Orientierungshilfe Datenschutz-Verordnung

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht.
Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Alle Gesundheitsdaten *gehören zu den* ***besonderen Kategorien*** *personenbezogener Daten, die grundsätzlich* ***nicht verarbeitet*** *werden dürfen, mit Ausnahme z. B. der* ***Gesundheitsvorsorge oder Versorgung und Behandlung im Gesundheitsbereich****.*

Gesundheitsdaten sind alle Daten, die sich auf den Gesundheitszustand einer Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand hervorgehen, wie z. B. Informationen über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen und alle Informationen den physiologischen Zustand betreffend.

Diese Daten sind besonders zu schützen.

Die neue Datenschutzverordnung gibt dabei einige klare Grundsätze für die Verarbeitung dieser Daten vor:

- *Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz*
- *Zweckbindung der Verarbeitung – festgelegte und eindeutige Zwecke*
- *Datenminimierung – nur notwendige Daten*
- *sachliche Richtigkeit der Daten und „neuester Stand“*
- *Speicherbegrenzung – erforderliche Aufbewahrung der Daten*
- *Integrität und Vertraulichkeit – Schutz der Daten vor unbefugtem Zugriff und unabsichtlichem Verlust oder Veränderung*

Insbesondere ist jede Einrichtung verantwortlich für die Einhaltung dieser Grundsätze sowie den Nachweis dafür.

Diese Orientierungshilfe informiert über alle wesentlichen Anforderungen der neuen Datenschutzverordnung.

Datenschutz 2018 – Rechte der betroffenen Person

Transparente Information, Kommunikation und Modalitäten

Alle Informationen, die sich auf die nachfolgenden Rechte der betroffenen Person beziehen (betroffene Personen sind die Kunden bzw. Bewohner und auch die Mitarbeiter), müssen in präziser, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache verfügbar gemacht und normalerweise schriftlich vorgelegt bzw. verfügbar gemacht werden.

Bearbeitungsfrist für das zur Verfügung stellen von Informationen auf Antrag ist „unverzüglich“, max. innerhalb 1 Monat.

1. Informationspflicht bei Datenerhebung

Zum Zeitpunkt der Erhebung der Daten muss die betroffene Person über den Zweck und die Rechtsgrundlage, mögliche Empfänger der Daten, die Dauer der Speicherung, das Bestehen ihrer Rechte (siehe 2. – 7.), das Beschwerderecht bei der Aufsichtsbehörde, vertragliche Grundlagen für die Datenerhebung usw. informiert und dies nachgewiesen werden.

2. Auskunftsrecht

Jede betroffene Person hat das Recht, eine Bestätigung zu verlangen, ob ihre Daten verarbeitet werden.
Wenn ja, dann hat sie das Recht auf Auskunft über die Verarbeitungszwecke, die Kategorien der Daten, mögliche Empfänger, die geplante Dauer der Speicherung, das Bestehen ihrer Rechte (siehe 1.), alle Informationen zur Herkunft der Daten, sowie eine Kopie aller personenbezogenen Daten, die Gegenstand der Verarbeitung sind.

3. Recht auf Berichtigung

Es besteht das Recht, dass unrichtige Daten unverzüglich berichtigt und unvollständige Daten vervollständigt werden.

4. Recht auf Löschung bzw. Einschränkung der Verarbeitung

Es kann die Löschung aller Daten verlangt werden – diese sind unverzüglich zu löschen, sofern nicht andere wichtige Gründe dagegen sprechen (z. B. Aufbewahrungspflicht). Dies gilt auch im Fall eines Widerrufs der Einwilligung.

Ist eine Löschung nicht mit angemessenen Mitteln möglich oder aus anderen Gründen nicht rechtmäßig, besteht die Pflicht zur eingeschränkten Verarbeitung der Daten bzw. zur Markierung der Einschränkung der Verarbeitung.

Die Einschränkung der Verarbeitung kann auch verlangt werden, wenn die Richtigkeit der Daten angezweifelt oder die Löschung abgelehnt wird, die Daten unrechtmäßig erhoben wurden oder ein Widerspruch gegen die Verarbeitung besteht.

5. Mitteilungspflicht bei Berichtigung und Löschung bzw. Einschränkung der Verarbeitung

Bei jeder Berichtigung, Löschung oder Einschränkung der Verarbeitung besteht die Pflicht, allen Empfängern der offengelegten Daten dies mitzuteilen – die Empfänger sind auf Verlangen der betroffenen Person mitzuteilen.

6. Recht auf Datenübertragbarkeit

Die Daten müssen der betroffenen Person in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden. Auch kann die Übermittlung der Daten an eine andere Stelle verlangt werden.

7. Widerspruchsrecht

Es besteht jederzeit ein Recht auf Widerspruch gegen die Verarbeitung der Daten. In diesem Fall dürfen die Daten nicht weiter verarbeitet werden, außer wenn es andere Rechtsansprüche gibt. In diesem Fall muss die betroffene Person darauf hingewiesen werden.

Quelle: Verordnung (EU) 2016/679, Datenschutz-Anpassungs- und Umsetzungsgesetz EU

Datenschutz 2018 – Pflichten des Verantwortlichen

Verarbeitung gemäß Datenschutz-Verordnung – Sicherstellen und Nachweis

Verantwortlicher ist das Unternehmen bzw. die Einrichtung – wer über die Zwecke und Mittel für die Verarbeitung der personenbezogenen Daten entscheidet.

Der Verantwortliche setzt geeignete technische und organisatorische Maßnahmen um, um sicherstellen und den Nachweis erbringen zu können, dass die Verarbeitung gemäß der Verordnung erfolgt – dazu gehören geeignete Datenschutzvorkehrungen. Die Maßnahmen werden regelmäßig überprüft und aktualisiert.

1. Datenschutz durch Technikgestaltung – technische und organisatorische Maßnahmen

Für die Umsetzung der Datenschutzanforderungen müssen zum Zeitpunkt der Wahl der Mittel wie bei der Verarbeitung geeignete technische und organisatorische Maßnahmen gewählt werden, um die Umsetzung zu garantieren und die Rechte der betroffenen Personen zu schützen.

Gleichermaßen stellen diese Maßnahmen durch geeignete Voreinstellungen sicher, dass nur die erforderlichen Daten verarbeitet werden – in Menge, Umfang der Verarbeitung, Speicherfrist – und die Zugänglichkeit eingeschränkt ist.

2. Auftragsverarbeiter

Erfolgt eine Bearbeitung der Daten im Auftrag des Verantwortlichen, dann nur mit Auftragsverarbeitern, die auf Grundlage eines Vertrages hinreichend Garantien für die Einhaltung der Datenschutzanforderungen bieten. Dazu gehört, dass weitere Aufträge und Verarbeitungen nur mit schriftlicher Genehmigung des Verantwortlichen möglich sind.

Der Vertrag regelt bindend die Pflichten und Rechte des Verarbeiters, Art und Zweck der Verarbeitung, die befugten Personen, das Zurückgeben bzw. Löschen der Daten nach Abschluss des Auftrags sowie aller erforderlichen Nachweise und Unterstützung des Verantwortlichen – einschließlich aktiver Unterstützung von Überprüfungen und Inspektionen.

3. Verzeichnis der Verarbeitungstätigkeiten

Der Verantwortliche führt ein Verzeichnis aller Verarbeitungstätigkeiten, das spezifische Beschreibungen enthält wie Zweck der Verarbeitung, Kategorien betroffener Personen, Kategorien von Empfängern der Daten, Fristen für die Löschung, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen. Dasselbe gilt für Auftragsverarbeiter.

4. Sicherheit der Verarbeitung

Geeignete technische und organisatorische Maßnahmen stellen einen angemessenen Schutz der Daten sicher.

Dazu gehören Pseudonymisierung und Verschlüsselung, die Integrität und Verfügbarkeit, Fähigkeiten und Belastbarkeit der Systeme und Dienste, rasche Wiederherstellungsmaßnahmen für Ausfälle sowie ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen.

Insbesondere sind die Daten vor unbeabsichtigtem Zugriff, aber auch Verlust, Vernichtung und Veränderung zu schützen.

5. Meldung der Verletzung des Schutzes

Im Falle einer Verletzung des Schutzes gilt eine unverzügliche Meldungspflicht an die Aufsichtsbehörde (innerhalb 72 Std).

Ebenso müssen alle betroffenen Personen informiert werden, dem Risiko für die Rechte der Personen angemessen.

6. Datenschutz-Folgenabschätzung

Da Gesundheitsdaten zu den besonderen Kategorien gehören, muss für alle Verarbeitungstätigkeiten mit erhöhtem Risiko eine Datenschutz-Folgenabschätzung durchgeführt werden.

Die Folgenabschätzung bewertet mögliche Folgen und Risiken der Verarbeitung und enthält Abhilfemaßnahmen, Garantien und Sicherheitsvorkehrungen zum Schutz der Daten und zur Bewältigung der Risiken. Werden keine angemessenen Maßnahmen zur Eindämmung der Risiken getroffen, muss vor der Verarbeitung die Aufsichtsbehörde konsultiert werden.

7. Datenschutz-Beauftragter

Da Gesundheitsdaten zu den besonderen Kategorien gehören, muss ein Datenschutzbeauftragter benannt werden – berufliche Qualifikationen und Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis werden vorausgesetzt. Der Datenschutzbeauftragte hat im Unternehmen eine besondere Stellung (z. B. Kündigungsschutz), berichtet unmittelbar der höchsten Managementebene, muss in alle Datenschutz-relevanten Prozesse einbezogen werden und alle erforderlichen Ressourcen für die Ausübung seiner Tätigkeit und die Erhaltung seines Fachwissens erhalten.

8. Externer Datenschutz-Beauftragter

Der Datenschutzbeauftragte kann auf Grundlage eines Dienstleistungsvertrages bestellt werden. Vorteile sind die meist größere fachliche und Erfahrungskompetenz sowie die wesentlich geringere Bindung und Ressourcenaufwendung.

Informationen, Unterstützung und Kontakt

www.pflege-besser.de
info@pflege-besser.de

PFLEGE BESSER
Qualitätsentwicklung in der Pflege