# Datenschutzgrundverordnung im Überblick

## Eine Zusammenfassung mit den für Vereine und Verbände wichtigen Punkten

Die Datenschutzgrundverordnung ist per se nichts komplett Neues. So war bis dato bereits im Datenschutzgesetz 2000 relativ konkret festgehalten, unter welchen Bedingungen welche Daten für welche Zwecke erhoben und verarbeitet werden dürfen. Die Datenschutzgrundverordnung und das Datenschutz-Anpassungsgesetz 2018 verschärfen diese Regelungen und verpflichten die Verantwortlichen (jene Person/Organisation, die Daten erhebt/verarbeitet) auch zu transparenterer und nachvollziehbarerer Dokumentation der erhobenen Daten. Der Grundsatz ist Datenminimierung, also nur jene Daten zu erheben, die zu einem berechtigten Zweck auch benötigt werden und diese sobald wie möglich auch wieder zu löschen. Für alle, die Daten erheben und verarbeiten, bedeutet dies, sich intensiv mit dem eigenen Tun und den eigenen Arbeitsprozessen auseinanderzusetzen und diese ggf. zu adaptieren. Denn es gibt keine allgemein gültigen Vorlagen, die ohne Zutun einfach implementiert werden können.

### DEFINITIONEN

**Verantwortlicher:** Jene Person/Organisation, die Daten erhebt/verarbeitet

**Betroffener:** Jene Person, deren Daten erhoben/verarbeitet werden

**personenbezogene Daten:** Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen – demnach auch z. B. die Verbands-/Arbeits-Emailadresse einer Person (Achtung: in Österreich fallen auch juristische Personen darunter).

**Verarbeitung von Daten:** Jeder mit oder ohne Hilfe automatisierter Verfahren (also auch „Offline-Systeme“) ausgeführter Vorgang 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 von Daten.

**Datenschutzbehörde/Aufsichtsbehörde:** Die Datenschutzbehörde/Aufsichtsbehörde (vormals Datenschutzkommission) sorgt für die Einhaltung des Datenschutzes in Österreich.

### BEDINGUNGEN ZUR DATENERHEBUNG

Personenbezogene Daten dürfen nur erfasst und verarbeitet werden, wenn zumindest eine dieser Bedingungen zutrifft:

1. betroffene Person gibt freiwillige **Einwilligung**
   Einwilligung der betroffenen Person ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Die Einwilligung erfolgt am besten schriftlich (z. B. Papier- oder Online-Formular). Die betroffene Person kann diese Einwilligung jederzeit widerrufen! Achtung: bei Kindern bis zur Vollendung des 14. Lebensjahres müssen immer die

Haftungsausschluss: Die Rechtsauskünfte dienen ausschließlich der Information des Adressaten. Sie wurden nach bestem Wissen und Gewissen erstellt. Für deren Vollständigkeit und Richtigkeit kann dennoch keine Haftung übernehmen.

Erziehungsberechtigten unterzeichnen.
Beispiele: Weitergabe von Daten an Dritte oder Zusendung eines Newsletters, sofern nicht eine andere der Bedingungen zur Datenerhebung greift. In den meisten Fällen betrifft eine Einwilligung jegliche besonderen Kategorien personenbezogener Daten („sensible Daten“).

2. **Erfüllung eines Vertrags** für betroffene Person
   Beispiel: Verarbeitung der Adressdaten für Zusendung einer Bestellung.

3. Erfüllung einer **rechtlichen Verpflichtung** des Verantwortlichen
   Beispiel: Behördliche Meldung von Arbeitnehmern.

4. Schutz **lebenswichtiger Interessen** der betroffenen Person
   Beispiel: Datenaufnahme nach Unfall.

5. Ausführung dem Verantwortlichen übertragene Aufgabe im **öffentlichen Interesse**
   Beispiel: Statistische oder wissenschaftliche Zwecke öffentlicher Stellen.

6. Wahrung **berechtigter Interessen** des Verantwortlichen oder eines Dritten
   Ein berechtigtes Interesse ist vor allem dann gegeben, wenn bereits eine Beziehung zwischen dem Verantwortlichen und dem Betroffenen (z. B. Kunde) besteht oder wenn für den Betroffenen bereits bei der Erhebung eine mögliche Verarbeitung absehbar war.
   Beispiel: Als berechtigtes Interesse im Sport sieht der SSLV Wien die Veröffentlichung von Ergebnislisten von Wettkämpfen, da diese ein wesentliches Element im Sport sind mit dem Ziel eines Leistungsvergleichs. Daher ist ein wesentlicher Bestandteil von öffentlichen Wettkämpfen, dass die Leistungen publik gemacht werden.

In der Regel unterzeichnen Personen, die Mitglied in einem Verein werden wollen, ein Mitgliedschaftsformular, in dem Sie auch das Statut annehmen. Daher ergeben sich gewisse Zwecke für eine Datenverarbeitung und ggf. auch berechtigte Interessen des Vereins bereits aus dem Statut.

In der Regel wird es der Sport bei der Datenerhebung mit den Gründen Vertragserfüllung (Betroffene möchte etwas und Verantwortlicher benötigt dafür bestimmte Daten), Einwilligung (Betroffene willigt ein, dass Daten verarbeitet werden) und berechtigtem Interesse (Verband/Verein besitzt objektives Interesse Daten zu verarbeiten – z. B. Ergebnislisten) zu tun haben.

## BESONDERE KATEGORIEN PERSONENBEZOGENER DATEN („SENSIBLE DATEN“)

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. Ausnahmen, z. B.:

- betroffene Person gibt Einwilligung
- betroffene Person hat Daten bereits offensichtlich öffentlich gemacht

Haftungsausschluss: Die Rechtsauskünfte dienen ausschließlich der Information des Adressaten. Sie wurden nach bestem Wissen und Gewissen erstellt. Für deren Vollständigkeit und Richtigkeit kann dennoch keine Haftung übernehmen.

- Schutz lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person und betroffene Person ist körperlich oder rechtlich außerstande, Einwilligung zu geben

Achtung: Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten (Strafregisterbescheinigung) ist heikel. Nach dem Datenschutz-Anpassungsgesetz 2018 ist diese zwar erlaubt, wenn es im Interesse des Verantwortlichen ist oder zur gesetzlichen Sorgfaltspflicht beträgt, es empfiehlt sich jedoch, dies auf ein Mindestmaß zu reduzieren.

Bei der Verarbeitung von Daten besonderer Kategorie ist in der Regel immer eine Einwilligung notwendig. Im Sport wird dies besonders im medizinischen Bereich und bei Leistungstests der Fall sein. Im Sinne eines berechtigten Interesses kann bei der Veröffentlichung von Ergebnissen, die z. B. Gewichts- oder Behinderungsklassen beinhalten, argumentiert werden.

**INFORMATIONSPFLICHT**

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

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
- ggf. Kontaktdaten des Datenschutzbeauftragten
- Verarbeitungszwecke sowie Rechtsgrundlage für Verarbeitung
- Datenkategorien die verarbeitet werden
- berechtigte Interessen, die vom Verantwortlichen oder einem Dritten verfolgt werden, wenn Verarbeitung darauf beruht
- ggf. Empfänger oder Kategorien von Empfängern
- ggf. Absicht des Verantwortlichen, Daten an ein Drittland oder eine internationale Organisation zu übermitteln
- Speicherdauer oder Kriterien für Festlegung dieser Dauer
- Recht auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung oder Widerspruchsrecht gegen Verarbeitung sowie Recht auf Datenübertragbarkeit
- ggf. Recht, die gegebene Einwilligung jederzeit zu widerrufen
- Beschwerderecht bei einer Aufsichtsbehörde
- Quelle aus der die Daten stammen
- ob Datenerhebung gesetzlich oder vertraglich vorgeschrieben oder für Vertragsabschluss erforderlich ist und welche mögliche Folgen Nichtbereitstellung hätte
- ob automatisierte Entscheidungsfindung einschließlich Profiling (Datenanalyse zu Verhalten, Gewohnheiten, Präferenzen…) besteht

Sollen die Daten für einen anderen Zweck verarbeitet werden, als sie erhoben wurden, so sind alle zu diesem Zweck relevanten Informationen ebenfalls anzuführen. Die Informationspflicht ist auch durchzuführen, wenn die Daten nicht direkt bei der betroffenen Person erhoben wurden – am besten bei nächster Kontaktgelegenheit (wie z. B. Mitgliedsbeitragsvorschreibung).

Haftungsausschluss: Die Rechtsauskünfte dienen ausschließlich der Information des Adressaten. Sie wurden nach bestem Wissen und Gewissen erstellt. Für deren Vollständigkeit und Richtigkeit kann dennoch keine Haftung übernehmen.

Betroffene müssen im Zuge der Datenerhebung immer im Sinne der Informationspflicht mit all den vorgeschriebenen Punkten informiert werden – ungeachtet der Bedingung für die Datenerhebung. Dies bedeutet, dass überall, wo Daten abgefragt werden, auch eine Informationspflicht besteht.

Haftungsausschluss: Die Rechtsauskünfte dienen ausschließlich der Information des Adressaten. Sie wurden nach bestem Wissen und Gewissen erstellt. Für deren Vollständigkeit und Richtigkeit kann dennoch keine Haftung übernehmen.

**RECHTE DER BETROFFENEN**

**1. Auskunftsrecht**
Die betroffene Person hat das Recht auf Auskunft über die gespeicherten personenbezogenen Daten und auf folgende Informationen:

- Verarbeitungszwecke
- Kategorien personenbezogener Daten, die verarbeitet werden
- Empfänger oder Kategorien von Empfängern, gegenüber denen die Daten offengelegt wurden oder werden, insbes. bei Empfängern in Drittländern oder bei int. Organisationen
- falls möglich geplante Dauer, für Speicherung, oder, falls dies nicht möglich ist, Kriterien für die Festlegung dieser Dauer
- Recht auf Berichtigung oder Löschung, auf Einschränkung der Verarbeitung oder Widerspruchsrechts gegen Verarbeitung
- Beschwerderecht bei Aufsichtsbehörde
- Informationen über die Herkunft der Daten, wenn nicht direkt bei Person erhoben
- Bestehen automatisierter Entscheidungsfindung einschließlich Profiling

Nimmt eine Person ihr Auskunftsrecht in Anspruch, kann sie eine Kopie ihrer personenbezogenen Daten, die Gegenstand der Verarbeitung sind, innerhalb eines Monats nach Antrag verlangen, sofern keine Rechte und Freiheiten anderer Personen beeinträchtigt werden. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

**2. Recht auf Berichtigung**
Die betroffene Person hat das Recht die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen.

**3. Recht auf Löschung**
Die betroffene Person hat das Recht, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern u. a. einer der folgenden Gründe zutrifft:

- Daten sind für Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig
- betroffene Person widerruft Einwilligung, auf die sich Verarbeitung stützte, und es fehlt an anderweitiger Rechtsgrundlage
- betroffene Person legt Widerspruch gegen Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für Verarbeitung vor
- Daten wurden unrechtmäßig verarbeitet

Müssen Daten gelöscht werden, die veröffentlicht wurden, so sind je nach verfügbarer Technologie und Implementierungskosten angemessene Maßnahmen zu treffen, um dieser Pflicht nachzukommen.

Haftungsausschluss: Die Rechtsauskünfte dienen ausschließlich der Information des Adressaten. Sie wurden nach bestem Wissen und Gewissen erstellt. Für deren Vollständigkeit und Richtigkeit kann dennoch keine Haftung übernehmen.

Eine Löschung ist nicht verpflichtend, u. a.:

- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

Wettkampf ist ein wesentliches Element im Sport. Ziel eines sportlichen Wettkampfes ist der Leistungsvergleich. Daher ist ein wesentlicher Bestandteil von öffentlichen Wettkämpfen, dass die Leistungen publik gemacht werden. Um eine Leistung eindeutig zuordnen zu können ist die Veröffentlichung bestimmter Daten notwendig. Insbesondere bei Wettkämpfen, die durch Fördernehmer gemäß § 3 BSFG 2017 veranstaltet bzw. beschickt werden oder bei denen diese technische Funktionäre benennen (vgl. § 3 Z 4 BSFG 2017), liegt ein berechtigtes öffentliches Interesse vor. Das öffentliche Interesse liegt auch darin begründet, dass diese Fördernehmer für die Veranstaltung bzw. Beschickung dieser Wettkämpfe öffentliche Mittel erhalten.

Der SSLV Wien sieht daher die Veröffentlichung von Sportergebnissen auch im Sinne eines berechtigten Interesse der Verantwortlichen (Sportverbände) als zulässig und von Antrag auf Löschung und Widerruf ausgenommen. Zu beachten gilt es, hier nur die für die Ergebnisbestimmung notwendigen Daten zu veröffentlichen und auch nur jene Ergebnisse zu publizieren, die durch Wettkämpfe im eigenen Verantwortungsbereich ermittelt werden.

**4. Recht auf Einschränkung der Verarbeitung**

Die betroffene Person hat das Recht, die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

- Richtigkeit der Daten wird bestritten
- Verarbeitung ist unrechtmäßig und betroffene Person lehnt Löschung der Daten ab
- Daten werden für Zwecke der Verarbeitung nicht länger benötigt, betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- betroffene Person legt Widerspruch gegen Verarbeitung ein und es steht noch nicht fest, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen

**5. Recht auf Datenübertragbarkeit**

Die betroffene Person hat das Recht, die von ihr selbst bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln. Voraussetzung: die Verarbeitung erfolgt auf einer Einwilligung oder auf einem Vertrag und mithilfe automatisierter Verfahren.
Sie hat weiters das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

Betroffene Personen können u. a. Auskunft über ihre Daten verlangen. Um dieser Pflicht innerhalb eines Monats nachkommen zu können, ist es sinnvoll, ein dementsprechendes System einzusetzen, dass die Daten sowie deren Erhebungsgrundlagen, Übertragungen an Dritte, usw. einerseits übersichtlich und vollständig abbildet und andererseits auch elektronisch auslesen kann.

Haftungsausschluss: Die Rechtsauskünfte dienen ausschließlich der Information des Adressaten. Sie wurden nach bestem Wissen und Gewissen erstellt. Für deren Vollständigkeit und Richtigkeit kann dennoch keine Haftung übernehmen.

**AUFTRAGSVERARBEITER („DRITTE“)**

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die 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.

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.

Werden die Daten einem Dritten zur Abwicklung des Auftrags übertragen (z. B. Logistikunternehmen für Versand von Publikationen oder externes Newsletter-Tool), ist für jeden Geschäftsfall ein Vertrag notwendig.

**VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN**

Jeder Verantwortliche hat ein Verzeichnis aller Verarbeitungstätigkeiten zu führen, das folgende Angaben enthält:

- Name und die Kontaktdaten des Verantwortlichen sowie ggf. des Datenschutzbeauftragten
- Verarbeitungszwecke
- Beschreibung der Kategorien betroffener Personen und personenbezogener Daten
- Kategorien von Empfängern, gegenüber denen personenbezogenen Daten offengelegt wurden oder werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen
- ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation
- wenn möglich, vorgesehene Fristen für Löschung der Datenkategorien
- wenn möglich, allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Datensicherheit (siehe Seite 8)

In der Regel muss jeder, der mit Daten zu tun hat, ein Verarbeitungsverzeichnis führen. Dieses sollte immer aktuell gehalten werden und übersichtlich darstellen, welche Daten zu welchem Zweck von welchen Personen erhoben werden und an wen diese ggf. weitergegeben werden. Es macht auch Sinn, die Grundlage bzw. Bedingung für die Erhebung der jeweiligen Daten und die Zwecke mitanzuführen.

Haftungsausschluss: Die Rechtsauskünfte dienen ausschließlich der Information des Adressaten. Sie wurden nach bestem Wissen und Gewissen erstellt. Für deren Vollständigkeit und Richtigkeit kann dennoch keine Haftung übernehmen.

## DATENSCHUTZBEAUFTRAGTER

Ein Datenschutzbeauftragter ist für folgende Vorgänge zu installieren:

- Verarbeitung wird von einer Behörde oder öffentlichen Stelle durchgeführt
- Kerntätigkeit des Verantwortlichen stellt aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung dar
- Kerntätigkeit des Verantwortlichen besteht in der umfangreichen Verarbeitung besonderer Kategorien von Daten

Der Datenschutzbeauftragte ist in erster Linie für die Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten zuständig sowie Kontakt für die Datenschutzbehörde. Er ist vor allem unabhängig und weisungsfrei, also nicht in leitender Funktion (dies bedeutet, dass der Geschäftsführer oder ein Mitglied des Leitungsorgans nicht der Datenschutzbeauftragte sein kann).

Die Bestellung eines Datenschutzbeauftragten ist zumindest für jene Verbände und Vereine zu prüfen, die personenbezogene Daten besonderer Kategorie (medizinischer Bereich, Leistungstests,…) umfangreich erheben und/oder verarbeiten.

## DRITTLÄNDER (AUSSERHALB DER EU) UND INTERNATIONALE ORGANISATIONEN

Eine Übermittlung personenbezogener Daten an ein Drittland (außerhalb der EU) oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung. Die Kommission veröffentlicht im Amtsblatt der Europäischen Union und auf ihrer Website eine Liste aller Empfänger, auf die dies zutrifft.

Falls kein positiver Beschluss vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

Solch eine Garantie wird in der Praxis in vielen Fällen eine Vertragsklausel sein, die zwischen dem Verantwortlichen und dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden. Diese muss aber durch die Aufsichtsbehörde (unabhängige Stelle im EU-Mitgliedsstaat) genehmigt werden. Sollten weder ein positiver Beschluss noch geeignete Garantien vorliegen, ist eine Übermittlung u. a. unter folgenden Voraussetzungen möglich:

- betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die bestehenden möglichen Risiken unterrichtet wurde
- Übermittlung ist für Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich

Haftungsausschluss: Die Rechtsauskünfte dienen ausschließlich der Information des Adressaten. Sie wurden nach bestem Wissen und Gewissen erstellt. Für deren Vollständigkeit und Richtigkeit kann dennoch keine Haftung übernehmen.

- Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich

Drittländer bzw. internationale Organisationen, an die Daten übertragen werden sollen, müssen entweder auf der „Positivliste" der EU-Kommission stehen oder es muss ein eigener Vertrag von der Aufsichtsbehörde genehmigt werden oder es besteht eine ausdrückliche Einwilligung bzw. ist nötig zur gewünschten Vertragserfüllung.

**DATENSCHUTZ-FOLGEABSCHÄTZUNG**

Hat eine Form der Verarbeitung 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. Eine Datenschutz-Folgenabschätzung ist insbesondere bei der Verarbeitung besonderer Kategorien von personenbezogenen Daten notwendig. Die Folgenabschätzung enthält zumindest Folgendes:

- systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich der berechtigten Interessen
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird

Die Durchführung einer Datenschutz-Folgenabschätzung ist zumindest für jene Verbände und Vereine zu prüfen, die personenbezogene Daten besonderer Kategorie (medizinischer Bereich, Leistungstests…) umfangreich erheben und/oder verarbeiten.

**DATENSICHERHEIT**

Generell ist der Verantwortliche verpflichtet, die Sicherheit der Daten in jeglicher Hinsicht zu gewährleisten. Dazu können u. a. folgende technische und organisatorische Maßnahmen („TOMs") gesetzt werden:

- Transparenz durch Dokumentation und Protokollierung der Vorgänge
- Schutz vor unbefugtem Zugriff (Zugangs- und Zutrittsberechtigungen)
- Schutz vor Verlust und Vernichtung (Backup, Wartung)
- Verschlüsselungen
- Überwachung (IT-Sicherheit)
- Interne Datenschutzrichtlinie
- Schulung der Mitarbeiter
- Verantwortlichkeiten definieren

Haftungsausschluss: Die Rechtsauskünfte dienen ausschließlich der Information des Adressaten. Sie wurden nach bestem Wissen und Gewissen erstellt. Für deren Vollständigkeit und Richtigkeit kann dennoch keine Haftung übernehmen.

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Hat die Verletzung des Schutzes personenbezogener Daten 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.

Die Meldungen an die Aufsichtsbehörde und Betroffene enthalten zumindest folgende Informationen (Punkt 1 nur an die Aufsichtsbehörde, Punkte 2-4 gelten für beide):

- Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, Kategorien und Datensätze
- Name und Kontaktdaten des Datenschutzbeauftragten oder sonstiger Anlaufstelle
- Beschreibung der wahrscheinlichen Folgen der Verletzung
- Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung

Datensicherheit ist zu gewährleisten. Ein erster Schritt dazu ist die Überprüfung der eigenen IT-Systeme auf Berechtigungen, Sicherheitslücken, Protokollierung und notwendiges Backup (wer hat wie und wann Zugriff worauf, wie ist der Passwortschutz, wo wird z. B. in eine Cloud ausgelagert und wo liegt diese…). Bei einer Verletzung des Schutzes ist, wenn ein Risiko für die Rechte und Freiheiten der Betroffenen besteht, binnen 72 Stunden eine Meldung an die Datenschutzbehörde zu übermitteln und ggf. auch an die betroffenen Personen.

**ONLINE-DATENSCHUTZ**

Neben der Datenschutzgrundverordnung ist die sogenannte E-Privacy Verordnung geplant. Sie soll den Datenschutz im Internet regeln. Bereits jetzt bestehen Regelungen, dass Websites z. B. auf verwendete Cookies hinweisen und der Benutzer dieses zustimmen muss. Dies ist v. a. datenschutztechnisch interessant, da im Tracking (Evaluierung des Benutzerverhaltens auf der Website) meist auch die IP-Adresse protokolliert wird und diese mitunter Rückschlüsse auf Personen zulassen kann. Es macht also Sinn, im Zuge der Implementierung der Datenschutzgrundverordnung auch die eigene Website auf datenschutzrelevante Prozesse zu überprüfen.

Bereits jetzt müssen Benutzer, wenn eine Website Cookies für personenbezogene Daten benutzt, diesen zustimmen. Erfahrungsgemäß betrifft dies fast alle Websites.

Im Interesse des Textflusses und der besseren Lesefreundlichkeit wurde auf geschlechtsspezifische Formulierungen verzichtet. Bezeichnungen wie Betroffener, Verantwortlicher usw. beziehen jeweils die weibliche Form mit ein.

Haftungsausschluss: Die Rechtsauskünfte dienen ausschließlich der Information des Adressaten. Sie wurden nach bestem Wissen und Gewissen erstellt. Für deren Vollständigkeit und Richtigkeit kann dennoch keine Haftung übernehmen.