

DSGVO

Die neue Datenschutzgrundverordnung
in der Praxis





Vorwort

Zum 25. Mai 2018 tritt EU-weit die neue EU-Datenschutzgrundverordnung (DSGVO) und das neue Bundesdatenschutzgesetz in Kraft. Es dient der Vereinheitlichung des Datenschutzrechts innerhalb der EU, stärkt die Rechte Betroffener und schafft Klarheit bei der Kontrolle und Verarbeitung personenbezogener Daten. Das DSGVO ist ein Verbotsgesetz: Wozu man keine Erlaubnis im Gesetz findet, das ist verboten.

Es stellt damit klar, dass alles in Sachen Datenschutz unternommen werden muss, was im Sinne der Kunden nötig ist. Denn es sollte jedem

klar sein, dass die personenbezogenen Daten nicht dem Daten-Verarbeiter, sondern den Kunden gehören!

Die DSGVO gibt keinen Anlass zur Panik. Sie sollte jedoch von Unternehmen ernst genommen werden, da die neuen Datenschutzregelungen zu Änderungen in der Dokumentation von Betriebsabläufen führen werden. Gefordert sind zudem Verfahren und Methoden, die dem heutigen Stand der Technik entsprechen.

Es besteht außerdem eine Meldepflicht bei Verstößen oder Datenschutzpannen. Werden die neuen

Regelungen nicht befolgt, drohen ab dem 25. Mai 2018 unter anderem Bußgelder, Werbeverbote oder Schadensersatzansprüche.

Was das neue Datenschutzrecht für Sie und für unsere Zusammenarbeit aus unserer Sicht bedeutet, haben wir in dieser Dokumentation zusammengestellt. Sie erhalten einen Überblick über die neue Rechtslage und viele praxisorientierte Hinweise zur Umsetzung innerhalb Ihres Betriebes.

Inhalt

I. Grundlagen

Gesetzlicher Rahmen/Ziele/wichtige Begriffe/Behörden und Sanktionen 5

II. Datenerhebung und Datenspeicherung

Gesetzliche Anforderungen/Pflichten von Betrieben/Rechte der Betroffenen/
Meldepflicht bei Verstößen 12

III. Notwendige Dokumentationen

Datenschutz-Folgeabschätzung/Verfahrensverzeichnis/Auftragsverarbeitung/
technische und organisatorische Maßnahmen 24

IV. Der Datenschutzbeauftragte (DSB)

Bestellung/Zuständigkeiten 34

V. Rechte und Pflichten der Arbeitgeber und Mitarbeiter

Allgemeiner Überblick 36

Gesetzlicher Rahmen

1995	2009	2016	2018
Erste EU-Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.	Start umfassender Reformen aufgrund des rasant wachsenden Internethandels mit den damit verbunden Risiken der Datenverarbeitung.	EU-Richtlinie Datenschutzgrundverordnung 2016/679 mit einer zweijährigen Übergangsfrist.	EU-DSGVO ist für alle EU-Mitglieder zwingend anzuwenden und tritt (gemeinsam mit dem neuen BDSG in Deutschland) am 25. Mai in Kraft.

Zielsetzungen der DSGVO



Rechtsgrundsätze der DSGVO



Wichtige Begrifflichkeiten

Was sind personenbezogene Daten?

Immer dann, wenn personenbezogene Daten nicht vollständig anonym erhoben werden, sondern einer bestimmten Person zugeordnet werden können, betrifft dies den Bereich des Datenschutzrechts.

- **Geburtsdaten/ Kontaktdaten**
- **Name & Anschrift**
- **IP-Adresse von Nutzern**
- **Kauf-, Surf- und Klick-Historie einzelner Nutzer**
- **Einkommen, Ausbildung & Gesundheitsdaten**

Der Verantwortliche ist eine natürliche oder juristische Person, Behörde, ein Unternehmen oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Der Betroffene ist die identifizierbare natürliche Person, deren Daten durch den Verantwortlichen erhoben, verarbeitet und genutzt werden.

Verarbeitung von Daten ist das Erfassen, Speichern, Bearbeiten, Löschen, Sperren, Drucken, Aufbereiten oder die Zusammenführung von Daten.

Nutzung von Daten ist die Verwendung der Daten für einen bestimmten Zweck (z.B. Werbung).

Übermittlung von Daten ist die Übertragung von Daten zu einer internen oder externen Stelle für einen bestimmten Zweck.

Der Auftragsverarbeiter ist eine natürliche oder juristische Person, eine Behörde, ein Unternehmen oder eine andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Überblick über bestehende und neue Regelungen

Was unverändert bleibt:

- Kundendaten bedürfen einer **angebbaren Herkunftsquelle**.
- In werblichen Ansprachen (Post, Email, Telefon) muss auf das **Widerspruchsrecht** des Betroffenen hingewiesen werden.
- Die **Auftragsverarbeitung** ist erlaubt, muss aber schriftlich vereinbart werden.
- Kunden haben ein **detailliertes Auskunftsrecht** über Herkunft, Inhalte und Speicherungszweck der sie betreffenden Daten.
- Die Bestellung eines **Datenschutzbeauftragten** ist bei der Verarbeitung von besonders sensiblen Daten zwingend erforderlich.

Wichtige Neuregelungen ab Mai 2018:

- **Dokumentationspflichten** und Pflicht zur **Führung eines Verzeichnisses aller Datenverarbeitungsprozesse**.
- **Technische und organisatorische Maßnahmen** (TOMs) zur Sicherung eines dauerhaft hohen Datenschutzniveaus sind zwingend erforderlich und zu dokumentieren.
- **Datenschutzfolgeabschätzung** bei erhöhten Risiken besonders sensibler Daten erforderlich.
- Pflicht zur Datenportabilität, Recht auf **Widerspruch und Löschung** von Daten, **Recht auf Vergessenwerden**.
- **Meldepflicht** bei Datenpannen.
- **Neue Haftungsregeln** mit deutlich erhöhten Sanktionen und Bußgeldern.

Kompetenzen der Aufsichtsbehörden



Die jeweils zuständige Landes- behörde ...

- darf **anlassfreie Kontrollen** mit vollen Zugriffsrechten durchführen.
- kann einzelne Verfahren und Prozesse **verbieten**, die nicht datenschutzkonform sind.
- hat das Recht, Unternehmen **zu schließen**, falls angeordnete Nachfristen nicht eingehalten werden.
- kann unqualifizierte Datenschutzbeauftragte **abbestellen**.
- hat **Strafantragsrecht**, wenn Verstöße vor Gericht verhandelt werden.
- bestimmt die Höhe und Erteilung von **Bußgeldern**.

Strafverfolgung und Strafmaß

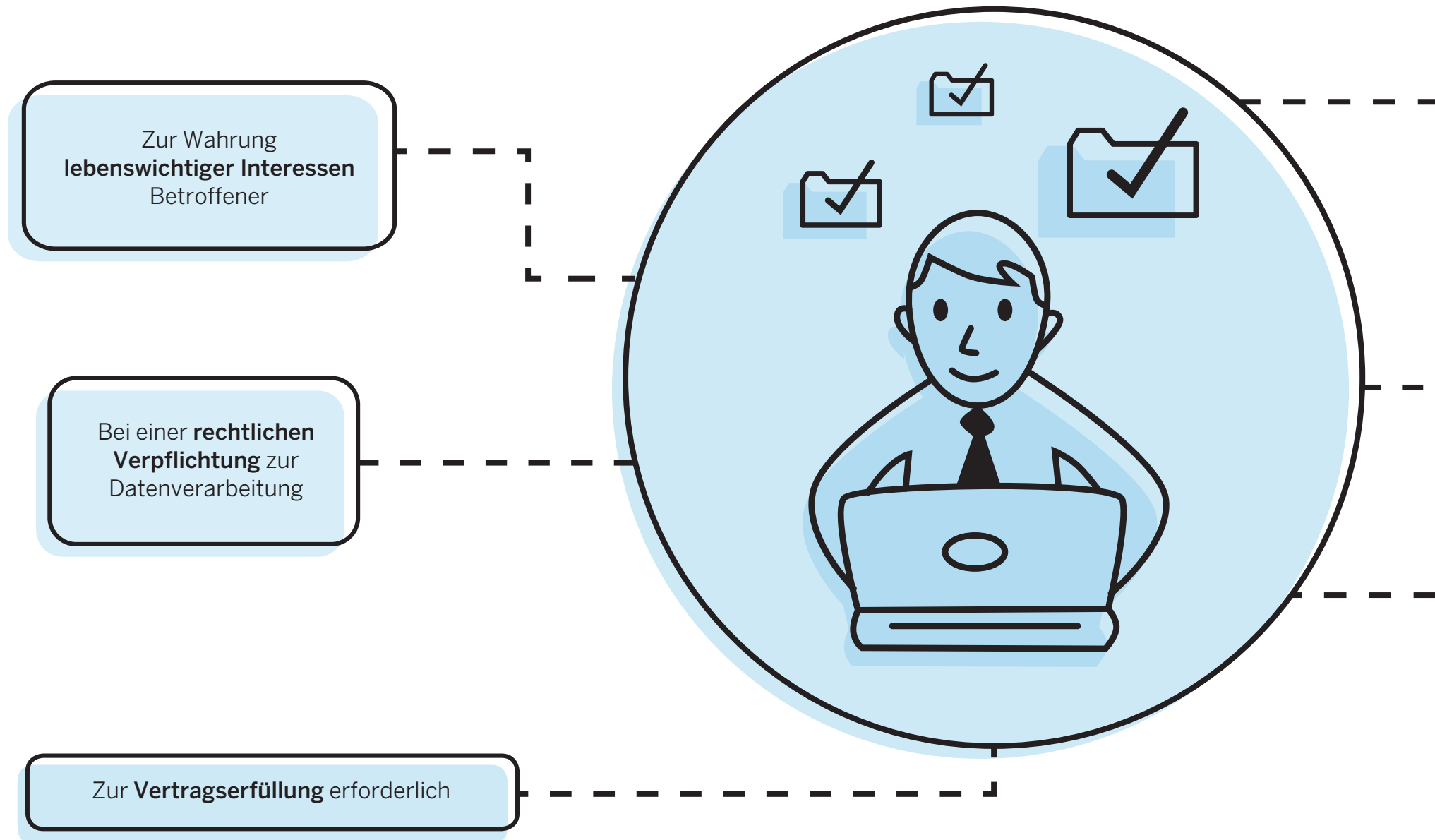
Wichtige Bemessungskriterien bei der Festlegung von Bußgeldern:

- **Art, Schwere, Dauer, Vorsätzlichkeit** oder **Fahrlässigkeit** des Verstoßes
- Die **getroffenen Maßnahmen** zur Minderung des entstandenen Schadens
- **Grad der Verantwortung** unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen.
- Etwaige einschlägige **frühere** Verstöße
- Umfang der **Zusammenarbeit mit der Aufsichtsbehörde**, um dem Verstoß abzuhelpen und seine möglichen nachteiligen Auswirkungen zu mindern
- **Kategorien personenbezogener Daten**, die von dem Verstoß betroffen sind

Achtung:

- Bußgelder werden bei Verstößen **Pflicht** (kein Ermessensspielraum mehr, ob ein Verstoß geahndet wird).
- Die Bußgelder werden aufgrund dieser Pflicht und der künftigen Meldepflicht bei Verstößen **wesentlich häufiger** verhängt werden.
- Das Strafmaß muss in jedem Einzelfall **wirksam, verhältnismäßig und abschreckend** sein.
- Das „durchschnittlich“ verhängte Bußgeld wird **deutlich steigen**. Im Maximalfall bis zu **20 Mio. Euro bzw. 4% des vorjährigen Jahresumsatzes**.
- Dies gilt auch für **Auftragsnehmer** (-verarbeiter), wenn sie gegen ihren Auftrag verstoßen oder es zu Datenpannen kommt.

Wann darf ich Daten verarbeiten?



Zur Durchführung
**vorvertraglicher
Maßnahmen**

Bei einer **Einwilligung
der betroffenen
Person**

Wenn eine gesetzliche
Erlaubnis besteht, ist
keine Einwilligung mehr
erforderlich!

Berechtigtes Interesse
des Verantwortlichen
oder eines Dritten*

* **Erlaubnistatbestand**, der die wesentlichen
„wirtschaftlichen oder ideell berechnete
Interessen“ beinhaltet.

Eine **Abwägung der berechtigten Interessen
des Unternehmens** gegen die Interessen des
Betroffenen muss dazu ergeben, dass die des
Unternehmens überwiegen.

Die **Datennutzung zur Direktwerbung ist
zulässig**, da diese als berechtigtes Interesse
angesehen wird.

-->

Postalische Werbeanschreiben (mit dem
Hinweis auf das Widerspruchsrecht) sind
auch künftig **ohne Einwilligung** erlaubt.

Besonderheiten im Gesundheitswesen: die Gesundheitsdaten

Definition:

Gesundheitsdaten sind alle Daten, die den physischen und psychischen Zustand von Menschen betreffen, im Zuge einer medizinischen Betreuung, Untersuchung, Pflege erhoben werden oder der Verrechnung von Gesundheitsdienstleistungen bzw. der Versicherung von Gesundheitsrisiken dienen.

Augenoptiker und Hörakustiker verarbeiten Gesundheitsdaten (Dioptrien, Audiometriedaten, etc.)!

Zulässige Datenverarbeitung (ohne vorherige Einwilligung)

Zur **Versorgung oder Behandlung** im Gesundheits- oder Sozialbereich

Zum Zwecke der **Gesundheitsvorsorge**

Zur Durchführung **vorvertraglicher Maßnahmen**

Zur **Vertrags-erfüllung** erforderlich

Ansonsten gilt:

Die Verarbeitung zu **sonstigen Zwecken** (wie z.B. Werbung) bedarf zwingend der **Einwilligung der Betroffenen!**

Anforderungen der datenschutzrechtlichen Einwilligung

Einwilligung muss **aktiv, freiwillig** und ohne weitere Verpflichtungen erfolgen.

Sie kann sowohl **schriftlich** als auch **mündlich** erteilt werden.

Der Einwilligende muss erkennen können, welche **Folgen** (Tragweite) seine Einwilligung für ihn hat.

Klare, verständliche und optisch gut wahrnehmbare Gestaltung.

Achtung:

Einsichtsfähigkeit bei Minderjährigen unter 16 Jahre

Achtung:

Die Einwilligungen sind **nicht** unbeschränkt gültig. Es gilt der Grundsatz:

Eine Einwilligung kann nur herangezogen werden, solange der Betroffene, der eingewilligt hat, **vernünftiger Weise** mit der Verarbeitung seiner Daten rechnen muss („Nachvollziehbarkeit der Verarbeitung“)

Anforderungen der datenschutzrechtlichen Einwilligung

Mitteilungspflichtige Informationen

1. Bei Direkterhebung (Art. 13 DSGVO)

Wer wir sind:

(Name bzw. Firma)

Identität
des
Verarbeiters

Sie erreichen uns unter:

(Verantwortlicher mit Kontaktdaten)

Datenschutzbeauftragter: ☐ vorhanden _____
(Name, Kontaktdaten)

☐ nicht vorhanden

Wir verwenden die folgenden Daten von Ihnen:

- ☐ Vorname ☐ Name
- ☐ Adresse
- ☐ Festnetz-Telefonnummer
- ☐ Mobil-Telefonnummer
- ☐ E-Mail-Adresse
- ☐ Sonstige, nämlich: _____

Art der
erhobenen
Daten

Wir verwenden die Daten zu den folgenden Zwecken:

- ☐ Vertragsanbahnung/ Vertragserfüllung gemäß Art. 6 Abs. 1 Buchst. b DSGVO*
- ☐ Information/Werbung für eigene Zwecke gemäß Art. 6 Abs. 1 Buchst. f DSGVO
- ☐ Sonstige, nämlich: _____

Zweck der
Datenverar-
beitung

Ihre Daten geben wir:

- ☐ nicht an andere Empfänger weiter
- ☐ an die folgenden Empfänger oder Kategorien von Empfängern weiter (z.B. Auftragsverarbeiter): _____

Die geplante Speicherdauer Ihrer Daten können wir:

- ☐ angeben, sie beträgt _____ Tage/Monate/Jahre.
- ☐ nicht angeben; die Kriterien für die Speicherdauer sind: _____

Ihre Rechte als betroffene Person sind: Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch sowie Datenübertragbarkeit (Art. 15 bis 22 DSGVO*). Außerdem haben Sie das Recht zur Beschwerde bei einer Aufsichtsbehörde (Art. 77 DSGVO).

* Mit DSGVO ist die Datenschutz-Grundverordnung gemeint (Abl. EU v. 4.05.2016, L 119/1), einsehbar unter <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679>

Hinweis auf
das Wider-
rufsrecht

Formelle Pflichten von Betrieben

Informationspflicht

Drei unterscheidbare Situationen:

- Daten werden **direkt bei der betroffenen Person** erhoben
- Daten werden **durch Dritte** erhoben
- Daten sind bereits vorhanden und sollen **zu einem anderen Zweck** genutzt werden

Inhalte der Information:

- Identität der Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Kategorien der personenbezogenen Daten
- Verarbeitungszweck der Datennutzung
- Rechtsgrundlage der Datenverarbeitung
- Mögliche Empfänger der Daten (Auftragsverarbeiter)
- Dauer der Datenverarbeitung und -speicherung
- Rechte der Betroffenen
- Hinweis auf Beschwerderecht bei der Aufsichtsbehörde
- Hinweis auf Notwendigkeit der Datenbereitstellung für die Vertragsabwicklung
- Datenquellen bei Erfassung über Dritte

Bei Zweckänderung:

- Neuer Zweck der Verarbeitung
- Dauer der Verarbeitung
- Rechte des Betroffenen
- Beschwerderecht

Informationsmöglichkeiten:

- Aushang im Geschäft
- Auf der Homepage
- Hand-Out an den Kunden

Formelle Pflichten von Betrieben

Transparenzgebot

Anforderungen an sämtliche Informationen:

- Präzise
- Transparent
- Verständlich
- Leicht zugänglich
- In klarer und einfacher Sprache
- Unverzüglich

Pflicht zur Dokumentation

Insbesondere:

- Verzeichnis der Verarbeitungstätigkeiten
- Ggf. Datenschutz-Folgeabschätzung
- Technische und organisatorische Maßnahmen

Die Rechte Betroffener

1. Recht auf Auskunft

Inhalte einer pauschalen Auskunftsanfrage:

- Alle über den Betroffenen gespeicherten Daten
- Daten-Kategorien (Vertrags-, Adress-, Kontaktdaten etc.)
- Bezeichnung der Datei (z.B. Kundendatei)
- Angaben zur Datenherkunft (selbst erhoben oder von Dritten gekauft)
- Empfänger, an die Daten weitergeleitet wurden
- Geplante Dauer der Datenspeicherung
- Zweck der Datenspeicherung
- Rechte des Betroffenen inkl. Beschwerderecht bei der Behörde

Achtung:

Vor Auskunftserteilung ist der Betrieb verpflichtet, die **Identität des Antragstellers** zu prüfen!

Die Auskunft ist innerhalb von 4 Wochen zu erteilen und ist **einmalig kostenlos**.

2. Recht auf Berichtigung

Daten müssen unverzüglich korrigiert werden, wenn sie:

- falsch sind,
- unvollständig sind,
- nicht mehr aktuell sind

Die Rechte Betroffener

3. Recht auf Löschung

Daten müssen auf Verlangen gelöscht werden, wenn:

- der Aufbewahrungszweck der ursprünglichen Datenaufbewahrung **nicht mehr erforderlich** ist,
- die Daten **unrechtmäßig** verarbeitet wurden oder
- der Betroffene seine Einwilligung für eine weitere Speicherung **widerrufen** hat.

4. Recht auf Einschränkung

Alternativ zur Löschung kann auch das Sperren der Daten zur weiteren Verarbeitung verlangt werden:

- die Richtigkeit der gespeicherten Daten wird bestritten und bedarf ggf. einer Überprüfung
- die Datenverarbeitung ist unrechtmäßig
- die Daten dürfen aufgrund bestehender Aufbewahrungsfristen nicht gelöscht werden

Achtung:

Daten dürfen aber nicht gelöscht werden, wenn gesetzliche **Aufbewahrungsfristen** bestehen (Rechnungsdaten etc.).

5. Recht auf Vergessenwerden

Zielt auf Daten, die veröffentlicht wurden (insbesondere im Internet)

6. Recht auf Übertragung

Daten sind demnach in:

- einem strukturierten,
- gängigen und ggf.
- maschinenlesbaren Format

dem Betroffenen auszuhändigen, damit dieser die Daten zu einem anderen Anbieter mitnehmen darf.

Achtung:

Ferner kann die **direkte Übermittlung** von einem Verantwortlichen zum anderen verlangt werden (soweit technisch überhaupt möglich).

Die Rechte Betroffener

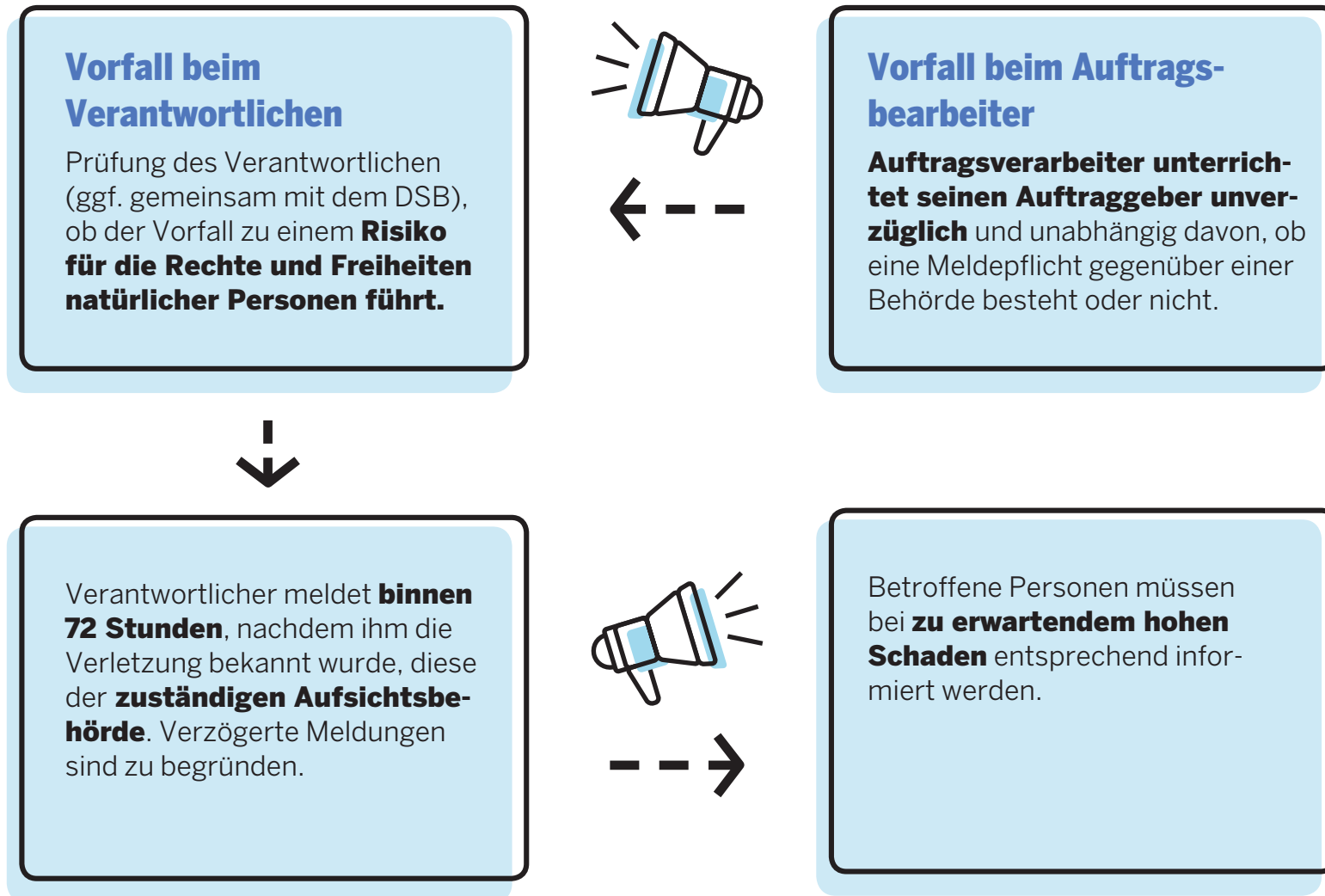
7. Recht auf Widerspruch

- Die Hinweispflicht ist **genereller gestaltet** und **schließt alle Werbewege** ein.
- Der Hinweis muss mit der **ersten Kommunikation** erfolgen, verständlich formuliert und von anderen Informationen getrennt für die betroffene Person verfügbar sein.
- Insbesondere bezogen auf eine Verarbeitung der Daten zum Zwecke der **Direktwerbung**
- **Widerspruch ist jederzeit und ohne Angaben von Gründen möglich**
- Danach darf der Betroffene nicht mehr beworben werden!

Beispiel:

Sie können der Nutzung Ihrer Daten zum Zweck der Werbung jederzeit widersprechen. Hierzu genügt ein Hinweis per Post, eine E-Mail an werbewiderspruch@mustermann.xyz oder ein Anruf unter 012345 / 678-90.

Meldepflicht bei Verstößen und Datenschutzpannen



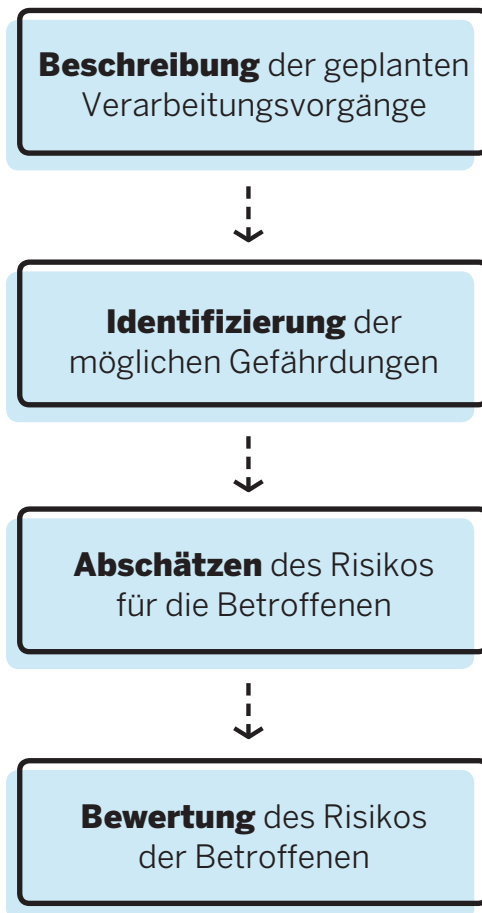
Verfahrensdokumentation

Grundsätzlich gilt:

1. Werden personenbezogene Daten verarbeitet, sind alle damit verbundenen Tätigkeiten im „**Verzeichnis von Verarbeitungstätigkeiten**“ zu dokumentieren.
2. Werden **besonders schutzwürdige Daten** (wie etwa Gesundheitsdaten) verarbeitet, ist zu bewerten, ob die Datenverarbeitung ein hohes oder geringes Risiko für die Betroffenen darstellt (**Risikobewertung**).
3. Besteht ein hohes Risiko, ist eine s.g. **Datenschutz-Folgeabschätzung** vorzunehmen.

Risikobewertung und Folgeabschätzung

Risiko-Analyse und -bewertung

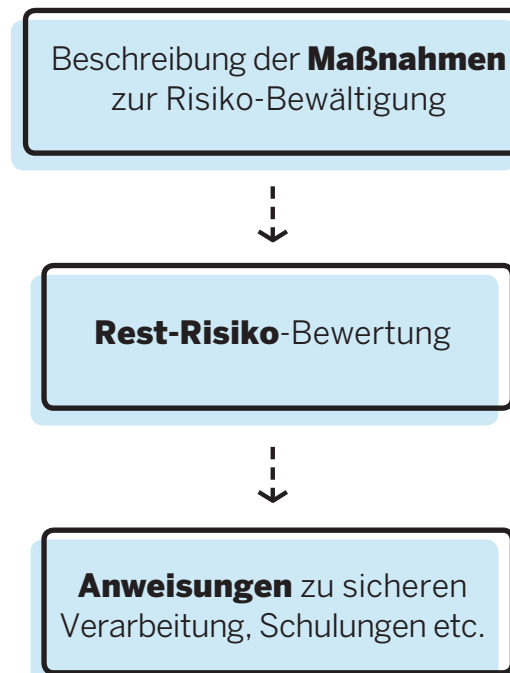


-->

Vertretbares Risiko

----->

Risiko-Bearbeitung

**NEIN****JA**

Risikobewertung und Folgeabschätzung

Fragestellung:

Was kann theoretisch mit Gesundheitsdaten (AO/HG) passieren?



Risikobewertung

Unberechtigter Zugriff

- von außen (Hack)
- von innen (Mitarbeiter/unbefugte Dritte)

Verlust

- von außen (Hack)
- von innen (unbefugtes Löschen, Diebstahl)

Geringes Risiko

- bei Beachtung der TOMs
- im Allgemeinen, da Daten zur Fehlsichtigkeit oder Schwerhörigkeit keine Gefahren für die Freiheitsrechte oder Lebenssituation der Betroffenen darstellen

Erstellung des Verarbeitungsverzeichnisses

1. Name/Kontaktdaten

- Optik Muster
- Geschäftsführer/Inhaber
- Datenschutzbeauftragter
- Zuständige Aufsichtsbehörde

2. Zweck der Verarbeitungstätigkeit

- Datenweitergabe an einen Steuerberater zur Lohnabrechnung
- Datenweitergabe der Buchhaltung an einen Steuerberater
- Kundenpflege mit Hilfe einer Branchen-Software
- Fernwartung und Onlinesicherung der Branchensoftware
- Datenweitergabe an einen Hersteller zum Zweck der Hilfsmittelfertigung
- Abrechnung von Rezepten / Verordnungen / Leistungsnachweisen über ein Rechenzentrum
- Übertragung elektronischer Kostenvoranschläge an Kostenträger
- etc.

Erstellung des Verarbeitungsverzeichnisses

3. Rechtsgrundlage der Verarbeitung

- Gesetzliche Vorschriften
- Interessenabwägung
- Vorliegende Einwilligungserklärung des Kunden
- Vertrag mit dem Kunden
- etc.

4. Beschreibung der Kategorien der betroffenen Personen

- Mitarbeiter/Beschäftigte
- Kunden/Patienten
- Interessenten
- Lieferanten
- Geschäftspartner
- etc.

5. Beschreibung der Daten-Kategorien der betroffenen Personen

- Adressdaten
- Geburtsdatum
- Angaben zur Krankenversicherung (wie Versichertennummer, Kostenträger etc.)
- Angaben zum ausstellenden Arzt
- Angaben zur verordneten Leistung bzw. zum Hilfsmittel
- Gesundheitsdaten, insbesondere zum Seh- und Hörvermögen

6. Empfänger/Kategorien von Empfängern

Interne Empfänger

- Interne Lohnbuchhaltung

Externe Empfänger

- Abrechnungszentren
- Sozialversicherungsträger
- Finanzbehörde
- Steuerberater
- Banken

Sonstige Auftragsverarbeiter

- EDV-Anbieter
- Unternehmensberater
- Werbeagentur & Druckerei

Erstellung des Verarbeitungsverzeichnisses

7. Die vorgesehenen Fristen für Löschung personenbezogener Daten bzw. deren gesetzliche Aufbewahrungsfristen

Löschung der Daten, wenn sie für die Erfüllung des Zwecks nicht mehr erforderlich sind.

Mindest-Aufbewahrungsfristen

- 10 Jahre für abrechnungsgegründete Unterlagen/Daten
- 10 Jahre für steuerrelevante Unterlagen/Daten
- 5 Jahre Gesundheitsdaten gem. Medizinproduktegesetz
- 6 Jahre für Handels- und Geschäftsbriefe
- Personaldaten 2 Jahre nach Beendigung des Arbeitsverhältnisses
- etc.

8. Allgemeine Beschreibung der für den Datenschutz getroffenen technischen und organisatorischen Maßnahmen (TOMs)

Vertraulichkeit der Datenverarbeitung

- u.a. Maßnahmen zur Zutritts- und Zugangskontrolle

Integrität der Datenverarbeitung

- u.a. Maßnahmen zur Protokollierung von Eingaben, Veränderungen, Löschvorgängen etc.

Verfügbarkeitskontrolle

- u.a. Maßnahmen zur Sicherung und Wiederherstellbarkeit personenbezogener Daten

Trennungsgebot

- u.a. Maßnahmen zur Trennung von Daten unterschiedlicher Auftraggeber

Beispiel:

Die folgenden Angaben sind die gesetzlichen Mindestangaben, die auf Anforderung der Aufsichtsbehörde dieser zur Verfügung gestellt werden müssen (Art. 30 Abs. 4 DSGVO).

Name und Anschrift des Verantwortlichen Datenschutzbeauftragter Zuständige Aufsichtsbehörde					
- Optik Mustermann - Anschrift - Kontaktdaten - Herr Mustermann - Anschrift - Kontaktdaten - Landesamt für Datenschutzaufsicht - Anschrift					
1. Zweck	Betroffenengruppe	Datenkategorien	Empfänger	Löschfrist	Tech. und org. Maßnahmen
Leistungs- erbringung	Kunden Interessenten	Stammdaten Auftrags- und Bestelldaten Fertigungsdaten	Glaslieferant Fassungslieferant	Nach Ablauf von handels- oder steu- errechtlichen Aufbe- wahrungspflichten	Gem. IT- Sicher- heitskonzept
2. Zweck	Betroffenengruppe	Datenkategorien	Empfänger	Löschfrist	Tech. und org. Maßnahmen
Steuerrechtliches Nachweiserbringung Finanzmanagement	Kunden Lieferanten Beschäftigte	Stammdaten Leistungs- und Ab- rechnungsdaten	Fibu Steuerberater Finanzamt	Nach Ablauf von handels- oder steu- errechtlichen Aufbe- wahrungspflichten	Gem. IT- Sicher- heitskonzept

Die Auftragsdatenverarbeitung

Grundsätzlich gilt:

Eine **Auftragsdatenverarbeitung** liegt vor, wenn ein Betrieb personenbezogene Daten für seine Zwecke nutzt, die Verarbeitung und Aufbereitung dieser Daten jedoch nicht selber durchführt, sondern von einem Dienstleister vornehmen lässt (**Auftragsverarbeiter**).

Beispiel: Weitergabe von Kundenlisten an eine Werbeagentur/Lettershop. Dabei gilt:

- Über das Verarbeitungsverzeichnis ist zu prüfen, an **welcher Stelle** und für **welchen Zweck** personenbezogene Daten den Betrieb **verlassen**.
- Die **Verantwortung** zur Rechtmäßigkeit der Datenverarbeitung verbleibt auch in diesem Falle bei dem Auftraggeber (Auftragsverarbeiter und Verantwortlicher **haften** bei Datenverstößen **gemeinsam**).
- Der Auftraggeber ist somit dafür zuständig, einen entsprechenden **Vertrag** mit dem Auftragsverarbeiter zu schließen und die Verarbeitung zu prüfen.

Mindest-Inhalte einer Auftragsverarbeitung:

- Gegenstand des Auftrags
- Dauer des Auftrags
- Zweck der Datenverarbeitung
- Art der zu verarbeitenden Daten
- Kategorien der betroffenen Personen
- Ergreifung der erforderlichen technischen und organisatorischen Maßnahmen
- Umfang der Weisungsbefugnisse und die Kontrollrechte des Auftraggebers
- Rückgabe von Datenträgern bzw. Löschung der Daten nach Beendigung des Auftrages

Technische und organisatorische Maßnahmen zur Sicherheit bei der Verarbeitung

Themenbereiche der TOMs:

Sensibilisierung der
Mitarbeiter

Datensicherungs-
Konzept

Schutz vor
Schadprogrammen

Regelungen für
Hard- und Software

Raum-
Anforderungen

Mobile-
Arbeitsplätze

Arbeitsplatz
Rechner

Mobiltelefone/
Smartphones

Netzwerke

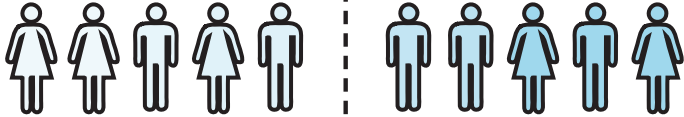
Mobile-
Datenträger

Internetnutzung

Checkliste zur regelmäßigen
Prüfung und Dokumentation

Der Datenschutzbeauftragte (DSB)

Die Benennung eines Datenschutzbeauftragten ist erforderlich wenn ...



...mindestens **10 Personen** angestellt sind, die **ständig** mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

...eine **Datenschutz-Folgeabschätzung** vorgenommen werden muss.

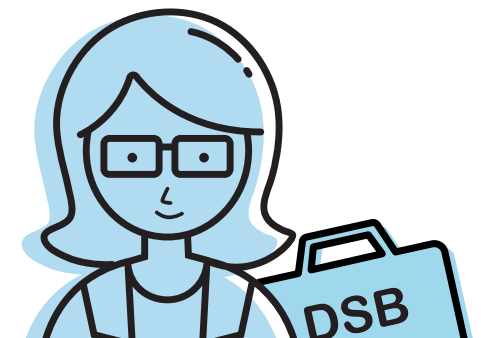
Nach der Benennung sind die Kontaktdaten des DSB zu **veröffentlichen** (z.B. auf der Homepage) und an die jeweils zuständige Landesbehörde zu **melden**.

Welche Aufgaben hat der DSB?

- **unterrichtet und berät** den Verantwortlichen/ die Beschäftigten hinsichtlich ihrer Pflichten rund um den Datenschutz
- **überwacht** die Einhaltung der Datenschutzgesetze
- **sensibilisiert und schult** alle mit der Datenverarbeitung befassten Mitarbeiter
- **berät und überwacht** die Durchführung der Datenschutz-Folgeabschätzung
- **ist Anlaufstelle** für die Aufsichtsbehörde.

Wer kann zum DSB ernannt werden?

- kann sowohl ein Mitarbeiter des Betriebs (**interner DSB**) oder ein außenstehender Dienstleister sein (**externer DSB**)
- muss die notwendigen **fachlichen Qualifikationen** besitzen (Datenschutzrecht und IT-Fachwissen)
- darf in keinen **Interessenskonflikt** geraten und darf bei der Erfüllung seiner Aufgaben **keine Anweisungen** erhalten.
- Daher: Geschäftsführer oder Inhaber dürfen **nicht gleichzeitig DSB** sein!



Der Umgang mit Mitarbeitern

Rechte/Pflichten der **Arbeitgeber**

- Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die **Entscheidung über die Begründung, Durchführung oder Beendigung** eines Beschäftigtenverhältnisses erforderlich ist.
- Die Verarbeitung von personenbezogene Daten zur **Aufdeckung von Straftaten** von Beschäftigten ist zulässig.
- Bei der Einholung von Einwilligungen im Beschäftigtenverhältnis ist weiterhin darauf zu achten, dass diese **freiwillig** erfolgen müssen (bestehende **Abhängigkeit** ist zu berücksichtigen).
- **Informationspflicht**, der Grundsatz der **höchstmöglichen Datensparsamkeit** sowie der **Zweckgebundenheit** gelten auch beim Datenschutz am Arbeitsplatz.

Rechte/Pflichten der **Arbeitnehmer**

- Mitarbeiter haben ein grundsätzliches **Recht auf Auskunft** bezüglich der beim Arbeitgeber gespeicherten Daten zu seiner Person. Das betrifft damit etwa auch die eigene Personalakte, die sie als Mitarbeiter stets einsehen dürfen.
- Sie haben zudem wie überall im Datenschutz auch am Arbeitsplatz das **Recht auf Löschung** unrechtmäßig gespeicherter Daten zu Ihrer Person.
- Auch die Arbeitnehmer müssen, wenn Sie in der Datenverarbeitung angestellt sind, Datenschutzgrundsätze beachten. Sie werden dann regelmäßig auch auf das **Datengeheimnis verpflichtet**.

Zusammenfassung: die wichtigsten To Do 's

- ☑ **Datenschutzrichtlinien veröffentlichen**
Homepage / Aushang / Handout an den Kunden [siehe Muster im Downloadverzeichnis]
- ☑ **Mitarbeiter-Sensibilisierung**
Verpflichtungserklärung einholen / Schulung zum Thema Datenschutz und TOMs [siehe Muster im Downloadverzeichnis]
- ☑ **Einwilligungserklärung für den Kunden**
Mündlich und optional schriftlich [siehe Muster im Downloadverzeichnis]
- ☑ **Verfahrensdokumentation erstellen**
[siehe Muster im Downloadverzeichnis]
- ☑ **Technische und organisatorische Maßnahmen (TOMs) überprüfen**
Checkliste / Schulung [siehe Muster im Downloadverzeichnis]
- ☑ **Vereinbarung zur Auftragsverarbeitung einholen**
Mit allen Partnern (EDV / Marketing / Lieferanten / etc.) [siehe Muster im Downloadverzeichnis]
- ☑ **Ggf. Datenschutzbeauftragten bestellen**



Zusammenfassende Feststellungen



1. **Eine Einwilligungserklärung** ist für die normale Verarbeitung nicht erforderlich, sofern diese Verarbeitung per Gesetz zulässig ist. Lediglich besondere Verarbeitungen wie Werbung mit Gesundheitsdaten oder die Weitergabe der Daten zu fremden Zwecken müssen genehmigt werden.

Eine schriftliche Einwilligung ist nicht zwingend erforderlich.

2. **Die Rechte der Betroffenen** (insbesondere die Daten-Herausgabe und die Löschung der Daten auf Verlangen) sind unbedingt zu beachten.

3. **Die Meldepflicht** bei Datenverstößen ist unbedingt zu beachten.

4. **Das Verzeichnissverzeichnis** und die TOMs sind ein Muss für alle Betriebe.

-
5. Ob und wie eine **Datenschutz-Folgeabschätzung** erfolgen muss, ist noch genauer zu klären (ggf. s.g. „Whitelists“ abwarten).
 6. Sämtliche Vereinbarungen zur **Auftragsdatenverarbeitung** müssen eingeholt werden.
 7. Der **Datenschutzbeauftragte** ist bei mindestens 10 Mitarbeitern unumgänglich.
Für kleinere Betriebe bleibt derzeit noch offen, inwieweit ein Datenschutzbeauftragter bestellt werden muss.
 8. Die **Verpflichtung der Mitarbeiter** auf das Datengeheimnis und die Beachtung des Datenschutzes, sowie deren Einverständniserklärungen sind ebenfalls ein Muss.

Muster-Formulare zum Download

- Auskunftserteilung
- Einwilligungserklärung
- Einwilligungserklärung für Minderjährige
- Datenschutzerklärung
- TOMs
- Verarbeitungsverzeichnis
- Mitarbeiter-Verpflichtungserklärung
- Verfahrensübersicht Meldepflicht
- Verfahrensübersicht Risikobewertung
- Mustervertrag zur Auftragsdatenverarbeitung
- Adressliste Aufsichtsbehörden



Wenn Sie den QR-Code nicht nutzen möchten
erreichen Sie die Download-Seite alternativ über:

www.euronet-ag.de/support

OPTIK MUSTER
Musterstr. 99
99999 Musterort

Schriftliche Einwilligung zur Datenverarbeitung

Herr
Max Mustermann
Musterstr. 11
11111 Musterort

Unser Unternehmen bietet seinen Kunden eine umfassende Beratung und Betreuung bei der Auswahl von Brillen/Contactlinsen/Hörgeräten. Zu diesem Zweck erhebt das Unternehmen personenbezogene Daten, wie Name, Anschrift, Geburtsdatum, Telefonnummer, Bankdaten und Gesundheitsdaten, insbesondere Angaben zum Sehvermögen/Hörvermögen.

Die Erhebung, Speicherung und Verarbeitung der personenbezogenen Daten ist vor allem zum Zweck der Durchführung des entstehenden Vertragsverhältnisses notwendig. Weiterhin werden die Daten für die Erstellung und Übermittlung von Service- und Produktinformationen verwendet. Dieses kann per Post oder per E-Mail/SMS erfolgen.

Ich erkläre mich mit dieser Datenerhebung, Speicherung und Verarbeitung, auch durch von uns beauftragte Dritte einverstanden. Eine anderweitige Weitergabe der Daten ist ausgeschlossen.

Ich bin mir darüber bewusst, dass diese Einwilligung freiwillig ist und ich diese jederzeit widerrufen kann. Meine unten aufgeführten Rechte habe ich zur Kenntnis genommen.

Ort/Datum

Unterschrift

Allgemeine Information

Auskunft, Berichtigung, Löschung, Einschränkungen der Verarbeitung und Widerspruchsrecht

Sie sind gemäß Art. 15 DS-GVO jederzeit berechtigt, gegenüber dem Unternehmen um umfangreiche **Auskunftserteilung** zu den zu Ihrer Person gespeicherten Daten zu ersuchen.

Gemäß den Art. 16, 17, 18 DS-GVO können Sie jederzeit gegenüber dem Unternehmen die **Berichtigung, Löschung** und die **Einschränkung der Verarbeitung** einzelner personenbezogener Daten verlangen.

Sie können darüber hinaus gemäß Art. 21 DS-GVO jederzeit ohne Angaben von Gründen von Ihrem **Widerspruchsrecht** Gebrauch machen und die erteilte Einwilligungserklärung mit Wirkung für die Zukunft abändern oder gänzlich widerrufen. Sie können den Widerruf entweder postalisch, per E-Mail oder per Fax an den Vertragspartner übermitteln. Es entstehen Ihnen dabei keine anderen Kosten als die Portokosten bzw. Übermittlungskosten nach den bestehenden Basisstarifen.

Des Weiteren steht Ihnen gemäß Art. 20 DS-GVO das Recht auf Datenübertragbarkeit zu. Dies bedeutet, dass Sie das Recht haben, die Sie betreffenden personenbezogenen Daten, welche Sie Ihrem Vertragspartner zur Verfügung gestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder auch auf Übertragung an eine andere verantwortliche Stelle.

Die zuvor dargestellten Rechte können bei dem nachbenannten Verantwortlichen geltend gemacht werden:

Fritz Muster, Optik Muster, Musterstr. 99, 99999 Musterort, f.muster@optikmuster.de

Unsere Datenschutzbeauftragten erreichen Sie unter datenschutz@optikmuster.de

Ihnen steht das **Weitern** ein Beschwerderecht bei der Aufsichtsbehörde zu.

Die folgende **Checkliste (Beispiel)** dient als Umsetzungshilfe für die Prüfung und Dokumentation des Umsetzungszustandes der Sicherheitsmaßnahmen (**technische und organisatorische Maßnahmen**). Die Checkliste kann ebenso als Nachweis der Bemühungen zur Umsetzung der IT-Sicherheit verwendet werden.

Nr.	Frage	Referenz	Umgesetzt
1.	Werden neue Mitarbeitende bei der Einstellung auf bestehende Regelungen und Handlungsanweisungen zur Informationssicherheit hingewiesen?	Abs. 1	☐
Beschreibung der getroffenen Maßnahmen			Bewertung durch DSb ☐ kritisch ☐ in Ordnung ☐ ungültig ☐
2.	Haben alle Mitarbeitenden eine Verpflichtung zur Wahrung des Datengeheimnisses unterschrieben?	Abs. 2	☐
Beschreibung der getroffenen Maßnahmen			Bewertung durch DSb ☐ kritisch ☐ in Ordnung ☐ ungültig ☐
3.	Werden Backup-Datenträger in einem gesonderten Raum bzw. außerhalb der Geschäftsräume aufbewahrt?	Abs. 3	☐
Beschreibung der getroffenen Maßnahmen			Bewertung durch DSb ☐ kritisch ☐ in Ordnung ☐ ungültig ☐
4.	Sind auf allen Arbeitsstationen Virenschutzprogramme installiert?	Abs. 4	☐
Beschreibung der getroffenen Maßnahmen			Bewertung durch DSb ☐ kritisch ☐ in Ordnung ☐ ungültig ☐

Verarbeitungsverzeichnis

lfd. Nr.	Bearbeitungskategorien	Bearbeiter	Betroffene	Datenkategorie	Empfänger	Auftragsdatenverarbeiter	Löschfrist	Risikobewertung
1	Erfassung von Daten	alle	Kunden, Mitarbeiter, Ärzte	Kundenstammdaten, Bankdaten, Aufträge Brille/ Cosmetologie / Hörgeräte/Reparaturen), optische Dokumentation, Videodokumentation, Vertragsverwaltung, Dokumentenarchiv, Terminkalender Mitarbeiterstammdaten, Arztstammdaten	Intern	keiner	nach Ablauf von handels- und steuerrechtlichen Aufbewahrungspflichten, bei Stammkunden darüber hinaus zur optimalen Beratung über die gesamte Kundenhistorie	gering
2	Ausdruck von Formularen, Versenden von E-Mail/SMS	alle	Kunden, Ärzte	siehe 1	Kunde/Ärzte/ Krankenkassen/ Abrechnungs- und Finanzdienstleister	keiner	nach Ablauf von handels- und steuerrechtlichen Aufbewahrungspflichten,	gering
3	Datenerfassung mit Hausbesuchs-Notebook	HM, SV	Kunden, Mitarbeiter, Ärzte	siehe 1	Intern	keiner	siehe 1.	mittel
4	Selektion über diverse Merkmale und Listenausgabe	HM, FM, JM	Kunden	siehe 1	Intern	Keiner	nach Verwendung/ bei Wiederverwertung spätestens nach 24 Monaten	gering
5	Bestellung unter Angabe der Kommission	HM, FM, JM, PW	Kunden	Stammdaten, Brillen-/ GL-Werte	Lieferanten	Hoya GmbH, Bodenstock GmbH	nach vollständiger Vertragsabwicklung	gering
6	Online-Terminkalender	Der Kunde selbst	Kunden	Stammdaten, Beratungswünsche	das Unternehmen	Europet Software AG	nach 24 Monaten	gering
7	Krankenkassenabrechnung/Abrechnung Abrechnungsdienstleister	HM, FM, JM	Kunden	Kundenstammdaten, Abrechnungsdaten	Krankenkassen, Abrechnungsdienstleister	Optode GmbH / Krankenkassen	nach Ablauf von handels- und steuerrechtlichen Aufbewahrungspflichten	gering
8	Export für Marketingzwecke	HM, FM, JM	Kunden	Name, Anschrift, Geb.-Datum	Marketingdienstleister	Europet Software AG / Werbeagentur Meyer	nach Verwendung	gering
9	Kundenbindung	HM, FM, JM	Kunden	Name, Anschrift, geb.-Datum, Auftragsdaten Brille, Hörgeräte	Marketingdienstleister	Europet Software AG / Werbeagentur Meyer	nach Zyklusende max. 48 Monate	gering
10	Debitorenbuchhaltung	HM, FM, JM	Kunden	Stammdaten, Rechnungsdaten	Steuerberater	Steuerberater Kunsmann	nach Ablauf von handels- und steuerrechtlichen Aufbewahrungspflichten,	gering
11	Brillen-Abo	HM, FM, JM	Kunden	Stammdaten, Auftragsdaten, Bankdaten	Finanzdienstleister	Bodenstock GmbH	nach Ablauf von handels- und steuerrechtlichen Aufbewahrungspflichten,	mittel

Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes gemäß der EU-Datenschutz-Grundverordnung

Sehr geehrte(r) Frau/Herr

da Sie im Rahmen Ihrer Tätigkeit mit personenbezogenen Daten und vor allem auch mit Gesundheitsdaten in Kontakt kommen, verpflichte ich Sie hiermit zur Beachtung des Datenschutzes, insbesondere zur Wahrung der Vertraulichkeit.

Ihre Verpflichtung besteht umfassend. Sie dürfen personenbezogene Daten selbst nicht ohne Befugnis verarbeiten und Sie dürfen anderen Personen diese Daten nicht unbefugt mitteilen oder zugänglich machen.

Unter einer Verarbeitung versteht die EU-Datenschutz-Grundverordnung (DS-GVO) jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

„Personenbezogene Daten“ im Sinne der DS-GVO sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, welche direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Ihre Verpflichtung besteht ohne zeitliche Begrenzung und auch nach Beendigung Ihrer Tätigkeit fort.

Unter Geltung der DS-GVO können Verstöße gegen Datenschutzbestimmungen nach § 42 ~~DSAnPUG~~-EU (BDSG-neu) sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden. Datenschutzverstöße können zugleich eine Verletzung arbeitsrechtlicher Pflichten bedeuten und entsprechende Konsequenzen haben.

Datenschutzverstöße sind ebenfalls mit möglicherweise sehr hohen Bußgeldern für das Unternehmen bedroht, die gegebenenfalls zu Ersatzansprüchen Ihnen gegenüber führen können. Ein unterschriebenes Exemplar dieses Schreibens reichen Sie bitte an das Unternehmen zurück.

Über die Verpflichtung auf das Datengeheimnis und die sich daraus ergebenden Verhaltensweisen wurde ich unterrichtet. Das Merkblatt zur Verpflichtungserklärung mit dem Abdruck der hier genannten Vorschriften habe ich erhalten.

Ort, Datum

Unterschrift des Mitarbeiters

Notizen:

Notizen:

Programmerweiterungen in Euronet

Verschlüsselung des Kundennamens in der Euronet-Datenbank

Einverständniserklärung (Einwilligungserklärung) in den Kundenstammdaten, jeweils für die Arten Brief, SMS, E-Mail, Telefon, Kundeninfocenter

Schriftliche **Einwilligungserklärung** mit Unterschrift des Kunden

- auf Papier
- auf Tablet-PC direkt in das Formular mit Übernahme ins Dokumentenarchivsystem
- auf Unterschriften-Pad direkt in das Formular mit Übernahme ins Dokumentenarchivsystem

Exportfunktion der Kundendaten

Kennzeichnung eines Kunden bei Wunsch auf **Löschung**

Kennzeichnung eines Kunden bei Wunsch auf **Sperrung**

Selektion nach Kunden, Aufträgen und sonstigen Daten (Optometrische Dokumentation, Dokumentenarchivsystem, etc.), die gelöscht werden können nach Ablauf der gesetzlichen Fristen

Selektion nach Kunden mit einem Löschkennzeichen, die gelöscht werden können nach Ablauf der gesetzlichen Fristen

Diese Präsentation bzw. die Inhalte dieser Broschüre sind keine rechtliche Beratung.
Die Inhalte wurden nach bestem Wissen und Gewissen zur Orientierung des Lesers zusammengestellt.

Die darin gemachten Feststellungen und Empfehlungen müssen gegebenenfalls auf die konkrete Situation
des Betroffenen angepasst oder juristisch überprüft werden.

Stand 05/2018

Quellenangabe:

- EU-Datenschutzgrundverordnung (DSGVO) Verordnung EU 2016/679
- Bundesdatenschutzgesetz (BDSG (neu)) (Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (DSAnpUG-EU))
- ZDH LEITFADEN „Das neue Datenschutzrecht/Hinweise für Handwerksbetriebe“
- Opta Data Broschüre „DSGVO für die sonstigen Leistungserbringer im Gesundheitswesen“
- markt intern Verlag GmbH – „Ratgeber Datenschutz und Werbung ab 2018“



Euronet Software AG

Augustinusstr. 9c
50226 Frechen-Königsdorf

Tel. +49 2234 4000 0
Fax +49 2234 4000 80
info@euronet-ag.de

www.euronet-ag.de