Gesundheitsberufe

Leitfaden zur Datenschutzgrundverordnung (DSGVO) für Gesundheitsberufe

Für Mitgliedsbetriebe der Berufsgruppen Augenoptiker, Kontaktlinsenoptiker, Hörakustiker, Orthopädieschuhmacher, Orthopädietechniker und Zahntechniker, die Gesundheitsdaten, biometrische und genetische Daten verarbeiten.

Ab **25. Mai 2018** treten die neue **EU-Datenschutz-Grundverordnung** und das österreichische **Datenschutz-Anpassungsgesetz** 2018 in Geltung. Besonders problematisch sind die nunmehr **sehr hohen Strafen** von bis zu 20 Mio Euro oder im Fall eines Unternehmens von bis zu 4 % seines weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres. Die Betroffenenrechte wurden erweitert und es wird mehr Eigenverantwortung von den Unternehmern verlangt.

- **Allgemeine Informationen zum Thema**
- **Falls Sie über ein Handelsunternehmen verfügen, bietet das Toolset einen Handlungsleitfaden zur praktischen Umsetzung**

FAQ zur DSGVO

- **Die wichtigsten Fragen und Antworten**
  Was Unternehmen auf jeden Fall wissen müssen
- **500 Fragen und Antworten nach Themenbereichen**
  Detailfragen zu speziellen Sachgebieten

Die Mitglieder der Bundesinnung der Gesundheitsberufe der Berufsgruppen Augenoptiker, Kontaktlinsenoptiker, Hörakustiker, Orthopädieschuhmacher, Orthopädietechniker und Zahntechniker verarbeiten jedoch **auch Gesundheitsdaten, biometrische und genetische Daten**, die besonders sensibel sind, daher sind in der DSGVO besondere Regeln dafür vorgesehen.

» Hier finden Sie eine Checkliste für die Gesundheitsberufe

» Hier finden Sie ausfüllbare Muster für die Gesundheitsberufe

» Hier finden Sie das DSGVO Vertiefungs-Webinar Gesundheitsdaten, biometrische und genetische Daten

» Hier finden Sie FAQ zur DSGVO für die Gesundheitsberufe

» DSGVO für Zahntechniker bei direktem Patientenkontakt

Leitfaden für Gesundheitsberufe

Verarbeitung von sensiblen Daten (= besondere Kategorien personenbezogener Daten)

Datenschutzbeauftragter

Datenschutz-Folgenabschätzung (DSFA)

Betroffenenrechte

Informationspflichten

Auskunftsrecht

Recht auf Löschung

Aufbewahrungsfristen

Recht auf Datenübertragbarkeit

Weitergabe/Erhalt von Daten

ELDA

Datensicherheit und Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Privacy by Design & Privacy by default)

Meldung von Datenschutzverletzungen (Data Breach Notification)

Auswirkungen auf Websites

Information und Schulung der Mitarbeiter

Musterverarbeitungsverzeichnisse

Verarbeitung von sensiblen Daten (= besondere Kategorien personenbezogener Daten)

Die DSGVO spricht nicht wie früher das DSG 2000 von sensiblen Daten, sondern von der Verarbeitung **besonderer Kategorien personenbezogener Daten**.

Dabei handelt es sich um Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die **Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten** oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Definitionen:

„**genetische Daten**" personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden

„**biometrische Daten**" mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten

„**Gesundheitsdaten**" personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen

Grundsatz: Die Verarbeitung ist untersagt, aber es gibt Ausnahmen.

Die wichtigsten Ausnahmen, die für die Gesundheitsberufe nutzbar sind:

- **ausdrückliche Einwilligung** (Art 9 Abs 2 lit a DSGVO)
  Die Einwilligung muss **freiwillig**, auf den **bestimmten Fall** bezogen (Koppelungsverbot) und in **informierter** Weise **unmissverständlich** abgegeben werden. Wir empfehlen eine schriftliche Einwilligungserklärung, falls man sich nicht auf eine andere Rechtsgrundlage stützen kann.

Beispiel:
Ein Orthopädieschuhmacher oder Orthopädietechniker rechnet im Interesse des Kunden/Patienten direkt mit der Krankenkasse ab bzw. holt für den Kunden/Patienten die chefärztliche Bewilligung für einen Heilbehelf ein.

Empfehlung:
Die Bundesinnung empfiehlt auch für diese Fälle eine schriftliche Einwilligung einzuholen und den Kunden/Patienten über die Abwicklung zu informieren. Die beispielhaft angeführten Daten sind daher bereits im Musterverarbeitungsverzeichnis so erwähnt.

Formulierungsbeispiel:
Ich, *Name, eventuell Kundenummer,* stimme zu, dass meine Daten *(Aufzählung der notwendigen Daten, insbesondere Vorname, Nachname, Sozialversicherungsnummer, Gegenstand der Lieferung/Leistung, Rechnungsbetrag)* zum Zweck der *Abrechnung mit der Krankenkassa (Name des Krankenversicherungsträgers)/zur Einholung einer chefärztlichen Bewilligung* an ..... mittels ..... weitergeleitet werden.

Diese Einwilligung kann jederzeit unter ..... (*Angabe der entsprechenden Kontaktdaten*) widerrufen werden."

Achtung:
Die Einwilligung wird z. B. auch benötigt, wenn man die Daten länger behalten möchte als es aufgrund der Löschungspflicht (siehe Betroffenenrechte) zulässig wäre. Wenn man den Kunden weitere Produkte/Dienstleistungen per E-Mail oder Telefon anbieten möchte (Direktwerbung), benötigt man dafür ebenfalls eine Zustimmung (beachten Sie dazu auch § 107 TKG).

Beispiel:
Ein Augenoptiker möchte die Ergebnisse aller Sehtests für die Dauer der Kundenbeziehung z.B. 30, 60, 90 Jahre behalten und seine Kunden per E-Mail über neue Angebote informieren.

Formulierungsbeispiel:
Ich, *Name, ev. Kundenummer,* stimme zu, dass meine Daten *(Aufzählung der gesammelten Daten z. B. Name, Geburtsdatum, Adresse, Ergebnisse von Sehtests, Verordnungen, Dokumentation der Behandlungen, ...)* zum Zweck (*Zweck angeben z. B. Herstellung eines Sehbehelfs, Abgabe von Kontaktlinsen, Durchführungen von Behandlungen, Kontaktpflege, Zusendung von Werbematerial über die Produkte und Serviceleistungen von ..... , ...)* verarbeitet und für ..... Jahre *(konkrete Jahre angeben, „Dauer der Kundebeziehung" ist zu unspezifisch)* gespeichert werden.

Ich bin damit einverstanden, dass ich Zusendungen, auch Werbezusendungen, per E-Mail und/oder Telefon erhalte. Diese Einwilligung kann jederzeit unter ..... (*Angabe der entsprechenden Kontaktdaten*) widerrufen werden."

» Weitere Informationen zur Einwilligungen

- Verarbeitung für die Zwecke der Gesundheitsvorsorge, Versorgung oder Behandlung im Gesundheits- oder Sozialbereich, aufgrund eines **Vertrages mit einem Angehörigen eines Gesundheitsberufs** (Art 9 Abs 2 lit h DSGVO). Hierbei ist es besonders wichtig, dass die Daten von Fachpersonal, das einer **Geheimhaltungspflicht** unterliegt, verarbeitet werden. Die Mitarbeiter sind entsprechend zu unterweisen.

Datenschutzbeauftragter

Ein Datenschutzbeauftragter wird unter anderem benötigt, wenn die **Kerntätigkeit** in der **umfangreichen Verarbeitung** von Daten besonderer Kategorien (Gesundheitsdaten, biometrische oder genetische Daten) besteht.

Was genau unter Kerntätigkeit zu verstehen und ab wann von einer umfangreichen Verarbeitung auszugehen ist, ist nicht klar geregelt.

Betreffend Kerntätigkeit reicht es gemäß Leitfaden der Artikel-29-Datenschutzgruppe [1] offenbar aus, dass die Sammlung von Gesundheitsdaten untrennbar mit der Haupttätigkeit verbunden ist (hier wird als Beispiel ein Krankenhaus genannt, dessen Kerntätigkeit es ist medizinische Versorgung zu leisten).

Der Leitfaden der Artikel-29-Datenschutzgruppe nennt als Beispiel für eine **umfangreiche** Verarbeitung „die Verarbeitung von Patientendaten im gewöhnlichen Geschäftsbetrieb eines **Krankenhauses**"; als Beispiel für **keine umfangreiche** Verarbeitung wird „die Verarbeitung von Patientendaten durch einen **einzelnen Arzt**" genannt.

Hier stellt sich die Frage, wann ein Betrieb der Gesundheitsberufe mit einem „**einzelnen Arzt**" vergleichbar ist, sodass keine Verpflichtung zur

Bestellung eines Datenschutzbeauftragten besteht.

[1] *Die Artikel-29-Datenschutzgruppe ist das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes.*

> **Empfehlung:**
> Da hier eine Grauzone vorliegt, empfehlen wir bei Überschreitung von 10.000 Datensätzen und/oder 10 Mitarbeitern (auf FTE-Basis [2]) einen Datenschutzbeauftragten zu benennen.

[2] *FTE (englisch „full time equivalent") = Vollzeitäquivalent (Abkürzung: VZÄ) oder Vollbeschäftigtenäquivalent*

» Mehr Informationen zum Datenschutzbeauftragten und seinen Aufgaben

Datenschutz-Folgenabschätzung (DSFA)

Eine Datenschutz-Folgenabschätzung ist unter anderem bei einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten durchzuführen (Art 35 DSGVO).

Die Datenschutzbehörde hat mittlerweile zwei Verordnung zur Konkretisierung erlassen:

- Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) sog. **White-List**
- Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V) sog. **Black-List**

In der DSFA-AV (**White-List**) findet sich folgende Ausnahme:

- DSFA-A12 **Patienten-/Klienten-/Kundenverwaltung** und Honorarabrechnung **einzelner** Ärzte, **Gesundheitsdiensteanbieter** und Apotheken
- Zweck der Datenverarbeitung: Patientenverwaltung und Honorarabrechnung von **einzelnen** Ärzten, Zahnärzten und Dentisten sowie Patienten-/Klientenverwaltung und Honorarabrechnung anderer freiberuflich oder **gewerblich einzeln tätiger Gesundheitsdiensteanbieter** und Apotheken.

In der DSFA-V (**Black-List)** hingegen ist geregelt, dass eine Datenschutz-Folgenabeschätzung durchzuführen ist, wenn unter anderem folgende Kriterien erfüllt sind:

- **umfangreiche Verarbeitung** besonderer Kategorien personenbezogener Daten (§ 2 Abs 3 Z 1) (z.B. Gesundheitsdaten, biometrische und genetische Daten) **und**
- Verarbeitung von Daten schutzbedürftiger betroffener Personen, wie unmündige Minderjährige, Arbeitnehmer, **Patienten**, psychisch Kranker und Asylwerber (§ 2 Abs 3 Z 4).

Es sind weder „umfangreiche Verarbeitung" noch „Patienten" definiert.

> **Empfehlung:**
> Da hier eine Grauzone vorliegt, empfehlen wir bei Überschreitung von 10.000 Datensätzen und/oder 10 Mitarbeitern (auf FTE-Basis [3]) eine Datenschutz-Folgenabschätzung durchzuführen.

[3] *FTE (englisch „full time equivalent") = Vollzeitäquivalent (Abkürzung: VZÄ) oder Vollbeschäftigtenäquivalent*

Es sind pro Datenkategorie zu erfassen:

- Bestehendes Risiko
- der mit dem Eintritt des Risikos verbundene mögliche Schaden
- zu treffende Maßnahmen um das Risiko zu minimieren
- zu treffende Maßnahmen um den möglichen Schaden zu minimieren.

» Muster-Formular für die Gesundheitsberufe

» Weitere Informationen zur Datenschutz-Folgenabschätzung

Betroffenenrechte

Die Betroffenenrechte umfassen:

- Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
- Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
- Auskunftsrecht
- Recht auf Berichtigung
- Recht auf Löschung ("Recht auf Vergessenwerden")

- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht

» Mehr Informationen zu den Betroffenenrechten

Informationspflichten

» Übersicht über die Informationspflichten laut DSGVO

> **Achtung:**
> Die Informationspflichten bestehen auch, wenn die Daten durch Dritte erhoben werden.

Auskunftsrecht

» Informationen zum Auskunftsrecht laut DSGVO

Recht auf Löschung

Schon aus den Grundsätzen der **Zweckbindung** und **Speicherbegrenzung** ergibt sich, dass Daten nur solange gespeichert werden dürfen, wie diese für den Zweck für den sie erhoben wurden, unbedingt benötigt werden.

» Mehr Informationen zu den Grundsätzen

Weiters steht jedem Betroffenen das Recht zu, die **Löschung** aller zu seiner Person verarbeiteten Daten zu verlangen. Dem Verlangen ist grundsätzlich Folge zu leisten, es sei denn spezielle Ablehnungsgründe liegen vor. Der wichtigste Ablehnungsgrund sind die gesetzlichen **Aufbewahrungsfristen**.

> **Achtung:**
> Daten, die nur aufgrund einer Einwilligung länger als die gesetzlichen Fristen gespeichert wurden, sind auf Verlangen des Betroffenen umgehend zu löschen.
> Im Verarbeitungsverzeichnis sind die Aufbewahrungsfristen, wenn möglich, ebenfalls anzuführen.

» Mehr Informationen zur Pflicht zur Löschung

Aufbewahrungsfristen

Allgemeine

- Steuerrechtliche Aufbewahrungspflicht nach § 132 Abs 1 BAO: **7 Jahre**
- Unternehmensrechtliche Aufbewahrungspflicht nach §§ 190, 212 UGB: **7 Jahre**
- Gewährleistung nach § 933 ABGB: **2 Jahre** (bewegliche Sachen)
- Kaufpreisforderung bei beweglichen Sachen nach § 1062 iVm § 1486 ABGB: **3 Jahre**
- Ansprüche aus einem Werkvertrag nach § 1486 ABGB (wenn die Leistung im Rahmen eines gewerblichen oder sonstigen geschäftlichen Betriebs erbracht wurde): **3 Jahre**
- Allgemeiner Schadenersatz nach § 1489 ABGB (Entschädigungsklagen): **3 Jahre** (wenn Schaden und Schädiger bekannt) /ansonsten **30 Jahre**

Besondere Normen

- Haftungsansprüche nach **§ 13 PHG**: **10 Jahre**
- Aufzeichnungen der Erzeuger und Arzneimittelgroßhändler über psychotrope Stoffe nach § 8 Psychotropenverordnung: **3 Jahre**
- Vormerkungen von Erzeugern und Arzneimittelgroßhändler nach § 8 Suchtgiftverordnung: **3 Jahre**
- Aufbewahrung der Unterlagen nach Art 3 und 4 der EU-Verordnung 111/2005 für die Überwachung des Handels mit Drogenausgangsstoffen: **3 Jahre**
- Aufbewahrungspflicht nach § 46 Arzneimittelgesetz (AMG): **15 Jahre**
- Aufbewahrungspflicht nach § 15 Abs. 1 Arzneimittelbetriebsordnung (AMBO): **5 Jahre**
- Aufbewahrungspflicht chargenbezogener Unterlagen nach § 15 Abs. 9 Arzneimittelbetriebsordnung (AMBO): **15 Jahre**
- Identifizierungspflicht innerhalb der Lieferkette nach Art 7 EU-Kosmetikverordnung 1223/2009: **3 Jahre**
- Produktinformationsdatei nach Art 11 EU-Kosmetikverordnung 1223/2009: **10 Jahre**
- Behandlungsdokumentation von medizinischen Masseuren und Heilmasseuren nach § 3 MMHmG: **10 Jahre**
- Dokumentationspflichten nach der Verordnung über die Konformitätsbewertung von Medizinprodukten: **5 bzw 15 Jahre**
- Implantatregister von Medizinproduktebetreibern nach § 10 Medizinproduktebetreiberverordnung: **30 Jahre**
- Medizinproduktebetreiberverordnung (Gerätedatei): **5 Jahre**
- Aufbewahrung der Unterlagen nach Art 5 der EU-Verordnung 273/2004 betreffend Drogenausgangsstoffen: **3 Jahre**

- Dokumentationspflicht nach § 35 Psychologengesetz: **10 Jahre**
- Schriftliche Einwilligung gemäß § 2 Abs. 1, schriftlichen Bestätigung gemäß § 2 Abs. 2 sowie eine Kurzbeschreibung der erbrachten Leistung und die Chargennummern der verwendeten Farben und Stoffe nach den Ausübungsregeln für das Piercen und Tätowieren: **10 Jahre**

Zusammenfassend kann man festhalten, dass Kundendaten jedenfalls 7 Jahre, wenn ein Produkt für den Kunden erzeugt wurde jedenfalls 10 Jahre, aufgehoben werden dürfen. Je nach gelagertem Fall können darüber hinaus die oben genannten weiteren Fristen einer Löschung der Daten entgegenstehen.

Recht auf Datenübertragbarkeit

» **Informationen zur Datenübertragbarkeit**

Beispiel:
Ein Kunde möchte den Augenoptiker wechseln und seine Daten mitnehmen. Um die Pflicht zu erfüllen reicht es aus, ihm die Daten in einem gängigen Format (Word, Excel,... elektronisch (E-Mail, USB-Stick,...) zukommen zu lassen.

Achtung:
PDF gilt aufgrund der eingeschränkten Weiterverarbeitungsmöglichkeiten als verpönt.

Anmerkung:
Voraussetzung für das Recht auf Datenübertragbarkeit ist, dass die Verarbeitung mithilfe automatisierter Verfahren erfolgt (d.h. Dokumente in Papierform sind ausgenommen) und auf einer Einwilligung der betroffenen Person oder auf einem Vertrag mit der betroffenen Person beruht.

Weitergabe/Erhalt von Daten

Die Mitgliedsbetriebe erhalten nicht nur direkt von Kunden/Patienten Daten, sondern auch von Ärzten z. B. erhält ein Zahntechniker die Patientendaten vom Zahnarzt, damit er den beauftragten Zahnersatz und eine dazugehörige Konformitätserklärung erstellen kann.

Weiters verrechnen viele Mitgliedsbetriebe insbesondere bei den Berufsgruppen Orthopädieschuhmacher und Orthopädietechniker direkt mit den Krankenkassen.

Diesbezüglich sind zwei Vorgehensweisen möglich:

- Der einzelne Mitgliedsbetrieb wird datenschutzrechtlich als Auftragsverarbeiter von Ärzten tätig. Diesfalls ist der Abschluss eines der DSGVO entsprechenden Auftragsverarbeitungsvertrags erforderlich. Sollte man in einer ständigen Beziehung Daten mit einem anderen Unternehmer austauschen, empfiehlt es sich, einen schriftlichen Vertrag zwischen Verantwortlichem und Auftragsverarbeiter abzuschließen: Musterverträge für Orthopädieschuhmacher und zahntechnische Labors zum Download.
- Der einzelne Mitgliedsbetrieb wird datenschutzrechtlich als Verantwortlicher tätig. Auch in diesem Fall dürfen die für die Vertragserfüllung notwendigen Daten, auch notwendige Gesundheitsdaten, unserer Ansicht nach vom Mitgliedsbetrieb verarbeitet werden.

Die elektronische Weitergabe von Gesundheitsdaten ist im **Gesundheitstelematikgesetz** geregelt. Hier sind Regeln für die Datensicherheit bei der elektronischen Weitergabe von Gesundheitsdaten vorgesehen.

» **Musterformulare zur Auftragsverarbeitung**

» **Das Gesundheitstelematikgesetz**

ELDA

Einige der Mitglieder der Bundesinnung der Gesundheitsberufe nutzen ELDA zwecks Kommunikation mit den Krankenkassen.

Die Datenanlieferung an ELDA mittels ELDA-Online, ELDA-Software oder FTPs-Übertragung erfolgt bereits jetzt verschlüsselt und ELDA ist auch in die vorliegenden Zugriffsprotokollierungsprozesse der Sozialversicherung eingebunden.

Die Datenlöschung erfolgt nach den vorliegenden Aufbewahrungsfristen. Da für ELDA eine gesetzliche Grundlage besteht, ist hier kein schriftlicher Auftragsverarbeitervertrag notwendig.

» **Weitere Infos zu ELDA**

Sollte ein Mitglied seine Datensätze nicht über die Erfassung ELDA-Online oder die Erfassung in ELDA-Software, sondern über ein anderes Softwaresystem mit Anbindung im Hintergrund an die ELDA-Schnittstelle anliefern, dann ist direkt mit dem ServiceSupport des Softwareherstellers

Kontakt aufzunehmen.

Datensicherheit und Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Privacy by Design & Privacy by default)

Es sind geeignete technische und organisatorische Maßnahmen und Verfahren (z. B. Pseudonymisierung) zu treffen, damit die Verarbeitung den Anforderungen der Verordnung genügt und die Rechte der betroffenen Personen geschützt werden.

Datenschutzrechtliche Voreinstellungen sollen sicherstellen, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Bei IT-System sind insbesondere, Zugriffskontrollen (sichere Passwörter), Pseudonymisierung und Verschlüsselungssysteme, Firewalls, Spam-Filter, Anti-Viren-Programme und Backups wichtig.

> **Achtung:**
> Die DSGVO findet nicht nur auf automatisierte Verarbeitung von personenbezogenen Daten, sondern auch auf nichtautomatisierte Verarbeitung, die in einem Dateisystem gespeichert ist Anwendung.
> Lediglich Akten in Papierform, die nicht nach bestimmten Kriterien geordnet werden, unterliegen nicht der DSGVO. Das bedeutet, wenn beispielsweise ein Augenoptiker seine Kundenkartei in Papierform führt, sollten diese Akten in einem versperrten Schrank aufbewahrt werden.

» Mehr Informationen zur Datensicherheit

» Weitere Infos zur Sicherheit von IT-Systemen

Meldung von Datenschutzverletzungen (Data Breach Notification)

Verletzungen des Schutzes personenbezogener Daten sind sowohl der Datenschutzbehörde (ohne unangemessene Verzögerung – möglichst binnen höchstens 72 Stunden nach dem Entdecken; außer die Verletzung führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten) als auch der betroffenen Person (ohne unangemessene Verzögerung, wenn die Wahrscheinlichkeit besteht, dass die Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten bewirkt) zu melden.

Inhalte dieser Meldung sind:

- Beschreibung des Vorfalles
- Auflistung der betroffenen Daten
- Beschreibung der Auswirkung auf die betroffenen Daten
- Beschreibung der geplanten/eingeleiteten Maßnahmen zur Beendigung des Vorfalls und der Wiederherstellung der Daten
- Beschreibung der Maßnahmen zur Minimierung des Schadens
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen

» Informationen und ein Musterformular zur Datenschutzverletzungen

Auswirkungen auf Websites

Wenn Sie auf Ihrer Website personenbezogene Daten verarbeiten (insbesondere Erheben, Erfassen, Speichern, Auslesen, Abfragen, Verwenden, Ändern, Abgleichen, Übermitteln, Bereitstellen, Verknüpfen) haben Sie die geltenden Datenschutzbestimmungen einzuhalten. Die IP-Adresse wird den personenbezogenen Daten zugeordnet.

Es ist empfehlenswert im Rahmen des Cookie-Hinweises auf diese Erklärung zu verlinken.

Diese Erklärung ersetzt jedoch nicht eine allenfalls notwendige Einwilligung für den Einsatz von Cookies. Dafür wird zumindest eine Infobox, die auf diese Erklärung verweist, mit Bestätigungsklick empfohlen.

Information und Schulung der Mitarbeiter

Mit den Mitarbeitern ist eine Vereinbarung abzuschließen, dass Sie Daten grundsätzlich vertraulich behandeln und diese nur für die dafür vorgesehenen Zwecke einsehen und verwenden.

» Muster für eine Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen

Weiters sind Mitarbeiter mit den technischen und organisatorischen Maßnahmen dafür vertraut zu machen.

Musterverarbeitungsverzeichnisse

Jeder Verantwortliche muss ein Verzeichnis sämtlicher Verarbeitungstätigkeiten, die in seiner Zuständigkeit liegen, führen.

Dieses Verzeichnis hat jedenfalls folgende Angaben zu enthalten:

- WER (wer als Verantwortlicher benannt wird)
- WAS (welche Daten-Kategorien erfasst werden)
- WO (Daten gespeichert und verarbeitet werden – betroffene Systeme)
- WARUM (was ist der Rechtsgrund der zur Anwendung kommt)
- WOZU (Zweck der jeweiligen Datenverarbeitung)
- WOHIN (wenn Daten weitergegeben werden - an wen werden die Daten übergeben, auch ob innerhalb der EU oder Drittland)
- WIE LANGE (werden Daten gespeichert – welche Löschfristen kommen zur Anwendung)
- WIE SICHER (welche Datensicherheitsmaßnahmen werden ergriffen).

» Allgemeine Informationen zur Dokumentationspflicht

» Musterverarbeitungsverzeichnisse für

- Augenoptiker/Kontaktlinsenoptiker,
- Hörakustiker,
- Orthopädieschuhmacher,
- Orthopädietechniker und
- Zahntechniker

Stand: 20.02.2019