

Datenschutzrichtlinie **MUSTERMANN**

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

Inhaltsverzeichnis

1.	Gegenstand und Ziel	3
2.	Anwendungsbereich.....	3
3.	Rollen und Verantwortlichkeiten.....	4
3.1	Jeder Mitarbeiter.....	4
3.2	Verarbeitung.....	4
3.3	Datenschutz.....	4
3.4	Datensicherheit.....	5
3.5	Datenschutz.....	5
4.	Einbindung.....	5
5.	Rechtskonformität.....	5
5.1	Datenschutz.....	5
5.2	Verarbeitung.....	7
5.3	Automatisierung.....	7
5.4	Verwendung.....	7
5.5	Datenschutz.....	8
6.	Rechtsgrundlagen.....	8
6.1	Voraussetzung.....	8
6.2	Besondere.....	9
6.3	Datenschutz.....	9
7.	Dienst- und Geschäftsbeziehungen.....	10
8.	Informationen.....	11
8.1	Datenerhebung.....	11
8.2	Datenerhebung bei einem anderen.....	11
8.3	Weitere Transparenzanforderungen.....	12
9.	Rechte der Betroffenen	12
9.1	Inhalt der Rechte.....	12
9.2	Erfüllung der Rechte von Betroffenen	14
10.	Dokumentation und Prüfung von Verarbeitungstätigkeiten.....	15
10.1	Vorliegen einer Verarbeitungstätigkeit.....	15
10.2	Planung von Verarbeitungstätigkeiten (Konzeptionsphase).....	16
10.3	Einführung von Verarbeitungstätigkeiten	17
10.4	Durchführung von Verarbeitungstätigkeiten (Regelprüfung).....	17
10.5	Änderung, Beendigung und Abschluss von Verarbeitungstätigkeiten.....	17

Nutzungshinweise:

Sie können dieses Dokument kostenlos bearbeiten und gewerblich nutzen, wenn Sie Logo und Autoreneinformationen in der Kopf- bzw. Fußzeile unverändert lassen.

Gegen eine einmalige Lizenzgebühr dürfen Sie auch das Logo und die Autoreneinformationen ändern. Zum Kauf einer Lizenz siehe: www.thomashelbing.com/dsgvo-sinfonie

Es gelten die vollständigen Lizenzbestimmungen unter: www.thomashelbing.com/dsgvo-sinfonie

Um das Dokument zu bearbeiten (und diese Box zu löschen) müssen Sie in Word den Bearbeitungsschutz aufheben (Menu: „Überprüfen“ > „Schützen“ > „Bearbeitung einschränken“ > Button unten „Schutz aufheben“. [Anleitung](#) für andere Wordversionen). Das hierfür nötige Passwort erhalten Sie automatisch mit der Bestätigungsmail, wenn Sie meinen Newsletter bestellen: www.thomashelbing.com/newsletter-bestellen

10.6	Führung des Verzeichnisses der Verarbeitungstätigkeiten	18
11.	Datenschutzfolgenabschätzung.....	18
11.1	Erforderlichkeit einer Datenschutzfolgenabschätzung.....	18
11.2	Durchführung der Datenschutzfolgenabschätzung	19
12.	Auftragsverarbeitung durch Dienstleister	19
12.1	Vorliegen einer Auftragsverarbeitung	19
12.2	Verträge mit Dienstleistern	20
12.3	Prüfung der Dienstleister	20
13.	Übermittlung in Länder außerhalb der EU	20
14.	Umgang mit Datenschutzvorfällen	21
14.1	Vorliegen eines Datenschutzvorfalls	21
14.2	Interne Meldepflicht.....	22
14.3	Weiteres Vorgehen	22
15.	Verpflichtung auf den Datenschutz und Schulungen	24
15.1	Verpflichtungserklärung	24
15.2	Schulungen	24
16.	Umsetzungs- und Dokumentationspflicht	25
17.	Datensicherheit	25
17.1	Ermittlung des Schutzniveaus	25
17.2	Datensicherheitsmaßnahmen.....	25
17.3	Verantwortlichkeit.....	26
18.	Überprüfungszyklus und Anpassung.....	26
19.	Änderungshistorie	26
Anhang: Begriffe und Definitionen		28
Anhang: Kontaktdaten.....		29
Anhang: Prozess Verarbeitungstätigkeit		30
Anhang: Prozess Datenschutzvorfall		31

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 für **Mustermann** haben, etwa Rufschäden, Schadenersatzansprüche und empfindliche Bußgelder.

Diese Anweisung enthält Regeln für alle Mitarbeiter, um die Vorschriften zum Schutz personenbezogener Daten einzuhalten. Dies sind insbesondere die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – „**DSGVO**“), und das Bundesdatenschutzgesetz („**BDSG**“).

Eine Übersicht und Zusammenfassung der wichtigsten Regelungen dieser Anweisung findet sich in der Anlage „Datenschutz Spickzettel“.

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**“).

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

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 Mitarbeiter

Jeder Mitarbeiter beachtet beim Umgang mit personenbezogenen Daten folgende Regeln:

- **Datenschutzbeauftragten** einbinden und unterstützen (Ziffer 4).
- Bei der Verarbeitung die Datenschutzgrundsätze beachten (Ziffern 5 und 6).
- Datenschutzpannen intern melden (Ziffer 14).

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

3.2 Verarbeitings-Verantwortlicher

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

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

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

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.

Der Verarbeitings-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 [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 sich im Anhang Kontaktdaten.

3.5 Datenschutzbeauftragter

Das Unternehmen hat einen Datenschutzbeauftragten benannt. Die Kontaktdaten des Datenschutzbeauftragten sind im Anhang Kontaktdaten aufgeführt.

Die Aufgaben des Datenschutzbeauftragten ergeben sich aus Art. 39 Abs. 1 DSGVO. Diese sind:

- Unterrichtung und Beratung des Unternehmens und seiner Mitarbeiter 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 Verbot 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 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 erläutern, wie die Daten verwendet werden.

5.1.3 Zweckbindung (Art. 5 Abs. 1 b) DSGVO)

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen später nur zu solchen Zwecken weiterverarbeitet werden, die mit den ursprünglichen Zwecken vereinbar sind.

Beispiel: Für Zugangsausweise aufgenommene Portraitfotos dürfen nicht zur Außendarstellung auf der Unternehmens-Webseite genutzt werden.

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)

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, z.B. Schutz vor unbefugtem Zugriff oder Verlust durch geeignete technische und organisatorische Maßnahmen (Einzelheiten siehe Ziffer 17).

5.1.8 Pseudonymisierung

Soweit der Zweck der Verarbeitung dies erlaubt, sollen personenbezogene Daten in pseudonymisierter Form verarbeitet werden. Pseudonymisierte Form bedeutet (vgl. Art. 4 Nr. 5 DSGVO), dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer Person zugeordnet werden können. Die eigentlichen Daten und die Angaben, die eine Zuordnung zu einer Person erlauben (z.B. Name, E-Mail, Anschrift, Telefonnummer) werden also getrennt. Die Informationen, die eine Zuordnung ermöglichen werden durch technische und organisatorische Maßnahmen speziell gesichert.

Beispiel: Patientendaten werden in zwei Datenbanken gespeichert, Datenbank A enthält nur Name, Anschrift und eine ID (Pseudonym), Datenbank B enthält nur die ID sowie zugehörige Röntgenbilder der Person (Inhaltsdaten). Auf Datenbank A haben nur Administratoren nach dem Vier-Augen Prinzip Zugriff. Mit Datenbank B wird eine Software zur Auswertung von Röntgenbildern entwickelt. Erhalten bei Entwicklungsarbeiten Unbefugte Zugriff auf die Datenbank B mit den Röntgenbildern, so ist der Schaden für Patienten geringer, da ohne Kenntnis von Datenbank A Patienten nur schwer identifizierbar sind.

5.2 Verarbeitung von Daten über Straftaten

Sollen Daten über strafrechtliche Verurteilungen oder Straftaten verarbeitet werden, stimmt der Verarbeitungs-Verantwortliche dies vorab mit dem Datenschutz-Manager ab, um die Einhaltung von Art. 10 DSGVO sicherzustellen.

5.3 Automatisierte Einzelentscheidung

Werden Einzelentscheidungen über Menschen getroffen, beruhen die Entscheidungen ausschließlich auf einer automatisierten Verarbeitung und haben die Entscheidungen gegenüber der Person rechtliche Wirkung oder beeinträchtigen diese in ähnlicher Weise („**automatisierte Einzelentscheidung**“), so ist dies nur unter den Voraussetzungen des Art. 22 DSGVO zulässig.

Beispiel: Bewerber müssen online einen Fragebogen ausfüllen. Aus den Antworten wird anhand einer Formel ein Punktwert errechnet. Alleine aufgrund des Punktwerts wird entschieden, ob der Bewerber zu einem Gespräch eingeladen wird.

Der Verarbeitungs-Verantwortliche stimmt vor Einführung einer automatisierten Einzelentscheidung die datenschutzrechtliche Zulässigkeit mit dem Datenschutz-Manager ab.

Der Verarbeitungs-Verantwortliche dokumentiert im Verzeichnis der Verarbeitungstätigkeiten (siehe Ziffer 10.6) Folgendes:

- das Vorliegen einer automatisierten Einzelentscheidung
- aussagekräftige Informationen zur involvierten Logik sowie der Tragweite und der angestrebten Auswirkungen für den Betroffenen
- Erläuterungen der etwaig nach Art. 22 Abs. 3 DSGVO getroffenen Maßnahmen

Beispiel für solche Maßnahmen im obigen Beispiel: Es ist ein Prozess einzurichten, der es dem Bewerber ermöglicht, seinen Standpunkt zum Punktwert darzulegen und die automatisiert getroffene Entscheidung durch einen Mitarbeiter der Personalabteilung prüfen zu lassen.

5.4 Verwendung von Wahrscheinlichkeitswerten zu Personen

Sollen Wahrscheinlichkeitswerte über ein bestimmtes zukünftiges Verhalten einer natürlichen Person verwendet werden, um über die Begründung, Durchführung oder Beendigung eines

Vertrages mit der Person zu entscheiden, sind die besonderen Anforderungen des § 31 BDSG zu beachten.

Das Unternehmen bezieht einen Scorewert über die Bonität eines potentiellen Kunden (Einzelperson) von einer Auskunft (oder ermittelt diesen selbst). Der Scorewert soll über das „Ob“ und die Konditionen eines Vertrages mit dem Kunden entscheiden.

Der Verarbeitungs-Verantwortliche stimmt vor einer entsprechenden Verwendung von Wahrscheinlichkeitswerten die datenschutzrechtliche Zulässigkeit mit dem Datenschutz-Manager ab.

5.5 Datenschutzfreundliche Voreinstellung

Soweit in einem System Voreinstellungen für die Datenverarbeitung getroffen werden können sind diese Einstellungen so vorzunehmen, dass mit Blick auf den Nutzungszweck nicht mehr Daten als nötig, nicht länger als nötig und nicht umfassender als nötig verarbeitet werden, und der Zugriff durch Dritte soweit wie möglich eingeschränkt wird, Art. 25 Abs. 2 DSGVO.

Beispiel: Das Unternehmen will ein Unternehmensinternes soziales Netzwerk auf Basis eines Standard-Softwareproduktes einführen, damit sich Mitarbeiter besser austauschen können. In der Software kann vom Unternehmen eingestellt werden, ob standardmäßig der Standort eines Mitarbeiters angezeigt wird, wenn dieser einen Beitrag einstellt. Die Option ist zu deaktivieren, da der Standort für den Zweck regelmäßig nicht benötigt wird.

6. Rechtsgrundlage für Verarbeitungen

Personenbezogene Daten dürfen nur verarbeitet werden, wenn für die Verarbeitung eine Rechtsgrundlage besteht (siehe Ziffer 6.1).

Bei sensiblen personenbezogenen Daten muss zudem eine Ausnahme nach Art. 9 Abs. 2 DSGVO vorliegen, da diese Daten einem grundsätzlichen Verarbeitungsverbot unterliegen (siehe Ziffer 6.2).

6.1 Voraussetzung für jede Verarbeitung

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn hierfür eine Rechtsgrundlage nach Art. 6 DSGVO vorliegt.

Wichtige Rechtsgrundlagen (nicht abschließend) sind:

- **Vertragserfüllung:** Die Verarbeitung ist für die Erfüllung eines Vertrags *mit dem Betroffenen* erforderlich. Die Verarbeitung muss, objektiv betrachtet, zur Erfüllung des Vertrags sinnvoll sein. „Erforderlich“ meint nicht „zwingend notwendig“.

Beispiele: Die Abfrage der Kontoverbindung von Mitarbeitern ist zur Auszahlung des Gehalts erforderlich. Die Analyse des Kaufverhaltens von Kunden zur Ermittlung von Kundenvorlieben ist nicht zur Erfüllung eines Vertrags mit dem Kunden erforderlich.

- **Rechtliche Verpflichtung:** Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung, der das Unternehmen unterliegt, erforderlich. Rechtliche Verpflichtungen sind vor allem deutsche Gesetze sowie Verordnungen der EU, ebenso Dienst- und Betriebsvereinbarungen (siehe Ziffer 7) oder Tarifverträge. Die Gesetze müssen die Zwecke der Verarbeitung festlegen.

Wenn das Gesetz konkret die Art und Weise der Verarbeitung festlegt („Welche Daten dürfen zu welchen Zwecken wie und wie lange verarbeitet werden?“), müssen diese Vorgaben eingehalten sein. Enthält das Gesetz solche Vorgaben nicht, ist sicherzustellen, dass die konkrete Verarbeitung zur Erfüllung des jeweiligen Gesetzes tatsächlich *erforderlich* ist.

- **Interessenabwägung:** Die Verarbeitung ist zur Wahrung eines berechtigten Interesses des Unternehmens oder eines Dritten erforderlich und die Interessen des Betroffenen überwiegen nicht. Soll die Verarbeitung auf eine

Interessenabwägung gestützt werden, so dokumentiert der Verantwortliche die durchgeführte Abwägung. Hierbei ist insbesondere die Erwartungshaltung der Betroffenen zu berücksichtigen. Der Betroffene ist zudem auf sein Widerspruchsrecht nach Art. 21 Abs. 1 DSGVO hinzuweisen (siehe Ziffer 9.1.6).

- **Einwilligung:** Es liegt eine Einwilligung des Betroffenen in die Verarbeitung seiner Daten zu den jeweiligen Zwecken vor (siehe hierzu ergänzend Ziffer 6.3).

6.2 Besondere Anforderungen bei sensiblen Daten

Bei der Verarbeitung sensibler personenbezogener Daten gelten besonders strenge Anforderungen. Die Verarbeitung ist grundsätzlich untersagt, außer es liegt einer der Ausnahmetatbestände des Art. 9 Abs. 2 DSGVO, § 22 BDSG vor.

„**Sensible personenbezogene Daten**“ sind alle personenbezogenen Daten, die Angaben enthalten, aus denen hervorgeht:

- die rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen, oder
- die Gewerkschaftszugehörigkeit

oder in denen folgende Daten enthalten sind:

- genetische Daten (Art. 4 Nr. 13 DSGVO)
- biometrische Daten (Art. 4 Nr. 14 DSGVO) zur eindeutigen Identifizierung einer natürlichen Person
- Gesundheitsdaten (Art. 4 Nr. 15 DSGVO), z.B. Krankheitsfehlzeiten, oder
- Daten zum Sexualleben oder der sexuellen Orientierung

Wichtige Ausnahmetatbestände vom Verbot der Verarbeitung sensibler personenbezogener Daten sind insbesondere (Aufzählung ist nicht abschließend, vgl. Art. 9 Abs. 2 DSGVO, § 22 BDSG):

- Die Verarbeitung erfolgt auf Grundlage einer ausdrücklichen Einwilligung des Betroffenen (siehe zur Einwilligung ergänzend Ziffer 6.3).
- Die Verarbeitung ist erforderlich, damit das Unternehmen oder der Betroffene die ihm aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen diesbezüglichen Pflichten nachkommen kann.

Beispiele: Verarbeitungen von Angaben zur Religionszugehörigkeit zur Abführung von Kirchensteuer

Bei Mitarbeiterdaten dürfen die Interessen der Mitarbeiter nicht überwiegen.

- Die Verarbeitung bezieht sich auf personenbezogene Daten, die der Betroffene offensichtlich öffentlich gemacht hat (z.B. auf einer frei zugänglichen Webseite),
- Die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich.

Daten zur Krankheit eines Mitarbeiters müssen in einem Kündigungsprozess vorgetragen werden.

- Die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten erforderlich, und die Verarbeitung erfolgt durch oder unter der Verantwortung einer Person, die einer gesetzlichen Schweigepflicht unterliegt (z.B. Arzt, Arzthelfer, Rechtsanwalt).
- Die Verarbeitung erfolgt auf Grundlage einer Dienst- oder Betriebsvereinbarung (siehe Ziffer 7).

6.3 Datenschutz-Einwilligung

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

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.

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

Enthält eine Dienst- oder Betriebsvereinbarung spezifische Regeln zur Verarbeitung personenbezogener Daten für einzelne Verarbeitungstätigkeiten, vermerkt der Verarbeitungs-Verantwortliche dies im Verzeichnis der Verarbeitungstätigkeiten (siehe Ziffer 10.6).

Alle Mitarbeiter beachten bei der Verarbeitung personenbezogener Daten die Bestimmungen der anwendbaren Betriebsvereinbarungen. Der Verarbeitungs-Verantwortliche bringt die konkreten Anforderungen den Mitarbeitern entsprechend zur Kenntnis und implementiert und dokumentiert die notwendigen Prozesse.

8. Informationen gegenüber Betroffenen

8.1 Datenerhebung beim Betroffenen selbst

Werden personenbezogene Daten *beim Betroffenen* erhoben, so stellt der Verarbeitungs-Verantwortliche sicher, dass dem Betroffenen zum Zeitpunkt der Erhebung die in Art. 13 DSGVO genannten Informationen mitgeteilt werden, sofern der Betroffene nicht bereits über die Informationen verfügt und kein Fall des Art. 32 BDSG vorliegt.

Beispiele:

- *Stellenbewerber sind über den Umgang mit ihren Bewerbungsunterlagen zu informieren.*
- *Webseiten des Unternehmens müssen Datenschutzhinweise bereitstellen.*
- *Mitarbeiter sind über den Umgang mit ihren Daten durch das Unternehmen als Arbeitgeber aufzuklären.*
- *Videoüberwachungen sind durch Schilder deutlich zu machen.*

Folgende Informationen sind mitzuteilen:

- Name und die Kontaktdaten des Unternehmens
- Kontaktdaten des Datenschutzbeauftragten, falls benannt
- Zwecke und Rechtsgrundlage der Verarbeitung
- wenn die Verarbeitung auf der Rechtsgrundlage der berechtigten Interessen beruht (siehe Ziffer 6.1), die berechtigten Interessen, die vom Unternehmen verfolgt werden
- Empfänger oder Kategorien von Empfängern der Daten
- Absicht, die Daten in ein Land außerhalb der EU zu übermitteln (siehe Ziffer 13) und, falls dem so ist, bestimmte ergänzende Informationen hierzu
- Speicherdauer oder Kriterien für die Bemessung der Speicherdauer
- Hinweis auf Betroffenenrechte
- ggf. Hinweis auf Widerrufbarkeit der Einwilligung
- Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde
- Erläuterung, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob der Betroffene verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung der Daten hätte und
- Bestehen einer automatisierten Einzelentscheidung (siehe Ziffer 5.3) einschließlich Profiling und ggf. ergänzende Informationen dazu.

Können aus Platzgründen nicht alle Informationen sinnvollerweise unmittelbar bereitgestellt werden, kann die Information in abgestufter Form erfolgen.

Beispiele: Kurz- und Langfassung von Datenschutzerklärungen auf der Webseite, Mitteilung nur der Kontaktdaten und der Verarbeitungszwecke und kurzer Hinweis auf die Betroffenenrechte auf einer Gewinnspielkarte und Verweis auf eine Internetseite zum Abruf von Detailinformationen.

8.2 Datenerhebung bei einem anderen

Werden personenbezogene Daten nicht beim Betroffenen, sondern *bei einem Dritten* erhoben, so stellt der Verarbeitungs-Verantwortliche sicher, dass dem Betroffenen die in Art. 14 DSGVO genannten Informationen innerhalb angemessener Frist (höchstens ein Monat) nach Erlangung der Daten (spätestens bis zur Offenlegung der Daten gegenüber einem Dritten) mitgeteilt werden, sofern kein Ausschlussgrund nach Art. 14 Abs. 5 DSGVO, § 33 BDSG vorliegt.

Beispiel: Im Rahmen des Einstellungsprozesses wurden mit Hilfe von Drittanbietern Background-Checks zur Zuverlässigkeit des Mitarbeiters durchgeführt. Der Bewerber ist entsprechend zu informieren.

Es sind ergänzend zu den Informationen nach Ziffer 8.1 auch die Kategorien der Daten und deren Herkunft anzugeben.

8.3 Weitere Transparenzanforderungen

Die vorgenannten Mitteilungspflichten gelten entsprechend, wenn bereits erhobene Daten für einen neuen Zweck verwendet werden sollen (siehe Ziffer 5.1.3).

Erfolgt eine Verarbeitung personenbezogener Daten auf Basis der Rechtsgrundlage der Interessenabwägung (siehe Ziffer 6.1) stellt der Verarbeitungs-Verantwortliche sicher, dass der Betroffene auf sein Widerspruchsrecht nach Art. 21 Abs. 1 DSGVO (Widerspruchsrecht aufgrund besonderer Situation) (siehe Ziffer 9.1.6) hingewiesen wird. Der Hinweis hat spätestens bei der ersten Kommunikation mit dem Betroffenen und in hervorgehobener Form (z.B. Fettdruck) zu erfolgen.

Erfolgt eine Verarbeitung personenbezogener Daten, um Direktwerbung zu betreiben (z.B. Newsletter, Werbebriefe, Telefonanrufe), so stellt der Verarbeitungs-Verantwortliche sicher, dass der Betroffene auf sein Widerspruchsrecht nach Art. 21 Abs. 2 DSGVO (siehe Ziffer 9.1.7) in hervorgehobener Form (z.B. Fettdruck) hingewiesen wird.

Der Verarbeitungs-Verantwortliche dokumentiert die Erfüllung der Dokumentationspflichten einschließlich des Inhalts der den Betroffenen gegenüber gemachten Mitteilungen.

[Weiterführende Informationen zu den Informationspflichten](#)

9. Rechte der Betroffenen

9.1 Inhalt der Rechte

Betroffene haben nach der DSGVO gegenüber dem Unternehmen bestimmte Rechte in Bezug auf ihre Daten („**Betroffenenrechte**“). Die Betroffenenrechte sind nachfolgend dargestellt.

9.1.1 Recht auf Auskunft (Art. 15 DSGVO)

Betroffene können vom Unternehmen Auskunft verlangen, ob das Unternehmen über sie personenbezogene Daten verarbeitet und wenn dies der Fall ist,

- welche Datenkategorien für welche Zwecke verarbeitet werden
- welchen Empfängern bzw. Empfängerkategorien die Daten offengelegt werden
- wie lange die Daten gespeichert werden
- woher die Daten stammen, und
- ob eine automatisierte Einzelentscheidung (siehe Ziffer 5.3) bzw. ein Profiling stattfindet

Ergänzend sind die weiteren Informationen gemäß Art. 15 Abs. 1 DSGVO zu geben.

Das Unternehmen hat dem Betroffenen zudem auf Verlangen eine Kopie aller

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 der betreffenden personenbezogenen 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.

- Die Daten werden für die vorgesehenen Zwecke vom Unternehmen nicht mehr benötigt, der Betroffene benötigt sie aber zur Rechtsausübung.

Beispiel: Ein erfolgloser Stellenbewerber klagt wegen Diskriminierung gegen das Unternehmen. Die Aufzeichnungen aus dem Bewerbungsgespräch sind zunächst nur zu sperren statt zu löschen.

- Der Betroffene hat aufgrund seiner besonderen persönlichen Situation ein Widerspruchsrecht gegen die Verarbeitung seiner Daten ausgeübt (siehe Ziffer 9.1.6). Während das Unternehmen den Widerspruch prüft müssen die Daten gesperrt werden.

9.1.5 Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Betroffene können vom Unternehmen verlangen, sie betreffende personenbezogene Daten, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

Dieses Recht auf Datenübertragbarkeit besteht nur, wenn und soweit die Datenverarbeitung automatisiert (nicht rein papiergebunden) und auf der Rechtsgrundlage der Vertragserfüllung oder Einwilligung (siehe Ziffer 6) erfolgt.

Der Anspruch auf Datenübertragbarkeit beschränkt sich auf solche Daten, die der Betroffene dem Unternehmen „bereitgestellt“ hat.

Der Betroffene hat zudem das Recht, die Daten an Dritte zu übermitteln, ohne dabei vom Unternehmen behindert zu werden. Soweit technisch machbar kann der Betroffene vom Unternehmen auch verlangen, dass das Unternehmen die Daten direkt an einen Dritten übermittelt.

9.1.6 Widerspruchsrecht aufgrund besonderer Situation (Art. 21 Abs. 1 DSGVO)

Wenn das Unternehmen die Daten auf der Rechtsgrundlage der Interessenabwägung (siehe Ziffer 6.1) verarbeitet können Betroffene gegen die Verarbeitung ihrer personenbezogenen Daten aus Gründen ihrer *besonderen Situation* Widerspruch einlegen. Es handelt sich also um kein bedingungsloses Widerspruchsrecht.

Beispiel: Speicherung von Daten eines Diplomaten aus einem Land mit erhöhter Terrorismusgefahr in einer Auskunftsdatei.

Das Unternehmen muss sodann gemäß Art. 21 Abs. 1 DSGVO prüfen, ob die Verarbeitung dennoch stattfinden kann, die Daten während dieser Zeit sperren (siehe Ziffer 9.1.4) und die Verarbeitung in Bezug auf den Betroffenen ggf. einstellen.

9.1.7 Widerspruchsrecht gegen Direktwerbung (Art. 21 Abs. 2 DSGVO)

Betroffene können der Verarbeitung ihrer personenbezogenen Daten für Direktwerbung (z.B. Newsletter, Werbebriefe oder -anrufe) jederzeit widersprechen. Das Unternehmen darf die Daten dann nicht mehr für Direktwerbung verwenden.

Im Falle eines solchen Werbe-Widerspruchs ist zudem jede mit der Direktwerbung in Verbindung stehende Datenverarbeitung zu beenden, mit der die potentiellen Interessen, Vorlieben, die wirtschaftliche Lage oder andere persönliche Aspekte des Betroffenen bewertet werden sollen (sog. „**Profiling**“, vgl. Art. 5 Nr. 4 DSGVO).

Beispiel: Ein Kunde (Verbraucher) teilt mit, dass er keine E-Mail Werbung mehr erhalten möchte. Die E-Mail Adresse ist aus entsprechenden Newsletter-Verteilern zu entfernen und ggf. in eine Sperrliste aufzunehmen. Wurde das Kaufverhalten des Betroffenen bisher ausgewertet, um ihm passgenaue E-Mail Werbung zu schicken (Profiling), so ist auch diese Auswertung in Bezug auf den Betroffenen einzustellen.

9.2 Erfüllung der Rechte von Betroffenen

Der Verarbeitungs-Verantwortliche hat durch geeignete technische und/oder

organisatorische Maßnahmen sicherzustellen, dass das Unternehmen Betroffenenrechte erfüllen kann. Die Maßnahmen sind zu dokumentieren.

Beispiel: IT-Systeme sind so auszuwählen bzw. zu gestalten, dass zur Erfüllung des Auskunftsrechts alle Angaben über einen Betroffenen ausgedruckt werden können, oder es ist durch ein Verfahren sicherzustellen, dass alle Angaben zu einer Person manuell aus dem System extrahiert werden können.

Wendet sich ein Betroffener an das Unternehmen bzw. einen Mitarbeiter und macht ein Betroffenenrecht geltend, so leitet dieser das Anliegen unverzüglich an den Datenschutz-Manager weiter.

Der Datenschutz-Manager ist für die Umsetzung des Anliegens verantwortlich. Er wird hierzu:

- dem Betroffenen den Eingang bestätigen
- das Anliegen und die Identität des Betroffenen prüfen
- etwaig erforderliche Informationen von den fachlich Verantwortlichen einholen bzw. die Umsetzung (z.B. Löschung) durch die fachlich Verantwortlichen veranlassen
- dem Betroffenen antworten

Kommentiert [Helbing13]: Hat das Unternehmen eine Richtlinie zum Umgang und zur Erfüllung von Betroffenenrechten kann am Ende dieses Abschnitts darauf verwiesen werden. Den Entwurf einer solchen Richtlinie biete ich als Zusatzleistung an.

10. Dokumentation und Prüfung von Verarbeitungstätigkeiten

Das Unternehmen ist kraft Gesetzes verpflichtet,

- Den – sofern benannt – Datenschutzbeauftragten frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängende Aktivitäten einzubinden, Art. 38 Abs. 1 DSGVO,
- alle Verarbeitungstätigkeiten in einem „**Verzeichnis der Verarbeitungstätigkeiten**“ zu dokumentieren und dieses den Datenschutzaufsichtsbehörden auf Verlangen vorzulegen, Art. 30 DSGVO,
- die Einhaltung der Datenschutzgrundsätze (siehe Ziffer 5.1) und sonstigen Bestimmungen der DSGVO nachweisen zu können, Art. 24 Abs. 1, Art. 5 Abs. 2 DSGVO (sog. Rechenschaftspflicht), und
- durch geeignete technische und organisatorische Maßnahmen bereits im Planungsstadium sowie auch im Umsetzungsstadium von Verarbeitungstätigkeiten sicherzustellen, dass die Anforderungen der DSGVO eingehalten werden, Art. 25 Abs. 1 DSGVO (sog. „Datenschutz durch Technikgestaltung“).

Das Unternehmen legt zur Sicherstellung dieser Anforderungen mit dieser Ziffer 10 Prozesse zur Prüfung und Dokumentation von „Verarbeitungstätigkeiten“ (zum Begriff siehe Ziffer 10.1) fest. Diese enthalten Pflichten des Verarbeitungs-Verantwortlichen für folgende Zeitpunkte:

- Planung: das Erreichen eines konkreten Planungsstadiums der beabsichtigten Verarbeitungstätigkeit, d.h. der Zeitpunkt zu dem wesentliche Aspekte des Inhalts und Umfangs der Datenverarbeitung feststehen oder absehbar sind, siehe Ziffer 10.2.
- Einführung der Verarbeitungstätigkeit, d.h. der Beginn der Verarbeitung personenbezogener Daten, siehe Ziffer 10.3.
- Durchführung der Verarbeitungstätigkeit, siehe Ziffer 10.4.
- Wesentliche Änderung oder Beendigung der Verarbeitungstätigkeit, siehe Ziffer 10.5.

Der Anhang „Prozess Verarbeitungstätigkeit“ stellt die einzelnen Phasen und den zugehörigen Prozess grafisch dar.

10.1 Vorliegen einer Verarbeitungstätigkeit

Eine „**Verarbeitungstätigkeit**“ ist ein Bündel von Verarbeitungsschritten, das einem einheitlichen, übergeordneten Zweck dient, z.B. ein bestimmter Geschäftsprozess oder ein IT-Tool. Beispiele für Verarbeitungstätigkeiten sind:

Nutzung spezieller Software oder Geräte, mit denen Mitarbeiterdaten erfasst, gespeichert oder

ausgewertet werden (z.B. Zeiterfassungssystem, digitale Personalakten, elektronische Zugangskartensystem, Videoüberwachung).

Standardisierte interne Abläufe, bei denen Mitarbeiterdaten kontinuierlich oder systematisch erfasst, gespeichert oder genutzt werden (z.B. Umgang mit Bewerberdaten, Verwaltung und Abwicklung von Fortbildungsmaßnahmen, Entgeltabrechnung, E-Mail Newsletter für Kunden).

Bei der Abgrenzungsfrage, ob bestimmte Verarbeitungen eine große oder mehrere kleinere Verarbeitungstätigkeiten darstellen, sind folgende Gesichtspunkte zu berücksichtigen:

Beispiel für Abgrenzungsfrage: eine Verarbeitungstätigkeit „Verwaltung Mitarbeitergespräche“ oder zwei Verarbeitungstätigkeiten „Zielvereinbarung“ und „Zielerreichungsmessung“?

- Eine zu feingliedrige Aufteilung führt zu unübersichtlich vielen Verarbeitungstätigkeiten und erhöht unnötig den Verwaltungsaufwand.
- Eine zu grobgliebrige Aufteilung (z.B. „Personaldatenverwaltung“) erlaubt keine sinnvolle Prüfung der Datenschutzkonformität mehr.
- Zur Ermittlung eines übergeordneten Zweckes bietet sich eine Orientierung an bestehenden Geschäftsprozessen oder Aufgabenbereichen an.
- Die Abgrenzung kann auch anhand der technischen Systeme erfolgen, die der Verarbeitungstätigkeit zu Grunde liegen. Nicht jedes IT-System muss aber als eigene Verarbeitungstätigkeit angesehen werden.
- Würde eine Verarbeitungstätigkeit in die Verantwortlichkeit mehrerer Fachbereiche fallen, kann eine Aufteilung sinnvoll sein.

Rein abstrakte Verarbeitungen ohne konkreten Zweck

Beispiele: allgemeine Nutzung von Office-Programmen, allgemeine Projektorganisation

oder nur gelegentliche Verarbeitungen

Beispiele: Führen von Teilnehmerlisten von Besprechungen

stellen keine „Verarbeitungstätigkeiten“ dar. Für diese Verarbeitungen gelten nicht die Prüf- und Dokumentationsanforderungen gemäß dieser Ziffer 10, es sind aber dennoch die Anforderungen des Datenschutzes zu beachten.

10.2 Planung von Verarbeitungstätigkeiten (Konzeptionsphase)

Mit Erreichen eines konkreten Planungsstadiums der beabsichtigten Verarbeitungstätigkeit entwirft der Verarbeitungs-Verantwortliche einen vorläufigen Eintrag für das Verzeichnis der Verarbeitungstätigkeiten. Er nutzt hierfür das vom Datenschutz-Manager bereitgestellte Formular bzw. IT-Tool. In der Meldung ist der Eintrag als „in Planung“ zu kennzeichnen.

Der Verarbeitungs-Verantwortliche stellt dem Datenschutz-Manager – und sofern benannt, dem Datenschutzbeauftragten – den Entwurf zur Verfügung.

Der Verarbeitungs-Verantwortliche füllt sodann mit Unterstützung des Datenschutz-Managers die „Checkliste DSGVO“ aus. Bei Unklarheiten zieht der Verarbeitungs-Verantwortliche – sofern benannt – den Datenschutzbeauftragten hinzu.

Mit Hilfe der Checkliste wird die Einhaltung der DSGVO-Anforderungen geprüft, dokumentiert und die Verarbeitungstätigkeit einer Risikoklasse (niedrig, mittel, hoch) zugeordnet (Risikoklassifizierung).

Ergeben sich aus der Checkliste noch erforderliche Datenschutz-Maßnahmen, werden diese vom Datenschutz-Manager schriftlich festgehalten und dabei folgendes dokumentiert: Inhalt der Maßnahme, Verantwortlicher und vereinbarte Umsetzungsfrist.

Beispiele für Datenschutz-Maßnahmen: Datenschutzinformationen zur Sicherstellung der Transparenz sind noch zu entwerfen und zu veröffentlichen, eine Datenschutzfolgenabschätzung ist durchzuführen.

Für den Inhalt der Checkliste und die Umsetzung der Datenschutz-Maßnahmen ist der Verarbeitungs-Verantwortliche verantwortlich. Die Umsetzung der Datenschutz-Maßnahmen

Kommentiert [Helbing14]: Hierzu kann das von der GDD bereitgestellte Formular genutzt werden. Siehe unter <https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo> > „Praxishilfe V“ > Muster als Word-Datei.

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 Verzeichnisse 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.

Werden im Rahmen der Verarbeitungstätigkeit keinerlei Daten mehr verarbeitet – d.h. auch nicht zu Aufbewahrungszwecken gespeichert – so vermerkt der Datenschutz-Verantwortliche im Verzeichnis der Verarbeitungstätigkeiten die Verarbeitungstätigkeit als „abgeschlossen“ und dokumentiert das Datum des Abschlusses.

Die Datenschutz-Dokumentation samt begleitender Unterlagen ist für weitere drei Jahre ab Abschluss der Verarbeitungstätigkeit aufzubewahren.

Bei Änderungen an der Datenschutz-Dokumentation nach dem Zeitpunkt der Einführung der Verarbeitungstätigkeit beachtet der ändernde Mitarbeiter folgendes:

- Alle Änderungen sind mit Datum und Verfasser kenntlich zu machen.
- Es ist sicherzustellen, dass Altfassungen weiterhin abrufbar bleiben.
- Soweit ein IT-Tool zur Führung des Verzeichnisses der Verarbeitungstätigkeiten genutzt wird, ist die Änderung dort vom verantwortlichen Mitarbeiter zu hinterlegen.
- Änderungen sind dem Datenschutz-Manager mitzuteilen.

10.6 Führung des Verzeichnisses der Verarbeitungstätigkeiten

Die Führung des Verzeichnisses der Verarbeitungstätigkeiten erfolgt durch den Datenschutz-Manager, indem er die von den Verarbeitungs-Verantwortlichen eingereichten Einträge und ausgefüllten Checklisten bei sich zentral sammelt und dokumentiert.

Kommentiert [Helbing15]: Alternativ ist möglich, dass jeder Verarbeitungs-Verantwortliche für seine Verarbeitungstätigkeiten die Einträge in das Verzeichnis der Verarbeitungstätigkeiten eigenständig pflegt und die Einträge zentral zusammengeführt werden (z.B. Gruppenlaufwerk, SharePoint, spezielles Tool)

11. Datenschutzfolgenabschätzung

Hat eine Verarbeitung personenbezogener Daten für Betroffene (z.B. Mitarbeiter oder Kunden) voraussichtlich ein hohes Risiko, so muss vor *Beginn* der Verarbeitung eine Datenschutzfolgenabschätzung durchgeführt werden, Art. 35 DSGVO („**Datenschutzfolgenabschätzung**“).

Bei dieser werden die Risiken für Betroffene ermittelt und bewertet, erforderlichenfalls Abhilfemaßnahmen zur Risikoreduzierung festgelegt und umgesetzt und dies dokumentiert. Die Datenschutzfolgenabschätzung ist ein gesetzlich vorgeschriebenes Verfahren, um Risiken bei besonders riskanten Verarbeitungen zu reduzieren und dies zu dokumentieren.

Die Datenschutzfolgenabschätzung ist häufig ein komplexer Prozess bei dem verschiedene Beteiligte (z.B. Fachabteilung, Datenschutz, Informationssicherheit, ggf. Mitarbeitervertretungen und Aufsichtsbehörden) mitwirken müssen. Die Datenschutzfolgenabschätzung muss deshalb mit ausreichender Vorlaufzeit noch im Planungsstadium der Verarbeitung begonnen werden.

11.1 Erforderlichkeit einer Datenschutzfolgenabschätzung

Eine Datenschutzfolgenabschätzung ist erforderlich, wenn die Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, Art. 35 Abs. 1 Satz 2 DSGVO.

Fälle, bei denen eine Datenschutzfolgenabschätzung notwendig sein kann: Verwendung von biometrischen Systemen zur Zutrittskontrolle, umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen (Großkanzlei), umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen (Flottenmanagement, Nachverfolgung der Laufwege von Kunden im Geschäft), Scoring durch Auskunfteien, Banken oder Versicherungen, Betrugserkennungssysteme, Betrieb von Bewertungsportalen, Geolokalisierung von Beschäftigten, Big-Data-Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden, Kundensupport mittels künstlicher Intelligenz, Erstellung umfassender Profile über das Kaufverhalten von Betroffenen.

Der Datenschutz-Manager prüft bei der Meldung von Verarbeitungstätigkeiten in der Planungsphase (siehe Ziffer 10.2), ob ein solches Risiko voraussichtlich besteht (sogenannte „**Schwellenwertanalyse**“) und informiert den Verarbeitungs-Verantwortlichen.

Kommentiert [Helbing16]: Siehe hierzu die „Muss-Liste“ der deutschen Datenschutzbehörden (abrufbar über den Link „Weiterführende Informationen“ am Ende der Ziffer):

11.2 Durchführung der Datenschutzfolgenabschätzung

Der Verarbeitungs-Verantwortliche führt die **Datenschutzfolgenabschätzung** durch und dokumentiert diese. Der Verarbeitungs-Verantwortliche

- holt dabei den Rat des Datenschutzbeauftragten ein, sofern ein solcher benannt ist
- bezieht diejenigen Fachbereiche ein, die bei der Ermittlung und Bewertung der Risiken, sowie bei der Festlegung und Umsetzung von Abhilfemaßnahmen fachliche Informationen oder Expertise zuliefern können (z.B. IT-Sicherheit, Auftragsverarbeiter)
- holt, soweit sinnvoll, den Standpunkt der Betroffenen ein
- zieht, soweit erforderlich, externe Expertise hinzu (z.B. zur IT-Sicherheitsexperten oder Rechtsberater).
- dokumentiert und koordiniert den Prozess der Datenschutzfolgenabschätzung und dessen Durchführung.

[Weiterführende Informationen zur Datenschutzfolgenabschätzung](#)

Kommentiert [Helbing17]: Je nach Unternehmensgröße und -gegenstand kann es sinnvoll sein, die Schwellenwertanalyse und die Durchführung einer Datenschutzfolgenabschätzung in einer gesonderten Richtlinie zu regeln und entsprechende Prüfkataloge und Vorlagen bereitzustellen. Entsprechende Entwürfe hierzu biete ich als Zusatzleistung an.

12. Auftragsverarbeitung durch Dienstleister

Werden personenbezogene Daten durch Dienstleister im Auftrag des Unternehmens verarbeitet (vgl. Ziffer 12.1), stellt der Verarbeitungs-Verantwortliche sicher, dass mit dem Dienstleister die erforderlichen Datenschutz-Vereinbarungen geschlossen (vgl. Ziffer 12.2) und die Dienstleister ausreichend überprüft (vgl. Ziffer 12.3) werden, Art. 28 DSGVO.

12.1 Vorliegen einer Auftragsverarbeitung

Eine Auftragsverarbeitung findet statt, wenn das Unternehmen personenbezogene Daten durch Dienstleister im Auftrag verarbeiten lässt und dabei vorgibt

- wofür und mit welchem Ziel die Daten verarbeitet werden sollen (Zwecke der Verarbeitung) und
- wie im Wesentlichen mit den Daten umzugehen ist (Mittel der Verarbeitung), z.B. wie lange die Daten gespeichert werden, welche Daten genutzt werden und an wen Daten weitergegeben werden sollen.

Auftragsverarbeitungen liegen häufig in **folgenden Fällen** vor:

- *Betrieb bzw. Hosting von Software oder Datenbanken mit personenbezogenen Daten durch IT-Dienstleister*
- *Nutzung von Cloud Diensten (z.B. Software as a Service), in denen personenbezogene Daten gespeichert sind*
- *Nutzung von Webseite-Analyse-Systemen (z.B. Google Analytics)*
- *Externes Scannen, Archivieren oder Vernichten von Unterlagen*

Maßgeblich ist dabei, ob das Unternehmen faktisch, also in der Praxis, die Zwecke und Mittel der Verarbeitung vorgibt.

Je detaillierter die Vorgaben zum Datenumgang an den Externen sind und je stärker der Externe kontrolliert wird, desto wahrscheinlicher ist eine Auftragsverarbeitung. Erhält der Externe hingegen eigene Nutzungsrechte an den Daten, hat er einen eigenen umfassenden Ermessensspielraum beim Datenumgang oder werden ganze Aufgabenbereiche zur eigenverantwortlichen Erledigung übertragen, so spricht dies gegen eine Auftragsverarbeitung.

Von einer Auftragsverarbeitung ist auch dann auszugehen, wenn der Externe Leistungen erbringt, bei dem die Verarbeitung personenbezogener Daten nicht unmittelbar Gegenstand

Kommentiert [Helbing18]: Zum Vorliegen einer Auftragsverarbeitung siehe auch die hilfreichen FAQs der Bayerischen Aufsichtsbehörde, abrufbar über den Link „Weiterführende Informationen“ am Ende der Ziffer.

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).

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.

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“.

45 DSGVO erfolgt, insbesondere in ein Land, Gebiet bzw. Sektor, für das die EU Kommission beschlossen hat, dass dieses ein angemessenes Schutzniveau aufweist (z.B. Übermittlung in die Schweiz; Übermittlung an ein US-Unternehmen, das nach dem PrivacyShield selbstzertifiziert ist)

- das Unternehmen geeignete Garantien im Sinne des Artikel 46 DSGVO vorgesehen hat, insbesondere mit den Datenempfängern einen Vertrag gemäß den Standardvertragsklauseln der EU Kommission geschlossen hat.

Der Verarbeitungs-Verantwortliche hat die Übermittlung personenbezogener Daten in ein Drittland vorher mit dem Datenschutz-Manager abzustimmen, außer die Übermittlung erfolgt nur vereinzelt und nur in geringem Umfang.

Der Verarbeitungs-Verantwortliche dokumentiert im Verzeichnis der Verarbeitungstätigkeiten, die Übermittlung in das Drittland (betroffene Datenarten und Drittland), sowie die Basis für deren rechtliche Zulässigkeit (z.B. konkreter Ausnahmefall nach Art. 49 DSGVO, Kopie des geschlossenen Vertrags gemäß den Standardvertragsklauseln der EU Kommission)

Die vorgenannten Anforderungen gelten auch, wenn die Übermittlung in ein Drittland durch einen Auftragsverarbeiter des Unternehmens oder durch dessen Subunternehmer erfolgt.

Das Unternehmen nutzt das Online-Angebot eines deutschen IT-Dienstleisters, dieser nutzt seinerseits Cloud-Dienste eines US-Anbieters (z.B. Amazon AWS).

[Weiterführende Informationen zu Übermittlungen in Drittländer](#)

14. Umgang mit Datenschutzvorfällen

Das Unternehmen ist verpflichtet, Datenschutzvorfälle zu dokumentieren, in bestimmten Fällen diese innerhalb von 72 Stunden Datenschutz-Aufsichtsbehörden zu melden und ggf. Betroffene zu benachrichtigen, Art. 33, 34, 4 Nr. 12 DSGVO.

Die wesentlichen Schritte sind im [Anhang „Prozess Datenschutzvorfall“](#) dargestellt.

14.1 Vorliegen eines Datenschutzvorfalls

„**Datenschutzvorfall**“ ist jede „Verletzung des Schutzes personenbezogener Daten“ im Sinne von Art. 4 Ziffer 12 DSGVO, d.h. jede Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität personenbezogener Daten.

Verletzung der Vertraulichkeit: Sie liegt vor bei der unbefugten oder versehentlichen Offenlegung von personenbezogenen Daten oder einem solchen Zugriff auf diese.

Aufgrund einer Fehlkonfiguration im System konnten Unberechtigte innerhalb des Unternehmens Beurteilungen von Mitarbeitern einsehen.

Gehaltsbescheinigungen wurden an einen falschen Adressaten gesendet.

Ein unverschlüsselter USB-Stick mit Kontaktdaten von Kunden wurde gestohlen.

Eine E-Mail mit Mitarbeiterdaten wurde versehentlich an einen zu großen Verteilerkreis gesendet.

Verletzung der Verfügbarkeit: Sie ist gegeben bei einem unbefugten oder versehentlichen Verlust des Zugriffs auf personenbezogene Daten oder der Vernichtung oder dem Verlust von personenbezogenen Daten. Ein Datenschutzvorfall liegt bereits dann vor, wenn die Verfügbarkeit von personenbezogenen Daten *vorrübergehend* nicht gegeben ist.

Der Zugriff auf die digitale Personalakte ist längere Zeit unmöglich.

Ein USB-Stick, Laptop oder Smartphone mit personenbezogenen Daten kommt abhanden.

Rechner wurden mit Ransomware infiziert (Schadsoftware, die Daten verschlüsselt und nur nach

Kommentiert [Helbing21]: Vollständige Länderliste abrufbar über den Link „weiterführende Informationen“ am Ende der Ziffer .

Kommentiert [Helbing22]: Prüfbar über die offizielle Webseite des PrivacyShields (siehe „weiterführende Informationen“)

Kommentiert [Helbing23]: Musterverträge abrufbar über den Link „weiterführende Informationen“

Zahlung eines „Lösegelds“ wieder entschlüsselt)

Verletzung der Integrität meint die unbefugte oder versehentliche Änderung von personenbezogenen Daten.

Versehentlich wurden Änderungen im Datensatz eines falschen Mitarbeiters oder Kunden eingetragen.

14.2 Interne Meldepflicht

14.2.1 Adressat der internen Meldung

Jeder Mitarbeiter meldet einen Datenschutzvorfall sowie jeden konkreten Verdacht auf einen Datenschutzvorfall bei Bekanntwerden sofort intern an den Datensicherheits-Manager. Dessen Kontaktdaten sind im Anhang Kontaktdaten genannt.

Kommentiert [Helbing24]: Alternativ: „im Intranet einsehbar unter *Link*“

14.2.2 Zeitpunkt und Form der internen Meldung

Die interne Meldung muss so schnell wie möglich erfolgen, insbesondere bei schwerwiegenden Datenschutzvorfällen und solchen, bei denen zum Schutz der Betroffenen Schutzmaßnahmen durch das Unternehmen getroffen werden können.

Die Meldung kann in jeder Form erfolgen. Bei mündlichen Meldungen sind diese unverzüglich schriftlich (z.B. per E-Mail) nachzuholen.

14.2.3 Inhalt der internen Meldung

Soweit bekannt sind in der Meldung folgende Fragen zu beantworten oder die Antworten unverzüglich nachzureichen:

- Was ist passiert? (möglichst genaue Beschreibung des Datenschutzvorfalls).
- Betrifft der Datenschutzvorfall eine Verarbeitung, die das Unternehmen für einen anderen im Auftrag ausführt oder für sich selbst?
- Um wessen personenbezogene Daten geht es? (z.B. Mitarbeiter, Ansprechpartner Kunde).
- Die Daten wie vieler Personen sind ungefähr betroffen? (z.B. 1-10, mehrere Tausend).
- Welche Arten von personenbezogenen Daten sind betroffen (z.B. „gesamtes E-Mail Postfach“, „Gehaltslisten“, „Name, Anschrift und berufliche Kontaktdaten“).
- Wie viele Datensätze sind ungefähr betroffen? (z.B. 10-20, 100-200, 10.000).
- Wer hat die Meldung vorgenommen und wie ist diese Person ggf. kurzfristig erreichbar?
- Seit wann (Datum und Uhrzeit) besteht Kenntnis von dem Datenschutzvorfall?

Soweit möglich ist zudem anzugeben:

- Von welchen Mitarbeitern können weitere Informationen zum Datenschutzvorfall erlangt werden und wie sind diese erreichbar?
- Was sind die wahrscheinlichen Folgen des Datenschutzvorfalls?
- Welche Maßnahmen zur *Behebung* des Datenschutzvorfalls wurden bereits ergriffen? Welche weiteren Maßnahmen werden vorgeschlagen? (z.B. Fernlöschung von Daten auf einem verloren gegangenen Smartphone).
- Welche Maßnahmen zur *Abmilderung möglicher nachteiliger Auswirkungen* wurden bereits ergriffen oder werden vorgeschlagen?

14.3 Weiteres Vorgehen

14.3.1 Information des Leiter Rechts

Der Datensicherheits-Manager informiert unverzüglich den Datenschutz-Manager über den Datenschutzvorfall.

Kommentiert [Helbing25]: Je nach Unternehmensgröße und -gegenstand kann es sinnvoll sein, den Umgang mit Datenschutzvorfällen in einer gesonderten Richtlinie detaillierter zu regeln und ggf. Vorlagen zu erstellen. Entsprechende Entwürfe biete ich als Zusatzleistung an.

Kommentiert [Helbing26]: Ggf. ergänzen: „sowie den Datenschutzbeauftragten“, „den Leiter Recht/Compliance“, „die Unternehmensleitung“.

14.3.2 Nachforschung und Sicherungsmaßnahmen

Handelt es sich bei der Meldung um einen *Verdacht* eines Datenschutzvorfalls leitet der Datensicherheits-Manager unverzüglich etwaig erforderliche Nachforschungsmaßnahmen ein. Gleiches gilt, wenn die wahrscheinlichen Folgen des Datenschutzvorfalls und damit das mögliche Risiko des Datenschutzvorfalls unklar sind. Bestätigt sich der Verdacht, dokumentiert der Datensicherheits-Manager Datum und Uhrzeit, zu dem ein hinreichendes Maß an Sicherheit betreffend den Datenschutzvorfall besteht. Dieser Zeitpunkt ist für den Beginn der 72-Stunden Frist zur etwaigen Meldung an eine Datenschutz-Aufsichtsbehörde maßgeblich.

Soweit erforderlich leitet der Datensicherheits-Manager sofort Maßnahmen zur Behebung des Datenschutzvorfalls oder zur Abmilderung möglicher nachteiliger Auswirkungen des Datenschutzvorfalls ein.

Sperrung von Zugängen, Änderung von Passwörtern, Einspielen von Backups

14.3.3 Information von Auftraggebern bei Auftragsverarbeitung

Betrifft der Datenschutzvorfall eine Verarbeitung, die das Unternehmen für einen anderen im Auftrag als Auftragsverarbeiter durchführt informiert der Datensicherheits-Manager unverzüglich den Auftraggeber.

Kommentiert [Helbing27]: Ggf. ergänzen „nach Rücksprache mit der Rechtsabteilung/Geschäftsführung“

14.3.4 Risikoanalyse

Der Datensicherheits-Manager führt eine Risikoanalyse nach Art 33 Abs. 1, 34 Abs. 1 DSGVO durch. Er zieht hierzu den Datenschutz-Manager und den Datenschutzbeauftragten hinzu. Im Rahmen der Risikoanalyse wird ermittelt, ob der Datenschutzvorfall

- zu *keinem* Risiko (dann siehe Ziffer 14.3.6) [grüne Kategorie]
- zu einem Risiko (dann siehe Ziffer 14.3.4 und 14.3.6) [gelbe Kategorie], oder
- zu einem *hohen* Risiko (dann siehe Ziffer 14.3.4, 14.3.5 und 14.3.6) [rote Kategorie]

Kommentiert [Helbing28]: Zu den dabei zu beachtenden Kriterien siehe WP250, deutsche Fassung Seite 26 ff, abrufbar unter dem Link „weiterführende Informationen“ am Ende der Ziffer.

für die Rechte und Freiheiten natürlicher Personen führt.

14.3.5 Ggf. Meldung an die Datenschutz-Aufsichtsbehörde

Führt ein Datenschutzvorfall voraussichtlich zu einem Risiko für die Rechte und Freiheiten einer natürlichen Person (gelbe oder rote Kategorie) ist eine Meldung an die Datenschutz-Aufsichtsbehörde gemäß Art. 33 DSGVO vorzunehmen, sofern das Unternehmen die Daten nicht lediglich im Auftrag eines anderen verarbeitet hat. Für die Meldung ist der Datenschutz-Manager verantwortlich.

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.

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 Präsenzs Schulung)

Kommentiert [Helbing29]: Die DSGVO verlangt nur bei Unternehmen, die als Auftragsverarbeiter handeln Vertraulichkeitsverpflichtungen, vgl. Art. 28 Abs. 3 b) DSGVO. Die deutschen Aufsichtsbehörden leiten aus der DSGVO aber eine umfassendere Pflicht zur Einholung von Verpflichtungserklärungen ab, siehe hier: https://www.lda.bayern.de/media/dsk_kpnr_19_verpflichtungBeschaefigte.pdf

Kommentiert [Helbing30]: 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_verpflichtungBeschaefigte.pdf).

Kommentiert [Helbing31]: Bitte ggf. anpassen

- 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 [Helbing32]: 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

- 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.

Kommentiert [Helbing33]: Hierzu bieten sich Konkretisierungen und Beispiele in unternehmensinternen IT-Richtlinien an.

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

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

Kommentiert [Helbing34]: Bei späteren Änderungen im Text der Richtlinie, diese Tabelle bitte fortführen. Spalte „Freigabe“ ggf. löschen, wenn kein Vier-Augen Prinzip für Änderung vorgesehen ist.

Die Unternehmensleitung:

(Name)

(Funktion)

(Ort, Datum)



Unterschrift

Datenschutzrichtlinie V1.0

Anhang: Begriffe und Definitionen

- „**automatisierte Einzelentscheidung**“: siehe Ziffer 5.3.
- „**Betroffener**“: siehe Ziffer 2.
- „**Betroffenenrechte**“: siehe Ziffer 9.1.
- „**Datenschutz-Dokumentation**“: siehe Ziffer 10.2
- „**Datenschutzbeauftragter**“: siehe Ziffer 3.3
- „**Datenschutzfolgenabschätzung**“: siehe Ziffer 10.2.
- „**Datenschutzverletzung**“: siehe Ziffer 12.
- „**Datenschutzvorfall**“: siehe Ziffer 14.1.
- „**Drittland**“: siehe Ziffer 13.
- „**personenbezogene Daten**“: siehe Ziffer 2.
- „**Profiling**“: siehe Ziffer 9.1.7.
- „**Schwellenwertanalyse**“: siehe Ziffer 11.1.
- „**sensible personenbezogene Daten**“: siehe Ziffer 6.2.
- „**Verarbeitungs-Verantwortliche**“: siehe Ziffer 3.1.
- „**Verarbeitung**“: siehe Ziffer 3.1.
- „**Verarbeitungstätigkeit**“: siehe Ziffer 10.1
- „**Verzeichnis der Verarbeitungstätigkeiten**“: siehe Ziffer 10.

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

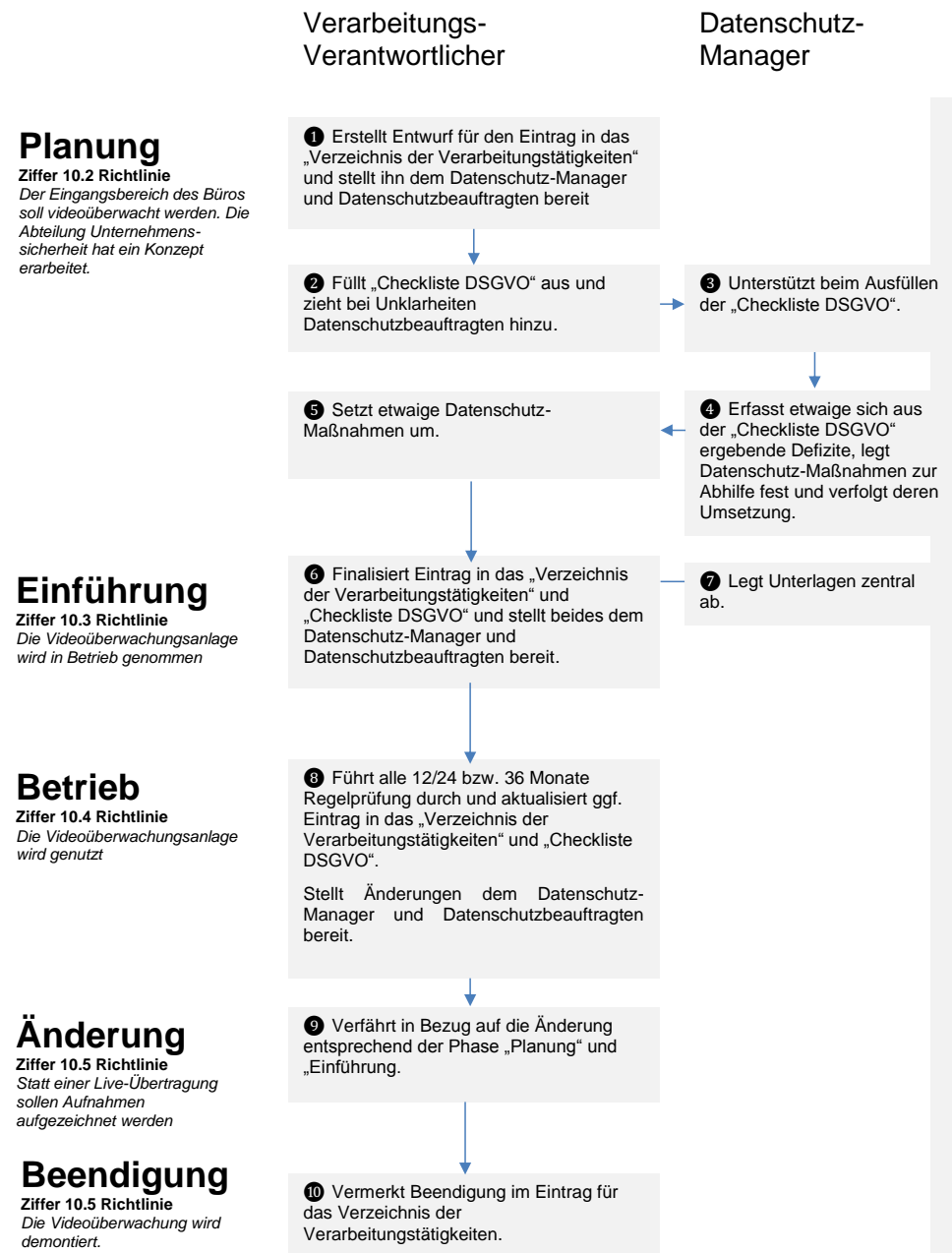
Die Kontaktdaten des Datenschutzbeauftragten sind:

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

Kommentiert [Helbing35]: 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 [Helbing36]: 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.

Anhang: Prozess Verarbeitungstätigkeit



Anhang: Prozess Datenschutzvorfall

