# Datenschutzrichtlinie MUSTERMANN

**Kommentiert [Helbing1]:** Bitte beachten Sie die Hinweise in der „Anleitung zur Umsetzung“

## Inhaltsverzeichnis

## 1. Gegenstand und Ziel

Der Schutz personenbezogener Daten ist für Mustermann von wesentlicher Bedeutung. Mitarbeiter, Kunden und Geschäftspartner erwarten einen vertrauensvollen Umgang mit ihren Daten. Verstöße gegen Datenschutzbestimmungen können gravierende Folgen, etwa Rufschäden, Schade



Diese Anweisung e … en zum Schutz personenbezogener … erordnung (EU) 2016/679 (Datensch … enschutzgesetz („***BDSG***“).

Eine Übersicht und … nweisung findet sich in der Anlage „D…

Die vorliegende Anweisung enthält keine konkreten Vorgaben zur Datensicherheit (z.B. Verschlüsselung, sicheres Löschen von Daten), diese sind in einer gesonderten Anweisung geregelt.

## 2. Anwendungsbereich

Diese Anweisung gilt für alle Mitarbeiter der Mustermann GmbH in Deutschland („**Unternehmen**“).

**Kommentiert [Helbing2]:** Bitte vollständige Firma und ggf. Standorte eintragen. Bei Konzernen und Unternehmensverbünden bitte den Anwendungsbereich klarstellen.

Sie gilt für jede Verarbeitung personenbezogener Daten (zu den Begriffen siehe unten), wenn diese

- ganz oder teilweise automatisiert erfolgt (z.B. mittels Computern)
- die Daten in einem Dateisystem (Art. 4 Nr. 6 DSGVO) gespeichert sind oder gespeichert werden sollen (z.B. auf einer Festplatte oder in Handakten), oder
- Daten über Mitarbeiter betrifft (z.B. Notizen aus einem Bewerbungsgespräch).

**„*Personenbezogene Daten*“** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Auf die Sensibilität kommt es nicht an.

> *Beispiele: Auch Angaben, die keinen Namen enthalten, sind personenbezogene Daten, wenn mit Hilfe von Zusatzinformation realistischer Weise eine Zuordnung zu einer natürlichen Person möglich ist (z.B. Liste mit Benutzerkennung und System-Anmeldezeiten kann vom Unternehmen problemlos einem Mitarbeiter zugeordnet werden). Auch im Geschäftsverkehr zwischen Unternehmen (B2B) liegen personenbezogene Daten vor, etwa Kontaktdaten von Ansprechpartnern (Herr Robert Schmidt arbeitet im Einkauf der ABC AG).*

**„*Verarbeitung*“** ist jeder Umgang mit personenbezogenen Daten, insbesondere das Erheben (z.B. per Fragebogen), Erfassen (z.B. per Formular, Software oder Kamera), Speichern (z.B. in einer Datenbank, Excel-Datei oder Personalakte), Ändern (z.B. Aktualisieren), Übermitteln (z.B. an eine Behörde oder ein verbundenes Unternehmen), Abgleichen, Verknüpfen, das Sperren oder Löschen.

**„*Betroffener*“** ist die natürliche Person, auf die sich die personenbezogenen Daten beziehen (z.B. Mitarbeiter, Kunde oder Ansprechpartner beim Lieferanten)

Diese Anweisung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten des Unternehmens oder seiner Niederlassung in der Europäischen Union erfolgt (z.B. Das Münchner Verkaufsbüro eines US-Unternehmens sammelt Daten über potentielle deutsche Kunden). Diese Anweisung gilt auch, soweit die Verarbeitung im Rahmen der Tätigkeiten des Unternehmens oder seiner Niederlassung außerhalb der EU erfolgt, wenn die Verarbeitung im Zusammenhang damit steht, Betroffenen in der EU Waren oder Dienstleistungen anzubieten, oder das Verhalten Betroffener in der EU zu beobachten (z.B. Muttergesellschaft in den USA richtet sich gezielt an Kunden in Deutschland).

**Kommentiert [Helbing3]:** Der folgende Absatz kann gestrichen werden, wenn das Unternehmen nur in der EU ansässig ist.

## 3. Rollen und Verantwortlichkeiten

Der nachfolgende Abschnitt zeigt, welche Aufgaben einzelne Mitarbeiter bei der Einhaltung des Datenschutzes haben.



## 3.1 Jeder Mitarb

Jeder Mitarbeiter bea nde Regeln:

- Datenschutzb
- Bei der Verarb nd 6).
- Datenschutzp

## 3.2 Verarbeitung

Wer im Unternehmen für einen Prozess, ein Verfahren oder ein Projekt, bei dem personenbezogene Daten verarbeitet werden, fachlich konzeptionell verantwortlich ist, gilt als „***Verarbeitungs-Verantwortlicher***".

*Beispiele: Die Personalabteilung ist für die Führung von Personalakten verantwortlich, der Leiter Personal ist Verarbeitungs-Verantwortlicher für elektronische Personalakten. Der für die Gebäudesicherheit zuständige Mitarbeiter ist Verarbeitungs-Verantwortlicher einer Videoüberwachung im Eingangsbereich.*

Im Verzeichnis der Verarbeitungstätigkeiten (siehe Ziffer 10) werden die Verarbeitungs-Verantwortlichen für jede Verarbeitungstätigkeit namentlich oder anhand ihrer Funktion (z.B. „Leiter Personal") dokumentiert. Soweit nichts anders festgelegt, ist der jeweilige Abteilungsleiter Verarbeitungs-Verantwortlicher.

Der Verarbeitungs-Verantwortliche beachtet in Bezug auf die ihm zugeordneten Verarbeitungstätigkeiten folgende Vorgaben:

- Bei der Planung, Einführung und später bei der Änderung der Verarbeitungstätigkeit (i) das Formular für den Eintrag ins Verzeichnis der Verarbeitungstätigkeiten und (ii) die Checkliste DSGVO ausfüllen und dem Datenschutz-Manager übergeben (Ziffer 10).
- Den Betroffenen transparent machen, wie mit ihren Daten umgegangen wird (Ziffer 8).
- Bei der Verarbeitung die Einhaltung der Datenschutzgrundsätze sicherstellen (Ziffer 5 und 6).
- Etwaige Regelungen in Betriebsvereinbarungen beachten (Ziffer 7).
- Sicherstellen, dass die Rechte von Betroffenen (z.B. auf Auskunft) erfüllt werden können (Ziffer 9).
- Eine Datenschutzfolgenabschätzung durchführen, wenn der Datenschutz-Manager darauf hinweist (Ziffer 11)
- Wenn Dienstleister für das Unternehmen Daten im Auftrag und nach den Vorgaben des Unternehmens verarbeiten, mit dem Dienstleister Auftragsverarbeitungsverträge schließen und die Dienstleister überwachen (Ziffer 12)
- Bei einer Weitergabe von Daten in nicht-EU Länder die besonderen Anforderungen zum Datenexport beachten (Ziffer 13)
- Alles so dokumentieren, dass die Einhaltung der Vorschriften zum Datenschutz nachweisbar ist (Ziffer 14)

## 3.3 Datenschutz-Manager

Das Unternehmen hat einen Datenschutz-Manager benannt, der bestimmte, in dieser Anweisung näher festgelegte Aufgaben übernimmt. Die Kontaktdaten des Datenschutz-Managers sind im Anhang Kontaktdaten genannt.

Der Datenschutz-Manager stimmt sich im Bedarfsfall mit dem Datenschutzbeauftragten ab (sofern benannt) oder holt externe Expertise ein.

**Kommentiert [Helbing4]:** Spiegelpunkt löschen, wenn kein Datenschutzbeauftragter benannt wurde.

**Kommentiert [Helbing5]:** Begriff „Abteilungsleiter" an die jeweilige Organisationsbezeichnung anpassen. Es ist eine möglichst hohe Position zu wählen, da nur so sichergestellt ist, dass der Abteilungsleiter die Verantwortung entsprechend delegiert.

**Kommentiert [Helbing6]:** Alternativ: „im Intranet einsehbar unter *Link*"

### 3.4 Datensicherheits-Manager

Das Unternehmen hat zudem einen Datensicherheits-Manager benannt. Dieser erfüllt Aufgaben in Bezug auf technische und organisatorische Maßnahmen zur Datensicherheit. Die Kontaktdaten finden



### 3.5 Datenschutzbe

Das Unternehmen hat ktdaten des Datenschutzbeauftragte

Die Aufgaben des Date GVO. Diese sind:

- Unterrichtung u ter zu den Pflichten nach den Datenschutzvorschriften (der EU und Deutschlands).
- Überwachung der Einhaltung der Datenschutzvorschriften.
- Überwachung der Strategien (z.B. Anweisungen/Richtlinien) des Unternehmens zum Datenschutz einschließlich der Verantwortungsverteilung, der Sensibilisierung und Schulung der Mitarbeiter und entsprechender Überprüfungen.
- Zusammenarbeit mit der Datenschutz-Aufsichtsbehörde und Anlaufstelle für diese.

Die Verantwortlichkeit für die Einhaltung der Datenschutzvorschriften verbleibt bei der Unternehmensleitung und den Verarbeitungs-Verantwortlichen.

Mit der vorliegenden Anweisung werden dem Datenschutzbeauftragten keine fachlichen Weisungs- oder Entscheidungsbefugnisse eingeräumt.

> *Beispiel: Der Datenschutzbeauftragte kann keine bestimmten Löschfristen festlegen oder Beschäftigte zur Löschung anweisen, sondern lediglich hierzu beraten und Löschvorgänge kontrollieren.*

## 4. Einbindung und Unterstützung des Datenschutzbeauftragten

Alle Mitarbeiter binden den Datenschutzbeauftragten frühzeitig in sämtliche mit dem Schutz personenbezogener Daten zusammenhängenden Fragen ein (Art. 38 Abs. 1 DSGVO).

> *Beispiele: Es besteht Unsicherheit, ob bestimmte Daten gespeichert werden dürfen, ob spezielle Datenschutzverträge nötig sind oder eine Datenschutzfolgenabschätzung durchzuführen ist.*

Alle Mitarbeiter unterstützen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben, zum Beispiel indem sie ihm auf Anfrage Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen gewähren, Auskünfte erteilen oder Unterlagen aushändigen.

## 5. Rechtskonforme Datenverarbeitung

Alle Mitarbeiter halten bei der Verarbeitung personenbezogener Daten die nachfolgend in Ziffer 5 dargestellten Datenschutzgrundsätze und die weiteren dort genannten Anforderungen ein.

### 5.1 Datenschutzgrundsätze

#### 5.1.1 Rechtmäßigkeit (Art. 5 Abs. 1 a) DSGVO)

Personenbezogene Daten dürfen nur verarbeitet werden, wenn für die Verarbeitung eine Rechtsgrundlage besteht. Sensible Daten (z.B. Gesundheitsdaten) dürfen nur verarbeitet werden, wenn eine Ausnahme vom Verarbeitungsverbot für sensible Daten besteht. (Einzelheiten siehe jeweils Ziffer 6).

#### 5.1.2 Transparenz (Art. 5 Abs. 1 a) DSGVO)

Personenbezogene Daten müssen in einer für den Betroffenen nachvollziehbaren, d.h. in transparenter Weise verarbeitet werden (zu Einzelheiten siehe Ziffer 8).

**Kommentiert [Helbing7]:** Alternativ: „im Intranet einsehbar unter *Link*“

**Kommentiert [Helbing8]:** Ggf. am Ende des Absatzes ergänzen: „Der Datensicherheits-Manager holt zur Aufgabenerfüllung externen Sachverstand ein. Er stimmt sich hierzu vorab mit der Unternehmensleitung ab.“

**Kommentiert [Helbing9]:** Ziffer 3.5 und 4 vollständig streichen, sofern kein Datenschutzbeauftragter zu benennen ist.

*Beispiele: Werden die von Mitarbeitern über geschäftliche Notebooks aufgerufenen Webseiten protokolliert und ausgewertet, muss dies den Mitarbeitern vorher mitgeteilt werden. Formulare für Kunden müssen*



### 5.1.3 Zweckbi

Personenbezogene Zwecke erhoben werden und dürfen den, die mit den ursprünglichen Zwe

*Beispiel: Für Zu Außendarstellung auf der Unterneh*

Sollen Daten später für andere Zwecke verwendet werden als diejenigen, für die sie erhoben wurden, prüft der Verarbeitungs-Verantwortliche die Vereinbarkeit (Art. 6 Abs. 4 DSGVO) der neuen mit den alten Zwecken und dokumentiert das Ergebnis.

*Beispiel: Login- und Logout-Zeiten von Mitarbeitern, die zur Datensicherheit gespeichert werden, sollen zur Arbeitszeitkontrolle genutzt werden.*

Soweit erforderlich aktualisiert der Verarbeitungs-Verantwortliche das Verzeichnis der Verfahrenstätigkeiten bei einer Zweckänderung entsprechend (siehe Ziffer 10.5) und stellt eine nachträgliche Information der Betroffenen sicher (siehe Ziffer 8).

### 5.1.4 Datenminimierung (Art. 5 Abs. 1 c) DSGVO)

Personenbezogene Daten müssen mit Blick auf den konkreten Nutzungszweck angemessen und erheblich sowie auf das notwendige Maß beschränkt sein. Es dürfen mithin nicht unnötig viele Daten zu einer Person oder Daten zu unnötig vielen Personen verarbeitet werden und Daten nicht über das erforderliche Maß hinaus genutzt werden. Bei jedem Datenfeld ist zu fragen, wofür die Daten konkret und wie lange benötigt werden.

*Beispiele: Bei einem Formular zur Bestellung eines Newsletters sind Angaben über Name und Firmenzugehörigkeit des Bestellers in der Regel nicht erforderlich.*

### 5.1.5 Richtigkeit (Art. 5 Abs. 1 d) DSGVO)

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.

*Die zu einem Mitarbeiter gespeicherte Anschrift muss aktuell sein, damit dieser angeschrieben werden kann. Die Angabe der Berufserfahrung im Lebenslauf einer Bewerbung muss hingegen später nicht aktualisiert werden, da die Angaben nur der Kandidatenauswahl zum Zeitpunkt der Bewerbung dienen.*

Der Verarbeitungs-Verantwortliche trifft angemessene Maßnahmen, damit personenbezogene Daten, die unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Der Verarbeitungs-Verantwortliche stellt zudem durch geeignete Maßnahmen die Richtigkeit der Daten sicher.

*Beispiele: Regelmäßige Abfrage der Richtigkeit der Daten beim Betroffenen. Technische Anbindung an ein System, das die jeweils aktuellen Daten bereitstellt.*

### 5.1.6 Speicherbegrenzung (Art. 5 Abs. 1 e) DSGVO)

Personenbezogene Daten müssen gelöscht werden, wenn Sie für den konkreten Nutzungszweck nicht mehr benötigt werden. Statt einer Löschung können Daten auch anonymisiert werden.

*Das Ergebnis aus Assessment Centern verliert nach einigen Jahren seine Relevanz, weil es keine Aussage mehr über die aktuellen Fähigkeiten des Mitarbeiters zulässt. Die Ergebnisse sind zu löschen oder alle Hinweise auf die Identität des Mitarbeiters (Name, Anschrift, Personalnummer) zu schwärzen.*

**Kommentiert [Helbing10]:** Hat das Unternehmen eine Richtlinie zu Löschung oder zur Erstellung von Löschkonzepten, so kann am Ende dieses Abschnitts darauf verwiesen werden. Den Entwurf einer Löschrichtlinie biete ich als Zusatzleistung an.

### 5.1.7 Integrität und Vertraulichkeit (Art. 5 Abs. 1 f) DSGVO)

Soll die Verarbeitung personenbezogener Daten auf Basis einer Einwilligung erfolgen, müssen folgende Anforderungen erfüllt sein (Art. 7, 4 Nr. 11 DSGVO):

- Es muss eine unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung des Betroffenen vorliegen, mit der sich der Betroffene zur Verarbeitung seiner personenbezogenen Daten einverstanden erklärt (Art. 4 Nr. 11 DSGVO). Bloßes Schweigen oder die Nutzung einer Webseite genügen nicht.
- Die Einwilligung muss freiwillig erteilt worden sein. Eine Einwilligung ist ggf. dann unfreiwillig, wenn ein Vertrag von der Abgabe der Einwilligung abhängig gemacht wird (Zwangseinwilligung), verschiedenartige Verarbeitungen in einer einheitlichen Einwilligung verknüpft werden (Alles-oder-Nichts Einwilligung) oder der Betroffene in einem Abhängigkeitsverhältnis zum Unternehmen steht (Art. 7 Abs. 4 DSGVO).
- Die Einwilligung muss für den bestimmten Fall und in informierter Weise erteilt werden. Es müssen insbesondere das verantwortliche Unternehmen, die Daten und Nutzungszwecke genannt sein. Wird die Einwilligung mit anderen Erklärungen verknüpft (z.B. Akzeptanz von AGB) muss sie von den anderen Erklärungen klar zu unterscheiden sein (Art. 7 Abs. 2 DSGVO).
- Bei sensiblen personenbezogenen Daten muss sich die Einwilligung ausdrücklich auf diese beziehen.
- Es muss auf die Widerrufbarkeit der Einwilligung mit Wirkung für die Zukunft hingewiesen werden (Art. 7 Abs. 3 DSGVO).
- Bei Einwilligungen von Kindern unter 16 Jahren im Online-Bereich sind die speziellen Anforderungen des Art. 8 DSGVO zu beachten.

Eine Einwilligung darf nur eingeholt werden, wenn und soweit für die Verarbeitung keine andere gesicherte Rechtsgrundlage besteht.

Einwilligungen von Mitarbeitern, betreffend das Beschäftigungsverhältnis, bedürfen grundsätzlich der Schriftform (z.B. genügt eine online Einwilligung nicht).

Der Verarbeitungs-Verantwortliche stellt sicher, dass

- der Wortlaut der Einwilligung sowie die Umstände der Abgabe sowie jede wesentliche Änderung vorher mit dem Datenschutz-Manager abgestimmt ist
- die Erteilung einer Einwilligung durch einen Betroffenen vom Unternehmen nachgewiesen werden kann, insbesondere die Identität des Einwilligenden, der Zeitpunkt der Abgabe und der Wortlaut der Einwilligung, und
- geeignete Prozesse für den Umgang mit dem Widerruf der Einwilligung implementiert und dokumentiert sind.

## 7. Dienst- und Betriebsvereinbarungen

**Kommentiert [Helbing11]:** Ziffer ggf. streichen oder durch „n/a“ ersetzen, wenn kein Betriebs-/Personalrat besteht.

Rechtsgrundlage für die Verarbeitung personenbezogener Daten – einschließlich sensibler personenbezogener Daten – kann auch eine Betriebsvereinbarung sein.

Wird eine Betriebsvereinbarung verhandelt, die die Verarbeitung personenbezogener Daten zum Gegenstand hat, so beachtet der auf Arbeitgeberseite für die Dienst- und Betriebsvereinbarung Zuständige Folgendes:

In der Dienst- und Betriebsvereinbarung soll angegeben werden, ob und ggf. inwieweit diese als Rechtsgrundlage im Sinne des Datenschutzrechts dient.

Soweit eine Dienst- und Betriebsvereinbarung als Rechtsgrundlage im Sinne des Datenschutzrechts dient, sind die Anforderungen des Art. 88 Abs. 2 DSGVO umzusetzen, d.h. es sind angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde und der berechtigten Interessen und der Grundrechte der Mitarbeiter zu vereinbaren. Dies betrifft etwa Vereinbarungen zur Transparenz der Verarbeitung, ggf. zur Übermittlung an verbundene Unternehmen oder zur Zulässigkeit und zu den Grenzen der Überwachung von Mitarbeitern.

personenbezogenen Daten zur Verfügung zu stellen, die das Unternehmen über ihn verarbeitet (z.B. Ausdruck aller Stammdaten, Korrespondenz und Vertragsdaten eines Kunden).

### 9.1.2 Recht auf Berichtigung (Art. 16 DSGVO)

Betroffene können verlangen, dass das Unternehmen unrichtige personenbezogene Daten unverzüglich berichtigt und – soweit der Zweck der Verarbeitung dies erfordert – unvollständige personenbezogene Daten ergänzt werden.

### 9.1.3 Recht auf Löschung (Art. 17 DSGVO)

Betroffene können – soweit kein Ausschlussgrund nach Art. 17 Abs. 3 DSGVO und § 35 BDSG greift – vom Unternehmen die Löschung sie betreffender personenbezogener Daten verlangen wenn,

- die Daten für den Zweck, für den sie erhoben oder sonst verarbeitet werden, nicht mehr benötigt werden

  *Beispiel: Bewerbungsunterlagen eines abgelehnten Bewerbers werden spätestens sechs Monate nach der Auswahlentscheidung nicht mehr benötigt.*

- der Betroffene seine Datenschutz-Einwilligung widerrufen oder erfolgreich Widerspruch gegen die Datenverarbeitung aufgrund seiner besonderen Situation eingelegt hat (siehe Ziffer 9.1.6) und keine andere Rechtsgrundlage die weitere Verarbeitung erlaubt

  *Beispiel: Ein Kunde (Einzelperson) hat eingewilligt, dass seine Daten verwendet werden, um seine potentiellen Interessen für bestimmte Produkte zu ermitteln. Der Kunde widerruft die Einwilligung. Die ermittelten potentiellen Interessen sind zu löschen.*

- der Betroffene der Nutzung seiner Daten für Direktwerbung (siehe Ziffer 9.1.7) widerspricht
- die Daten unrechtmäßig erhoben wurden
- die Löschung zur Erfüllung einer gesetzlichen Verpflichtung erforderlich ist, oder
- die Daten betreffen ein Onlineangebot, die auf Basis der Einwilligung eines Kindes erhoben wurden, das jünger als 16 Jahre ist.

Hat das Unternehmen die Daten öffentlich gemacht, sind ggf. Dritte gemäß Art. 17 Abs. 2 DSGVO über das Löschbegehren zu informieren.

> *Im Rahmen einer online-Veröffentlichung auf der Unternehmenswebseite wurde über das Ausscheiden eines Mitarbeiters „im Bösen“ berichtet. Der Mitarbeiter stellt einen berechtigten Löschantrag.*

### 9.1.4 Recht auf Sperrung (Einschränkung der Verarbeitung) (Art. 18 DSGVO)

Betroffene können in den nachfolgend genannten Fällen vom Unternehmen verlangen, dass ihre personenbezogenen Daten gesperrt werden. Sperrung bezeichnet das Markieren von Daten mit dem Ziel, dass diese nur noch eingeschränkt verarbeitet werden.

Nach einer Sperrung dürfen die Daten grundsätzlich nur noch gespeichert aber nicht mehr anderweitig verarbeitet werden (z.B. keine Auswertung, keine Nutzung zur Ansprache, keine Leseberechtigung für „einfache“ Nutzer). Eine anderweitige Verarbeitung gesperrter Daten ist nur in den Grenzen des Art. 18 Abs. 2 DSGVO zulässig, etwa im Rahmen von Rechtsstreitigkeiten oder mit Einwilligung des Betroffenen.

Ein Anspruch auf Sperrung besteht in folgenden Fällen:

- Der Betroffene bestreitet die Richtigkeit der über ihn gespeicherten Daten. Während das Unternehmen die Richtigkeit prüft, sind die Daten zu sperren.
- Die Verarbeitung ist unrichtig, der Betroffene verlangt aber statt einer Löschung zunächst nur eine Sperrung.

wird durch den Datenschutz-Manager nachverfolgt.

## 10.3 Einführung von Verarbeitungstätigkeiten

Bis spätestens zum Zeitpunkt der Einführung der Verarbeitungstätigkeit vervollständigt und finalisiert der Verarbeitungs-Verantwortliche den Eintrag für das Verzeichnis der Verarbeitungstätigkeiten und die „Checkliste DSGVO“ und übersendet diese dem Datenschutz-Manager und, sofern benannt, dem Datenschutzbeauftragten.

Sonstige Informationen, die zur Dokumentation der Einhaltung der Vorschriften zum Schutz personenbezogener Daten erforderlich sind, verwahrt der Verarbeitungs-Verantwortliche bei sich.

> *Dies können z.B. sein: Rollen- und Berechtigungskonzepte, Löschkonzepte, Datenbankstrukturen/Listen mit Datenfeldern, Kopien von Datenschutzhinweisen, Dokumentation interner Prozesse und Geschäftsabläufe bei der Datenverarbeitung, Datensicherheitskonzepte, Leistungs- und Funktionsbeschreibungen von Software, Administrationshandbücher, Arbeitsanweisungen, Protokolle zur Datenlöschung*

## 10.4 Durchführung von Verarbeitungstätigkeiten (Regelprüfung)

Der Verarbeitungs-Verantwortliche nimmt in regelmäßigen Abständen sowie anlassbezogen eine Regelprüfung der Verarbeitungstätigkeit vor. Das Intervall der Regelprüfung beträgt:

- bei Risikoklassifizierung „niedrig“: 36 Monate
- bei Risikoklassifizierung „mittel“: 24 Monate
- bei Risikoklassifizierung „hoch“: 12 Monate

Der Termin der nächsten Regelprüfung dokumentiert der Verarbeitungs-Verantwortliche.

Im Rahmen der Regelprüfung prüft der Verarbeitungs-Verantwortliche, ob der Eintrag ins Verfahrensverzeichnis und die ausgefüllte „Checkliste DSGVO“ („**Datenschutz-Dokumentation**“) noch aktuell sind, und ob die getroffenen Maßnahmen wirksam und ausreichend sind. Erforderlichenfalls aktualisiert er die Datenschutz-Dokumentation und stellt Sie dem Datenschutz-Manager und soweit benannt dem Datenschutzbeauftragten bereit. Das Ergebnis der Prüfung dokumentiert der Verarbeitungs-Verantwortliche.

> *Beispiele: Mit Einführung des Verfahrens wurde eine Speicherfrist von drei Jahren für die Daten festgelegt. Im Rahmen der Regelprüfung zeigt sich, dass die Daten eigentlich nach wenigen Monaten nicht mehr benötigt werden. Die Speicherfrist ist anzupassen.*
>
> *Nach Einführung der Verarbeitungstätigkeit wurden Auslegungshinweise von Aufsichtsbehörden zur DSGVO veröffentlicht oder es ergeht Rechtsprechung, aus der sich Anpassungsanforderungen bei den Datenschutzinformationen für Betroffene ergeben.*

## 10.5 Änderung, Beendigung und Abschluss von Verarbeitungstätigkeiten

Ergeben sich bei einer Verarbeitungstätigkeit wesentliche Änderungen, so verfährt der Verarbeitungs-Verantwortliche bis zur Umsetzung der Änderung entsprechend Ziffer 10.2 und 10.3.

Eine wesentliche Änderung liegt vor, wenn sich durch die Frage der Konformität mit den Vorschriften zum Schutz personenbezogener Daten neu stellt oder sich die bisherige Dokumentation als unvollständig oder sonst unzutreffend darstellt.

> *Beispiele für wesentliche Änderungen: Es werden neue Arten von Daten erfasst. Bereits erhobene Daten werden für neue Zwecke verwendet. Die zu Grunde liegende Software wird durch ein Upgrade um zusätzliche Funktionen erweitert, wodurch neue Datenauswertungen möglich sind.*

Eine Beendigung der Verarbeitungstätigkeit ist vom Verarbeitungs-Verantwortlichen durch entsprechenden Vermerk im Eintrag des Verzeichnisses der Verarbeitungstätigkeiten zu dokumentieren. Eine Beendigung liegt vor, wenn Daten nur noch zu Zwecken der Einhaltung von Aufbewahrungspflichten verarbeitet werden.

der Leistung ist, ein Zugriff auf personenbezogene Daten aber nicht vermieden werden kann.

> *Ein IT-Dienstleister erbringt Fernwartungsleistungen (Fehlerbehebung, Einspielen von Updates) bei einer Software/Datenbank, die das Unternehmen im eigenen Rechenzentrum betreibt. Der IT-Dienstleister könnte bei der Leistungserbringung Zugriff auf in der Software gespeicherte personenbezogene Daten nehmen.*

In Zweifelsfällen stimmt der Verarbeitungs-Verantwortliche das Vorliegen einer Auftragsverarbeitung mit dem Datenschutzbeauftragten – sofern benannt – ab und dokumentiert das Ergebnis.

### 12.2 Verträge mit Dienstleistern

Bevor Verarbeitungsleistungen von Auftragsverarbeitern in Anspruch genommen werden ist mit diesen ein Vertrag zur Auftragsverarbeitung zu schließen, der den Anforderungen des Art. 28 DSGVO genügt.

Für die Verträge ist das Muster zu verwenden, dass der Datenschutz-Manager bereitstellt. Das Muster füllt der Verarbeitungs-Verantwortliche mit Unterstützung des Datenschutz-Managers aus.

Soll von dem Muster inhaltlich abgewichen oder ein Vertragsmuster des Auftragsverarbeiters verwendet werden, bedarf die finale Fassung der Freigabe durch den Datenschutz-Manager.

Die Verträge zur Auftragsverarbeitung sind schriftlich zu schließen und werden vom Datenschutz-Manager zentral verwahrt bzw. dokumentiert. Der Vertragsschluss kann auch in einem elektronischen Format erfolgen (z.B. PDF-Scan).

**Kommentiert [Helbing19]:** Ein gängiges Muster ist das der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD). Dieses hat allerdings aus meiner Sicht einige Schwächen und sollte als Vorlage nicht unreflektiert übernommen werden:
Word-Datei zum Herunterladen:
https://www.gdd.de/downloads/praxishilfen/Mustervertrag_zur_Auftragsverarbeitung_DS-GVO.docx
Anleitung zum Ausfüllen:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_4.pdf

**Kommentiert [Helbing20]:** Ggf. ersetzen durch „Datenschutzbeauftragten“ oder „die Rechtsabteilung“.

### 12.3 Prüfung der Dienstleister

Bevor Auftragsverarbeiter eingeschaltet werden sind diese daraufhin zu prüfen, ob sie die Bestimmungen der DSGVO, insbesondere zur Datensicherheit (Art. 32 DSGVO), einhalten. Die Prüfung ist vom Verarbeitungs-Verantwortlichen zu veranlassen und erfolgt durch den Datenschutz-Manager und soweit die Datensicherheit betroffen ist, durch den Datensicherheits-Manager. Der Datenschutzbeauftragte ist, sofern benannt, in die Prüfung mit einzubinden. Zu prüfen ist insbesondere, ob die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit ausreichend sind. Der Datenschutz-Manager dokumentiert Inhalt und Ergebnis der Prüfung.

Der Datenschutz-Manager wiederholt die Prüfung regelmäßig, in der Regel alle 24 Monate. Wurde das Risiko für die der Auftragsverarbeitung zu Grunde liegenden Verarbeitungstätigkeit mit „hoch“ klassifiziert, erfolgt die Prüfung in der Regel alle 12 Monate, wurde sie mit „niedrig“ klassifiziert alle 36 Monate (zur Risikoklassifizierung siehe Ziffer 10.2).

Weiterführende Informationen zur Auftragsverarbeitung

## 13. Übermittlung in Länder außerhalb der EU

Werden personenbezogene Daten in ein Land übermittelt, das nicht Mitglied der EU ist („**Drittland**“), so stellt der Verarbeitungs-Verantwortliche sicher, dass die Anforderungen der Artikel 44 ff. DSGVO an einen Datenexport eingehalten werden. Keine Drittländer sind auch die anderen Länder des Europäischen Wirtschaftsraums (Island, Liechtenstein und Norwegen).

Eine Übermittlung in ein Drittland ist nach diesen Bestimmungen nur zulässig wenn,

- ein Ausnahmefall nach Art. 49 DSGVO vorliegt (z.B. Einwilligung, erforderlich zur Erfüllung eines Vertrags mit dem Betroffenen, Rechtsverteidigung),
- die Datenübermittlung auf Grundlage eines Angemessenheitsbeschlusses nach Art.

Die Meldung gegenüber der Datenschutz-Aufsichtsbehörde muss unverzüglich und möglichst binnen 72 Stunden ab Kenntnis erfolgen, Art. 33 Abs. 1 DSGVO. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen, Art. 33 Abs. 1 DSGVO.

Wenn und soweit die Informationen nicht vollständig oder nicht rechtzeitig bereitgestellt werden können (z.B. noch andauernde interne IT-forensische Untersuchungen zu einem Hackerangriff), sind die Angaben ohne unangemessene Verzögerung schrittweise der Datenschutz-Aufsichtsbehörde bereitzustellen. Sollen später noch Informationen nachgereicht werden, ist dies der Datenschutz-Aufsichtsbehörde möglichst vorab anzuzeigen.

### 14.3.6 Ggf. Benachrichtigung von Betroffenen

Führt ein Datenschutzvorfall voraussichtlich zu einem *hohen* Risiko für die Rechte und Freiheiten einer natürlichen Person (rote Kategorie) so sind die Betroffenen von dem Datenschutzvorfall gemäß Art. 34 DSGVO zu benachrichtigen, sofern das Unternehmen die Daten nicht lediglich im Auftrag eines anderen verarbeitet hat und kein Ausnahmefall nach Art. 34 Abs. 3 DSGVO vorliegt.

Für die Benachrichtigung ist der Datenschutz-Manager verantwortlich, der sich hierzu mit der Unternehmensleitung abstimmt.

### 14.3.7 Dokumentation im Verzeichnis für Datenschutzvorfälle

Jeden Datenschutzvorfall (grüne, gelbe und rote Kategorie) dokumentiert der Datensicherheits-Manager in einem Verzeichnis, Art. 33 Abs. 5 DSGVO.

Darin sind festzuhalten:

- Datenschutzvorfall betrifft Unternehmen als Verantwortlichen oder Auftragsverarbeiter?
- Alle im Zusammenhang mit dem Datenschutzvorfall stehende Fakten.
- Auswirkungen des Datenschutzvorfalls.
- Abhilfemaßnahmen betreffend den Datenschutzvorfall.
- Erwägungen und Ergebnis der Risikoeinschätzung zum Datenschutzvorfall.

Die Dokumentation muss der Datenschutz-Aufsichtsbehörde die Überprüfung der Einhaltung der Meldepflicht nach Art. 33 DSGVO ermöglichen und auf Anfrage dieser vorgelegt werden, Art. 33 Abs. 5 DSGVO.

Weiterführende Informationen zu Datenschutzvorfällen

## 15. Verpflichtung auf den Datenschutz und Schulungen

### 15.1 Verpflichtungserklärung

Alle Personen, die Zugriff auf personenbezogene Daten haben, sind zur Vertraulichkeit und auf die Einhaltung der Grundsätze der DSGVO zu verpflichten. Dies können neben Mitarbeitern auch Externe sein (z.B. Freelancer).

Die Verpflichtung erfolgt durch Unterzeichnung eines Formblatts „Verpflichtung zum Datenschutz“ (Datenschutz-Verpflichtung). Mit der Datenschutz-Verpflichtung ist der „Spickzettel Datenschutz“ zur Information bereitzustellen.

Zuständig für die Einholung und Dokumentation der Datenschutz-Verpflichtung ist bei Mitarbeitern (einschließlich Auszubildenden und Praktikanten) der Leiter des Fachbereichs Personal und bei externen Personen der Datenschutz-Manager.

**Kommentiert [Helbing28]:** Die deutschen Aufsichtsbehörden leiten aus der DSGVO eine umfassendere Pflicht zur Einholung von Verpflichtungserklärungen ab, siehe hier: https://www.lda.bayern.de/media/dsk_kpnr_19_verpflichtungBeschaeftigte.pdf

**Kommentiert [Helbing29]:** Hierzu kann das Formblatt der Aufsichtsbehörden genutzt werden, d.h. die letzten beiden Seiten dieses Dokuments: (https://www.lda.bayern.de/media/dsk_kpnr_19_verpflichtungBeschaeftigte.pdf ).

**Kommentiert [Helbing30]:** Bitte ggf. anpassen

Die Datenschutz-Verpflichtung ist bei allen betroffenen Mitarbeitern und Dritten nach Inkrafttreten dieser Richtlinie neu einzuholen und sodann regelmäßig, spätestens alle 36 Monate, zu erneuern. Bei neu eingestellten Beschäftigten ist die Verpflichtung erstmals zusammen mit Unterzeichnung des Arbeitsvertrags einzuholen, bei Externen im Zusammenhang mit deren Beauftragung.

### 15.2 Schulungen

Verantwortlich für die Durchführung bzw. Bereitstellung und für die Dokumentation der Schulungen zum Datenschutz ist der Datenschutzbeauftragte, sofern ein solcher nicht benannt ist, der Datenschutz-Manager.

Dieser erstellt einen Schulungsplan für einen Zeitraum von 24 Monate und legt darin fest

- zu schulende Personengruppen (z.B. Personalabteilung, Führungskräfte) und für diese jeweils;
- nächste Schulung (z.B. Quartal 1/20xx)
- Periodizität der Schulung (z.B. Wiederholung alle 24 Monate)
- Art der Schulung (z.B. Online-Schulung oder Präsenzschulung)
- Schulungsinhalte (z.B. Basisschulung, IT-Sicherheit, Betroffenenrechte)
- Weitere Maßnahmen zur Schaffung von Bewusstsein für den Datenschutz (z.B. Fragerunde in Abteilungsbesprechungen, Beitrag in Mitarbeiterzeitschriften oder Intranet, Aushänge, Bekenntnis der Geschäftsführung zum Datenschutz)

## 16. Umsetzungs- und Dokumentationspflicht

Der Verarbeitungs-Verantwortliche trifft risikoangemessene technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung personenbezogener Daten gemäß der DSGVO erfolgt und dies auch nachweisbar ist. Sofern nicht bereits durch Ziffer 10 geregelt, hat der Verarbeitungs-Verantwortliche hierzu entsprechende Dokumentationen anzufertigen, bei sich vorzuhalten und erforderlichenfalls zu prüfen und zu aktualisieren (Art. 24 Abs. 1 DSGVO).

*Siehe Beispiele bei Ziffer 10.3.*

## 17. Datensicherheit

Das Unternehmen ist verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um personenbezogene Daten risikoangemessen zu schützen, Art. 32 DSGVO. Hierfür ist zunächst das Schutzniveau zu ermitteln (Ziffer 17.1). Sodann sind entsprechende Datensicherheitsmaßnahmen festzulegen (Ziffer 17.2).

**Kommentiert [Helbing31]:** Die Ziffer gibt die Anforderungen der DSGVO recht abstrakt wieder. Das Unternehmen sollte hierzu eine spezifische Informationssicherheitsrichtlinie verfassen. Der Inhalt von Ziffer 17 kann dann durch einen Verweis auf diese ersetzt werden.

### 17.1 Ermittlung des Schutzniveaus

Bei der Verarbeitung personenbezogener Daten ist abhängig von den jeweiligen Daten und der Verarbeitung das Schutzniveau zu bestimmen (z.B. niedrig, mittel, hoch, sehr hoch). Dabei sind die Risiken für Betroffene zu berücksichtigen. Diese können sich insbesondere ergeben aus

**Kommentiert [Helbing32]:** Hierzu bieten sich Konkretisierungen und Beispiele in unternehmensinternen IT-Richtlinien an.

- einer Vernichtung von personenbezogenen Daten
- einem Verlust von personenbezogenen Daten
- der Veränderung von personenbezogenen Daten
- der unbefugten Offenlegung von personenbezogenen Daten
- dem unbefugten Zugang zu personenbezogenen Daten

Bei den Risiken sind die Schwere des potentiellen Schadens für die Betroffenen und die Eintrittswahrscheinlichkeit zu berücksichtigen.

### 17.2 Datensicherheitsmaßnahmen

Sodann sind dem Schutzniveau entsprechend angemessene Datensicherheitsmaßnahmen umzusetzen.

Bei der Frage, welche Datensicherheitsmaßnahmen „angemessen“ sind, ist zu berücksichtigen (Art. 32 Abs. 1 DSGVO):

- Stand der Technik (gemeint sind nicht die neuesten technischen Entwicklungen und Fortschritte, sondern die am Markt verfügbare Technologie)
- Kosten für die Umsetzung der Datensicherheitsmaßnahmen
- Art, Umfang, Umstände und Zweck der Verarbeitung
- Eintrittswahrscheinlichkeit und Schwere der Risiken für die Betroffenen (also das ermittelte Schutzniveau)

Als Beispiele für Datensicherheitsmaßnahmen nennt Artikel 32 Abs. 1 DSGVO:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten
- Maßnahmen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste dauerhaft sicherstellen.

  *Vertraulichkeit: Personenbezogene Daten müssen vor unbefugter oder unbeabsichtigter Preisgabe geschützt werden. Dabei sind externe wie interne Angreifer (z.B. Hacker, frustrierte oder neugierige Mitarbeiter) sowie fahrlässige oder strukturelle Gefährdungen (z.B. ungeschulte Mitarbeiter, mangelhafte Rollen-/Berechtigungskonzepte) zu berücksichtigen.*

  *Integrität: Personenbezogene Daten sind vollständig und richtig bereitzustellen. Unzulässige Änderungen an den Daten sind zu erkennen (z.B. durch Protokollierung/Logfiles) und Verfahren zur Berichtigung vorzuhalten.*

  *Verfügbarkeit: Personenbezogene Daten müssen zur Verfügung stehen, wenn sie benötigt werden. Dies setzt auch voraus, dass sie bei Verlust oder Vernichtung wiederhergestellt werden können (z.B. Backups).*

- Maßnahmen, die die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen sicherstellen (Wiederherstellung bei einem physischen oder technischen Zwischenfall).
- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Datensicherheits-Maßnahmen (z.B. Penetrationstests, externe Begutachtung).

### 17.3 Verantwortlichkeit

Der Datensicherheits-Manager ist dafür verantwortlich, dass für alle verarbeiteten personenbezogenen Daten ein Schutzniveau ermittelt wird und angemessene Maßnahmen zur Datensicherheit umgesetzt werden. Der Datensicherheits-Manager empfiehlt hierzu der Unternehmensleitung entsprechende Richtlinien und sonstige Maßnahmen zur Umsetzung.

## 18. Überprüfungszyklus und Anpassung

Der Datenschutz-Manager wird die vorliegende Anweisung mindestens alle 24 Monate fachlich prüfen, hierzu – sofern benannt – den Datenschutzbeauftragten konsultieren und ggf. der Unternehmensleitung Änderungen vorschlagen.

## 19. Änderungshistorie

**Kommentiert [Helbing33]:** Bei späteren Änderungen im Text der Richtlinie, diese Tabelle bitte fortführen. Spalte „Freigabe“ ggf. löschen, wenn kein Vier-Augen Prinzip für Änderung vorgesehen ist.

| Version | Datum | Verfasser | Anmerkung/Änderung | Freigabe |
|---|---|---|---|---|
| 1.0 | Bitte ergänzen | Bitte ergänzen | Ersterstellung | Bitte ergänzen |

## Anhang: Kontaktdaten

Als Datenschutz-Manager benannt wurde:

Name, Telefon, E-Mail des Datenschutz-Managers

Als Datensicherheits-Manager benannt wurde:

Name, Telefon, E-Mail des Datensicherheits-Managers

Die Kontaktdaten des Datenschutzbeauftragten sind:

Name, ggf. Anschrift, Telefon und E-Mail-Adresse des Datenschutzbeauftragten

**Kommentiert [Helbing34]:** Hier können die konkreten Kontaktdaten der Person genannt werden, oder es erfolgt ein dynamischer Verweis, z.B. „Leiter Recht". Tipps zur Auswahl der zu benennenden Person finden Sie in der Anleitung.

**Kommentiert [Helbing35]:** Auch hier kann wieder eine konkrete Person benannt werden oder ein dynamischer Verweis erfolgen (z.B. „Chief Security Officer - CSO"). Tipps zur Auswahl der zu benennenden Person enthält die Anleitung.