BUNDESVERBAND NIERE E.V.
Selbsthilfe Niere – Prävention, Dialyse, Transplantation –

Wissenswertes über die EU-Datenschutzgrundverordnung

EU-DSGVO

Eine Handreichung des Bundesverbands Niere e.V. für seine Mitgliedsorganisationen

Mainz, im Mai 2018

Die Regelung des Datenschutz in Deutschland

Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (ABl. v. 04.05.2016, L119/1)

Bundesdatenschutzgesetz (BDSG) in der Fassung vom 30.06.2017 (BGBl. I S. 66), zuletzt geändert durch Artikel 7 des Gesetzes vom 30.06.2017 (BGBl. I S. 2097)

16 Landesdatenschutzgesetze (z.B. Rheinland-Pfälzisches Landesdatenschutzgesetz vom 05.07.1994 zuletzt am 20.12.2011 (GVBl. S. 427))

EU-DSGVO

- Warum besteht Handlungsbedarf für die Vereine?
- Welche Konsequenzen können sich für den Vorstand ergeben
- Personenbezogene Daten – Datenverarbeitung – Dateiensysteme
- Vorgaben für die Vereine
- Einwilligung und Informationspflicht
- Sicherheit und Zuverlässigkeit bei der Datenverarbeitung
- Risikoabschätzung
- Der Datenschutzbeauftragte

Warum besteht Handlungsbedarf für Vereine?

Die allgemeinen Pflichten des Vorstands sind u.a.:

„Den Inhabern eines Vorstandsamts obliegt die Sorge für das rechtmäßige Verhalten des Vereins nach außen hin; diese haben dafür einzustehen, dass die Rechtspflichten – sowohl privatrechtlicher oder öffentlich-rechtlicher Natur - erfüllt werden, die den Verein als juristische Person treffen.“

Somit ist die Einhaltung des Datenschutzrechts ein Teil der allgemeinen Pflichten des Vorstands!

Der Vorstand ist rechenschaftspflichtig

Art. 5 Abs 2 DSGVO:

Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können.

Daraus folgt: die Beweislast liegt beim Verein (Vorstand)

Verstöße werden verfolgt

Art. 83 Abs. 1 DSGVO:

“Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall **wirksam**, verhältnismäßig und **abschreckend** ist.

Wo findet die EU-DSGVO Anwendung?

Art. 2 Abs. 1 DSGVO:

Diese Verordnung gilt für die ganz oder teilweise **automatisierte** Verarbeitung **personenbezogener** Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem **Dateisystem** gespeichert sind oder gespeichert werden sollen.

Was sind personenbezogene Daten?

Art. 4 DSGVO:

Im Sinne dieser Verordnung bezeichnet der Ausdruck … **personenbezogene** Daten alle Informationen, die sich auf eine identifizierte oder **identifizierbare natürliche Person** beziehen…

Personenbezogene Daten sind u.a.:

Name, Anschrift, Bankverbindung, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Größe, Gewicht… (d.h. alle Daten, die zur Identifizierung einer Person beitragen können)

Was bedeutet eigentlich „Datenverarbeitung“?

Art. 4 Nr. 2 DSGVO:

Im Sinne dieser Verordnung bezeichnet der Ausdruck „Verarbeitung“ **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; …

Die DSGVO betrifft alle Formen von „Dateisystemen“

Art. 4 Nr. 6 DSGVO:

Im Sinne dieser Verordnung bezeichnet der Ausdruck ... „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird; ...

Die DSGVO unterscheidet nicht zwischen digitalen, elektronischen Ablageorten (PC, Laptop) und analogen Speicherorten (Karteikasten, Leitzordner)

Wann ist die Verarbeitung personenbezogener Daten rechtmäßig?

Art. 6 Abs. 1b DSGVO:

Die Verarbeitung ist nur rechtmäßig, wenn folgende Bedingung erfüllt ist:

die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen

Der Beitritt zu einem Verein setzt voraus, dass zwischen Bewerber und Verein ein Aufnahmevertrag geschlossen wird.

Wichtig: Die Einwilligung

Art. 6 Abs. 1a DSGVO

Die Verarbeitung ist nur rechtmäßig, wenn die betroffene Person ihre Einwilligung zur Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat.

Für den Vereinsvorstand bedeutet das: ohne eindeutige schriftliche Einwilligung darf keine Datenverarbeitung oder Speicherung stattfinden

Die Form der Einwilligung

Art. 7 Abs. 2 DSGVO

Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

Im Aufnahmeantrag des Vereins sind somit mindestens 2 Unterschriften zu leisten – eine für die Mitgliedschaft und eine für die Einwilligung zur Datenverarbeitung und Speicherung und ggf. eine für den Lastschrifteinzug

Wie kann die Einwilligung widerrufen werden?

Art. 7 Abs. 3 DSGVO:

Die betroffene Person hat das Recht, ihre Einwilligung **jederzeit** zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt.

Der Widerruf der Einwilligung muss **so einfach** wie die **Erteilung** der Einwilligung sein.

Datenverarbeitung von „besonderen Kategorien“

Art. 9 Abs. 1 DGSVO:

Die Verarbeitung personenbezogener 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 **ist untersagt**.

Es sei denn, die betroffene Person hat ausdrücklich eingewilligt

Ausnahmen bei der Verarbeitung von „besonderen Kategorien“

Art. 9 Abs. 2e DGSVO:

Das Verarbeitungsverbot gilt nicht, wenn die betroffene Person diese Daten bereits offensichtlich* öffentlich gemacht hat.

(* offensichtlich setzt einen unzweideutigen, bewussten Willensakt voraus)

Beispiel: Preisgabe von Gesundheitsdaten in einer öffentlich zugänglichen Facebook-Gruppe

Die Informationspflicht bei der Datenerhebung

Art. 13 Abs. 1 DSGVO:

Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

- den Namen und die Kontaktdaten des Verantwortlichen
- die Kontaktdaten des Datenschutzbeauftragten (nicht immer erforderlich)
- die Zwecke für die Verarbeitung
- wenn die Verarbeitung berechtigte Interessen berührt
- Zeitdauer der Speicherung (bzw. Kriterien für die Festlegung der Zeitdauer)
- Auskunfts-, Widerrufs- und Löschmodalitäten

Zusätzliche Informationspflicht

Art. 13 Abs. 2 DSGVO

Wie wird eine **faire und transparente** Verarbeitung gewährleistet?

Durch die Information, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte.

Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Wichtig ist der Identitätsbeweis der betroffenen Person.

Sicherheit bei der Datenverarbeitung

Art. 32 Abs. 4 DSGVO

Der Verantwortliche (Vereinsvorstand) und ggf. der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten.

Es wird gefordert, ein dem Risiko angemessenes Schutzniveau zu gewährleisten

Verfahrensverzeichnis ist (manchmal) Pflicht!

Zur Dokumentation der Verarbeitungstätigkeiten ist i.d.R. ein Verfahrensverzeichnis erforderlich

Art. 30 Abs. 5 DSGVO

Hier ist individuell zu prüfen, ob es wirklich erforderlich ist – Grundlage ist die Risikoabschätzung, die Verantwortlichen sind jedoch nachweispflichtig

Wenn ein **Verfahrensverzeichnis Pflicht** ist, empfiehlt sich die Erstellung einer excel-Liste mit folgenden Spalten:

- Name des Verfahren
- Als Auftragsverarbeiter (j / n)
- Datum der Erfassung
- Name des Verantwortlichen
- E-mail des Verantwortlichen
- Telefonnummer des Verantwortlichen
- Beschreibung der Verarbeitung / Zweck
- Betroffene Personengruppen
- Betroffene Daten
- Empfänger der Daten
- Empfänger der Daten in einem Drittland
- Beschreibung der Absicherung der Datenübermittlung in das Drittland
- Löschfrist
- Beschreibung der IT-Sicherheit der Daten
- Beschreibung der physikalischen Sicherheit der Daten

Datenschutz-Folgenabschätzung

Art. 35 Abs. 1 Satz 1 DSGVO:

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

Beispiel: Speicherung und Verarbeitung personenbezogener Daten in der “Cloud”

Melde- und Informationspflicht bei Datenschutzverletzungen

Sofern die Verletzung des Schutzes personenbezogener Daten ein Risiko für die betroffene Person darstellt sind diese Datenschutzverletzungen binnen 72 bei der zuständigen Aufsichtsbehörde zu melden.

Besteht voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

Datenschutzverletzungen sind dokumentationspflichtig!

Zuverlässigkeit bei Auftragsverarbeitung

Art. 28 Abs. 1 DSGVO:

Wird ein Auftragsverarbeiter (natürliche oder juristische Person, Behörde oder andere Stelle) mit der Verarbeitung personenbezogener Daten beauftragt, sind hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Wann brauchen wir einen Datenschutzbeauftragten?

Artikel 37 Abs. 1 c DSGVO:

Der Datenschutzbeauftragte ist erforderlich bei der umfangreichen Verarbeitung **besonderer Kategorien von Daten** gemäß Artikel 9 oder von personenbezogenen Daten über Verurteilungen und Straftaten gemäß Artikel 10

Und **wenn mindestens zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen (§ 38 Abs. 1 BDSG (neu))

Datenschutzbeauftragter kann ein Beschäftigter oder ein Freiberufler sein.

Wenn ein Datenschutzbeauftragter erforderlich ist, müssen seine Kontaktdaten veröffentlicht und der Aufsichtsbehörde mitgeteilt werden