

Datenschutzgrundverordnung (DSGVO) für Gesundheitsberufe

Ab 25. Mai 2018 treten die neue EU-Datenschutz-Grundverordnung und das österreichische Datenschutz-Anpassungsgesetz 2018 in Geltung.

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

1. Grundsätze bei der Datenverarbeitung

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

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dies setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung der personenbezogenen Daten leicht zugänglich und verständlich in klarer und einfacher Sprache abgefasst sind. Der Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung sowie die Auskunft darüber, welche sie betreffende personenbezogene Daten verarbeitet werden.

1.1. Was sind personenbezogene Daten?

Personenbezogene Daten im Sinne der DSGVO (Art. 4 Abs. 1 Nr. 1 DSGVO) sind alle Daten, die sich auf eine identifizierte oder identifizierbare Person beziehen. Hierzu zählt beispielsweise

- Ihr Name, Adresse, Geburtstag, Telefonnummer und/oder Ihre E-Mail-Adresse, aber auch die IP-Adresse, mit der Sie unsere Dienste nutzen.
- Sozialversicherungsnummer (ggf. bei Abrechnung über eine Krankenkasse)
- Auftragsdaten der Bestellung
- Werbe- und Vertriebsdaten
- Daten zur Erfüllung vertraglicher Pflichten wie Gewährleistung oder Garantie
- Kontodaten im Rahmen des Zahlungsverkehrs (SEPA Lastschrift, Vorauskassa)

Soweit Sie im Rahmen der Nutzung unserer Dienste Angaben zu Ihrer Sehstärke oder sonstige medizinische Angaben machen, die für eine Versorgung mit korrigierenden Sehhilfen wie Kontaktlinsen und/oder Brillen erforderlich sind, handelt es sich hierbei um Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DSGVO, die als personenbezogene Daten besonders geschützt sind.

1.2. Was sind sensible Daten?

Das sind personenbezogene 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.

Zu den sensiblen Daten, die verarbeitet werden, zählen:

- Gesundheitsdaten (Anamnese, Sehvermögen etc.)
- Biometrische Daten: Foto-/Videodokumentation des vorderen Augenabschnitts, Topographie der Hornhaut, sofern für die Produktauswahl erforderlich (dann sind persönliche Kundendaten anonymisiert).
-

1.2.1. Unter welchen Voraussetzungen ist die Verarbeitung von sensiblen Daten rechtmäßig?

Bei Einhaltung der oben genannten Grundsätze ist die Verarbeitung - sofern es sich nicht um „sensible Daten“ (= besondere Kategorie von personenbezogenen Daten) handelt - rechtmäßig, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

Die betroffene Person hat ihre Einwilligung zur Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben. Die Einwilligung muss durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Diese Einwilligung kann schriftlich, elektronisch oder auch mündlich erfolgen, etwa auch durch Anklicken eines Kästchens auf einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder andere Erklärungen oder Verhaltensweisen, die im jeweiligen Kontext eindeutig das Einverständnis der betroffenen Person zur Datenverarbeitung signalisieren. Stillschweigen, bereits vorangekreuzte Kästchen oder Untätigkeit können keine Einwilligung darstellen. Wenn die Verarbeitung mehreren Zwecken dient, ist für jeden Zweck der Verarbeitung eine gesonderte Einwilligung nötig.

1.2.2. Verarbeitung von sensiblen Daten

Die Verarbeitung von sensiblen Daten ist untersagt.

Dieses Verbot gilt ausschließlich in folgenden Fällen nicht (dh. die Verarbeitung sensibler Daten ist nur in folgenden Fällen zulässig):

- Vorliegen einer ausdrücklichen Einwilligung
- Vorliegen einer gesetzlichen Grundlage (einschließlich Kollektivverträge und Betriebsvereinbarungen) zur Ausübung von Rechten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes
- Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person (und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben)
- die personenbezogenen Daten wurden durch die betroffene Person offensichtlich öffentlich gemacht
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit
- aufgrund eines erheblichen öffentlichen Interesses auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats
- Gesundheitsvorsorge, Arbeitsmedizin, medizinische Diagnostik, Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich (auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaates oder eines Vertrages mit einem Angehörigen eines Gesundheitsberufs). Die Daten müssen von Fachpersonal, das nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einem Berufsgeheimnis unterliegt, oder Personen, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegen, verarbeitet werden.
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke (auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaates).

1.3. Dokumentationspflicht

Die DSGVO verpflichtet zum Führen von Verzeichnissen über die Verarbeitung von Daten. Diese Pflicht trifft sowohl den Verantwortlichen als auch den Auftragsverarbeiter (siehe dazu auch „Verantwortlicher und Auftragsverarbeiter“). Der Umfang der Dokumentationspflicht ist für den Auftragsverarbeiter geringer als für den Verantwortlichen.

1.4. Zweckbindung / Wofür denn?

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise

weiterverarbeitet werden. Als nicht unvereinbar gilt eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Zwecke oder für statistische Zwecke.

1.5. Datenminimierung

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Dazu zählt auch, dass Verantwortliche durch technische Voreinstellungen sicherzustellen haben, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

1.6. Richtigkeit

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden.

1.7. Speicherbegrenzung

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Daher sollte der Verantwortliche Fristen für die Löschung oder regelmäßige Überprüfungen vorsehen. Eine längere Speicherung ist vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen für ausschließlich im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke zulässig.

1.8. Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Durch geeignete technische und organisatorische Maßnahmen soll insbesondere auch gewährleistet werden, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.

1.9. Wie lange aufbewahren?

Daten werden nur so lange aufbewahrt, solange sie tatsächlich gebraucht werden; Zusammenfassend kann man festhalten, dass Kundendaten jedenfalls 7 Jahre, wurde ein Produkt für den Kunden erzeugt jedenfalls 10 Jahre, aufgehoben werden dürfen. Je nach gelagertem Fall können darüber hinaus die oben genannten weiteren Fristen einer Löschung der Daten entgegenstehen.

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.

1.10. Widerrufsrecht

Der/Die Betroffene muss über sein Recht aufgeklärt werden, dass er/sie die Einwilligung jederzeit mit Wirkung für die Zukunft ohne Angabe von Gründen widerrufen kann. Hierbei muss auch darauf hingewiesen werden, dass ab Zugang des Widerrufs Einwilligung DSGVO die Daten unverzüglich gelöscht werden, wenn keine gesetzlichen Aufbewahrungspflichten bestehen und der Widerruf wirksam ist. Dabei bleibt jedoch die Wirksamkeit der bis zum Widerruf der Einwilligung getätigten Datenverarbeitung unberührt.