sind i. d. R. mit der Reisebuchung folgende Personen befasst:

–

–

–

Die genannten Mitarbeiter sind schriftlich und nachweislich auf die Einhaltung des Datenschutzes verpflichtet worden.

Ort, Datum Einwilligung per Unterschrift

Revision: Änderungsdatum: Seite: 1 von 1

Der Text ist nicht zufällig im Fettdruck optisch hervorgehoben. Einwilligungserklärungen müssen separat, auf den konkreten Fall bezogen und deutlich herausgestellt erfolgen.

Wie aus dieser Textpassage deutlich wird, sind weitere Verpflichtungen mit der Erhebung und Verarbeitung sowie Übermittlung personenbezogener Daten mit der Dienstreisebuchung verbunden. Der Personenkreis, der mit Reisebuchungen im Unternehmen beauftragt wird, ist konkret zu benennen, auf das notwendige Maß zu beschränken und entsprechend datenschutzrechtlich zu belehren. Auch hier fehlen häufig in der Praxis die Datenschutzerklärungen der Mitarbeiter.

Weiterhin bleibt durch den DSB zu verfolgen, auf welche Weise die für Reisezwecke erhobenen Daten an Dritte (zum Beispiel Reisebüros) übermittelt werden. Folgende Fragen sind aus datenschutzrechtlicher Sicht u. a. zu behandeln:

- Welche Daten werden auf welche Weise an wen übermittelt?
- Sind diese Übermittlungswege geschützt? (also nicht per E-Mail)
- Wie sind die Mitarbeiter des Datenempfängers datenschutzrechtlich unterwiesen?
- Welche Datenschutzerklärungen des Reisedienstleisters gegenüber der verantwortlichen Stelle gibt es?

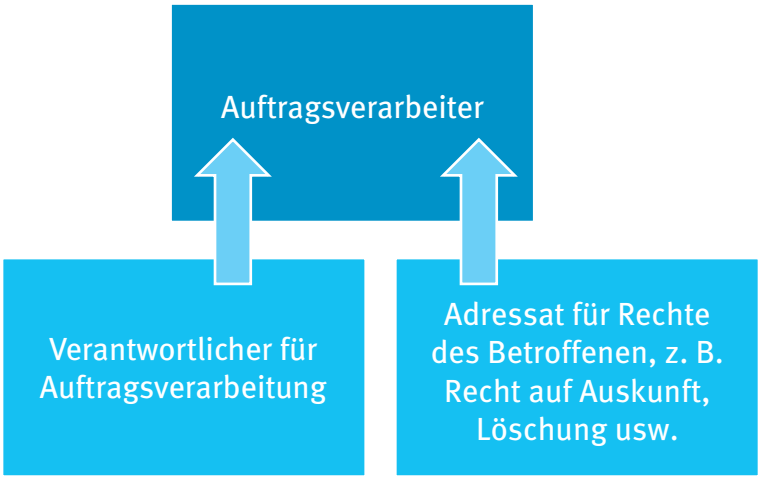
Von der Versendung von E-Mails in ungeschützten Verbindungen sollte hierbei abgesehen werden. Alternativen sind die postalische Überstellung der Daten oder die Direkteingabe in Buchungsmasken.

Im Unternehmen ist die Frage zu regeln, wie lang die erhobenen Daten gespeichert werden sollen. Eine Vorratsdatenspeicherung der Daten ist nicht zulässig. Auch hier ist eine sinnvolle Regelung mit den Betroffenen abzustimmen.

8 Auftragsverarbeitung

8.1 Pflichten des Auftragsverarbeiters

Ein Auftragsverarbeiter ist per Definition der EU-DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.



Grundsätzlich darf der Verantwortliche für die Verarbeitung eine Auftragsverarbeitung nur dann zulassen, wenn der Auftragnehmer über die notwendigen technischen und organisatorischen Voraussetzungen verfügt und er grundsätzlich davon ausgehen kann, dass die Verarbeitung personenbezogener Daten im Einklang mit datenschutzrechtlichen Bestimmungen erfolgt. Dazu gehören auch die allgemein üblichen Informationen zu einem Dienstleister, z. B. Umsatzsteueridentifikationsnummer, Anschrift, Inhaber/Geschäftsführung, Kontaktdaten wie E-Mail-Adresse, Telefonnummer, ggf. Nachweis der steuerlichen Unbedenklichkeit u. a. m. Der Verantwortliche sollte sich vor Auftragserteilung vergewissern, wie die Geschäftsräume aussehen, welche technischen und organisatorischen Vorkehrungen getroffen wurden, wie die Absicherung der Verarbeitung personenbezogener Daten erfolgt.

Von einer Verarbeitung personenbezogener Daten im Auftrag wird demnach gesprochen, wenn die verantwortliche Stelle sich eines Dienstleisters bedient,

- der im Auftrag und
- weisungsabhängig
- personenbezogene Daten erhebt, verarbeitet oder nutzt.

Der Dienstleister darf keine Unterauftragnehmer ohne Kenntnis und Zustimmung des Verantwortlichen für die Verarbeitung beschäftigen.

So sich beide Parteien darüber einig sind, dass ein weiterer Auftragsverarbeiter hinzugezogen werden soll, so muss dieser die gleichen Vertragsinhalte hinsichtlich des Datenschutzes übernehmen.

Unternehmen sind immer mehr dazu übergegangen, einzelne Geschäftsprozesse auszulagern, die entweder zu kostenintensiv waren oder für die nicht die geeignete Technik oder das entsprechend qualifizierte Personal zur Verfügung stand. Diese Tendenz spiegelt sich auch im Outsourcing von Datenverarbeitungsprozessen wider. Eine Vielzahl von Anbietern hat sich auf Teilaufgaben in der Datenverarbeitung spezialisiert. Beispiele hierfür sind die Lohn- und Gehaltsabrechnung durch Steuerbüros und Call-Center.

Prinzipiell stellt sich aus datenschutzrechtlicher Sicht die Frage, welche Datenverarbeitungsprozesse in welcher Art und Weise ausgelagert werden können. Hierfür spielen die Auswahl geeigneter Dienstleister und deren vertragliche Bindung eine große Rolle. Grundsätzlich bleibt

das Unternehmen die verantwortliche Stelle im Prozess der Auftragsverarbeitung. Trotz der Auslagerung des betreffenden Datenverarbeitungsprozesses an den Dienstleister bleibt das Unternehmen in der datenschutzrechtlichen Verantwortung für die überlassenen Daten und damit auch in der Haftung. Demnach kommt der Überwachung der mit der Erbringung der Dienstleistung beauftragten Unternehmung eine große Bedeutung zu. Leider werden Datenverarbeitungsprozesse häufig ohne konkrete Kontrolle der installierten technischen und organisatorischen Maßnahmen im Datenschutz outgesourct.

Welche Anforderungen konkret an die Gestaltung des Dienstleistungsvertrags aus datenschutzrechtlicher Sicht gestellt werden, kann im Kapitel 11 nachgelesen werden. Dort werden auch Auszüge aus Verträgen mit Dienstleistern zur Adaption an die betriebliche Praxis abgebildet.

Pflichten in der Auftragsverarbeitung § 62 BDSG:

Auftraggeber	Auftragnehmer
– sorgfältige Auswahl des Dienstleisters – schriftlicher Vertrag – Kontrolle und Überwachung – Einräumung Zugangsrecht	– Weisungsgebundenheit – keine Beauftragung von Unterauftragnehmern ohne Zustimmung des Verantwortlichen – sofortige Meldung besonderer Vorkommnisse – Einhaltung der datenschutzrechtlichen Bestimmungen – Verpflichtung des Personals auf das Datengeheimnis, Gewährleistung von Vertraulichkeit – Bereithalten von Nachweisen für die Erfüllung seiner Pflichten bezüglich der Protokollierung gemäß § 76 BDSG – Führen des Verzeichnisses aller Verarbeitungen im Auftrag des Verantwortlichen

Obwohl die Haftung für die Auslagerung personenbezogener Daten zur Verarbeitung durch Dritte beim Auftraggeber verbleibt, sind auch durch den Auftragnehmer gesetzliche Pflichten zu erfüllen. Sie betreffen vor allem die Gewährleistung der Anforderungen an die Sicherheit der Datenverarbeitung (§ 64 BDSG), siehe Checkliste.

Anforderungen an die Protokollierung gemäß § 76 BDSG sind:

1) Erhebung
2) Veränderung
3) Abfrage
4) Offenlegung einschließlich Übermittlung
5) Kombination
6) Löschung

Im Fall der Offenlegung müssen folgende Daten mindestens zur Verfügung stehen:

– Begründung für die Offenlegung
– Datum und Uhrzeit der Vorgänge
– Identität der Person, die die Abfrage/Offenlegung tätigt, soweit möglich
– Identität des Empfängers der Daten.

Die Protokolldaten sind am Ende des auf deren Generierung folgenden Jahres zu löschen (§ 76 (4)).

Die Protokolle müssen auf Anforderung des Bundesdatenschutzbeauftragten durch den Verantwortlichen und Auftragsverarbeiter zur Verfügung gestellt werden.

Der Auftragsverarbeiter hat eine Verzeichnis aller Kategorien von Verarbeitungen bezüglich seiner Auftragsverarbeitung zu führen mit folgenden Angaben:

- Name und Kontaktdaten des Auftragverarbeiters
- Name und Kontaktdaten jedes Verantwortlichen, für den er tätig ist
- Name und Kontaktdaten des Datenschutzbeauftragten des Verantwortlichen, so vorhanden
- ggf. Übermittlungen personenbezogener Daten an einen Drittstaat
- ggf. Übermittlungen an eine internationale Organisation
- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 64 BDSG
- die Verzeichnisse sind schriftlich und elektronisch zu führen und dem Bundesbeauftragten auf Anforderung zur Verfügung zu stellen.

So der Auftragsverarbeiter Verarbeitungen vornimmt, die einer Datenschutz-Folgeabschätzung unterliegen, muss er diese durchführen.

Er hat einen Datenschutzbeauftragten zu bestellen, wenn er mehr als 10 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt. Die anderen Gründe zur Bestellung eines Datenschutzbeauftragten bleiben auch für Auftragsverarbeiter verbindlich.

8.2 Vertragliche Regelungen in der Auftragsverarbeitung

Bei der Verarbeitung von Daten im Auftrag bleibt der Auftraggeber die verantwortliche Stelle. Er zeichnet für den ordnungsgemäßen Umgang mit personenbezogenen Daten gemäß BDSG und weiteren rechtlichen Anforderungen verantwortlich. Folglich hat der Auftragnehmer die notwendigen technischen und organisatorischen Maßnahmen sicherzustellen, die einen wirksamen Schutz personenbezogener Daten gewährleisten. Der Auftraggeber, d. h. die verantwortliche Stelle, muss die Art und Weise der Auftragsverarbeitung unter Datenschutzgesichtspunkten vertraglich regeln. Dabei ist darauf zu achten, dass die datenschutzmäßigen Sicherheitsmaßnahmen dem Schutzzweck angemessen sind, der Frage der Verhältnismäßigkeit gebührend Rechnung getragen wird.

In der Praxis sind solche Verträge eher selten. Aus Sicht der Autorin besteht hier nach wie vor ein großer Nachholbedarf. Nicht selten schrecken Auftraggeber vor der vertraglichen Regelung technischer und organisatorischer Schutzmaßnahmen zurück, um Dienstleister, gerade im Bereich der Steuerberatung, nicht zu verprellen. Auf die Nachfrage hin, wie der Schutz personenbezogener Daten geregelt sei, erhält das Unternehmen häufig nur die Antwort, dass es (irgendwie) geregelt sei. Schließlich arbeite man in dem Metier schon langjährig. Dennoch sollte der Auftraggeber darauf drängen, sich die Schutzmaßnahmen konkret erläutern zu lassen, und diese in einem Vertrag festhalten. Kann er selbst oder auch sein DSB nicht die Situation beim Auftragnehmer beurteilen, so sollte er sich externer Hilfe bedienen. Teilweise können auch die Datenschutzbehörden angefragt werden oder durch eine Vor-Ort-Kontrolle helfend eingreifen. Maßgeblich erscheint dabei der Autorin der Wille beider Parteien, eine produktive Lösung für eine datenschutzrechtlich konforme Datenverarbeitung zu finden.

8.3 Leitfaden für einen Dienstleistungsvertrag aus datenschutzrechtlicher Sicht

Welche Punkte sollte eine vertragliche Vereinbarung zwischen Auftraggeber und Auftragnehmer beinhalten? Selbstverständlich richtet sich dies nach der Sensibilität der personenbezogenen Daten, dem allgemeinen Datenschutzniveau beim Dienstleister und der Art der Datenverarbeitung. Eine mögliche Auswahl ist im Folgenden dargestellt:

- Beschreibung der zu erbringenden Dienstleistung, so konkret wie möglich und unter Nennung der zu verarbeitenden Datenkategorien und Übermittlungswege
- Einräumung eines vertraglichen Weisungsrechts: Kundendaten dürfen nur nach den Weisungen des Auftraggebers verarbeitet werden, eine andere Nutzung ist strikt zu untersagen
- Beschreibung der technischen und organisatorischen Schutzmaßnahmen gemäß § 11 Abs. 2 BDSG für jede Art des Umgangs mit personenbezogenen Daten
- möglichst Festlegung des Personenkreises, der mit den überlassenen Daten umgeht (vorzugsweise Nennung der Funktion oder des Arbeitsplatzes anstelle des Familiennamens)
- Treffen von Festlegungen hinsichtlich der Berichtigung, Sperrung und Löschung, Einschränkung der Verarbeitung von Daten

Bearbeiter (Funktion)	Art der Daten	Verantwortlich für Berichtigung	Verantwortlich für Sperrung	Verantwortlich für Löschung
...	...	...	...	...

- Festlegungen für Notfallszenarien, z. B. für die Meldekette bei einem Verlust von Daten, bei Datendiebstahl, Diebstahl der EDV-technischen Anlagen u. a. m.
- Absicherung der Eigentumsrechte an den überlassenen Daten (für den Fall der Insolvenz des Auftragnehmers und die Herausgabe wichtig)
- Klärung, ob Unterauftragnehmer eingesetzt sind und wie diese den Anforderungen des BDSG gerecht werden
- Regelung der Informationspflicht bei Einschaltung weiterer Unterauftragnehmer
- Regelung der allgemeinen Informationspflicht und des Kontrollrechts durch die verantwortliche Stelle (Auftraggeber)
- Recht auf Übergabe der Verfahrensverzeichnisse und anderer relevanter Unterlagen, z. B. Schulungsnachweise, Anweisungen
- Hinweis auf Sorgfaltspflicht im Umgang mit personenbezogenen Daten
- Hinweis auf Verpflichtung auf das Datengeheimnis all jener Mitarbeiter, die mit der Auftragsverarbeitung betraut sind
- Regelungen zur Löschung der Daten und Herausgabe im Falle der Vertragskündigung
- Verankerung von Haftungsansprüchen
- Regelung der Vertragsdauer, der eventuellen automatischen Verlängerung
- Regelung zu Entgelten und Zahlungsfristen
- Benennung der gebräuchlichsten rechtlichen Rahmenbedingungen, wie zum Beispiel: BDSG, Telekommunikations- und Telemediengesetz
- gegenseitige Vertraulichkeitserklärung
- Salvatorische Klausel.

Dem DSB sollte vertraglich das Recht eingeräumt werden, vor Ort beim Dienstleister die ergriffenen technischen und organisatorischen Maßnahmen zu kontrollieren. Gestaltet man einen solchen Besuch auf Augenhöhe in dem gemeinsamen Interesse der Einhaltung des Datenschutzes, kann häufig der eine vom anderen lernen. Im Fokus sollte also die Zusammenarbeit stehen und nicht der Kontrollaspekt, um eine datenschutzkonforme Auftragsverarbeitung zu gewährleisten.

In Kapitel 8.4 sind verschiedene Auszüge aus Verträgen mit unterschiedlichen Dienstleistern abgedruckt. Sie dienen als Muster und Anregung für die eigene Vertragsgestaltung.

8.4 Verträge mit Dienstleistern der Auftragsverarbeitung

Ein Beispiel für einen Vertrag mit einem Steuerbüro ist nachstehend abgebildet.

Vorlage

Vereinbarung für die Auftragsverarbeitung durch ein Steuerbüro

zwischen

_____

_____

– im Folgenden Auftragnehmer genannt –

und

_____

_____

– im Folgenden Auftraggeber genannt –

1 Gegenstand des Auftrags

Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung vom ..., auf die hier verwiesen wird.

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben:

–

–

–

Dauer des Auftrags

Der Auftrag ist auf unbefristete Zeit erteilt und kann von beiden Parteien mit einer Frist von _____ gekündigt werden. Die Möglichkeit der fristlosen Kündigung bleibt davon unberührt.

2 Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und Nutzung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck der Aufgaben des Auftragnehmers:

Art der Daten (Zutreffendes ankreuzen):

☐ Personenstammdaten
☐ Kommunikationsdaten (z. B. Telefon, E-Mail)
☐ Vertragsstammdaten
☐ Kundenhistorie
☐ Vertragsabrechnungs- und Zahlungsdaten
☐ Planungs- und Steuerungsdaten
☐ Auskunftsangaben (von Dritten, z. B. Auskunfteien)
☐ Weitere:

Kategorien betroffener Personen (Zutreffendes ankreuzen):

☐ Kunden
☐ Lieferanten
☐ Interessenten

☐ Abonnenten
☐ Beschäftigte
☐ Handelsvertreter
☐ Mitarbeiter von Tochtergesellschaften
☐ Ansprechpartner

Verarbeitung der Daten:

Datenkategorie	Zweck der Verarbeitung	Übermittlungs-weg	Übermittlung an:	Speicherung wo? Dauer?

Die Verarbeitung der Daten findet ausschließlich in der Bundesrepublik Deutschland statt, in einem Mitgliedstaat der EU. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Bedingungen nach Art. 44 ff. DSGVO erfüllt sind.

3 Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

Soweit die Prüfung einen Anpassungsbedarf ergibt, ist der einvernehmlich umzusetzen.

Der Auftragnehmer hat die Sicherheit gemäß Art. 28 Abs. 3 c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen.

Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Auswirkung für die Rechte und Freiheiten von Personen im Sinne von Art. 32 Abs. 1 der DSGVO zu berücksichtigen (Einzelheiten in Anlage 1).

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insofern ist dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4 Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen. Die Kosten hierfür trägt der Auftraggeber.

5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zur Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO, insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Schriftliche Bestellung eines Datenschutzbeauftragten mit Kontaktdaten
- Ein Wechsel des Datenschutzbeauftragten ist unverzüglich dem Auftraggeber zu melden.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3, S. 2, 29, 32 Abs. 4 DSGVO ist sicherzustellen.
- Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet sind und zuvor mit den für sie relevanten rechtlichen Bestimmungen vertraut gemacht worden sind. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf den Auftrag beziehen.
- Sollten dadurch dem Auftragnehmer Mehrkosten entstehen, werden diese auf Nachweis dem Auftraggeber zum Ausgleich übermittelt.
- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um deren Wirksamkeit zu überprüfen.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen nach Ziffer 6 dieses Vertrags
- Unterauftragnehmerverhältnisse sind dem Auftraggeber kundzugeben. Er besitzt bei der Beauftragung Mitspracherechte.

6 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer, Überprüfungen vorzunehmen oder durch zu benennende Prüfer Stichproben tätigen zu lassen. Ziel ist es, sich von der Einhaltung datenschutzrechtlicher Regelungen in der betrieblichen Praxis zu überzeugen, insbesondere von Art. 28 DSGVO.

(2) Der Nachweis solcher Maßnahmen kann durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
- aktuelle Testate, Berichte o. Ä. von Datenschutzbeauftragten, der Revision
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits

erfolgen.

7 Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer ist verpflichtet, umgehend Verstöße gegen die Einhaltung des Datenschutzes dem Auftraggeber zu melden.

Weiterhin erklärt sich der Auftragnehmer bereit, den Auftraggeber bei der Datenschutz-Folgeabschätzung zu unterstützen.

8 Weisungsbefugnis des Auftraggebers

Mündliche Weisungen des Auftraggebers werden zugleich schriftlich vom Auftragnehmer bestätigt.

Revision: Änderungsdatum: Seite: 4 von 5

9 Löschung und Rückgabe personenbezogener Daten

(1) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind jene Sicherungskopien, die zu einer ordnungsgemäßen Datenverarbeitung erforderlich sind.

(2) Rückgabe sämtlicher Unterlagen an den Auftraggeber bei Beendigung des Vertrags.

(3) Dokumentationen, die belegen, dass der Auftragnehmer seiner Datenverarbeitung ordnungsgemäß nachgegangen ist, sind entsprechend den rechtlichen Vorschriften aufbewahrungspflichtig.

Ort, Datum

Auftragnehmer Auftraggeber

Anlagen:

Leistungsvertrag mit dem Steuerbüro

Revision: Änderungsdatum: Seite: 4 von 4

[in Anlehnung an Horst G.A. (2012): Praxiskommentar Bundesdatenschutzgesetz, 6. Aufl., WEKA-Verlag]

9 Übermittlung personenbezogener Daten in Drittstaaten und internationale Organisationen

Eine Übermittlung personenbezogener Daten an Stellen in Drittstaaten oder an internationale Organisationen ist nur beschränkt möglich. Folgende Voraussetzungen sind hierfür zu erfüllen:

– die Stelle oder internationale Organisation verarbeitet Daten für die Verhütung, Ermittlung, Aufdeckung, Verfolgung und Ahndung von Straftaten oder Ordnungswidrigkeiten

– die EU-Kommission hat einen Angemessenheitsbeschluss gemäß Art. 36 EU-DSGVO gefasst.

Letzteres bedeutet, dass eine vorherige Konsultation der Aufsichtsbehörde zu erfolgen hat, so die Datenschutz-Folgeabschätzung ein hohes Risiko der Datenverarbeitung ergibt und sofern keine Maßnahmen der Begrenzung getroffen werden können. Erst nach Freigabe der Aufsichtsbehörde kann eine Übermittlung der personenbezogenen Daten stattfinden.

Dennoch kann die Übermittlung verboten werden, wenn

– im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit personenbezogenen Daten beim Empfänger nicht hinreichend gesichert ist oder

– sonst überwiegende schutzwürdige Interessen einer betroffenen Person entgegenstehen.

Der Verantwortliche hat einzuschätzen, ob der Empfänger einen angemessenen Schutz der personenbezogenen Daten garantiert.

Auch für den Empfang personenbezogener Daten gilt:

– So Daten zu Straftaten oder Ordnungswidrigkeiten aus einem anderen Mitgliedstaat der EU übermittelt werden sollen, bedarf es einer zuvorigen Genehmigung von der zuständigen Stelle des anderen Mitgliedstaats.

– Eine Zulässigkeit ist nur dann gegeben, wenn es gilt, eine unmittelbare Gefahr abzuwenden, die ein solches Vorgehen rechtfertigt oder die Genehmigung nicht rechtzeitig genug erteilt werden kann.

– Eine Weitergabe der personenbezogenen Daten zu Straftaten und Ordnungswidrigkeiten durch den Empfänger ist nur möglich, wenn der Verantwortliche der Datenübermittlung seine vorherige Erlaubnis gegeben hat. Der Verantwortliche hat durch geeignete Maßnahmen sicherzustellen, dass keine mißbräuchliche Weiterübermittlung stattfinden kann.

9.1 Datenübermittlung mit geeigneten Garantien

Eine Übermittlung personenbezogener Daten kann auch ohne Beschluss nach § 36 EU-DSGVO erfolgen, wenn

– in einem Rechtsinstrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind,

– der Verantwortliche bei der Beurteilung des Sachverhalts zu dem Schluss gelangt, dass geeignete Garantien vorliegen.

Letzteres bedarf der akribischen Dokumentation, welche Argumente für eine Übermittlung der personenbezogenen Daten gesprochen haben. Weiterhin muss die Dokumentation Folgendes enthalten:

– Zeitpunkt der Übermittlung

– Identität des Empfängers

– Grund der Übermittlung

– übermittelte personenbezogene Daten.

Der Bundesbeauftragte ist mindestens jährlich über die Übermittlung zu informieren.

9.2 Datenübermittlung ohne geeignete Garantien

Für den Fall, dass

– kein Beschluss vorliegt und

– keine geeigneten Garantien heranzuziehen sind

ist eine Zulässigkeit der Übermittlung personenbezogener Daten gegeben:

– zum Schutz lebenswichtiger Interessen,

– zur Wahrung berechtigter Interessen der betroffenen Person,

– zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit,

– im Einzelfall für die Zwecke der Strafverfolgung,

– im Einzelfall für die Geltendmachung von Rechtsansprüchen.

Der Verantwortliche hat immer von der Übermittlung abzusehen, wenn Grundrechte der betroffenen Person das öffentliche Interesse überschreiten.

9.3 Sonstige Datenübermittlungen an Empfänger in Drittstaaten

Im besonderen Einzelfall können zur Erfüllung ihrer Aufgaben unbedingt erforderliche personenbezogene Daten unmittelbar an in § 78 Absatz 1 nicht genannte Stellen in Drittländern übermittelt werden:

– wenn keine Grundrechte der betroffenen Person das öffentliche Interesse überwiegen,

– wenn die Übermittlung an Stellen der Strafverfolgung wirkungslos wäre oder ungeeignet,

– wenn der Verantwortliche den Empfänger auf die Zwecke der Verarbeitung hinweist.

Im Fall der Übermittlung hat der Verantwortliche die Stelle der Strafverfolgung über die Übermittlung in Kenntnis zu setzen.

Die Übermittlungen sind zu dokumentieren wie oben bereits beschrieben.

Der Empfänger ist durch den Verantwortlichen zu informieren, dass eine Verarbeitung nur zu den vorgesehenen Zwecken erfolgen darf.

10 Datenschutz im Personalwesen – Bewerbungsverfahren

Datenschutzrechtliche Fragestellungen sind bei der Vorlage von Bewerbungsunterlagen und im Rahmen ihrer Bewertung oder ggf. Weitergabe an Entscheider von nicht untergeordneter Bedeutung. Oftmals werden Verstöße gegen das Bundesdatenschutzgesetz nicht erkannt oder für lapidar gehalten. Wie erfolgreiche Beschwerden der Betroffenen vor Gericht zeigen, werden der Schutz personenbezogener Daten und die Missachtung der Vorschriften im Datenschutz weit unterschätzt. Die Unterweisung verantwortlicher Mitarbeiter im Personalwesen und Sensibilisierung für datenschutzrechtliche Belange im Arbeitsalltag sind Schlüssel zu Rechtskonformität und Persönlichkeitsschutz.

Bereits Name, Anschrift und Familienstand, Informationen zu Ausbildung, Referenzen, Urlaubsplanung, Verhalten am Arbeitsplatz stellen schützenswerte personenbezogene Daten dar. Der Unternehmer hat sicherzustellen, dass personenbezogene Daten nur im rechtmäßigen Umfang mit Zweckbindung und unter angemessenen technischen und organisatorischen Maßnahmen erhoben und verarbeitet werden. Hierzu hat er die notwendigen Anweisungen und organisatorischen Regelungen aufzustellen und die mit der Verarbeitung personenbezogener Daten beauftragten Mitarbeiter auf das Datengeheimnis zu verpflichten.

Wie nachstehendes Beispiel zeigt, ist im Rahmen von Bewerbungsverfahren genauer auf die Einhaltung des Datenschutzes zu achten:

Beispiel

Ein Arbeitnehmer bewirbt sich auf eine Stelle in einer rechtlich selbständigen Tochterunternehmung eines Konzerns in Hannover. Aus der Stellenausschreibung ist die Konzernzugehörigkeit jedoch nicht ersichtlich. Eine Verpflichtung des Bewerbers, sich über gesellschaftsrechtliche Verflechtungen zu erkundigen, besteht nicht.

Der für den Auswahlprozess der Bewerber zuständige Personalreferent sichtet die Unterlagen und leitet die Bewerbungsunterlagen an die Personalabteilung der Muttergesellschaft in Dortmund weiter, die das Einstellungsgespräch und auch die Auswahl des Bewerbers vornehmen wird.

Damit werden Bewerbungsunterlagen, d. h. personenbezogene Daten, ohne vorherige Zustimmung bzw. Information des Bewerbers an Dritte (an eine andere rechtlich selbständige Unternehmung) weitergeleitet.

Ähnlich stellt sich der Fall dar, wenn das Auswahlverfahren in dem Unternehmen stattfindet, auf das sich beworben wird, die endgültige Zusage gegenüber dem Bewerber jedoch von der Zustimmung der Konzernleitung (oder der Personalabteilung im Konzern) abhängig ist. Auch dann werden die Bewerbungsunterlagen ohne vorherige Zustimmung bzw. Information des Bewerbers unbefugt an Dritte übermittelt.

Fazit: Eine Überlassung der Bewerbungsunterlagen an Dritte ist grundsätzlich nur mit Information und Einwilligung des Bewerbers in Schriftform möglich.

Doch diese Einwilligungserklärung bleibt aus rechtlicher Sicht umstritten. Gibt der Bewerber seine Zustimmung zur Weiterleitung seiner Unterlagen nicht, so läuft er Gefahr, vom Bewerbungsverfahren oder zumindest von einem erfolgreichen Bewerbungsverfahren ausgeschlossen zu werden. Die Einwilligungserklärung könnte daher als erzwungen angesehen werden. De facto wäre sie damit ungültig.

Lösungsvorschlag: Eine Weitergabe der Bewerbungsunterlagen an Dritte (Entscheider) könnte anonymisiert erfolgen, d. h., aus den vorliegenden Bewerbungsunterlagen wird eine Art Steckbrief erstellt.

Steckbrief

Beispiel

Ingenieur (FH)

38 Jahre alt

männlich

verheiratet, 2 Kinder

Berufserfahrung von 10 Jahren, vorwiegend im Maschinen- und Anlagenbau in drei Unternehmen der mittelständischen Wirtschaft (Größenordnung 250–500 Mitarbeiter)

betreute Projekte:

- Erstellung von CE-Konformitätserklärungen für Maschinen und verkettete Anlagen
- Risikoanalysen aus technischer Sicht
- Genehmigungsbeantragung für BImSch-Anlage

Führungserfahrung:

- bisher keine, Mitarbeiter in diversen Teams

Zusatzqualifikationen:

- Immissionsschutzbeauftragter
- Fachkraft für Arbeitssicherheit

Hobby:

- Sport

Auf dieser Grundlage kann ein Vergleich verschiedener Bewerber erfolgen, bevor ein enger Kreis von Bewerbern für Einstellungsgespräche ermittelt wird. Für den Bewerberkreis, der in die enge Auswahl gerät, kann dann eine Einwilligungserklärung der Bewerber zur Weiterleitung der Original-Bewerbungsunterlagen eingeholt werden.

Weiter Lösungsmöglichkeit: Information des Bewerbers über die Weiterleitung der Bewerbungsunterlagen mit Bitte um Einwilligung (in schriftlicher Form und aktiv) vor Übermittlung der Daten an andere Stellen.

10.1 Verarbeitung von Beschäftigtendaten

Die Verarbeitung von Beschäftigtendaten bedarf der Einwilligung des Betroffenen, es sei denn, eine Rechtsvorschrift lässt diese ausdrücklich zu.

An dieser Stelle sollen nochmals die Voraussetzungen für eine wirksame Einwilligung dargestellt werden.

Hinweis

Voraussetzungen sind:

- Die Einwilligung beruht auf der freien Entscheidung der Betroffenen.
- Die Schriftform ist einzuhalten. In Formulartexten/Vertragstexten müssen die Textpassagen zur Einwilligung in die Speicherung oder Nutzung personenbezogener Daten optisch hervorgehoben werden, z. B. durch Fettdruck.
- Die Einwilligungserklärung ist getrennt von anderen Erklärungen mit Datum und Unterschrift des Einwilligenden zu zeichnen.
- Anzugeben sind auch die Folgen für eine Verweigerung der Einwilligung, soweit es nach den Umständen des Einzelfalls erforderlich ist.
- Die Einwilligung zur Verwendung besonderer Kategorien personenbezogener Daten muss sich ausdrücklich auf diese beziehen, z. B. Gesundheitsdaten.
- Die Einwilligung muss aktiv erfolgen.
- Aufklärung über Rechte des Betroffenen hinsichtlich Widerruf, Löschung, Berichtigung, Auskünften usw.

Beachten Sie: Pauschalerklärungen für die Weitergabe von personenbezogenen Daten sind stets ungültig.

Beispiel

Sie geben die Einwilligung für die Veröffentlichung Ihres Fotos in der Telefonliste im Intranet. Dies bedeutet nicht, dass Sie die Einwilligung für die Preisgabe Ihres Fotos auch auf der Homepage des Unternehmens oder für sonstige Zwecke gegeben haben.

Angeschlossen wird eine Anweisung für die Verarbeitung personenbezogener Beschäftigtendaten vorgestellt.

Beispiel

Verarbeitung personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses

1 Zweck

Diese Verfahrensanweisung regelt, welche personenbezogenen Daten für Zwecke des Beschäftigungsverhältnisses auf welche Weise und unter welchen Rahmenbedingungen verarbeitet werden dürfen.

2 Anwendungsbereich

Sie gilt für den Bereich Personal/Human Resources.

3 Verfahren

Die Verarbeitung personenbezogener Daten für Beschäftigungszwecke ist zulässig, wenn dies „für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung eines Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte oder Pflichten der Interessenvertretung der Beschäftigten erforderlich ist“. (BDSG § 26)

Sonderfall im Rahmen von Straftaten ist zu beachten:

Eine Verarbeitung ist nur dann rechtlich möglich, wenn

- die Person im Beschäftigungsverhältnis eine Straftat begangen hat und es dafür eindeutige Anhaltspunkte gibt,
- die Verarbeitung zur Aufdeckung der Straftat erforderlich ist,
- das schutzwürdige Interesse des Beschäftigten nicht überwiegt,
- insbesondere Art und Ausmaß der Verarbeitung nicht unverhältnismäßig sind.

Einwilligung

Erfolgt die Verarbeitung personenbezogener Daten im Rahmen des Beschäftigungsverhältnisses auf der Grundlage einer Einwilligung des Betroffenen, so ist dennoch die Frage der Freiwilligkeit dieser Einwilligung zu stellen. Der Wert der Einwilligungserklärung wird vor allem an

- der bestehenden Abhängigkeit der beschäftigten Person,
- den Umständen, unter denen die Einwilligungserklärung erfolgte,
- den Vorteilen, die mit dieser Einwilligungserklärung zu erwarten waren in rechtlicher und wirtschaftlicher Hinsicht

bemessen und kann unter Umständen auch von einem Gericht rechtswirksam angezweifelt werden.

Die Einwilligung bedarf für Beweiszwecke der Schriftform, der Aufnahme oder Ähnlichem.

Informationspflichten

Gegenüber dem Beschäftigten bestehen Informationspflichten, die nachweislich zu erfüllen sind, vgl. dazu **Checkliste Informationspflichten nach Artikel 13 und Artikel 14 EU-DSGVO**.

Den Informationspflichten ist mit Begründung des Arbeitsverhältnisses und ggf. bereits bei der Bewerbung durch die Personalabteilung nachzukommen. Der Leiter Personal übergibt dazu dem Bewerber eine Übersicht über die zu verarbeitenden Daten im Falle der Begründung eines Beschäftigungsverhältnisses.

Bei bestehenden Beschäftigungsverhältnissen wird diese Pflicht bis zum Mai 2018 durch Mitteilung gemeinsam mit der Gehalts- oder Lohnabrechnung erfolgen.

Mit der Erfüllung der Informationspflichten wird der Beschäftigte auch über seine Widerrufsrechte oder Rechte auf Auskunft, Berichtigung, Ergänzung und Löschung aufgeklärt, vgl. **Information über Auskunftsrechte des Betroffenen**.

Rechtmäßige Verarbeitung besonderer Kategorien personenbezogener Daten unabhängig von einer Einwilligung des Betroffenen

Eine rechtmäßige Verarbeitung besonderer Kategorien personenbezogener Daten im Rahmen des Beschäftigungsverhältnisses kann dann erfolgen, wenn sie

- zur Ausübung von Rechten oder
- zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit oder des Sozialschutzes erforderlich sind und
- kein Grund besteht, dass das schutzwürdige Interesse überwiegen könnte.

Das gilt auch für den Fall der Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten, wenn sich die Einwilligung auf diese Daten explizit erstreckt.

Die Verarbeitung ist auf der Grundlage von Kollektivvereinbarungen zulässig.

Treffen geeigneter Schutzmaßnahmen

Es sind geeignete Schutzmaßnahmen in technischer und organisatorischer Hinsicht zu ergreifen, die den Schutz personenbezogener Daten gewährleisten. Dabei sind die Grundsätze der Verarbeitung personenbezogener Daten zu beachten.

Verpflichtung auf das Datengeheimnis

Alle am Prozess der Verarbeitung personenbezogener Daten beteiligten Personen, auch Dienstleister, sind auf den Datenschutz zu verpflichten.

4 Mitgeltende Unterlagen

Checkliste Informationspflichten nach Artikel 13 und Artikel 14 EU-DSGVO
Information über Auskunftsrechte des Betroffenen
Einwilligungserklärung
Verpflichtung auf den Datenschutz
Vertrag mit dem Steuerbüro (Auftragsverarbeitung)

10.2 Erhebung von Daten beim Bewerber

Grundsätzlich dürfen im Bewerbungsverfahren nur die Daten erhoben werden, die für die Einstellung und spätere vertragliche Bindung des Arbeitnehmers auch vonnöten sind. Auch hier gilt das Prinzip der Datensparsamkeit. Der Bewerber ist bereits zu diesem Zeitpunkt von der Verarbeitung seiner überlassenen Bewerberdaten zu informieren (Informationspflicht). Ausgeschlossen von der Erhebung personenbezogener Daten sind beispielsweise

- die Einholung von Referenzen,
- Alkohol- und Drogentests (und nur, soweit es aus sicherheitstechnischen Gründen für die Ausübung der Tätigkeit erforderlich scheint).

Weiterhin sind bestimmte Fragen unzulässig. Beispielsweise darf nach Vorstrafen nur dann gefragt werden, wenn die zu besetzende Stelle eine besondere Vertrauensstellung erfordert. Schwangerschaften dürfen nur dann erfragt werden, wenn ein Einsatz zum Schutz des Kindes nicht möglich wäre, z. B. in der Chemischen Industrie beim Umgang mit Gefahrstoffen.

Personalfragebögen zur Einstellung von Mitarbeitern:

Immer häufiger werden Fragen an Bewerber anhand von elektronischen Fragebögen gestellt. Die Antworten auf diese Fragen werden elektronisch gespeichert.

Zulässig sind nur Fragen aus dem Berufs- und Privatleben, die einen eindeutigen Bezug zur Stelle haben, auf die sich jemand bewirbt.

Unzulässig sind darüber hinaus gehende Fragen, insbesondere Fragen nach dem Sexualleben, der Religion oder politischen Einstellung sowie nach Details aus dem Gesundheitsbereich.

Die Nutzung von Personalfragebögen unterliegt dem Mitbestimmungsrecht der Arbeitnehmervertretung.

Mit der Speicherung der Personalfragebögen müssen besondere Vorkehrungen getroffen werden, um die Persönlichkeitsrechte der Bewerber zu schützen.

Der Bewerber muss darüber informiert werden, wer und wie viele Personen konkret Zugriff auf seine personenbezogenen Daten haben, siehe Informationspflichten gegenüber Beschäftigten. Umso wichtiger gestaltet sich damit die Frage der Zugriffsregelung auf die Daten. Nur ein auf das notwendige Minimum beschränkter Personenkreis darf diese personenbezogenen Daten lesen. Gleiches gilt für den Zugang zu den Räumen oder DV-Anlagen.

Generell gilt, dass nur jene Mitarbeiter Zugriff auf Personalakten oder Bewerbungsunterlagen haben dürfen, die mit dem Personalwesen betraut sind und eine entsprechende Datenschutzerklärung unterzeichnet haben.

Der Personenkreis ist schriftlich festzulegen bzw. über Zugriffsrechte elektronisch zu protokollieren.

Bewerberdaten müssen, soweit keine Einstellung des Mitarbeiters erfolgt, zeitnah gelöscht werden. Eine Vorratsdatenspeicherung darf nicht vorgenommen werden.

Sollen Bewerberdaten für einen späteren Bewerbungszeitpunkt aufbewahrt bzw. gespeichert werden, so bedarf dies der Einwilligung des Bewerbers.

Weithin verbreitet ist die Unsitte, Bewerbungsunterlagen den zuständigen Führungskräften „schutzlos“ zuzuleiten. Nicht selten befinden sich in Papierstapeln bei der Produktionsleitung Bewerbungsunterlagen im Original oder in Kopie. Eine Einsichtnahme Unbefugter ist zumindest nicht auszuschließen. Häufig werden die Bewerbungsunterlagen „auf Vorrat“ aufbewahrt. Klare Regelungen für das Rücksenden der Bewerbungsunterlagen existieren nicht. Kopien sind ggf. noch verteilt.

Hinweis

Besser: Personal- bzw. Bewerberunterlagen werden nur im Personalbüro eingesehen. So notwendig oder sinnvoll, werden Steckbriefe erstellt. Diese können bedenkenlos verteilt werden.

10.3 Führen von Personalakten

Nochmals sei betont, dass alle Mitarbeiter, die mit der Verarbeitung personenbezogener Daten beschäftigt sind, bei Aufnahme ihrer Tätigkeit auf das Datengeheimnis in besonderem Maße zu verpflichten sind. Die Verpflichtung ist schriftlich zu fassen und in der Personalakte zu hinterlegen. Wesentliche Inhalte der Einverständniserklärung wurden bereits andernorts dargestellt und sind in Form zweier Beispiele in der Mediathek abrufbar.

In den Personalakten, zu dem jeder Beschäftigte jederzeit Einsichtsrecht hat, dürfen nur die Daten aufbewahrt werden, die für das Arbeitsverhältnis objektiv erforderlich sind:

- Arbeitszeitdaten für Abrechnungszwecke
- Familienstand und Anzahl der Kinder für die Lohnsteuerberechnung
- Religionszugehörigkeit für die Kirchensteuer
- Krankentage für Fragen der Lohnfortzahlung und des Ersatzes
- Kontaktdaten zur Erreichbarkeit.

Eine Verarbeitung besonderer Kategorien von personenbezogenen Daten ist nur zulässig, wenn dies für die Rechtsposition des Unternehmens erforderlich ist.

Abmahnungen haben einen Zeitwert, der, wenn er abgelaufen ist, zur Vernichtung bzw. Löschung der Daten führt. Diese Lösch- bzw. Vernichtungsfristen sind unbedingt einzuhalten.

10.4 Verpflichtung auf das Datengeheimnis

Mitarbeiter und ggf. Externe sind auf das Datengeheimnis zu verpflichten. Die Notwendigkeit einer nachvollziehbaren Verpflichtung auf das Datengeheimnis ergibt sich u. a. aus § 53 BDSG, selbstverständlich auch aus dem § 47 „Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten“.

§ 53 BDSG

„Mit Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis). Sie sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort.“

Eine Kopie der Verpflichtungserklärung ist den Personalakten hinzuzufügen. Wesentliche Inhalte der Verpflichtung auf das Datengeheimnis sind die in Kapitel 12 aufgeführten Themen bei der Unterweisung zum Datenschutz. Sie sollten um die besonderen bereichsspezifischen Regelungen in Umgang mit personenbezogenen Daten erweitert werden. Mitarbeiter des Einkaufs unterzeichnen damit nicht die gleiche Verpflichtungserklärung wie Mitarbeiter des Personalwesens.

Vorlage

Verpflichtung zur Einhaltung des Datenschutzes
(Einhaltung der Inhalte der EU-Datenschutz-Grundverordnung und des BDSG)

Präambel

Auszug aus dem BDSG

§ 53 BDSG

„Mit Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis). Sie sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort.“

Revision: Änderungsdatum: Seite: 1 von 3

Verpflichtung zur Einhaltung des Datenschutzes

Hiermit bestätige ich, ...

Bereich .....

dass ich heute über die einschlägigen Inhalte der EU-Datenschutz-Grundverordnung (EU-DSGVO) und des BDSG in Kenntnis gesetzt, über die sich daraus ergebenden besonderen Anforderungen an die Datensicherheit und den Datenschutz bei der Ausübung meiner Tätigkeit vertraut gemacht und auf das Datengeheimnis verpflichtet wurde.

Ich wurde insbesondere darüber belehrt, dass es mir gemäß § 47 BDSG untersagt ist, geschützte personenbezogene Daten zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu erheben, zu verarbeiten oder zu nutzen.

Hierunter fallen:

- Sonderfreigaben für die Speicherung von Daten auf flexiblen Medien,
- das Untersagen der Weitergabe von Telefonlisten an Dritte (außer GL, Mitarbeiter Buchhaltung),
- das Versenden von Faxen ohne persönliche Präsenz bzw. das Beauftragen Dritter mit dem Versenden von Faxen mit personenbezogenen Daten,
- das sofortige Entgegennehmen und geschützte Aufbewahren auch von Faxprotokollen, die nachvollziehbare schützenswerte Daten enthalten,
- die Vermeidung der Einsichtnahmen in schützenswerte Daten auf dem Monitor,
- die Einschränkung des Zutritts von Dritten in das jeweilige Büro zur Vermeidung des Ausspionierens personenbezogener Daten,
- das Sperren des PCs bei Verlassen des Raumes,
- die Verweigerung der Herausgabe von Akten, Dokumenten mit personenbezogenen Daten an unbefugte Dritte,
- die Meldung von besonderen Auffälligkeiten und Vorfällen im Zusammenhang mit der Einhaltung des Datenschutzes,
- das Untersagen des Aufspielens von nicht zugelassener Software auf dem PC,
- die Vermeidung der Einsichtnahme unbefugter Kollegen nach dem Scannen in das Scanverzeichnis,
- die Weitergabe von Passwörtern,
- die strikte Untersagung des Weiterleitens von unternehmens- oder personenbezogenen Daten an Dritte per Mail oder auf irgendeinem anderen Wege.

Insbesondere sind die im Rahmen des Datenschutzes erlassenen Verfahrensanweisungen im Managementsystem und die Betriebsanweisungen zum Thema zu beachten.

Diese Pflicht besteht auch nach Beendigung meiner Tätigkeit fort.

Mir ist bekannt, dass Verstöße gegen das Datengeheimnis sowohl arbeits- als auch strafrechtlich verfolgt werden können. Sie können auch Anlass zu einer außerordentlichen Kündigung sein.

Meine sich aus Arbeitsvertrag und -ordnung ergebende Geheimhaltungsverpflichtung wird durch diese Verpflichtung nicht berührt.

Einen Abdruck dieser Verpflichtungserklärung und ein Merkblatt zum Datenschutz habe ich erhalten.

Definition „Dritte“: „Dritte“ sind z. B. alle Mitarbeiter, die nicht in gleichem Maße auf personenbezogene Daten zugreifen dürfen oder Mitarbeiter anderer Tochtergesellschaften, der Muttergesellschaft oder Fremde, Besucher etc.

_____

(Ort, Datum)

_____ _____

(Unterschrift: Verpflichteter) (Unterschrift: Verpflichtender)

_____

Revision: Änderungsdatum: Seite: 3 von 3

[Quelle: in Anlehnung an: Forum-Verlag (2011): Mitarbeiter-Merkblatt Datenschutz April 2011. Forum Verlag Herkert GmbH]

Dabei ist zu beachten, dass eine Einwilligung durch einen abhängig Beschäftigten stets problematisch bleibt. In einem Streitfall vor Gericht bleibt die Frage zu klären, ob ein Arbeitnehmer aus freien Stücken oder aufgrund eventuell ihm entstehender Nachteile seine Einwilligung gegeben hat.

11 Vertragliche Regelungen mit Dienstleistern

In Unternehmen sind in der Regel unterschiedliche Dienstleister tätig (Wartungsfirmen für Kopier- und Drucktechnik, externe IT-Dienstleister, Reinigungsunternehmen u. a. m.), die Zutritt, Zugang und ggf. auch Zugriff auf personenbezogene Daten haben. Auch in den vertraglichen Beziehungen mit diesen Dienstleistern ist der Datenschutz gebührend zu berücksichtigen. In der Folge sind verschiedene Beispiele abgedruckt, die zeigen, wie einzelne Passagen dieser Verträge textlich gestaltet werden könnten. Dabei bleibt jedoch der Einzelfall stets zu berücksichtigen. Die hier abgedruckten Vertragsmuster erheben keinen Anspruch auf Vollständigkeit, da sie nur aus datenschutzmäßiger Sicht an dieser Stelle betrachtet werden.

Nachstehendes Beispiel betrachtet die vertragliche Regelung mit einem Reinigungsdienstleister.

Vorlage

Vereinbarung

Zwischen

_____

_____

– im Folgenden Auftragnehmer genannt –

und

_____

_____

– im Folgenden Auftraggeber genannt –

§ 1 Gegenstand der Vereinbarung

Der Auftragnehmer ist als Dienstleister für die Reinigung des ..... am oben genannten Standort tätig.

§ 2 Pflichten des Auftraggebers

1. Der Auftraggeber versichert, dass der Eignung des Auftragnehmers hinsichtlich der Einhaltung der Vorschriften nach dem Bundesdatenschutzgesetz vor der Auftragsvergabe zunächst nichts entgegensteht.
2. Der Auftraggeber erteilt alle Aufträge oder Teilaufträge in schriftlicher Form.
3. Etwaige Unterauftragsverhältnisse hat der Auftraggeber schriftlich zu genehmigen.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer setzt für die Verarbeitung personenbezogener Daten nur Personal ein, das auf das Datengeheimnis verpflichtet wurde.
2. Der Auftragnehmer verpflichtet sich, die mit der Erfüllung des Leistungsauftrags betrauten Mitarbeiter namentlich anzuzeigen.

   Änderungen in der Personalauswahl sind sofort und vor Aufnahme der Tätigkeiten beim Auftraggeber zu melden.

   Sollten Eintragungen im Führungszeugnis der Arbeitnehmer vorhanden sein, die einen strafrechtlichen Hintergrund für Betrugs-, Einbruchs- und Diebstahlvergehen bilden, muss der Mitarbeiter zurückgewiesen werden.
3. Im Rahmen der Leistungserbringung hat der Auftragnehmer sicherzustellen, dass der freie Zugang zu den Räumlichkeiten des Auftraggebers wirksam verhindert wird (keine offenstehenden Eingangstüren).

4. Räume der Geschäftsleitung, der Buchhaltung und des Bereichs Personal sind unverzüglich nach Reinigung wieder zu verschließen. Grundsätzlich wird nur der Raum aufgeschlossen, der gereinigt werden soll. Das gleichzeitige Aufschließen aller Räume ist nicht zulässig, da diese dann unbeobachtet begangen werden könnten.
5. Grundsätzlich ist keiner fremden Person während der Reinigungszeiten Zutritt zu den Räumlichkeiten des Auftraggebers zu gewähren.
6. Sollten an den Geschäftsführer oder den Objektleiter des Auftragnehmers ausgegebene Schlüssel abhandenkommen, so ist dieser für den Austausch der Schließanlage schadenersatzpflichtig. In jedem Fall ist der Verlust der Schlüssel sofort zu melden.
7. Der Auftragnehmer verpflichtet sich und seine Mitarbeiter, keine der im Rahmen der Leistungserbringung gewonnenen Erkenntnisse zu einzelnen Personen oder der Gesellschaft Dritten zugänglich zu machen und absolutes Stillschweigen zu bewahren. Das Stillschweigen währt auch über das Beschäftigungsverhältnis beim Auftragnehmer fort.
8. Generell ist die Mitnahme von Daten und Akten gleich welcher Art unzulässig und unterliegt der strafrechtlichen Verfolgung.
9. Der Auftragnehmer setzt für die Leistungserbringung nur Personal ein, welches auf das Datengeheimnis schriftlich verpflichtet wurde. Auf Anforderung des Auftraggebers hat der Auftragnehmer diese Verpflichtungserklärung/Belehrung nachzuweisen.
10. Aufträge an Subunternehmer werden nur nach schriftlicher Zustimmung des Auftraggebers vergeben.
11. Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen im Betriebsablauf, Verdacht auf Verletzungen von Datenschutzbestimmungen oder anderen Unregelmäßigkeiten (Art. 32 ff. EU-DSGVO).

§ 4 Schadenersatz

Bei Verstoß gegen die Abmachungen dieses Vertrags, insbesondere gegen die Einhaltung der Maßnahmen zum Datenschutz, macht sich die Gesellschaft in vollem Umfang schadenersatzpflichtig. Die Anwendung weiterer Vorschriften über Bußgeld- und Strafverfahren sowie die Geltendmachung der Rechte Betroffener bleiben davon unberührt.

§ 5 Sonstiges

1. Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung, ein Insolvenz- oder Vergleichsverfahren oder sonstige Ereignisse, gefährdet werden, hat der Auftragnehmer den Auftraggeber unverzüglich und vor Eintritt dieser Maßnahmen zu verständigen, damit die Auftraggeberdaten rechtzeitig von den DV-Systemen des Auftragnehmers genommen werden können.
2. Es besteht bei den Vertragsparteien Einigkeit darüber, dass die „Allgemeinen Geschäftsbedingungen“ des Auftragnehmers auf diesen Vertrag keine Anwendung finden.

§ 6 Gerichtsstand und Schlussbestimmungen

Gerichtsstand ist ...

_____

(Ort, Datum)

_____ _____

Auftragnehmer Auftraggeber

Anlagen:

Leistungsvertrag (nicht abgedruckt)

Auch Fachkräfte für Arbeitssicherheit und Arbeitsmediziner gehören zu den Externen, die Zugang und Zugriff auf personenbezogene Daten haben und folglich in den Verträgen (oder anderen Vereinbarungen) zur Einhaltung des Datenschutzes verpflichtet werden. Dies betrifft vor allem die im Zusammenhang mit Befähigungsnachweisen stehenden Geburtsdaten der Arbeitnehmer, Unfalldaten, Auswertung von Bagatellunfällen und eventuell personenbezogene Daten im Rahmen von Wiedereingliederungen für die Sicherheitsfachkraft. Im nachstehenden Beispiel wird aufgezeigt, wie eine Vereinbarung mit der Sicherheitsfachkraft im Einzelnen aussehen könnte.

Vorlage

Datenschutzvereinbarung

Zwischen

Sicherheitsfachkraft

– im Folgenden Auftragnehmer genannt –

und

Muster GmbH

– im Folgenden Auftraggeber genannt –

§ 1 Gegenstand der Vereinbarung

Der Auftragnehmer ist als … bei der Muster GmbH tätig und hat hierüber Zugang und Zugriff zu personenbezogenen Daten des Auftraggebers.

§ 2 Pflichten des Auftraggebers

1. Der Auftraggeber versichert, dass er personenbezogene Daten gemäß § 47 BDSG „Allgemeine Grundsätze der Verarbeitung personenbezogener Daten“ verarbeitet. Insbesondere achtet er auf die Einhaltung der Grundsätze von Datenminimierung und Datensparsamkeit.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer gewährleistet für die ihm im Rahmen des Auftrags überlassenen bzw. zur Kenntnis gelangten personenbezogenen Daten alle notwendigen technischen und organisatorischen Sicherheitsmaßnahmen. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen oder jenen des Auftraggebers nicht genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
2. Der Auftragnehmer setzt nur Personal ein, das auf das Datengeheimnis nach § 53 BDSG verpflichtet wurde und das über genügend Sachkunde für eine ordnungsgemäße Abwicklung der Aufgaben verfügt. Der Auftragnehmer verwendet die überlassenen Daten nicht für andere Zwecke und bewahrt sie nicht auf.
3. Nicht mehr benötigte personenbezogene Daten werden gemäß geltenden datenschutzrechtlichen Vorschriften vernichtet.
4. Aufträge an Subunternehmer werden nur nach schriftlicher Zustimmung des Auftraggebers vergeben, da hiermit eine unkontrollierte Weitergabe personenbezogener Daten verbunden sein könnte.
5. Der Auftragnehmer gewährleistet eine Protokollierung aller Systemleistungen, insbesondere wenn Dritte auf seine DV-Systeme zugreifen mussten.
6. Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen im Betriebsablauf, Verdacht auf Verletzungen von Datenschutzbestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers.

7. Bei Störungen im Betriebsablauf, etwa bei Hard- und Softwareaustausch, sorgt der Auftragnehmer dafür, dass keine personenbezogenen Daten an Dritte weitergegeben werden bzw. dass die Datenträger vor der Weitergabe zuverlässig gelöscht wurden.

§ 4 Schadenersatz

Bei Verstoß gegen die Abmachungen dieses Vertrags, insbesondere gegen die Einhaltung der Maßnahmen zum Datenschutz, macht sich die Gesellschaft in vollem Umfang schadenersatzpflichtig. Die Anwendung weiterer Vorschriften über Bußgeld- und Strafverfahren sowie die Geltendmachung der Rechte Betroffener bleiben davon unberührt.

§ 5 Sonstiges

Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung, ein Insolvenz- oder Vergleichsverfahren oder sonstige Ereignisse, gefährdet werden, hat der Auftragnehmer den Auftraggeber unverzüglich und vor Eintritt dieser Maßnahmen zu verständigen, damit die Auftraggeberdaten rechtzeitig von den DV-Systemen des Auftragnehmers genommen werden können.

§ 6 Gerichtsstand und Schlussbestimmungen

Gerichtsstand ist ...

_____

Ort, Datum

_____ _____

Auftragnehmer Auftraggeber

Anlagen:

Leistungsvertrag

12 Schulungen und Unterweisungen im Datenschutz

12.1 Schulungen

Mitarbeiter sind sich des Umgangs mit personenbezogenen Daten häufig nicht bewusst. Durch Unterweisungen und Schulungen ist sicherzustellen, dass Mitarbeiter über Folgendes informiert sind:

- den Zweck des Bundesdatenschutzgesetzes
- die Definition von personenbezogenen Daten
- die Bedeutung des Datengeheimnisses
- besondere Arten von personenbezogenen Daten
- die Bedeutung der Vorabkontrolle
- die Definition des Umgangs mit personenbezogenen Daten (Erhebung, Verarbeitung, Nutzung)
- die Grundsätze von Datenvermeidung, -sparsamkeit, -anonymisierung und Pseudonymisierung
- Auskunftsrechte
- Maßnahmen zur Datensicherheit
- Besonderheiten im Datenschutzrecht
- die Abgrenzung von Funktionsübertragung und Auftragsverarbeitung
- Straf- und Bußgeldvorschriften gemäß §§ 43 und 44 BDSG.

Aus dieser Aufstellung der Forderungen an eine gute Unterweisung im Datenschutz ergibt sich gleichzeitig deren Gliederung. Ein praxisorientiertes und bewährtes „Merkblatt zur Verpflichtung auf das Datengeheimnis nach § 5 Bundesdatenschutzgesetz“ wurde durch den Forum Verlag herausgegeben.

Neben der mündlich stattfindenden Unterweisung zu o. g. Themen im Datenschutz wird das Merkblatt jedem Mitarbeiter zur Verfügung gestellt. Ein Exemplar des Merkblatts wird vom Mitarbeiter unterzeichnet und in der Personalakte aufbewahrt. Das Merkblatt ist gemäß rechtlichen Änderungen zu aktualisieren. Ein Überwachungsrhythmus im Abstand von einem Jahr hat sich dabei in der Praxis bewährt. Im Rahmen der Unterweisung haben sich neben der Verwendung des Merkblatts auch Präsentationen durchgesetzt, die an den Mitarbeiter entweder ausgegeben werden oder über Intranet abrufbar sind.

Auch in diesem Fall soll auf die Überwachungs- und Aktualisierungspflicht hingewiesen werden.

12.2 Unterweisungen

Unterweisungspflichten entstehen

- bei der Ersteinweisung von Mitarbeitern, die mit personenbezogenen Daten umgehen,
- bei der Einstellung von Aushilfen, Zivilarbeitskräften, Auszubildenden, Praktikanten,
- so nicht anders geregelt auch für Fremdfirmen (z. B. Dienstleister für Reinigung, Wartung von IT-Komponenten und Druck- und Kopiertechnik) und Besucher.

Zur Sensibilisierung von Mitarbeitern und zur Aufrechterhaltung des betrieblichen Datenschutzes im Unternehmen empfehlen sich regelmäßige Schulungen, i. d. R. auf jährlicher Basis. Im Fokus dieser Schulungen sollen neben der Wiederholung der grundlegenden Unterweisungsthemen vor allem aktuelle Änderungen im Bundesdatenschutzgesetz und in anderen rechtlichen Rahmenbedingungen für den Datenschutz sowie in Rechtsprechungen, Veröffentlichungen in den Medien und aktuelle Themen stehen. Best-practice-Beispiele zeigen, dass die Beschäftigung mit dem Datenschutz keineswegs ein trockenes Thema sein muss. Mit etwas didaktisch-

methodischem Geschick lassen sich Schulungen für den Datenschutz recht abwechslungsreich und interessant gestalten. Neben der allseits bekannten Power-Point-Präsentation zur Vermittlung von neuen Kenntnissen können Auszüge aus Gerichtsurteilen zur Diskussion stehen und Fallbeispiele aus der gelebten Praxis in Gruppenarbeit untersucht, bewertet und mit Lösungen versehen werden. Dazu empfiehlt sich die Bildung von Kleinstgruppen (2–3 Mitarbeiter), die an je einem Fallbeispiel arbeiten.

Hinweis

Je größer hier die Gruppe gewählt wird, desto weniger sind alle Beteiligten in die Arbeit einbezogen, was den Identifikationsgrad schmälert. Generell sollen nicht mehr als 20 Mitarbeiter an einer Schulung teilnehmen, um Fragen und Diskussionen von vornherein nicht zu begrenzen.

Die Teilnehmer müssen zunächst herausfinden, ob die Handhabung der am Fallbeispiel beteiligten Personen korrekt ist oder nicht. Dazu lesen sie in der EU-DSGVO und im BDSG die entsprechenden Passagen und evaluieren die Situation. Sie entscheiden dann, welche Maßnahmen aus ihrer Sicht getroffen werden müssen, um die Konformität mit den Rechtsforderungen herauszustellen. In der Regel entwickelt sich mit dieser Vorgehensweise ein reger Austausch unter den Gruppenmitgliedern. Letztlich müssen die Teilnehmer ihr erworbenes Wissen anwenden und betriebliche Regelungen an der Stelle schaffen, wo sich organisatorische Lücken im Datenschutz gebildet haben. In der Mediathek werden exemplarisch Fallbeispiele zum Download bereitgestellt.

Diese Fallbeispiele folgen nachstehendem Muster:

Der Fall:

Im Unternehmen werden arbeitsmedizinische Untersuchungen durchgeführt. Die Arbeitsmedizinerin schickt die Ergebnisse der Blutbleiuntersuchungen (notwendig für Beschäftigte einer Zinkhütte) dem Geschäftsführer per E-Mail über das Sekretariat zu. In der Leitungsbesprechung werden die Blutbleiuntersuchungen mitarbeiterbezogen ausgewertet. Konkrete personenbezogene Präventionsmaßnahmen werden abgeleitet, um die Situation zu verbessern.

Welche Fragen leiten Sie aus der Schilderung des Sachverhalts ab?

Beispiele:

Gibt es eine Betriebsvereinbarung für die Durchführung besonderer arbeitsmedizinischer Untersuchungen unter Veröffentlichung der mitarbeiterbezogenen Testergebnisse an den Geschäftsführer bzw. einen definierten Personenkreis?

Wurde diese Vereinbarung eingehalten?

Weshalb wird die Übermittlung dieser sensiblen Daten öffentlich per E-Mail durchgeführt?

Weshalb ist die Sekretärin (und ggf. weitere Mitarbeiter) im Empfängerkreis?

Weshalb ist die Auswertung der Untersuchungsergebnisse mitarbeiterbezogen und nicht team- oder gruppenbezogen und damit anonym möglich?

Weshalb muss der Adressatenkreis die gesamte Leitungsebene umfassen, wenn z. B. Leiter Entwicklung, Leiter Einkauf, Leiter Vertrieb mit den Blutbleiwerten der Mitarbeiter Produktion nichts zu tun haben?

Welche Wertung des Sachverhalts nehmen Sie vor?

- Notwendigkeit des Vorliegens einer Einwilligungserklärung
- keine Bekanntgabe der Daten an Empfängerkreis, der nicht absolut zur Ergreifung von Präventionsmaßnahmen unabdingbar notwendig ist – Festlegung des Adressatenkreises
- anonymisierte Auswertung der Daten
- keine ungeschützte Übermittlung besonderer Kategorien personenbezogener Daten.

Wie könnte der Sachverhalt datenschutzrechtlich korrekt bzw. besser abgewickelt werden?

- Betriebsvereinbarung abschließen unter Benennung des konkreten Adressatenkreises, der die personenbezogenen Testergebnisse unverfälscht erhalten soll und darf (Geschäftsführer, Sicherheitsfachkraft, eventuell Produktionsleiter)
- Bericht über die Ergebnisse der Untersuchungen nur team- oder gruppenbezogen
- Übersendung der sensiblen medizinischen Daten per Post „persönlich/vertraulich“ an den Geschäftsführer.

12.3 Schulungsplanung

Schulungen müssen geplant werden. Nicht immer ist es möglich, alle Mitarbeiter gleichzeitig zu schulen. Weiterhin sollte der unterschiedliche Grad im Umgang mit personenbezogenen Daten bei der Schulungsplanung berücksichtigt werden. In der Praxis durchgesetzt haben sich abteilungs- oder bereichsbezogene Schulungen, in denen Mitarbeiter mit nahezu gleichem Umgang mit personenbezogenen Daten teilnehmen. Möglich ist daher auch die Zusammenlegung von Abteilungen oder Bereichen. Vorstellbar wäre hierzu folgender Schulungsplan:

Vorlage

Schulungsplan für Datenschutzschulungen

Abteilung/Bereich	Schulung zum Schwerpunkt:	Termin		Veranstalter
		Soll	Ist	
Personal/ Sekretariat/ Geschäftsleitung	Bewerbungsverfahren/ Personalverwaltung/Zeiterfassung/Informationspflichten gegenüber Arbeitnehmern	März 20..		DSB
Vertrieb	Umgang mit kundenbezogenen Daten, Informationspflichten, Geheimhaltung	April 20..		Muster GmbH
Einkauf	Umgang mit lieferantenbezogenen Daten, Informationspflichten Geheimhaltung	Mai 20..		Muster GmbH

Stand: 1.01.20..

Revision: Änderungsdatum: Seite: 1 von 1

Neben den gesamten Schwerpunktthemen sind die betrieblichen Regelungen zu wiederholen. Fallbeispiele können auch andere Themen zur praktischen Übung betreffen.

Als Schulungsnachweis ist eine reine Unterschriftenliste aus Sicht der Autorin nicht empfehlenswert. Neben dem Ort, Datum, den Teilnehmern, dem Referenten sollten die Inhalte der Schulung so konkret wie möglich benannt werden. In der Praxis wird häufig die Teilnehmerliste mit den konkreten Schulungsunterlagen zusammengeklammert, oder es wird auf eine konkrete Präsentation (Ausgabedatum nicht vergessen!) verwiesen. Im Fall eines Rechtsstreits kann der Datenschutzbeauftragte in eine Nachweispflicht hinsichtlich vermittelter Inhalte in der Datenschutzschulung gelangen.

Unternehmen, die ein Qualitäts- oder anderes Managementsystem verwalten, sollten die Schulungen für den Datenschutz in den Gesamtschulungsplan integrieren.

13 Datenschutzkonzept und Datenschutzhandbuch

13.1 Datenschutzhandbuch

In der Praxis haben sich die Strukturierung und Zusammenfassung aller erarbeiteten Vorlagen und eventuell auch Nachweise für Schulungen, Datenschutzerklärungen, Verfahrensverzeichnisse, Jahresberichte u. a. m. in einem Datenschutzhandbuch bewährt. Das Handbuch soll der systematischen Ablage der Dokumente und Aufzeichnungen dienen und vom Datenschutzbeauftragten „gehalten", d. h. verwaltet, werden. Die Gliederung des Datenschutzhandbuchs ergibt sich aus den unternehmensbezogenen Anforderungen an den betrieblichen Datenschutz. Daher kann kein allgemeingültiges Inhaltsverzeichnis an dieser Stelle wiedergegeben werden. Wesentliche Inhalte stellen jedoch

- Datenschutzgrundsätze, -politik
- Bestellurkunde Datenschutzbeauftragter, Aufgabenbeschreibung
- diverse (inhaltlich differierende) Datenschutzerklärungen für unterschiedliche Personengruppen
- Verzeichnisse für die Verarbeitung personenbezogener Daten
- Auditberichte von Datenschutzaudits und To-do-Listen
- Verträge mit Dienstleistern zum Thema Datenschutz
- Datenschutzanweisungen
- Vorlage für die Durchführung der Datenschutz-Folgeabschätzung
- Formblätter für das Beschwerdemanagement
- Checklisten zur Überprüfung des Datenschutzes in der Praxis
- Aufzeichnungen/Vorlagen zur Erfüllung der Informationspflichten
- Schulungsunterlagen, Präsentationen zum Datenschutz u. a. m.

dar.

Das Datenschutzhandbuch umfasst damit alle Nachweisdokumente gegenüber der Datenschutzbehörde.

Am Anfang des Datenschutzhandbuchs sollten ein Organigramm und eine kurze Beschreibung des Unternehmens stehen, um nachvollziehen zu können, mit welchen Kategorien personenbezogener Daten das Unternehmen umgeht. Das Datenschutzhandbuch sollte bei jeder Änderung der dort eingestellten Unterlagen überarbeitet werden, mindestens jedoch einmal jährlich. Erfahrungsgemäß werden mit diesem gewählten Zeitraum auch sich ändernde rechtliche Grundlagen zeitnah einbezogen.

Die Aktualisierung obliegt in der Praxis in der Regel dem Datenschutzbeauftragten.

Neben dieser Vorgehensweise hat sich auch die Einbindung in ein Qualitäts- oder integriertes Managementsystem bewährt. In den meisten Fällen werden die Anweisungen zum Datenschutz als Verfahrensanweisungen gefasst, die Formblätter und Checklisten als MGU (Mitgeltende Unterlagen) aufgenommen. Der Vorteil ist, dass die genannten Dokumente damit automatisch bzw. systematisch einer jährlichen Revision unterzogen werden.

13.2 Schritte zum Aufbau eines betrieblichen Datenschutzkonzepts – eine Zusammenfassung

Merke

1. Durchführung einer Ist-Aufnahme anhand der Anforderungen der EU-Datenschutz-Grundverordnung und des BDSG 2018, u. a. in der Form eines Datenschutzaudits möglich
2. Aufstellung eines Maßnahmenkonzepts mit daraus resultierendem Jahresarbeitsplan des DSB
3. Installation von Datenschutzrunden mit den Führungskräften
4. Information und Unterweisung der Mitarbeiter, Erstellung von Verpflichtungserklärungen
5. Umsetzung der Informationspflichten gegenüber Mitarbeitern im Bereich Personal
6. Umsetzung der Informationspflichten gegenüber Kunden und Lieferanten
7. Analyse der Datenkategorien, der Kategorien der Verarbeitung und der Schutzstufen
8. Eruieren, inwiefern Datenschutz-Folgeabschätzungen notwendig sind bzw. deren Erarbeitung
9. Planung, Durchführung und Protokollierung von Prüfungen (z. B. in Form bereichs-, themenspezifischer Datenschutzaudits) zur
   - Einhaltung von datenschutzrechtlichen Vorschriften
   - rechtskonformen Anwendung von IT-Systemen
10. Erarbeitung betrieblicher Regelungen, Aufstellung einer Datenschutzkonzeption (z. B. in Form eines Datenschutzhandbuchs), Realisierung des technischen und organisatorischen Schutzkonzepts
11. Verifizierung betrieblicher Regelungen im Geschäftsalltag (z. B. über Datenschutzaudits)
12. Erstellen der Verzeichnisse der Verarbeitung personenbezogener Daten
13. Validierung des Datenschutzkonzepts und Ableitung Folgemaßnahmen
14. Erarbeitung des Jahresberichts zur Darstellung der Tätigkeit als betrieblicher Datenschutzbeauftragter.

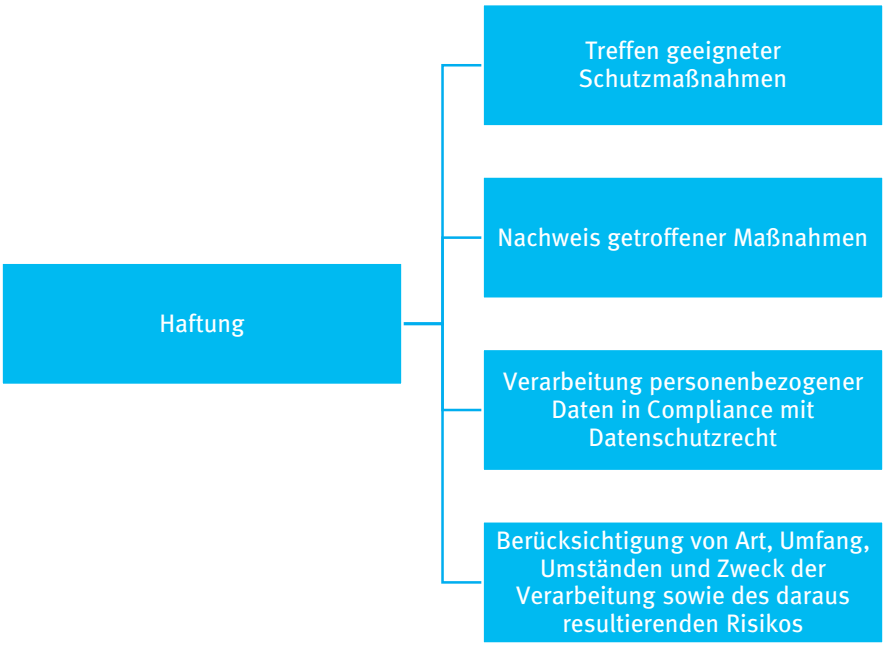
14 Liste der Mindestregelungen im betrieblichen Datenschutz

Merke

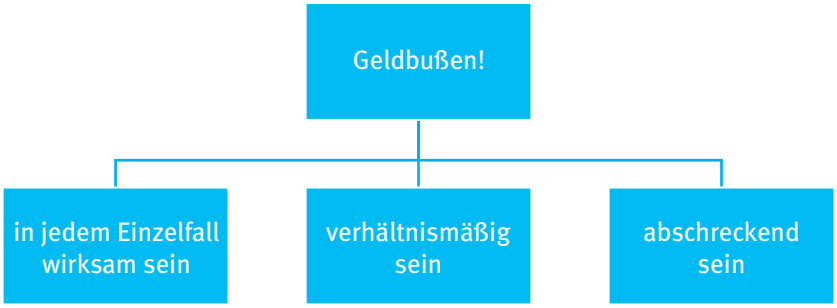
- Betriebsvereinbarung zur privaten Nutzung von Telekommunikationseinrichtungen und -systemen
- Betriebsvereinbarung zur Kontrolle privater IT im Unternehmen
- Betriebsvereinbarung über den Einsatz eines maschinellen Zutrittskontrollsystems
- Betriebsvereinbarung über den Einsatz und die Nutzung von Videosystemen
- Betriebsvereinbarung zur Telefondatenerfassung
- Betriebsvereinbarung zur E-Mail- und Internetnutzung
- Regelung zur Nutzung von multifunktionalen Endgeräten
- Regelung zur Daten- und Datenträgervernichtung
- Regelung zur Nutzung von USB-Sticks
- Regelungen zum sicheren Telefax-Betrieb
- Regelung zur Bearbeitung externer Anfragen
- Regelung zur Nutzung betrieblicher Laptops
- Anweisung zum datenschutzgerechten Versand von Datenträgern
- Anweisung zum Passwortverfahren
- Anweisung zur Umsetzung der Datenschutz-Folgeabschätzung
- Anweisung zur Pseudonymisierung personenbezogener Daten
- Anweisung zur Übermittlung von personenbezogenen Daten an Drittländer und internationale Organisationen
- so nicht anders geregelt: Verfahren zum internen Beschwerdemanagement
- so nicht anders geregelt: Verfahren zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die betreffende Behörde
- so nicht anders geregelt: Aufklärung über die Rechte des Betroffenen
- so nicht anders geregelt: Anforderungen an die Verarbeitung personenbezogener Daten
- so nicht anders geregelt: Benachrichtigung betroffener Personen über die Verarbeitung
- so nicht anders geregelt: Einschränkung der Verarbeitung personenbezogener Daten
- so nicht anders geregelt: Informationspflichten gegenüber Kunden und Lieferanten über die Verarbeitung personenbezogener Daten.

15 Sanktionen

Der Verantwortliche der Verarbeitung übernimmt Haftungsrisiken (EG 74 EU-DSGVO) für die Erfüllung der datenschutzrechtlichen Anforderungen gemäß EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz. Grundsätzlich hat der Verantwortliche für die Verarbeitung personenbezogener Daten folgende Pflichten zu erfüllen:

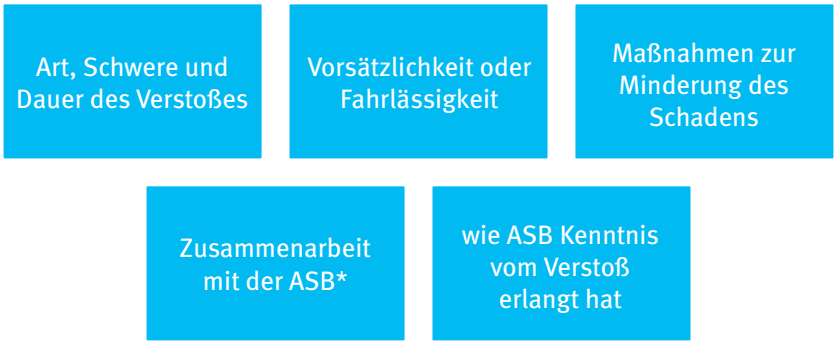


Die Sanktionen im Datenschutz haben sich deutlich erhöht und sind umfassender geworden. Gemäß EU-Datenschutz-Grundverordnung (Art. 83 Abs. 1) sollen sie



Artikel 83 EU-Datenschutz-Grundverordnung sieht Geldbußen zusätzlich oder anstelle von Sanktionen vor.

Sie richten sich nach:

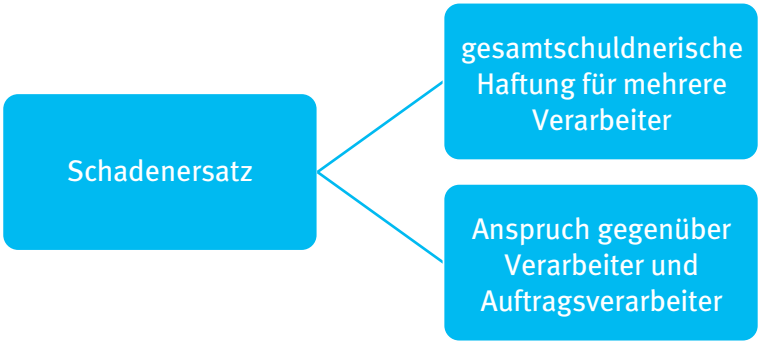


* ASB = aufsichtführende Behörde

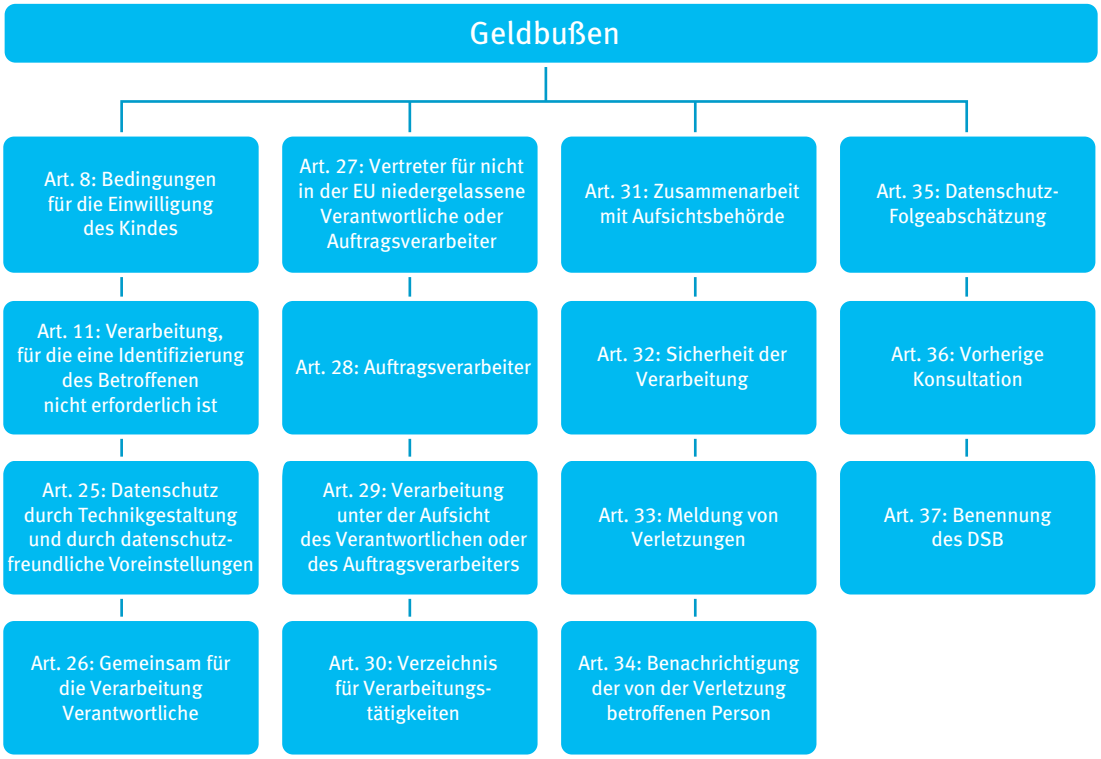
Gemäß Art. 82 EU-DSGVO ergibt sich ein Schadenersatz für materiellen und immateriellen Schaden.

Der Schadenersatz kann abgewendet werden, wenn den Verantwortlichen oder den Auftragsverarbeiter keine Schuld trifft. Den Nachweis der Unschuld muss der Verantwortliche bzw. Auftragsverarbeiter erbringen.

Die Haftung gilt:



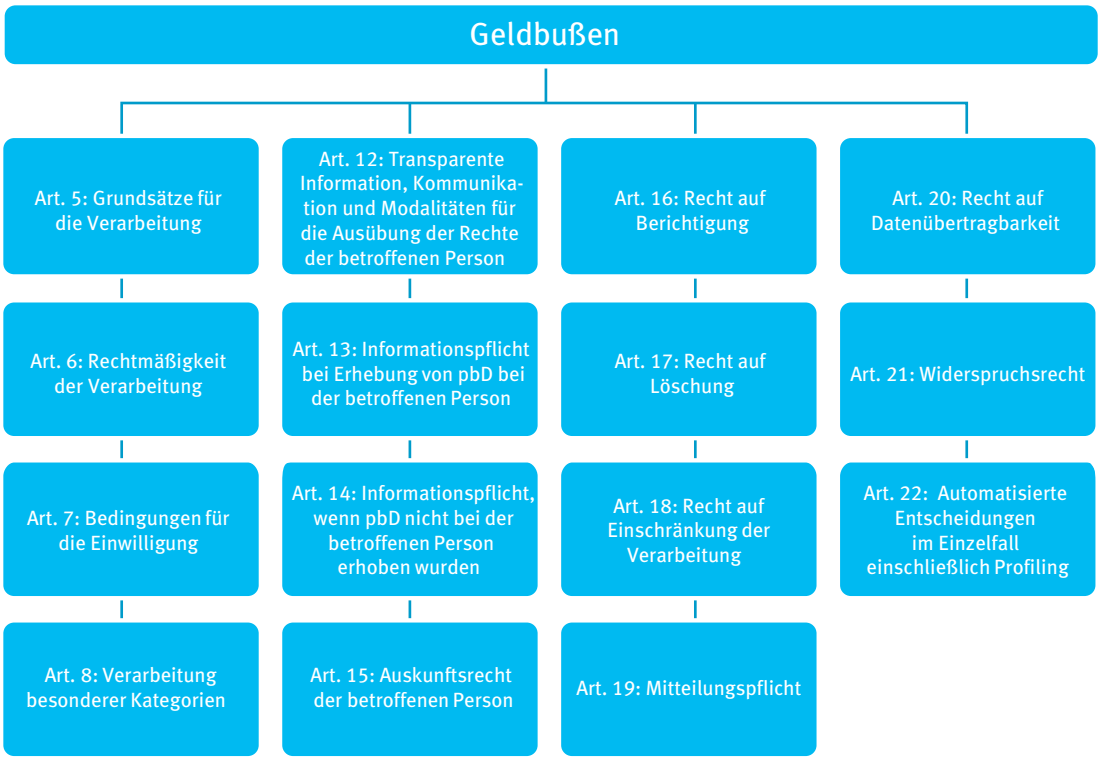
Mit Geldbußen bis zu 10 Mio. € oder 2 % des globalen Umsatzes des Vorjahres werden folgende Verstöße bestraft:



Sanktionen und Geldbußen werden auch verhängt wegen

- Art. 38 Stellung des Datenschutzbeauftragten und
- Art. 39 Aufgaben des Datenschutzbeauftragten.

Geldbußen bis 20 Mio. € werden verhängt bei Verstößen gegen:



Weitere Sanktionen werden verhängt wegen der Datenübermittlung, vgl. Art. 44–49 und Art. 85–88.

Anhang mit ergänzenden Vorlagen

Anhang 1

Checkliste Informationspflichten nach Artikel 13 und Artikel 14

Vorlage

	Information	Art. 13	Art. 14
☐	Mitteilung zum Zeitpunkt der Erhebung	✓	
☐	Kontaktdaten des für die Verarbeitung Verantwortlichen, sowie Vertreter	✓	✓
☐	Falls vorhanden: Kontaktdaten Datenschutzbeauftragter	✓	✓
☐	Zwecke	✓	✓
☐	Rechtsgrundlage der Verarbeitung	✓	✓
☐	Falls Art. 6 Abs. 1f: Nennung der berechtigten Interessen, die verfolgt werden	✓	✓
☐	Kategorien der personenbezogenen Daten, die verarbeitet werden		✓
☐	Ggf. Empfänger oder Kategorien von Empfängern	✓	✓
☐	Ggf. Drittländer oder internationale Organisationen, an die Daten übermittelt werden, dazu:	✓	✓
☐	Ggf. das Fehlen oder Vorhandensein eines Angemessenheitsbeschlusses der Kommission	✓	✓
☐	Ggf. Hinweis auf geeignete Garantien (z. B. Standardklauseln, genehmigte Verhaltensregeln, genehmigte Zertifizierungen, BCRs) und wo diese verfügbar sind	✓	✓
☐	Speicherdauer der Daten oder die Kriterien für die Festlegung der Dauer	✓	✓
☐	Hinweise auf die Rechte auf *Auskunft (Art. 15), Berichtigung (Art. 16), Löschung (Art. 17), Einschränkung der Verarbeitung (Art. 18), eines Widerspruchsrechts (Art. 21) sowie des Rechts auf Datenübertragbarkeit (Art. 20)*	✓	✓
☐	Bei Verarbeitung aufgrund einer Einwilligung: das Recht, die Einwilligung mit Wirkung auf die Zukunft zu widerrufen	✓	✓
☐	Hinweis, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist	✓	
☐	Hinweis, ob die Bereitstellung der personenbezogenen Daten für einen Vertragsabschluss erforderlich ist	✓	
☐	Hinweis, ob das betroffene Personal verpflichtet ist, die Daten bereitzustellen	✓	
☐	Hinweis, welche Folgen die Nichtbereitstellung hätte	✓	
☐	Hinweis auf das Beschwerderecht bei der Aufsichtsbehörde	✓	✓
☐	Hinweis, aus welcher Quelle die Daten stammen und ob sie aus öffentlich zugänglichen Quellen stammen	✓	✓
☐	Bei automatisierten Einzelentscheidungen: aussagekräftige Informationen über die Logik	✓	✓

Revision: Änderungsdatum: Seite: 1 von 2

	Information	Art. 13	Art. 14
☐	Bei automatisierten Einzelentscheidungen: Tragweite und Auswirkungen der Verarbeitung für die betroffene Person	✓	✓
☐	Bei geplanter Zweckänderung: neuen Zweck und alle vorher genannten Informationen angeben	✓	✓
☐	Ein-Monats-Frist einhalten		✓

[Quelle: Karsten Schulz. TÜV-Nord Akademie]

Revision: Änderungsdatum: Seite: 2 von 2

Anhang 2

Vorlage

Auskunftsrechte des Betroffenen über die Verarbeitung personenbezogener Daten (Aushang)

Sehr geehrte Mitarbeiter und Mitarbeiterinnen,

der Schutz Ihrer personenbezogenen Daten ist für uns Anliegen und eine rechtliche Verpflichtung zugleich. Wir informieren Sie hiermit als Betroffene über Ihre Auskunftsrechte sowie ihre Rechte auf Berichtigung, Ergänzung und Löschung personenbezogener Daten. Ihre Rechte sind in der EU-Datenschutz-Grundverordnung insbesondere in den Artikeln 15, 16 18, den Erwägungsgründen 59, 63, 64, 65, 66 und 67 und darüber hinaus im Bundesdatenschutzgesetz 2018 §§ 34, 57, 58 geregelt.

Auskunftsrechte Ihrerseits bestehen für Sie hinsichtlich:

- des Verarbeitungszwecks personenbezogener Daten
- der Kategorien der verarbeiteten Daten
- der Empfänger der personenbezogenen Daten
- der geplanten Dauer der Speicherung
- Ihres Rechts auf Berichtigung oder Löschung
- Ihres Rechts auf Einschränkung der Verarbeitung
- des Widerspruchsrechts
- des Beschwerderechts bei der Aufsichtsbehörde
- verfügbarer Informationen über die Herkunft der Daten, die nicht direkt bei Ihnen (dem Betroffenen) erhoben werden
- des Bestehens einer automatisierten Entscheidungsfindung einschließlich Profiling (Information über Logik, Tragweite der angestrebten Auswirkungen für Sie als betroffene Person).

Im Fall der Übermittlung in ein Drittland ist es Ihr Recht, den Nachweis der geeigneten Garantien nach Artikel 46 für die ordnungsgemäße Verarbeitung Ihrer personenbezogenen Daten einzufordern.

Sollte es sich um größere Mengen unterschiedlicher personenbezogener Daten oder Verarbeitungsstellen handeln, möchten wir Sie bitten, Ihr Auskunftsersuchen dahingehend zu präzisieren, über welche personenbezogenen Daten bei welcher Verarbeitung Sie Auskunft erhalten wollen.

Revision: Änderungsdatum: Seite: 1 von 2

Sie haben das Recht auf **Erhalt einer Kopie der verarbeiteten personenbezogenen Daten**.

Vor Auskunftserteilung ist es uns vom Gesetzgeber erlaubt, Ihre Identität in geeigneter Art und Weise festzustellen bzw. zu prüfen, um Informationen an Unbefugte im Sinne des Datenschutzes zu vermeiden.

Von diesem **Auskunftsrecht** können Sie **jederzeit wieder** Gebrauch machen, es besteht also nicht einmalig.

Weiterhin obliegt Ihnen das Recht auf **Widerspruch** gegen die Verarbeitung unrichtiger, unvollständiger oder vermeidbarer personenbezogener Daten. Sie haben in diesen Fällen das **Recht auf Berichtigung, Ergänzung und Löschung personenbezogener Daten**. Dies kann einerseits zu einer **Einschränkung der Verarbeitung oder auch zur Berichtigung oder Löschung der personenbezogenen Daten** führen, soweit rechtliche Belange dem nicht entgegenstehen.

Anträge auf Auskunft können Sie formlos an die Datenschutzbeauftragte stellen:

per Mail an: _____ _____

oder telefonisch an: _____ _____

Kontaktadresse: _____

_____

_____

Ort, Datum: _____ _____ Bad Harzburg, 20.01.2018

Ihre Datenschutzbeauftragte

Revision: Änderungsdatum: Seite: 2 von 2

Anhang 3

Interne Datenschutzgrundsätze im Unternehmen

Vorlage

- Datenschutz genießt im Unternehmen höchste Priorität. Alle personenbezogenen und anderen vertraulichen Daten und Informationen sind in den Schutzbereich einbezogen.
- Schutzwürdige Daten dürfen nur in dem Umfang erhoben, verarbeitet, genutzt oder anderen Mitarbeitern, Aushilfen und Auszubildenden zur Verfügung gestellt werden, wie es unter Beachtung datenschutzrechtlicher Zulässigkeitsvoraussetzungen für eine bestimmte, rechtmäßige Aufgabenerfüllung erforderlich ist.
- Nicht mehr benötigte Daten sind wirksam und endgültig zu löschen. Daten, die einer gesetzlich vorgeschriebenen Aufbewahrungspflicht unterliegen, sind gegen eine weitere Nutzung zu sperren.
- Die Verarbeitung und sonstige Nutzung – dazu zählen auch Auskünfte personenbezogener Daten – ist auf Grund von Rechtsvorschriften, Vertragsbeziehungen bzw. beabsichtigter Vertragsbeziehungen, mit schriftlicher Einwilligung des Betroffenen oder im berechtigten Geschäftsinteresse zulässig, wenn kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.
- Jeder Mitarbeiter, der Umgang mit personenbezogenen Daten hat, ist durch den Datenschutzbeauftragten über die Datenschutzvorschriften zu belehren und schriftlich auf seine Verpflichtung hinzuweisen.

Revision: Änderungsdatum: Seite: 1 von 2

Er hat die ihm anvertrauten, schutzwürdigen Informationen und Materialien zur Wahrung des Datengeheimnisses ausschließlich im Rahmen ihrer Zweckbestimmung zu verwenden und gegen unberechtigte Zugriffe und unbefugte Einsichtnahme zu sichern. Die Straftatbestände richten sich nach Art. 83 und 84 EU-DSGVO.

- In sicherheitskritischen Bereichen (Personal-, Lohn- und Gehaltsabrechnungsbereiche) dürfen ohne ausreichende Kontrollmöglichkeiten keine neu eingestellten Mitarbeiter, Aushilfen, Praktikanten oder Mitarbeiter von Fremdfirmen eingesetzt werden.

  Dieser Personenkreis ist ebenfalls auf das Datengeheimnis zu verpflichten.
- Jeder Betroffene hat einen unabdingbaren gesetzlich fixierten Anspruch auf Auskunft sowie ggf. auf Berichtigung, Sperrung und Löschung der zu seiner Person gespeicherten Daten. Sofern er keine Kenntnis von der Verarbeitung seiner Daten hat, ist er bei der erstmaligen Speicherung zu benachrichtigen.
- Um den Benachrichtigungs- und Auskunftsansprüchen sowie den Kontrollerfordernissen gerecht werden zu können, ist jede DV-Anwendung mit personenbezogenen Daten dem Datenschutzbeauftragten zu melden. Seine Einbeziehung bei der Einführung neuer DV-Anwendungen mit personenbezogenen Daten hat bei Projektbeginn zu erfolgen, so dass Rechtmäßigkeit und Zulässigkeit der Datenverarbeitung garantiert werden können.
- Daten und Programme müssen entsprechend ihrer Schutzbedürftigkeit in angemessener Weise vor unberechtigter Einsichtnahme, unbefugter Manipulation, Diebstahl, Sabotage, unbeabsichtigtem Datenverlust sowie Störungen jeglicher Art abgesichert werden. Detaillierte Regelungen werden in Betriebsvereinbarungen und Anweisungen zum Datenschutz getroffen.
- Die Verantwortung für die Einhaltung der gesetzlichen und internen Datenschutzvorschriften liegt bei den Geschäftsführern. Zur Umsetzung der datenschutzrelevanten Forderungen wurde ein Datenschutzbeauftragter bestellt. Dieser besitzt gegenüber dem Geschäftsführer ein direktes Vortrags-, Empfehlungs- und Beratungsrecht. In der Anwendung seiner Fachkunde ist er weisungsfrei.
- Den Bereichen, die personenbezogene Daten verarbeiten, gibt der Datenschutzbeauftragte entsprechende fachliche Anleitung und Unterstützung. Er belehrt die Mitarbeiter über den Inhalt dieser und weiterer einschlägiger Datenschutzvorschriften und hat deren Einhaltung durch Kontrolle und andere Maßnahmen sicherzustellen.
- Bei Verletzung von Datenschutzbestimmungen, festgestellten oder vermeintlichen Mängeln im Datensicherungssystem sowie über andere datenschutzrelevante Vorkommnisse ist der Datenschutzbeauftragte zu informieren.
- Datenschutzbeauftragte:

Ort, _____

Datum: _____

_____	_____	_____
Geschäftsführer	Betriebsrat	Datenschutzbeauftragter

Revision: Änderungsdatum: Seite: 2 von 2

Anhang 4

Merkblatt Datenminimierung

Vorlage

Stets ist zu prüfen, ob personenbezogene Daten überhaupt erhoben werden müssen und wenn ja, ob der Umfang zu beschränken wäre.

Dazu sollten Sie sich als Verarbeiter der personenbezogenen Daten folgende Fragen stellen:

1. Geht es auch ohne personenbezogene Daten?
   Beispiel: eine anonyme rein statistische Zusammenstellung von Daten
2. Welche personenbezogenen Daten sind absolut notwendig, welche sind (zunächst) verzichtbar, da ich sie nur in Ausnahmefällen überhaupt brauche?
   Beispiel: Telefonnummer für Rückfragen, aber diese gibt es praktisch nicht
3. Ist eine Pseudonymisierung der personenbezogenen Daten möglich? (Ersetzen durch ein Kennzeichen)
   Beispiel: Personalnummer statt Namen nennen
4. Ist eine Anonymisierung möglich?
   Beispiel: anderen Namen wählen für „jedermann“
5. So personenbezogene Daten erhoben werden müssen und keine anderen rechtlichen Aufbewahrungspflichten dagegen sprechen, ist eine frühestmögliche Löschung der personenbezogenen Daten anzustreben.
   Beispiel: Löschung der Fotos mit KfZ-Kennzeichen nach Ablauf der OWIG-Frist für unsachgemäße Ladungssicherungen bei Transporten

Revision: Änderungsdatum: Seite: 1 von 1

Anhang 5

Merkblatt Personenbezogene Daten:

Vorlage

direkt oder indirekt bestimmbar mittels Zuordnung:

- zu einer Kennung (Name, Adresse, Geburtsdatum ...)
- zu einer Kennnummer (ID, Personalnummer ...)
- zu Standortdaten (Ortung mittels Mobiltelefon, Navigation...)
- zu einer Online-Kennung (IP-Adressen, Cookie-Kennungen, die ein Gerät oder Software-Anwendungen, -Tools oder -protokolle liefern, Funkfrequenzkennungen)
- zu Merkmalen wie:
  - physische M.
  - physiologische M.
  - genetische M.
  - psychische M.
  - wirtschaftliche M.
  - kulturelle M.
  - soziale Identität

Revision: Änderungsdatum: Seite: 1 von 1

Anhang 6

Vorlage

Checkliste Rechtmäßigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten Kapitel 2 BDSG

Zulässige Verarbeitung durch öffentliche und nicht-öffentliche Stellen wie in der Tabelle benannt:

Bedingung	Konkretisierung	Erfüllt?	Handlungs-bedarf	Verant-wortlich	Termin	Erledigt am:
Erforderlichkeit liegt vor	aufgrund der Ausübung der Rechte und Pflichten der sozialen Sicherheit und des Sozialschutzes					
für Zweck der Gesund-heitsvorsorge						
für die Beurteilung der Arbeitsfähigkeit des Be-schäftigten						
für die medizinische Di-agnostik						
für die Versorgung oder Behandlung im Gesund-heits- und Sozialbereich						
für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozial-bereich						
aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs						
Verarbeitung durch ärzt-liches Personal oder sons-tigem unter Einhaltung der Geheimhaltungspflicht						
Gründe des öffentlichen Interesses	Schutz vor schwerwiegen-den grenzüberschreitenden Gesundheitsgefahren Gewährleistung hoher Qua-litäts- und Sicherheits-standards bei der Gesund-heitsversorgung, bei Arzneimitteln und Medizin-produkten					

Revision: Änderungsdatum: Seite: 1 von 2

Zulässige Verarbeitung durch öffentliche Stellen wie in der Tabelle benannt:

Bedingung	Konkretisierung	Erfüllt?	Handlungs-bedarf	Verant-wortlich	Termin	Erledigt am:
aus Gründen eines erheblichen öffentlichen Interesses						
zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit						
zur Abwehr erheblicher Nachteile für das Gemeinwohl						
aus zwingenden Gründen der Verteidigung						
soweit die Interessen des Verantwortlichen denen des Betroffenen überwiegen						

Anhang 7

Vorlage

Checkliste zu Auskunftsrechten des Betroffenen

Abschnitt/EG/ § BDSG	Anforderung	Erfüllt?	Handlungs-bedarf	Verant-wortlich	Termin	Erledigt am:
Art. 15 §§ 34, 57	Ist das Recht auf Auskunft über verarbeitete personenbezogene Daten mit einer schriftlichen Bestätigung darüber umgesetzt?					
	Sind in der schriftlichen Bestätigung alle erforderlichen Punkte enthalten? – Verarbeitungszweck – Kategorien der verarbeiteten Daten – Empfänger – geplante Dauer der Speicherung – Recht auf Berichtigung oder Löschung – Recht auf Einschränkung der Verarbeitung – Nennung des Widerspruchsrechts – Beschwerderecht bei der Aufsichtsbehörde					

Abschnitt/EG/ § BDSG	Anforderung	Erfüllt?	Handlungs-bedarf	Verant-wortlich	Termin	Erledigt am:
	– verfügbare Informationen über die Herkunft der Daten, die nicht direkt beim Betroffenen erhoben werden – Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling (Information über Logik, Tragweite der angestrebten Auswirkungen für die betroffene Person)					
	Bei Übermittlung in ein Drittland: Nachweis der geeigneten Garantien nach Artikel 46					
	Wurde eine Kopie der personenbezogenen Daten, die verarbeitet werden, unentgeltlich zur Verfügung gestellt?					
	Ist gewährleistet, dass die Rechte der und Freiheiten anderer Personen durch die Kopie nicht beeinträchtigt werden (Kategorien personenbezogener Daten, geistiges Eigentum, Geschäftsgeheimnisse, Urheberrechte an Software)?					
EG 63	Wird dem Betroffenen die Ausübung des Auskunftsrechts so leicht wie möglich gemacht?					
	Ist gewährleistet, dass dieses Recht in angemessenen Abständen wieder wahrgenommen werden kann/darf?					
	Ist sich der Betroffene dessen bewusst?					
	Bei Verarbeitung großer Mengen personenbezogener Daten: Ist die Präzisierung der personenbezogenen Daten durch den Antragsteller bei größeren Datenmengen in die Formblätter einbezogen?					
EG 64	Ist mit allen vertretbaren Mitteln die Identität des Auskunftersuchenden festgestellt worden?					

Anhang 8

Vorlage

Checkliste zur Einschränkung der Verarbeitung

Artikel/EG/ § BDSG	Anforderung	Erfüllt?	Handlungs-bedarf	Verant-wortlich	Termin	Erledigt am:
Artikel 18 §§ 35, 36, 58 BDSG	Recht auf Einschränkung der Verarbeitung, wenn – die Richtigkeit der personenbezogenen Daten bestritten wird – unrechtmäßige Verarbeitung personenbezogener Daten stattfindet, die betroffene Person die Löschung ablehnt und stattdessen die Einschränkung der Datennutzung verlangt – die erhobenen personenbezogenen Daten nicht mehr benötigt werden, jedoch der Betroffene die Daten zur Durchsetzung von Rechtsansprüchen braucht – die betroffene Person Widerspruch eingelegt hat gegen die Verarbeitung und dies noch nicht rechtsgültig geklärt ist					
	Ist die Einschränkung der Verarbeitung betreffender personenbezogener Daten für die Dauer der Überprüfung der Richtigkeit der Daten gegeben?					
	Ist die Einschränkung der Verarbeitung technisch zuverlässig gelöst? Sind alle zugangsberechtigten Personen informiert?					
	Ist die Verantwortlichkeit für die Umsetzung der Einschränkung der Verarbeitung personenbezogener Daten geregelt?					
	Ist das Freigabeverfahren für die weitere Verarbeitung geregelt?					
	Ist geregelt, wer (und wie) die Einschränkung der Verarbeitung an den Betroffenen bekannt gibt?					
	Ist eine versehentliche Weiterverarbeitung der personenbezogenen Daten ausgeschlossen?					
	Ist gewährleistet, dass die weitere Verarbeitung nur mit Einwilligung der betroffenen Person möglich ist?					

Artikel/EG/ § BDSG	Anforderung	Erfüllt?	Handlungs-bedarf	Verant-wortlich	Termin	Erledigt am:
	Wie erfolgt die Information an den Betroffenen, dass aus dem Grund der Verteidigung, Geltend-machung, Ausübung von Rechts-ansprüchen eine weitere Verarbei-tung der personenbezogenen Daten stattfindet?					
	Information an den Betroffenen zur Aufhebung der Einschränkung in der Verarbeitung nachvollziehbar erfolgt?					
EG 67	Werden u. U. ausgewählte perso-nenbezogene Daten auf andere Verarbeitungssysteme übertragen?					
	Werden diese betreffenden Daten für Nutzer gesperrt?					
	Werden diese Daten u. U. aus der Website vorübergehend entfernt?					
	Ist im System ein unmissverständ-licher Hinweis auf die Sperrung der Daten gegeben?					

Anhang 9

Vorlage

Checkliste zur Realisierung des Rechts auf Berichtigung und Löschung (Recht auf Vergessenwerden)

Abschnitt/EG/ § BDSG	Anforderung	Erfüllt?	Handlungs-bedarf	Verant-wortlich	Termin	Erledigt am:
Abschnitt 3, Art. 16 EG 59 §§ 34, 35, 36 BDSG	Bekanntgabe der Kontaktdaten des Datenschutzbeauftragten zur Ver-wirklichung des Rechts auf Berich-tigung oder Löschung					
	unverzügliche Berichtigung: Zeitfenster festgelegt, Verantwort-lichkeit festgelegt technische Machbarkeit vor Eintritt des Falls geprüft					
	unverzügliche Ergänzung: Zeitfenster festgelegt, Verantwort-lichkeit festgelegt technische Machbarkeit vor Eintritt des Falls geprüft					

Abschnitt/EG/ § BDSG	Anforderung	Erfüllt?	Handlungs-bedarf	Verant-wortlich	Termin	Erledigt am:
	unverzügliche Löschung unter Berücksichtigung des Absatzes 3, weil – nicht mehr zur Zweckerfüllung notwendig – betroffene Person widerruft die Einwilligung – keine vorrangig berechtigten Gründe für die Verarbeitung – unrechtmäßig verarbeitet – Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung nach Unionsrecht oder des Rechts eines Mitgliedstaats erforderlich – personenbezogene Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 erhoben					
	Hinweis auf jederzeitigen Widerruf der Einwilligungserklärung gegeben?					
	Belehrung zur Zweckbindung bei der Erhebung personenbezogener Daten gegeben?					
	über Widerspruchsrecht informiert?					
EG 59	unentgeltlicher Zugang zu personenbezogenen Daten realisiert?					
	Elektronische Anträge möglich zur Berichtigung oder Löschung elektronischer Daten?					
	Frist der Bearbeitung des Antrags der betroffenen Person unterhalb eines Monats gegeben (Antwortschreiben)?					
	Begründung für Ablehnung des Antrags fundiert gegeben?					
EG 65	Sind die besonderen Rechte des Betroffenen umgesetzt für den Fall, er hat die Einwilligung im Kindesalter gegeben?					

Abschnitt/EG/ § BDSG	Anforderung	Erfüllt?	Handlungs-bedarf	Verant-wortlich	Termin	Erledigt am:
EG 66	Ist das Recht auf Vergessenwerden insofern umgesetzt, als dass alle an der Verarbeitung im Netz Beteiligten über den Löschanspruch benachrichtigt werden? (Löschung aller Links, Kopien, Replikationen)					
	Sind die ergriffenen Maßnahmen zur Information aller am Prozess der Datenverarbeitung Beteiligten im Netz unter Berücksichtigung der verfügbaren Technik, der Mittel und Methoden angemessen?					

Anhang 10

Vorlage

Checkliste Anforderungen an die Sicherheit der Datenverarbeitung

Anforderung	Erfüllt?	Handlungsbedarf	Termin	Verant-wortlich	Erledigt am:
Verwehrung des Zugangs zu Verarbeitungsanlagen (Zugangskontrolle)					
Verhinderung des unbefugten Lesens, Kopierens, Veränderns, Löschens von Datenträgern (Weitergabekontrolle)					
Verhinderung von unbefugten Eingaben sowie der unbefugten Kenntnisnahme; Veränderung und Löschung personenbezogener Daten (Speicherkontrolle)					
Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen der Datenübertragung durch Unbefugte (Benutzerkontrolle)					
ausschließlicher Zugang zu von ihrer Zugangsberechtigung umfassten personenbezogenen Daten (Zugriffskontrolle)					
Gewährleistung der Überprüfung, wohin personenbezogene Daten übermittelt wurden (Übertragungskontrolle)					

Anforderung	Erfüllt?	Handlungsbedarf	Termin	Verant-wortlich	Erledigt am:
Möglichkeit der nachträglichen Überprüfung, von wem personenbezogene Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (Eingabekontrolle)					
Vertraulichkeit und Integrität bei der Datenübermittlung und beim Transport der Datenträger (Transportkontrolle)					
Wiederherstellbarkeit von eingesetzten Systemen nach Störungen (Wiederherstellbarkeit)					
Gewährleistung, dass alle Funktionen im System zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit)					
Sicherstellung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)					
Gewährleistung der Verarbeitung personenbezogener Daten im Auftrag nur entsprechend Weisung des Auftraggebers (Auftragskontrolle)					
Gewährleistung, dass personenbezogene Daten gegen Verlust und Zerstörung geschützt sind (Verfügbarkeitskontrolle)					
Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennbarkeit)					

Anhang 11

Beispiel

Datenschutz-Folgeabschätzung

1 Allgemeines

Bereich: Personal

Datum: 16.02.2018

Verantwortlicher für die Verarbeitung: Geschäftsführung in Genf, Leiter Personal

Datenschutzbeauftragter: _____

_____

_____

Verarbeitungstätigkeit:

Erhebung, Verarbeitung und Speicherung personenbezogener Daten im Rahmen der Zeiterfassung, Erfassung der Anwesenheitszeiten (Beginn und Ende der Arbeitszeit), Erfassung der Schichten für die Lohn- und Gehaltsabrechnung einschließlich der Zuschläge für Spät-, Nachtschichten, Sonn- und Feiertage, Erfassung der Abwesenheitszeiten ohne Unterscheidung in Urlaub und Krankheit

Beginn der Verarbeitung: seit Gründung des Unternehmens 20__

Zweck der Verarbeitung: Lohn- und Gehaltsabrechnung, Erfassung der An- und Abwesenheitszeiten, Führen des Überstundenkontos

Art der personenbezogenen Daten: Anwesenheitsdaten der Mitarbeiter

Umfang der personenbezogenen Daten: umfasst sowohl Angestellte als auch gewerbliche Mitarbeiter außer Geschäftsführung und leitende Angestellte

Berechtigtes Interesse: für Zwecke der Berechnung der Löhne und Gehälter unabdingbar

Besondere Schutzbedürftigkeit gemäß Art. 9 Abs. 1 DSGVO: keine Anwendung

Für den Zugriff berechtigte Personen: Geschäftsführung in Genf, Personalleitung, Leiter FIBU (in Vertretung), Administrator

Auftragsverarbeitung durch (falls zutreffend): entfällt

Übermittlung an: Konzernmutter xy in Genf

Löschfristen: 10 Jahre

2 Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten

Grundsatz	ja	nein	Kommentar
Rechtmäßigkeit der Verarbeitung	x		
Verarbeitung nach Treu und Glauben	x		
Transparenz	x		
Zweckbindung (notwendig und verhältnismäßig)	x		Selbst nach Ausscheiden des Mitarbeiters müssen die Daten noch gespeichert werden. Beispiele sind: Rechtfertigung der Schichtzuschläge gegenüber dem Finanzamt bei der Lohnsteuerprüfung, Prüfung durch Sozialversicherungsträger, Rentenversicherungsträger.

Grundsatz	ja	nein	Kommentar
			Abrechnungen werden auch nach dem Ausscheiden des Mitarbeiters aufgrund von schwebenden Rechtsstreitigkeiten noch notwendig.
Datenminimierung	x		Es werden keine über den Verarbeitungszweck hinausgehenden Daten erhoben.
Richtigkeit	X		
Speicherbegrenzung	X		Frist von 10 Jahren nach Ausscheiden des Mitarbeiters, Aufbewahrungspflicht wegen Lohnsteuerprüfungen
Integrität und Vertraulichkeit	x		Die Personalleitung wurde auf die Geheimhaltung verpflichtet.
Anforderungen an Eignung technischer und organisatorischer Maßnahmen erfüllt?	x		Ja
Bestehen eigene berechtigte Interessen?		x	nicht über den gesetzlich notwendigen Rahmen hinaus
Überwiegen Rechte der betroffenen Person die eigenen berechtigten Interessen?		x	
Verarbeitung zur Zweckerreichung notwendig?	x		
Ist die Verarbeitung verhältnismäßig? Interessenabwägung	x		

3 Datenschutz-Folgeabschätzung

Risikofaktoren (RF)	Nähere Erläuterung des RF	Eintrittswahrscheinlichkeit (EWS)		Tragweite der Auswirkung (TA)		Risiko* (R)	Präventionsmaßnahmen	EWS*		TA*		R**	Korrekturmaßnahmen
physischer, materieller oder immaterieller Schaden	Verlust der Daten	2	×	2	=	4	geeignete technische Maßnahmen gewählt	1	×	2	=	2	Aufzeichnung des Vorfalls und Ursachenanalyse Überprüfung der getroffenen technischen Maßnahmen und deren Anpassung zur Ursachenbeseitigung
Diskriminierung, Identitätsdiebstahl, Identitätsbetrug	nicht vorstellbar	–		–		–							
finanzieller Verlust	nicht vorstellbar	–		–		–							
Rufschädigung	nicht vorstellbar	–		–		–							
Verlust der Vertraulichkeit der dem Berufsgeheimnis unterliegenden Daten	nicht zutreffend	–		–		–							
Aufhebung der Pseudonymisierung	keine Folgen ableitbar	–		–		–							
erhebliche wirtschaftliche und gesellschaftliche Nachteile	nicht gegeben, selbst nicht bei Verlust der Daten	1	×	2	=	2	redundante Speicherung der Daten, Zugangs- und Zugriffsschutz	1	×	2	=	2	Spiegelung der Daten
Hinderung an der Ausübung der Rechte des Betroffenen	gesetzliche Notwendigkeit der Datenerfassung und -verarbeitung zu Abrechnungszwecken	–		–		–							
unerlaubte Verarbeitung von besonderen Kategorien personenbezogener Daten	nicht zutreffend	–		–		–							

Risikofaktoren (RF)	Nähere Erläuterung des RF	Eintritts-wahr-scheinlich-keit (EWS)	Tragweite der Aus-wirkung (TA)	Risiko* (R)	Präventionsmaßnahmen	EWS*	TA*	R**	Korrektur-maßnahmen
Bewertung persönlicher Aspekte, z. B. Arbeitsleistung, Gesundheit, wirtschaftliche Lage	ggf. Erkenntnisse über Kurzerkrankungen je-weils am Wochenende und -beginn	2	2	4	Die Interpretation der Daten zur Erfassung von Abwesenheiten durch Krankheit ist zulässig.	2	2	4	–
Ausspionieren des Verhaltens, des Aufenthaltsorts	Anwesenheitsdaten sind dazu wenig ge-eignet, ggf. Erkennt-nisse über Kurzerkran-kungen jeweils am Wochenende und -beginn	2	2	4	Die Interpretation der Daten zur Erfassung von Abwesenheiten durch Krankheit ist zulässig.	2	2	4	–
Erstellung persönlicher Profile	nicht gegeben	–	–	–					
unerlaubte Verarbeitung von Daten Schutzbedürftiger	nicht gegeben	–	–	–					
eine große Anzahl von Personen betreffend	alle Mitarbeiter wären betroffen	2	2	4	geeignete technische Sicherungsmaßahmen	1	2	2	

Skala:

EWS/TA und EWS*/TA*

1 = gering

2 = mittel

3 = hoch

R* und R** = Produkt der Faktoren

Skala Risiko gesamt:

bis 4 = gering

5–7 = mittel, Maßnahmen erforderlich

über 7 = hoch, Maßnahmen einzuleiten, zu überprüfen und ggf. Konsultation der Aufsichtsbehörde erforderlich

4 Hinnehmbares Risiko

Stellen die risikobehafteten Verarbeitungsvorgänge dennoch bezüglich

- Eintrittswahrscheinlichkeit,
- Umfang, Umstände,
- Schwere des Risikos und
- aufgrund der getroffenen Maßnahmen

ein hinnehmbares Risiko dar?

ja ☒ nein ☐

5 Hohes Risiko

Falls ein hohes Risiko die Folge wäre und keine Maßnahmen der Verringerung des Risikos getroffen wurden oder getroffen werden konnten:

- Wurde die Datenschutzbehörde vor Beginn der Verarbeitung kontaktiert?
- Wurde der Datenschutzbeauftragte einbezogen?

entfällt

Existieren Ausnahmetatbestände gemäß gesetzlichen Erlaubnisnormen (Art. 35 Abs. 10 DSGVO)?

entfällt

6 Zusammenfassung

Die Verarbeitung ist zulässig, die Schutzmaßnahmen sind geeignet.

Datum:

Unterschrift	Verantwortlicher	Datenschutzbeauftragter

Anhang 12

Vorlage

Anweisung: Umsetzung der Rechte der Betroffenen auf Berichtigung, Ergänzung und Löschung personenbezogener Daten

1 Zweck

In dieser Verfahrensanweisung wird geregelt, wie die Rechte des Betroffenen auf Berichtigung, Ergänzung und Löschung personenbezogener Daten in unserem Unternehmen umgesetzt werden.

2 Anwendungsbereich

Die vorliegende Verfahrensanweisung gilt für Verarbeiter personenbezogener Daten.

3 Verfahren

Der Betroffene hat das Recht auf Berichtigung, Ergänzung und Löschung (Recht auf Vergessenwerden) seiner personenbezogenen Daten. Zur Durchsetzung seiner Rechte ist er zunächst über Aushang und auch schriftlich mit einer der Gehalts- oder Lohnabrechnungen über den Namen und die Kontaktdaten des Datenschutzbeauftragten zu informieren, sodass einer Geltendmachung seines Rechts nichts im Wege steht. Seinem Begehren auf Berichtigung unrichtiger personenbezogener Daten ist unverzüglich Folge zu leisten, sobald die Identität des Betroffenen, der die Berichtigung oder Löschung verlangt, festgestellt wurde. Dazu wird folgendes Vorgehen festgelegt:

1. Benennung des für die Korrektur, Ergänzung oder die Löschung verantwortlichen Mitarbeiters, soweit dies nicht durch die Art der Daten eindeutig ist
2. Feststellung der Identität des Betroffenen
3. Information der ggf. noch am Prozess Beteiligten (IT; andere Verarbeiter, alle an der Verarbeitung im Netz Beteiligten)
4. Berücksichtigung der Gründe für eine unverzügliche Löschung, siehe unten
5. Festlegung des Zeitfensters (möglichst innerhalb eines Monats gemäß EU-DSGVO)
6. Prüfung der technischen Machbarkeit
7. Information des Datenschutzbeauftragten in Fällen, die einer technischen Machbarkeit entgegenstehen oder falls die Löschbarkeit der Daten nicht eindeutig ist; dieser legt die weitere Vorgehensweise mit dem verantwortlichen Mitarbeiter und ggf. anderen Beteiligten fest
8. Information des Betroffenen zu den Punkten 1, 5 und 6 oder Begründung der Ablehnung des Antrags (innerhalb eines Monats)
9. Umsetzung der Korrektur, Ergänzung oder Löschung (einschließlich aller Links, Kopien, Replikationen)
10. Nachweiserbringung der Berichtigung bzw. Löschung für die Akten und den Betroffenen

Gründe für die unverzügliche Löschung von personenbezogenen Daten:

- Zweckbindung der personenbezogenen Daten ist entfallen
- Widerruf der Einwilligung in die Verarbeitung personenbezogener Daten, soweit nicht rechtlich erforderlich
- Widerruf der Einwilligung, die im Kindesalter gegeben wurde, ggf. ohne die Tragweite der Einwilligung in die Verarbeitung personenbezogener Daten einschätzen zu können (besondere Rechte des Betroffenen berücksichtigen)
- keine vorrangig berechtigten Gründe für die Verarbeitung

- unrechtmäßige Verarbeitung personenbezogener Daten
- Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung nach Unionsrecht oder dem Recht eines Mitgliedstaats
- personenbezogene Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 erhoben (Einwilligung des Kindes bis zum 16. Lebensjahr oder später)

Gründe, die einer Löschung entgegenstehen

Im Fall nicht-automatisierter Verarbeitung:

Keine Löschung erforderlich, wenn

- unverhältnismäßig hoher Aufwand entsteht und das schutzwürdige Interesse eher gering einzuschätzen ist,
- der Löschung satzungsmäßige oder rechtliche Aufbewahrungspflichten entgegenstehen.

Dafür:

- **Einschränkung der Verarbeitung**

Diese Ausnahme gilt nicht bei unrechtmäßiger Erhebung von personenbezogenen Daten.

Eine Unterrichtung der betroffenen Person über die Einschränkung der Verarbeitung ist erforderlich, so diese nicht unmöglich ist oder unverhältnismäßig hohen Aufwand erfordert.

4 Mitgeltende Unterlagen

Informationsschreiben an den Betroffenen

Protokolle der Sitzungen

Löschnachweise

Revision: Änderungsdatum: Seite: 2 von 2

Anhang 13

Vorlage

Antrag auf Berichtigung, Ergänzung oder Löschung personenbezogener Daten

Name, Vorname:

Bereich:

Tätig als:

Personalnummer:

Kontaktadresse:

E-Mail-Adresse:

Telefon:

Hiermit stelle ich den Antrag auf (Zutreffendes bitte ankreuzen)

- Berichtigung
- Ergänzung
- Löschung

folgender personenbezogener Daten:

Revision: Änderungsdatum: Seite: 1 von 2

Berichtigung/Ergänzung durch:

Löschung von:

wegen:

Datum: Unterschrift:

Revision: Änderungsdatum: Seite: 2 von 2

Anhang 14

Anweisung: Einschränkung der Verarbeitung personenbezogener Daten

Vorlage

1 Zweck

In dieser Verfahrensanweisung wird geregelt, wie im Fall der Einschränkung der Verarbeitung personenbezogener Daten einschließlich der Sperrung und Wiederfreigabe von personenbezogenen Daten zu verfahren ist.

2 Anwendungsbereich

Die vorliegende Verfahrensanweisung gilt für Verarbeiter personenbezogener Daten.

3 Verfahren

Der Betroffene hat das Recht auf Einschränkung der Verarbeitung personenbezogener Daten, sofern die Rechtmäßigkeit und Korrektheit der vorliegenden personenbezogenen Daten bestritten wird. Das Recht auf Einschränkung der Verarbeitung gilt bis zur rechtlichen Klärung der Angelegenheit.

Gründe für die Einschränkung der Verarbeitung personenbezogener Daten sind demnach:

a) Richtigkeit der Verarbeitung personenbezogener Daten wird bestritten

b) unrechtmäßige Verarbeitung

c) unrechtmäßige Verarbeitung ohne Löschung, sondern nur mit Einschränkung

d) die Verarbeitung personenbezogener Daten hat die Zweckbindung verloren, die Daten werden jedoch zur Durchsetzung von Rechtsansprüchen noch benötigt

e) Einlegung des Widerspruchs gegen die Verarbeitung personenbezogener Daten durch den Betroffenen bis zur Rechtsklärung.

Im Fall des Bestreitens der Richtigkeit der personenbezogenen Angaben dürfen die Daten nur eingeschränkt verarbeitet werden. Der Datenschutzbeauftragte ist von der verantwortlichen Abteilung über den Fall zu informieren. Unter Beteiligung des Datenschutzbeauftragten werden alle an der Verarbeitung dieser personenbezogenen Daten beteiligten/zugangsberechtigten Personen von der Einschränkung der Verarbeitung schriftlich wie mündlich informiert. Im gemeinsamen Gespräch werden alle erforderlichen zuverlässigen und möglichst technischen Vorkehrungen getroffen, um eine tatsächliche Einschränkung der Verarbeitung zu gewährleisten und eine versehentliche Weiterverarbeitung für die Dauer der Klärung zu verhindern. Dies bedeutet u. U.:

Revision: Änderungsdatum: Seite: 1 von 2

- Sperrung der Daten für die Nutzer
- Stoppen des Übertragens dieser Daten auf andere Verarbeitungssysteme
- ggf. vorübergehendes Entfernen der personenbezogenen Daten aus der Website
- Etablierung eines unmissverständlichen Hinweises auf die Sperrung der Daten im System.

Verantwortlich für die Umsetzung der Einschränkung ist der verantwortliche Verarbeiter. Sind dies mehrere, so wird ein Verantwortlicher namentlich bestimmt. Der Verantwortliche informiert den Betroffenen von der Umsetzung der eingeschränkten Verarbeitung auf schriftlichem Weg.

Die Wiederfreigabe der Verarbeitung personenbezogener Daten bedarf eines geregelten Verfahrens. Hierzu wird erneut der Datenschutzbeauftragte vom verantwortlichen Verarbeiter informiert. Er prüft, ob alle Voraussetzungen vorliegen, die Einschränkung der Verarbeitung aufzulösen, beispielsweise die Einwilligung der betroffenen Person zur weiteren Verarbeitung, ein Gerichtsbeschluss o. Ä. Unter seiner Beteiligung werden alle beteiligten bzw. zugangsberechtigten Personen zu einem Meeting einberufen. In diesem Meeting werden die Maßnahmen besprochen, die eine Weiterverarbeitung der betreffenden personenbezogenen Daten ermöglichen. Die Einschränkung der Verarbeitung wird mit Protokoll der Sitzung aufgehoben. Der verantwortliche Verarbeiter informiert formal den Betroffenen.

Gleichermaßen wird in den Fällen b) und e) vorgegangen.

Im Fall c) erlaubt der Betroffene die Löschung der personenbezogenen Daten nicht, er fordert die eingeschränkte Verarbeitung. Diese ist so lange zu gewähren, wie er seinen Anspruch beibehält.

Im Fall d) informiert der für die Verarbeitung Verantwortliche oder dessen Rechtsvertreter über die Einschränkung der Verarbeitung zur Durchsetzung von Rechtsansprüchen. Er legt nachvollziehbar dar, welche personenbezogenen Daten er aus welchen Gründen eingeschränkt verarbeitet.

4 Mitgeltende Unterlagen

Informationsschreiben an die an der Verarbeitung Beteiligten

Informationsschreiben an den Betroffenen

Protokolle der Sitzungen

Revision: Änderungsdatum: Seite: 2 von 2

Anhang 15

Vorlage

Anweisung: Anforderungen an die Sicherheit von DV-Anlagen

1 Zweck

In dieser Verfahrensanweisung wird geregelt, welche Anforderungen an die Sicherheit der Datenverarbeitung personenbezogener Daten gestellt werden.

2 Anwendungsbereich

Die vorliegende Verfahrensanweisung gilt für den Verantwortlichen der Verarbeitung personenbezogener Daten, die Mitarbeiter IT, Führungskräfte bzw. den Datenschutzbeauftragten.

Revision: Änderungsdatum: Seite: 1 von 3

3 Verfahren

Anforderungen

Für die Datenverarbeitung sind durch den Verantwortlichen folgende Vorkehrungen und Maßnahmen zu treffen:

Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen

Weitergabekontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns, Löschens von Datenträgern

Speicherkontrolle

Verhinderung von unbefugten Eingaben sowie der unbefugten Kenntnisnahme; Veränderung und Löschung personenbezogener Daten

Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen der Datenübertragung durch Unbefugte

Zugriffskontrolle

ausschließlicher Zugang zu von ihrer Zugangsberechtigung umfassten personenbezogenen Daten

Übertragungskontrolle

Gewährleistung der Überprüfung, wohin personenbezogene Daten übermittelt wurden

Eingabekontrolle

Möglichkeit der nachträglichen Überprüfung, von wem personenbezogene Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind

Transportkontrolle

Vertraulichkeit und Integrität bei der Datenübermittlung und beim Transport der Datenträger

Wiederherstellbarkeit

Wiederherstellbarkeit von eingesetzten Systemen nach Störungen

Zuverlässigkeit

Gewährleistung, dass alle Funktionen im System zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden

Datenintegrität

Sicherstellung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können

Auftragskontrolle

Gewährleistung der Verarbeitung personenbezogener Daten im Auftrag nur entsprechend Weisung des Auftraggebers

Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Verlust und Zerstörung geschützt sind

Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können

4 Mitgeltende Unterlagen

Checkliste der Anforderungen an die Verarbeitung personenbezogener Daten

§ 42 Strafvorschriften

Revision: Änderungsdatum: Seite: 3 von 3

Anhang 16

Vorlage

Anweisung: Speichern und Scannen von Daten

1 Zweck

Diese Anweisung soll ein schnelles Auffinden von Dateien im Netz ermöglichen und damit die Arbeit aller Mitarbeiter erleichtern.

2 Geltungsbereich

Der Geltungsbereich erstreckt sich auf alle Mitarbeiter, die Zugang zu einem PC haben und über Schreibrechte verfügen.

3 Verfahren

Alle Mitarbeiter mit Schreibrechten am PC sind gehalten, Daten möglichst im Intranet in den entsprechenden Arbeitsverzeichnissen zu speichern. Neben den sachbezogenen Verzeichnissen, die über Zugriffsrechte geöffnet werden können, steht jedem Mitarbeiter ein über Zugriffsrechte geschütztes persönliches Verzeichnis im Intranet zur Verfügung. Obwohl dieses Verzeichnis den Namen des Mitarbeiters trägt, ist ein Auslesen der Daten über Administratoren und die täglichen Back-ups möglich. Aus Datenschutzgründen wird darauf verwiesen, hier nur Daten zu speichern, die mit der eigenen Arbeit und Aufgabe verbunden sind, so diese Daten nicht sachbezogen im Zugriff einer Benutzergruppe auf den öffentlichen Verzeichnissen gespeichert werden müssen.

Personenbezogene Daten sind möglichst zusätzlich mit einem Passwort zu schützen. Handelt es sich um besondere Kategorien personenbezogener Daten ist eine weitere Verschlüsselung Pflicht.

Auf die Speicherung privater Daten ist möglichst zu verzichten, da sie im Netz u. U. von mehreren Personen sowie den Administratoren einsehbar sind. In vertretbarem Umfang können diese Daten auf der Festplatte gespeichert werden. Die Daten auf der Festplatte des Rechners sind nicht in den automatischen Datensicherungsrhythmus integriert. Ein Datenverlust ist hier also nicht abgesichert.

Einzelne Dateien sind der Übersichtlichkeit wegen möglichst einzelnen Unterordnern zuzuordnen. Nicht mehr benötigte Dateien sind in regelmäßigen Abständen zu löschen. Die Löschung und damit Einhaltung der Aktualität von Daten trägt sehr viel zur Übersichtlichkeit und damit Auffindbarkeit von Daten bei. Diese Verfahrensweise folgt dem datenschutzrechtlichen Grundsatz der Datensparsamkeit.

Revision: Änderungsdatum: Seite: 1 von 2

In diesem Zusammenhang wird noch einmal darauf verwiesen, dass es sich bei den gespeicherten Daten teilweise um kunden-, lieferanten- oder personenbezogene Daten handelt, z. B. Adressen in Anschreiben, private Telefonnummern. Diese Daten sind bereits schützenswerte Daten gemäß Bundesdatenschutzgesetz. Datensparsamkeit, d. h. die Überlegung anzustellen, ob diese Daten überhaupt (so lange) aufbewahrt/gespeichert werden müssen, trägt wesentlich zur Einhaltung der rechtlichen Bestimmungen zum Datenschutz bei.

Passwörter sind regelmäßig gemäß automatischer Aufforderung durch das System zu wechseln. Die Beschaffenheit des Passwortes sollte den empfohlenen Regeln für ein gutes Passwort folgen. Passwörter dürfen nicht veröffentlicht (Klebezettel am PC) oder weitergegeben werden. Bei Weitergabe des Passwortes im Vertretungsfall ist im Anschluss ein neues Passwort zu wählen.

E-Mail-Nachrichten sind nach den Datensparsamkeitsprinzipien entweder zu archivieren, so dass eine Wiederauffindbarkeit schnell möglich ist, also z. B. in sachbezogenen Unterordnern, oder aufgrund der Entbehrlichkeit zu löschen. Die Archivierung und Löschung der E-Mail-Nachrichten sollte mindestens vierteljährlich erfolgen. Private E-Mails sollten möglichst nicht unter Lotus Notes gespeichert werden. Sie sind über Back-ups auslesbar.

Besitzer eines betrieblichen Laptops sind gehalten, möglichst wenig private Daten auf den Laptops zu speichern und kunden-, lieferanten- und personenbezogene Daten nur in absolut notwendigem Maße vorzuhalten. Hier ist die Gefahr eines Datenverlustes, des Diebstahls oder Ausspionierens am größten. Ein regelmäßiger Datenübertrag auf das betriebliche Netzwerk unter Einhaltung aller notwendigen Sicherheitsmaßnahmen ist unabdingbar. Bei einem Datenverlust auf dem Laptop ist dann kein Back-up gegeben.

Das Brennen von betrieblichen Daten auf CD oder DVD, das Überspielen dieser Daten auf einen USB-Stick sollte nur in begründeten Ausnahmefällen erfolgen. Die Mitnahme von Datenträgern außer Haus birgt besondere Gefahren des Datenmissbrauchs, Ausspionierens und auch Datendiebstahls. Betriebliche Daten sollten i. d. R. nicht mit nach Hause zur Bearbeitung mitgenommen werden, da auch hier die Sicherheitsvorkehrungen oftmals nicht ausreichend sind.

Für das Scannen von Daten steht jedem Befugten ein eigener Ordner zur Ablage der gescannten Daten zur Verfügung. Die Daten werden nach der Auswahl des Zieles (Name des Befugten) am Scanner nach dem Scannen direkt auf den entsprechenden Ordner übertragen. Die personalisierten Ordner sind vor dem Zugriff von anderen Benutzern geschützt. Administratoren und das Backupsystem können auf die Scanordner zugreifen. Beim Scannen muss auf die Auswahl des Zieles geachtet werden, anderenfalls ist es möglich, dass Daten auf fremde Ordner übertragen werden. Gescannte Daten sollten umgehend auf die Arbeitslaufwerke bzw. -ordner übernommen und aus dem Scanordner gelöscht werden.

4 Mitgeltende Unterlagen

Anweisungen zum Datenschutz

Verpflichtung auf das Datengeheimnis

Anhang 17

Vorlage

Anweisung: Datenschutz-Folgeabschätzung

1 Zweck

In dieser Verfahrensanweisung wird geregelt, welche Anforderungen an die Datenschutz-Folgeabschätzung gestellt werden.

2 Anwendungsbereich

Die vorliegende Verfahrensanweisung gilt für den Verantwortlichen der Verarbeitung personenbezogener Daten bzw. den Datenschutzbeauftragten.

3 Verfahren

Eine Datenschutz-Folgeabschätzung ist insbesondere unter Verwendung neuer Technologien durchzuführen, wenn

- aufgrund der Art,
- des Umfangs,
- der Umstände,
- der Zwecke der Verarbeitung

voraussichtlich eine erhebliche Gefahr für Rechtsgüter der betroffenen Person besteht.

Die Risiken für die Rechte und Freiheiten natürlicher Personen sind:

- Risiken
- physischer, materieller oder immaterieller Schaden
- Diskriminierung, Identitätsdiebstahl, Identitätsbetrug
- finanzieller Verlust
- Rufschädigung
- Verlust der Vertraulichkeit der dem Berufsgeheimnis unterliegenden Daten
- Aufhebung der Pseudonymisierung
- erhebliche wirtschaftliche und gesellschaftliche Nachteile
- Hinderung an der Ausübung der Rechte des Betroffenen
- unerlaubte Verarbeitung von besonderen Kategorien personenbezogener Daten
- Bewertung persönlicher Aspekte, z. B. Arbeitsleistung, Gesundheit, wirtschaftliche Lage
- Ausspionieren des Verhaltens, des Aufenthaltsorts
- Erstellung persönlicher Profile
- unerlaubte Verarbeitung von Daten Schutzbedürftiger
- eine große Anzahl von Personen betreffend

Der Katalog der Risikofaktoren, mithilfe derer eine Datenschutz-Folgeabschätzung vorzunehmen ist, kann der Einstufung von personenbezogenen Daten in sogenannte Schutzstufen dienen.

Schutzstufen personenbezogener Daten sind demnach:

Schutzstufe A	• frei zugängliche Daten • keine Geltendmachung berechtigter Interessen notwendig
Schutzstufe B	• Missbrauch stellt keine besondere Beeinträchtigung dar • beschränkt öffentlich zugängliche Daten, Verteiler für Unterlagen, z. B. akademischer Grad, Berufsbezeichnung, Zugehörigkeit zu einem Verein/Interessensgruppe/Berufsgruppe
Schutzstufe C – Ansehensschädigung	• durch Missbrauch Beeinträchtigung der gesellschaftlichen Stellung oder in wirtschaftlichen Verhältnissen möglich • z. B. Einkommen, Sozialleistungen, Ordnungswidrigkeiten, Grundsteuer
Schutzstufe D – Existenzschädigung	• durch Missbrauch Beschädigung der gesellschaftlichen Stellung oder der wirtschaftlichen Verhältnisse • z. B. Straffälligkeit, schwerwiegende Ordnungswidrigkeiten, psychologische Gutachten, Schulden, Pfändungen, Insolvenzen
Schutzstufe E – Frage von Leben, Tod	• Missbrauch schädigt Gesundheit, Leben, Freiheit • z. B. Daten über mögliche Opfer einer strafbaren Handlung

Eine Datenschutz-Folgeabschätzung sollte erst bei Datenschutzstufe C erfolgen.

Es sind Maßnahmen zu treffen, den Erfolg der Risiken zuverlässig abzuwenden. Dazu ist zu betrachten, inwiefern und in welchem Ausmaß die Risiken auftreten können (Eintrittswahrscheinlichkeit und Tragweite der Auswirkung). Diese Betrachtung wird auch Datenschutz-Folgeabschätzung genannt.

Pflichtbestandteile der Datenschutz-Folgeabschätzung sind folgende Angaben:

1. systematische Beschreibung der geplanten Verarbeitungsvorgänge
2. Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den verfolgten Zweck
3. Beschreibung der Präventionsmaßnahmen zur Abwendung der Gefahren

   einschließlich

   Garantien,

   Sicherheitsvorkehrungen und Verfahren,

   die den Nachweis der Compliance enthalten.

Auf der Grundlage dieser Angaben wird die Datenschutz-Folgeabschätzung durch den Verantwortlichen gemäß beiliegendem Formblatt und unter Beteiligung des Datenschutzbeauftragten durchgeführt.

Die Datenschutz-Folgeabschätzung wird in der Praxis mindestens einmal jährlich überprüft. Ggf. werden Korrekturmaßnahmen getroffen und das Datenschutzkonzept geändert.

4 Mitgeltende Unterlagen

Formblatt Datenschutz-Folgeabschätzung

§ 42 Strafvorschriften

Anhang 18

Vorlage

Anweisung: Meldung von Verletzungen des Schutzes personenbezogener Daten an den Bundesbeauftragten für Datenschutz

1 Zweck

In dieser Verfahrensanweisung wird geregelt, in welchen Fällen eine Meldung von Verletzungen des Schutzes personenbezogener Daten an den Bundesbeauftragten für Datenschutz erfolgen muss.

2 Anwendungsbereich

Die vorliegende Verfahrensanweisung gilt für den Verantwortlichen der Verarbeitung personenbezogener Daten bzw. den Datenschutzbeauftragten.

3 Verfahren

Verantwortlicher für die Verarbeitung

Der Verantwortliche für die Verarbeitung personenbezogener Daten hat bei einer Verletzung des Schutzes personenbezogener Daten unverzüglich und binnen 72 Stunden eine Meldung an den Bundesbeauftragten für Datenschutz zu tätigen. Ausnahme: Die Verletzung des Schutzes personenbezogener Daten birgt voraussichtlich keine Gefahr für die Rechtsgüter des Betroffenen.

Bei Nicht-Einhaltung der Frist ist die verspätete Meldung zu begründen.

Auftragsverarbeiter

Ein Auftragsverarbeiter hat die Verletzung des Schutzes personenbezogener Daten unverzüglich dem Verarbeiter zu melden.

Inhalte der Meldung

Die Meldung hat folgende Inhalte zu umfassen:

- Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten
- Angaben zu den Kategorien der personenbezogenen Daten
- Angaben zur Kategorie und Anzahl der betroffenen Personen
- Angaben zur ungefähren Anzahl der betroffenen personenbezogenen Datensätze
- Kontaktdaten des Datenschutzbeauftragten
- Beschreibung der wahrscheinlichen Folgen der Verletzung
- Beschreibung der ergriffenen Sofortmaßnahmen und der geplanten

Ggf. sind die Angaben nachzureichen.

Soweit übermittelte personenbezogene Daten in oder aus einem Mitgliedstaat der EU betroffen sind, muss der jeweilige Verantwortliche für die Verarbeitung informiert werden.

Die Verletzung des Schutzes personenbezogener Daten ist zu dokumentieren:

- Tatsachen
- Auswirkungen
- ergriffene Abhilfemaßnahmen

Kontaktdaten:

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

_____

_____

Tel.: _____

E-Mail: _____

4 Mitgeltende Unterlagen

Meldung an den Bundesbeauftragten für Datenschutz

§ 42 Strafvorschriften

Dokumentation des Vorfalls

Information des Verantwortlichen in anderen EU-Mitgliedstaaten

Anhang 19

Anweisung: Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten

Vorlage

1 Zweck

In dieser Verfahrensanweisung wird geregelt, in welchen Fällen eine Benachrichtigung von betroffenen Personen bei Verletzungen des Schutzes personenbezogener Daten zu erfolgen hat.

2 Anwendungsbereich

Die vorliegende Verfahrensanweisung gilt für den Verantwortlichen der Verarbeitung personenbezogener Daten bzw. den Datenschutzbeauftragten.

3 Verfahren

Verantwortlicher für die Verarbeitung

Im Fall von Verletzungen des Schutzes personenbezogener Daten, die voraussichtlich eine erhebliche Gefahr für die Rechtsgüter der betroffenen Person darstellen, muss eine Benachrichtigung der betroffenen Person durch den Verantwortlichen für die Verarbeitung erfolgen.

Anforderungen an die Benachrichtigung sind:

- Verwendung einer klaren, einfachen Sprache
- Beschreibung der Verletzung
- Kontaktdaten des Datenschutzbeauftragten oder Verantwortlichen
- Beschreibung der wahrscheinlichen Folgen der Verletzung
- Beschreibung der ergriffenen und geplanten Maßnahmen.

Die Benachrichtigung muss dann nicht erfolgen, wenn

- geeignete technische und organisatorische Vorkehrungen getroffen wurden, um den Erfolg der Verletzung abzuwenden, z. B. Verschlüsselung von Daten,
- im Anschluss Maßnahmen getroffen wurden, die den Erfolg der Verletzung abwenden,
- ein unverhältnismäßiger Aufwand besteht.

Die Benachrichtigung kann eingeschränkt oder verschoben werden, soweit

- die Erfüllung der Ahndung von Straftaten (§ 45 BDSG)
- die öffentliche Sicherheit oder
- Rechtsgüter Dritter

gefährdet würden.

4 Mitgeltende Unterlagen

Benachrichtigung an den Betroffenen

§ 42 Strafvorschriften

Vorlage

Checkliste zu Grundsätzen der Verarbeitung personenbezogener Daten

Kriterium	Rechtsgrund	Kommentare	Verantwortlich	Termin	Erledigt am:
Die Verarbeitung ist rechtmäßig.	Art. 5 Abs. 1 a				
Die Verarbeitung erfolgt nach Treu und Glauben.	Art. 5 Abs. 1 a				
Die Transparenzpflichten sind eingehalten.	Art. 5 Abs. 1 a, EG 58				
Alle Informationen und Mitteilungen zur Verarbeitung sind leicht erreichbar.	EG 39				
Alle Informationen und Mitteilungen zur Verarbeitung sind verständlich und in klarer, einfacher Sprache verfasst.	EG 39				
Der Umfang der Verarbeitung ist dokumentiert.	EG 39				
Die Zwecke der Verarbeitung sind dokumentiert.	EG 39				
Es werden nur die für die Verarbeitung erforderlichen Daten verarbeitet.	Art. 5 Abs. 1 c				
Die verarbeiteten Daten sind aktuell und sachlich richtig.	Art. 5 Abs. 1 d				
Unrichtige Daten müssen unverzüglich gelöscht und berichtigt werden.	Art. 5 Abs. 1 d				
Es werden kürzestmögliche Löschfristen gewählt.	Art. 5 Abs. 1 e				
Die Daten werden vor unbefugter und unrechtmäßiger Verarbeitung geschützt.	Art. 5 Abs. 1 f				
Die Daten werden vor unbeabsichtigter Zerstörung und Schädigung geschützt.	Art. 5 Abs. 1 f				
Die Maßnahmen zu Vorgenanntem sind nachweisbar.	Art. 5 Abs. 2				

Anhang 21

Vorlage

Information an den Betroffenen nach Artikel 13
(Anschreiben aller Kunden, Integration in neue Kundenverträge)

Wir, die xy GmbH, informieren Sie nach Artikel 13 der EU-Datenschutz-Grundverordnung (EU-DSGVO) gern und ausführlich über die Verarbeitung Ihrer personenbezogenen Daten, z. B. Adresse, Ansprechpartner, Funktion, Telefonnummern.

Mit der EU-DSGVO sind uns Pflichten auferlegt worden, um den Schutz Ihrer personenbezogenen Daten bei der Verarbeitung sicherzustellen. Nachfolgend erläutern wir Ihnen, welche Daten wir von Ihnen zu welchen Zwecken verarbeiten und welche Rechte für Sie daraus erwachsen.

Verarbeitung personenbezogener Daten

Die Verarbeitung Ihrer Daten ist zur Erfüllung von Vertragsleistungen notwendig.

Wir verarbeiten Ihre Daten zu folgenden konkreten Zwecken:

Nach Artikel 6 Abs. 1 b) der EU-DSGVO auf der Basis des mit Ihnen geschlossenen Vertrages:

- Erfüllung der Vertragsleistung
- Zahlungsabwicklung
- Lieferung vertraglich bestellter Produkte und Leistungen
- Übermittlung Ihrer Adressdaten an Logistikunternehmen für die Lieferung der Waren
- Übermittlung Ihrer Kontaktdaten an .....
  - ..... gilt nach dem Angemessenheitsbeschluss der EU-Kommission vom 19. Oktober 2010 als sicheres Drittland. Informationen zu anerkannten sicheren Drittländern finden Sie auf der EU-Website: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Nach Artikel 6 Abs. 1 a) der EU-DSGVO auf der Basis der von Ihnen gegebenen Einwilligung

- Zusendung interessanter Informationen über Produkte und Aktionen
- Übermittlung Ihrer Kontaktdaten an unseren Außendienst ..... zum Zwecke der individuellen Kundenbetreuung.

Dauer der Verarbeitung

Wir verarbeiten Ihre Daten nur so lange, wie es zur Erfüllung der vertraglichen Leistungen und Pflege der Kundenbeziehung erforderlich ist.

Wir halten die gesetzlichen Aufbewahrungs- und Speicherfristen nach den Vorgaben des HGB (höchstens 6 und 10 Jahre) ein.

Soweit Sie nicht widersprechen, werden wir Ihre Daten zur Pflege und Intensivierung unserer Geschäftsbeziehung zu beiderseitigem Vorteil nutzen.

Sollten Sie eine Löschung Ihrer Daten wünschen, werden wir entsprechende Maßnahmen unverzüglich einleiten unter der Voraussetzung, dass rechtliche Anforderungen dabei nicht berührt werden und unserem Tun entgegenstehen.

Ihre Rechte als betroffene Person

Gemäß EU-DSGVO haben Sie das Recht auf:

- Auskunft über die Verarbeitung Ihrer Daten
- Berichtigung oder Löschung Ihrer Daten
- Einschränkung der Verarbeitung (nur noch Speicherung möglich)
- Widerspruch gegen die Verarbeitung

- Datenübertragbarkeit
- Widerruf Ihrer gegebenen Einwilligung mit Wirkung auf die Zukunft
- Beschwerde bei der Datenschutz-Aufsichtsbehörde. Zuständig ist die Aufsichtsbehörde des Hauptsitzes/Wohnorts.

Sie haben weiterhin das Recht, eine Bestätigung über die Verarbeitung Ihrer personenbezogenen Daten zu erlangen mit Blick auf

- Verarbeitungszwecke,
- Kategorien der personenbezogenen Daten,
- Wissenschaft, Statistik, Forschungszwecke.

Bei **Fragen** wenden Sie sich bitte vertrauensvoll an die **Datenschutzbeauftragte**:

Anhang 22

Information an den Betroffenen nach Artikel 13
(Anschreiben aller Lieferanten, Integration in neue Lieferverträge oder AGB)

Vorlage

Wir, die xy GmbH, informieren Sie nach Artikel 13 der EU-Datenschutz-Grundverordnung (EU-DSGVO) gern und ausführlich über die Verarbeitung Ihrer personenbezogenen Daten, z. B. Adresse, Ansprechpartner, Funktion, Telefonnummern.

Mit der EU-DSGVO sind uns Pflichten auferlegt worden, um den Schutz Ihrer personenbezogenen Daten bei der Verarbeitung sicherzustellen. Nachfolgend erläutern wir Ihnen, welche Daten wir von Ihnen zu welchen Zwecken verarbeiten und welche Rechte für Sie daraus erwachsen.

Verarbeitung personenbezogener Daten

Die Verarbeitung Ihrer Daten ist zur Erfüllung von Vertragsleistungen notwendig.

Wir verarbeiten Ihre Daten zu folgenden konkreten Zwecken:

Nach Artikel 6 Abs. 1 b) der EU-DSGVO auf der Basis des mit Ihnen geschlossenen Vertrages:

- Erfüllung der Vertragsleistung
- Zahlungsabwicklung
- Lieferung vertraglich bestellter Produkte und Leistungen
- Übermittlung Ihrer Adressdaten an Logistikunternehmen für die Lieferung der Waren
- Übermittlung Ihrer Kontaktdaten an .....
  - ..... gilt nach dem Angemessenheitsbeschluss der EU-Kommission vom 19. Oktober 2010 als sicheres Drittland. Informationen zu anerkannten sicheren Drittländern finden Sie auf der EU-Website: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Dauer der Verarbeitung

Wir verarbeiten Ihre Daten nur so lange, wie es zur Erfüllung der vertraglichen Leistungen und Pflege der Kundenbeziehung erforderlich ist.

Wir halten die gesetzlichen Aufbewahrungs- und Speicherfristen nach den Vorgaben des HGB (höchstens 6 und 10 Jahre) ein.

Soweit Sie nicht widersprechen, werden wir Ihre Daten zur Pflege und Intensivierung unserer Geschäftsbeziehung zu beiderseitigem Vorteil nutzen.

Sollten Sie eine Löschung Ihrer Daten wünschen, werden wir entsprechende Maßnahmen unverzüglich einleiten unter der Voraussetzung, dass rechtliche Anforderungen dabei nicht berührt werden und unserem Tun entgegenstehen.

Ihre Rechte als betroffene Person

Gemäß EU-DSGVO haben Sie das Recht auf:

- Auskunft über die Verarbeitung Ihrer Daten
- Berichtigung oder Löschung Ihrer Daten
- Einschränkung der Verarbeitung (nur noch Speicherung möglich)
- Widerspruch gegen die Verarbeitung
- Datenübertragbarkeit
- Widerruf Ihrer gegebenen Einwilligung mit Wirkung auf die Zukunft
- Beschwerde bei der Datenschutz-Aufsichtsbehörde. Zuständig ist die Aufsichtsbehörde des Hauptsitzes/Wohnorts.

Sie haben weiterhin das Recht, eine Bestätigung über die Verarbeitung Ihrer personenbezogenen Daten zu erlangen mit Blick auf

- Verarbeitungszwecke,
- Kategorien der personenbezogenen Daten,
- Wissenschaft, Statistik, Forschungszwecke.

Bei **Fragen** wenden Sie sich bitte vertrauensvoll an die **Datenschutzbeauftragte**:

Basis EU-Datenschutz-Grundverordnung (GAP Analyse für den nicht-öffentlichen Bereich)

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
Art. 5 – EU-DSGVO – Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten	(1) a)	EG 39, EG 44, EG 45, EG 46, EG 47, EG 60, EG 61, EG 62, EG 64, EG 65	Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, EG 68	Nachvollziehbarkeit heißt Information der Betroffenen (Wie soll informiert werden? An wen? Inhalte der Information festlegen) Folgende Personengruppen sind zu informieren: – Kunden – Lieferanten – Lieferanten von Leistungen – Mitarbeiter/innen – Leiharbeitnehmer u. a.	A	24.05.2018			
	(1) b)	EG 39, EG 50	Verarbeitung für festgelegte, eindeutige und legitime Zwecke (Zweckbindung). Ausnahme: Artikel 89 Absatz 1	Information an die Personengruppen muss den Zweck der Verarbeitung der personenbezogenen Daten enthalten	A	24.05.2018			
	(1) c)	EG 39, EG 67	Grundsatz der Datenminimierung einhalten	nur absolut notwendige personenbezogene Daten erheben und verarbeiten (Rechtsbindung/Datenminimierung)	A	24.05.2018			
	(1) d)	EG 39, EG 59, EG 63, EG 65	Richtigkeit der Daten	Möglichkeit für den Betroffenen eröffnen, die Aktualität der Daten zu prüfen, Betroffener hat jederzeitiges Recht zur Berichtigung oder Löschung unrichtiger Daten	A	24.05.2018			

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
	(1) f)	EG 39, EG 78	Geeignete technische und organisatorische Maßnahmen zum Auslesen der personenbezogenen Daten gewährleisten (im Fall des Verlangens der Löschung oder bei Weggang von Mitarbeiter/innen) Ausnahme: Artikel 89 Absatz 1	Löschung oder Berichtigung von Daten muss leicht möglich sein, ggf. Getrennthaltung von pflichtgemäß zu archivierenden und anderen personenbezogenen Daten	A	24.05.2018			
	(1) f)	EG 39	Integrität und Vertraulichkeit: angemessene Sicherheit bei der Verarbeitung personenbezogener Daten, Schutz vor unbefugter und unrechtmäßiger Verarbeitung	Zugang zu EDV-Anlagen schützen, befugten Personenkreis festlegen, Zugriffsregelungen treffen, technisches und organisatorisches Schutzkonzept aufstellen, Datenschutzvereinbarungen mit den mit der Verarbeitung personenbezogener Daten beauftragten Personen schriftlich treffen	A	24.05.2018			
	(1) e)	EG 39	zweckgebundene Speicherbegrenzung auf das notwendige Maß	Speicherfrist festlegen und dem Betroffenen bekannt geben, Frist der Überprüfung der Speicherfrist bekannt geben	A	24.05.2018			
	2	EG 39, EG 49		schriftliche Festlegungen treffen zur Nachweisbarkeit der Handlungen im Datenschutz	B	Juni 18			

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
Art. 6 – EU-DSGVO – Rechtmäßigkeit der Verarbeitung	(1) a)	EG 40, EG 32	Einwilligung des Betroffenen unter Nennung des Zwecks vorhanden und nachweisbar	Einwilligungserklärungen prüfen auf Vorhandensein bzw. hinsichtlich der Angabe der Zweckbindung, Einwilligung bedarf einer aktiven Handlung, Prüfung auf ggf. Umstellung der Systeme auf eindeutigende bestätigende Handlung, Prüfung, ob sich der ursprüngliche Zweck und damit die Einwilligungserklärung des Betroffenen geändert hat, neue Einwilligungserklärung einholen oder Daten löschen/vernichten	A	24.05.2018			
	(1) b)	EG 44	Zulässigkeit der Verarbeitung zur Erfüllung eines Vertrags	Prüfung der Grundlage der Verarbeitung und Rechtmäßigkeit	A	24.05.2018			
	(1) c)	EG 45	Zulässigkeit der Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung	Prüfung der Grundlage der Verarbeitung und Rechtmäßigkeit	A	24.05.2018			
	(1) d)	EG 46	Zulässigkeit wegen Erfüllung lebenswichtiger Interessen	Prüfung der Grundlage der Verarbeitung und Rechtmäßigkeit	A	24.05.2018			
	(1) e)	EG 45	Zulässigkeit wegen Wahrnehmung öffentlichen Interesses	Prüfung der Grundlage der Verarbeitung und Rechtmäßigkeit	A	24.05.2018			

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
	(1) f)	EG 47	Zulässigkeit wegen Wahrnehmung berechtigter Interessen des Verantwortlichen oder dessen Beauftragten unter Abwägung, ob schutzwürdiges Interesse überwiegt	Prüfung der Grundlage der Verarbeitung und Rechtmäßigkeit	A	24.05.2018			
Art. 7 – EU-DSGVO – Bedingungen für die Einwilligung	1	EG 32, EG 40, EG 42	Nachweis der Einwilligung	schriftlicher Nachweis der Einwilligung	A	24.05.2018			
	2	EG 42	Einwilligung des Betroffenen von anderen Texten optisch hervorheben, in einfacher, verständlicher Sprache verfassen, leicht zugänglich halten	Prüfung und ggf. Neufassung der Einwilligungserklärungen	A	24.05.2018			
	3	EG 42, EG 59	Recht auf jederzeitigen Widerruf der Einwilligungserklärung	Recht in der Einwilligungserklärung verankern auf jederzeitigen Widerruf der Einwilligung	A	24.05.2018			
	4	EG 42, EG 43	Freiwilligkeit der Einwilligung	Beurteilung durchführen, ob die Einwilligung freiwillig oder abhängig erteilt wurde (bei Lieferanten, Dienstleistern, Beschäftigten)	A	24.05.2018			
Art. 9 – EU-DSGVO – Verarbeitung besonderer Kategorien personenbezogener Daten	1	EG 34, EG 35, EG 51, EG 52–54	Untersagung der Verarbeitung beonderer Kategorien personenbezogener Daten gemäß Definition Art. 9 (1)	Kontrolle durchführen, ob besondere Kategorien personenbezogener Daten unrechtmäßig verarbeitet werden	A	24.05.2018			

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
	2 a)–j)	EG 34, EG 35, EG 51, EG 52–54	Regelung der Ausnah-men für die Untersagung	Prüfung, ob die verarbei-tung besoderer Kategorien personenbezogener Daten diesen Ausnahmen unter-liegt	A	24.05.2018			
Art. 12 – EU-DSGVO – Transparente Infor-mation, Kommunika-tion und Modalitäten für die Ausübung der Rechte der betroffe-nen Person	1	EG 39, EG 58, EG 59, EG 60	Informationspflichten gemäß den Artikeln 13 und 14 und Mitteilungs-pflichten gemäß den Artikeln 15–22 und Ar-tikel 34	Prüfung auf Erfüllung der Informations- und Mittei-lungspflichten	A	24.05.2018			
Art. 13 – EU-DSGVO – Informationspflicht bei Erhebung von per-sonenbezogenen Daten bei der betrof-fenen Person	1	EG 39, EG 60, EG 61, EG 62	Informationspflicht zum Zeitpunkt der Erhebung personenbezogener Daten	Umsetzung der Informati-onspflichten gemäß Checkliste Artikel 13 und 14 EU-DSGVO	A	24.05.2018			
Art. 14 – EU-DSGVO – Informationspflicht, wenn die personen-bezogenen Daten nicht bei der betroffe-nen Person erhoben wurden	1	EG 39, EG 60, EG 61, EG 62	Informationspflicht zum Zeitpunkt der Erhebung personenbezogener Daten	Umsetzung der Informati-onspflichten gemäß Checkliste Artikel 13 und 14 EU-DSGVO	A	24.05.2018			
Art. 15 – EU-DSGVO – Auskunftsrecht der betroffenen Person	1	EG 63, EG 64	Recht auf Auskunft, welche personenbezoge-nen Daten verarbeitet werden	Umsetzung der Auskunfts-pflichten gemäß Check-liste	A	24.05.2018			

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
	2	EG 61, EG 63, EG 64	Recht der betroffenen Person auf Auskunft, welche Garantien gemäß Art. 46 der Datensicherheit bestehen bei Übermittlung der Daten in Drittländer oder an eine internationale Organisation	Umsetzung der Auskunftspflichten	A	24.05.2018			
	3	EG 61	Erstellung einer Kopie der personenbezogenen Daten, weitere ggf. gegen Entgelt	Kopie der Zusammenstellung der übermittelten personenbezogenen Daten	A	24.05.2018			
	4	EG 61	keine Beeinträchtigung der Freiheiten des Betroffenen wegen Abforderung einer Kopie	keine Benachteiligung des Betroffenen gewährleisten	A	ständig			
Art. 16 – EU-DSGVO – Recht auf Berichtigung		EG 59	Recht auf unverzügliche Berichtigung und Vervollständigung unvollständiger Daten	Verfahren für Beantragung der Korrektur personenbezogener Daten festlegen und Bearbeitungsfrist determinieren, in der EU-DSGVO wird von einer Frist von 1 Monat ausgegangen	B	Juni 18			
Art. 17 – EU-DSGVO – Recht auf Löschung („Recht auf Vergessen-werden“	1	EG 65, EG 66	Recht auf Löschung der Daten	Prüfung des Rechts und der Pflicht auf Löschung der Daten gemäß Checkliste	B	Juni 18			

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
	2	EG 65, EG 66	wurden die Daten öffentlich gemacht, so muss unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten auf angemessene Art und Weise eine Information erfolgen, dass die betroffene Person einen Antrag auf Löschung gestellt hat	Umsetzung der Forderung, Verfahren im Vorfeld bestimmen und dokumentieren	B	bei Vorliegen des Sachverhalts			
	3	EG 65	Ausnahmen von der Löschung	Umsetzung der Checkliste	B	bei Vorliegen des Sachverhalts			
Art. 18 – EU-DSGVO – Recht auf Einschränkung der Verarbeitung	1	EG 67	Recht auf Einschränkung der Verarbeitung gemäß speziellen Voraussetzungen	Umsetzung der Checkliste zur Feststellung, ob ein Recht zur Einschränkung der Verarbeitung besteht	B	bei Vorliegen des Sachverhalts			
	2	EG 67	bei Einschränkung der Verarbeitung nur mit Willen des Betroffenen oder zur Verteidigung von Rechtsansprüchen Verarbeitungsmöglichkeit	Verfahren festlegen, Hinweis auf Beschränkung der Verarbeitung unmissverständlich geben	B	bis Ende 2018			
	3		Unterrichtung vor erster Verarbeitung	Verfahren festlegen	B	bis Ende 2018			

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
Art. 19 – EU-DSGVO – Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personen-bezogener Daten oder der Einschränkung der Verarbeitung		EG 66	Mitteilungspflicht an alle Empfänger	Verfahren festlegen	B	bis Ende 2018			
Art. 20 – EU-DSGVO – Recht auf Datenüber-tragbarkeit	1	EG 68	Recht auf Datenüber-tragbarkeit, Erhalt der Daten in einem gängi-gen, strukturierten und maschinenlesbaren Format	Verfahren festlegen	B	bis Ende 2018			
	(1) a)	EG 68	zu realisieren, wenn Ver-arbeitung auf Einwil-ligung oder Vertrag beruht	Verfahren festlegen	B	bis Ende 2018			
	(1) b)	EG 68	zu realisieren, wenn Ver-arbeitung automatisiert erfolgt	Verfahren festlegen	B	bis Ende 2018			
	2	EG 68	Recht auf Erwirken der direkten Übermittlung zum nächsten Verant-wortlichen	Verfahren festlegen	B	bis Ende 2018			
Art. 22 – EU-DSGVO – Automatisierte Ent-scheidungen im Ein-zelfall einschließlich Profiling	1	EG 71, EG 72	keine Unterwerfung unter eine automati-sierte Verarbeitung ein-schließlich Profiling	Prüfung vor Verarbeitung	B	bei Vorlie-gen des Sachver-halts			

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
	a)	EG 71, EG 72	Ausnahme: für Abschluss/Erfüllung eines Vertrags wichtig	Prüfung vor Verarbeitung	B	bei Vorliegen des Sachverhalts			
	b)	EG 71, EG 72	Ausnahme: wegen geltender Rechtsvorschriften	Prüfung vor Verarbeitung	B	bei Vorliegen des Sachverhalts			
	c)	EG 71, EG 72	mit ausdrücklichem Willen des Betroffenen	Prüfung vor Verarbeitung	B	bei Vorliegen des Sachverhalts			
Art. 24 – EU-DSGVO – Verantwortlicher und Auftragsverarbeiter Allgemeine Pflichten Verantwortung des für die Verarbeitung Verantwortlichen	1	EG 74, EG 75, EG 76	Einsatz geeigneter technischer und organisatorischer Maßnahmen unter Berücksichtigung der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Schwere des Risikos	Risikoabschätzung durchführen, geeignete technische und organisatorische Maßnahmen treffen und diese regelmäßig überprüfen, Regelung von Verantwortung und Haftung	A	24.05.2018			
	2	EG 74, EG 75, EG 76	Anwendung geeigneter Datenschutzmaßnahmen durch Verantwortlichen für die Verarbeitung	Datenschutzmaßnahmen festlegen	A	24.05.2018			
	3	EG 77	Nachweis ordnungsgemäßer Verarbeitung kann durch Verhaltensregeln Art. 40 oder durch Zertifizierung gemäß Art. 42 nachgewiesen werden	Anforderungen Art. 40 umsetzen oder Zertifizierungsverfahren einleiten	A	31.12.2018			

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
Art. 25 – EU-DSGVO – Datenschutz durch Technikgestaltung und durch daten-schutzfreundliche Voreinstellungen	1	EG 77, EG 78, EG 79	Einsatz geeigneter tech-nischer und organisato-rischer Maßnahmen unter Berücksichtigung der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Schwere des Risikos	geeignete technische und organisatorische Maß-nahmen treffen und diese regelmäßig überprüfen, Maßnahmen, z. B. der Pseudonymisierung, er-greifen, um den Daten-schutzgrundsätzen und der Datenminimierung zu genügen	A	24.05.2018			
	2	EG 77, EG 78, EG 79	Sicherstellung, dass personenbezogene Daten durch Voreinstel-lungen nicht ohne Ein-greifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden	Verfahren ableiten. Tech-nische und organisatori-sche Maßnahmen ergrei-fen	A	24.05.2018			
	3	EG 77, EG 78, EG 79	Nachweis der guten Ver-arbeitungspraxis durch Zertifizierungsverfahren	Zertifizierung anstreben	A	31.12.2018			
Art. 28 – EU-DSGVO – Auftragsverarbeiter	1	EG 77, EG 78, EG 81, EG 83, EG 84	Vergewissern, dass beim Auftragsverarbeiter ge-eignete technische und organisatorische Maß-nahmen im Einklang mit der EU-DSGVO ergriffen wurden	Datenschutzaudit durch-führen, klare vertragliche Regelungen mit Auftrags-verarbeitern	A	24.05.2018			

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
	2	EG 81	keine Unterbeauftra-gung weitere Auftrags-verarbeiter ohne Kennt-nis des Verantwort-lichen, Information über jede beabsichtigte Än-derung	vertragliche Regelung	A	24.05.2018			
	3	EG 79, EG 81, EG 86, EG 87	Auftragsverarbeitung auf der Grundlage eines schriftlichen Vertrags oder eines anderen Rechtsinstruments	Vertrag fertigen mit Inhal-ten zu: Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verar-beitung, Art der personen-bezogenen Daten, Kategorien betroffener Personen, Pflichten und Rechte des Verantwortlichen, Check-liste zu den Vertragsinhal-ten anwenden	A	24.05.2018			
Art.29 – EU-DSGVO – Verarbeitung unter der Aufsicht des Ver-antwortlichen oder des Auftragsverarbei-ters		EG 79	Arbeit ausschließlich auf Weisung des Verant-wortlichen	vertragliche Regelung	A	24.05.2018			

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
Art. 30 – EU-DSGVO – Verzeichnis von Ver-arbeitungstätigkeiten	1	EG 82	Pflicht der Führung eines Verzeichnisses aller Ver-arbeitungstätigkeiten durch den Verantwort-lichen	Verarbeitungsverzeichnis erstellen mit Kontaktdaten des Verantwortlichen, dessen Vertreter, des Da-tenschutzbeauftragten, mit dem Zweck der Ver-arbeitung, der Beschrei-bung der Kategorien be-troffener Personen und Daten, der Empfänger, ggf. Übermittlungen in ein Drittland, mit Fristen der Löschung, mit allgemeiner Beschreibung der tech-nischen und organisatori-schen Maßnahmen gemäß Art. 32	A	24.05.2018			
	2	EG 82	Pflicht der Führung eines Verzeichnisses aller Ver-arbeitungstätigkeiten durch den Auftragsver-arbeiter	siehe oben	A	24.05.2018			
	3	EG 82	schriftliches Verarbei-tungsverzeichnis	schriftliches Verarbei-tungsverzeichnis vom Auf-tragsverarbeiter abfordern	A	24.05.2018			
	4	EG 82	Verarbeitungsverzeich-nis der Behörde auf Antrag zur Verfügung stellen		A	24.05.2018			
	5	EG 82	gilt nicht für KMU unter 250 Beschäftigten						

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
Art. 32 – EU-DSGVO – Sicherheit der Verarbeitung	1	EG 83	Gewährleistung eines angemessenen Schutzniveaus: Pseudonymisierung und Verschlüsselung personenbezogener Daten, Sicherstellen von Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit der Systeme und Dienste, rasche Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem Zwischenfall, Einführung eines wiederkehrenden Verfahrens zur Evaluierung der Eignung getroffener Maßnahmen	Treffen technischer und organisatorischer Maßnahmen unter Abschätzung des Risikos	A	24.05.2018			
	2	EG 83, EG 84	Berücksichtigung von Risiken	Risikoabschätzung durchführen	A	24.05.2018			
	3	EG 83, EG 84	Einhaltung der Verhaltensregeln oder Zertifizierung als Nachweis ordnungsgemäßen Handelns	Einhaltung der Verhaltensregeln überprüfen, z. B. im Datenschutzaudit oder Zertifizierungsverfahren	A	31.12.2018			
	4	EG 83, EG 84	Sicherstellung der Verarbeitung personenbezogener Daten nur auf Anweisung des Verantwortlichen	Anweisungen im Datenschutz treffen	A	31.12.2018			

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
Art. 33 – EU-DSGVO – Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde	1	EG 85	Meldung bei Verletzung des Schutzes von Daten binnen 72 h an die Behörde	Meldeverfahren etablieren	A	24.05.2018			
	2	EG 85	Meldung von Schäden durch Auftragsverarbeiter an den Verantwortlichen	Meldeverfahren etablieren	A	24.05.2018			
	3	EG 88	Inhalt der Meldung ist vorgegeben	Meldeverfahren etablieren	A	24.05.2018			
	5	EG 85	Dokumentation der Verletzungen des Schutzes personenbezogener Daten, auch zur Vorlage bei der Behörde		A	bei Eintritt des Sachverhalts			
Art. 34 – EU-DSGVO – Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person	1	EG 86	bei hohen Risiken unverzügliche Benachrichtigung der betroffenen Person über Verletzungen des Datenschutzes	Verfahren ausarbeiten	A	24.05.2018			
	2	EG 86	Benachrichtigung in klarer, verständlicher Sprache		A	bei Eintritt des Sachverhalts			
	3	EG 89	Benachrichtigung entfällt unter gewissen Voraussetzungen	Verfahren ausarbeiten und Ausnahmen berücksichtigen	A	24.05.2018			
Art. 35 – EU-DSGVO – Datenschutz-Folgeabschätzung	1	EG 89, EG 90, EG 91	Datenschutz-Folgeabschätzung bei hohem Risiko	Datenschutz-Folgeabschätzung vornehmen		24.05.2018			

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
	2		Einbezug des Daten-schutzbeauftragten, sofern benannt		A	bei Eintritt des Sach-verhalts			
	3	EG 90, EG 91	Datenschutz-Folge-abschätzung zwingend notwendig in beschrie-benen Fällen ebenda	Datenschutz-Folge-abschätzung durchführen		24.05.2018			
	4	EG 92	Aufsichtsbehörde kann Liste erlassen mit not-wendigen Fällen für Datenschutz-Folge-abschätzungen	Liste interpretieren und auf Umsetzungsnotwen-digkeit prüfen					
	7		festgelegte Inhalte für Datenschutz-Folge-abschätzung	Formblatt erarbeiten	A	24.05.2018			
Art. 36 – EU-DSGVO – Vorherige Konsulta-tion	1	EG 94	gilt für hohes Risiko und keine adäquaten Schutz-maßnahmen	Konsultation vor Verarbei-tung der Behörde erforder-lich					
Art. 37 – EU-DSGVO – Benennung eines Da-tenschutzbeauftrag-ten	1	EG 97	Benennung eines Daten-schutzbeauftragten gemäß Voraussetzungen wie benannt	schriftliche Bestellung des Datenschutzbeauftragten					
	7	EG 97	Veröffentlichung der Kontaktdaten notwendig	Veröffentlichung Kontakt-daten		24.05.2018			
Art. 38 – EU-DSGVO – Stellung des Daten-schutzbeauftragten	3	EG 97	Weisungsfreiheit ge-währleisten		A	24.05.2018			

Artikel		Erwägungs-grund	wesentliche Inhalte	Handlungsbedarf	Priorität (a–c)	Termin	Verant-wortlichkeit	Erledigt	Wirksam-keitsprüfung
Art. 39 – EU-DSGVO – Aufgaben des Daten-schutzbeauftragten	1	EG 97	Unterrichtung, Beratung, Überwachung der Ein-haltung der Verordnung, Zusammenarbeit mit Aufsichtsbehörde, An-laufstelle für die Auf-sichtsbehörde, DSB trägt dem Risiko Rech-nung	Datenschutzbeauftragten bestellen		24.05.2018			
Art. 40 – EU-DSGVO – Verhaltensregeln	1	EG 98	Förderung der Verab-schiedung von Verhal-tensregeln für Kleinst-unternehmen	Einhaltung der Verhaltens-regeln überprüfen, z. B. im Datenschutzaudit oder Zertifizierungsverfahren					
Art. 44 – EU-DSGVO – Allgemeine Grund-sätze der Datenüber-mittlung		EG 111	Zulässigkeit der Über-mittlung an ein Drittland oder eine internationale Organisation unter Be-rücksichtigung der unter Art. 45 benannten Be-dingungen	Checkliste berücksichtigen zur Prüfung der Zulässig-keit einer Datenübermitt-lung					

Zusatzmaterial zu diesem Titel erhalten Sie kostenlos unter www.beuth-mediathek.de – den Media-Code finden Sie im Buch auf der gelben Seite.

Die Autorin

Dr. Grit Reimann ist seit vielen Jahren als Datenschutzbeauftragte für Unternehmen tätig. Ihre methodischen Kenntnisse in der praktischen Umsetzung gibt sie als Unternehmensberaterin, Auditorin und Trainerin weiter.

PRAXIS

Die Verarbeitung personenbezogener Daten unterliegt datenschutzrechtlichen Regelungen, deren Nicht-Einhaltung zu empfindlichen Strafen führen kann.

Dieser Band bietet eine leicht verständlich geschriebene und praxisorientierte Einführung in die Thematik und versteht sich als Handlungsanleitung für den Datenschutzbeauftragten im nicht-öffentlichen Bereich.

Zahlreiche Best-Practice-Lösungen helfen ihm bei der schnellen Umsetzung seiner Aufgaben. Die enthaltenen, über die Beuth-Mediathek auch digital kostenlos zugänglichen Mustervorlagen können leicht an die eigenen Belange angepasst werden.

Die Autorin versteht es, die grundlegenden Aspekte des Datenschutzes in einfacher und verständlicher Form zu erläutern.

Diese 2., vollständig überarbeitete und erweiterte Auflage berücksichtigt die am 25.5.2018 in Kraft getretene EU-Datenschutz-Grundverordnung.

ISBN 978-3-410-27981-5
9 783410 279815

Aus dem Inhalt:

- Aufbau und wesentliche Inhalte der EU-DSGVO
- Personenbezogene Daten und ausgewählte Inhalte der EU-DSGVO sowie des BDSG 2018
- Der Datenschutzbeauftragte (DSB)
- Technische und organisatorische Maßnahmen im Datenschutz
- Datenschutz-Folgeabschätzung, Risikobewertung, Schutzstufenkonzept
- Betriebliche Regelungen für den Datenschutz
- Auftragsdatenverarbeitung
- Übermittlung personenbezogener Daten in Drittstaaten und internationale Organisationen
- Datenschutz im Personalwesen – Bewerbungsverfahren
- Vertragliche Regelungen mit Dienstleistern
- Schulungen und Unterweisungen
- Datenschutzkonzept und Datenschutzhandbuch
- Liste der Mindestregelungen im betrieblichen Datenschutz
- Sanktionen

www.beuth.de