

Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung



Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung

Vorbemerkung

In fast allen Sportvereinen werden Personendaten verarbeitet, z. B. die Daten bei Aufnahme in den Verein, die Ergebnisse von Wettkämpfen und die Teilnehmer- oder Telefonlisten.

Grundsätzlich hat jedoch jede Person das Recht, selbst zu entscheiden, wem wann welche seiner persönlichen Daten zugänglich sein sollen. Deshalb müssen die Mitglieder darüber informiert werden, welche Daten zu welchem Zweck vom Verein gesammelt werden.

Der Verein zeigt durch einen verantwortungsbewussten Umgang mit personenbezogenen Daten, dass er modern aufgestellt ist und vorbildlich geführt wird.

Wer sich bereits mit dem Datenschutz beschäftigt hat, dem wird vieles bekannt und vertraut vorkommen. Für die Vereine bedeutet die aktuelle Datenschutz-Grundverordnung eine **erweiterte Dokumentations- und Nachweispflichten**, um der Rechenschaftspflicht zu genügen.



Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung

Bestandsaufnahme aller Daten, die im Verein bearbeitet werden

Vereinsmitglieder / Vereinsführungskräfte

Damit dürfen alle Daten erhoben werden, die zur Verfolgung der Vereinsziele und für die Betreuung und Verwaltung der Mitglieder notwendig sind. (Name, Anschrift, in der Regel auch das Geburtsdatum, Geschlecht und Bankverbindung).

Beschäftigte des Vereins

Personenbezogene Daten von Beschäftigten, die in einem abhängigen hauptamtlichen Verhältnis stehen, dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich sind.

Erhebung von Daten Dritter

Der Verein kann Daten von anderen Personen als von Vereinsmitgliedern (z. B. von Gästen, Besuchern, fremden Schützen, Teilnehmern an Wettkämpfen, Vertragspartner) erheben, soweit dies zur Wahrnehmung berechtigter Interessen des Vereins erforderlich ist.

Die bereits erfassten personenbezogenen Daten sind auf Erforderlichkeit zu prüfen. Es gilt der Grundsatz der Datenminimierung.



Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung

Risikoanalyse

Für Euren Verein müsst Ihr eine Risikoanalyse erstellen, d. h. Mängel und Defizite ermitteln und beheben. Bei der Verarbeitung personenbezogener Daten müsst Ihr geeignete technische und organisatorische Maßnahmen treffen, um ein angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen sollte der Verein - unabhängig von gesetzlichen Vorgaben - aus eigenem Interesse umsetzen. So ist z. B. zu verhindern, dass die in einem Computersystem abgelegten Mitgliederdaten von Unbefugten genutzt werden können. An die Einrichtung von passwortgeschützten Nutzer-Accounts und eines Firewall-Systems sowie eine Verschlüsselung der Mitgliederdaten zu denken. Grundsätzlich sind die Maßnahmen auch dann geboten, wenn die Datenverarbeitung von Mitgliedern ehrenamtlich zu Hause mit eigener EDV-Ausstattung erledigt wird.



Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung

Rechtsgrundlage und Erforderlichkeit der Erfassung prüfen

Damit eine Verarbeitung personenbezogener Daten rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden.

Die Mitgliedschaft in einem Verein ist als Vertragsverhältnis zwischen den Mitgliedern und dem Verein anzusehen. Die Vereinssatzung bestimmt die Vereinsziele, für welche die Mitgliederdaten genutzt werden können.

Der Verein sollte schriftlich festlegen, welche Daten beim Vereinseintritt für die Verfolgung des Vereinsziels/-zweckes und für die Mitgliederbetreuung und -verwaltung notwendigerweise erhoben werden.

Der Verein sollte außerdem regeln, welcher Funktionsträger zu welchen Daten Zugang hat und zu welchem Zweck er Daten von Mitgliedern und Dritten verarbeiten und nutzen darf.

Daten, die nicht zulässig und sinnvoll sind, müssen gelöscht werden.



Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung

Datenschutz – Folgeabschätzung

Eine Datenschutz-Folgeabschätzung ist nur dann vorzunehmen, wenn die Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke ein hohes Risiko für die Rechte und Freiheiten für die betroffene Person zur Folge hat. Dies ist insbesondere dann der Fall, wenn eine umfangreiche Verarbeitung besonderer Kategorie von Daten erfolgt oder wenn im Wege der Verarbeitung auf Grundlage von personenbezogenen Daten systematische und umfassende Bewertungen persönlicher Aspekte vorgenommen werden.

Verarbeitungsverzeichnis erstellen

Da in jedem Verein die Verarbeitung personenbezogener Daten nicht nur gelegentlich erfolgt, ist ein Verzeichnis von Verarbeitungstätigkeiten zu führen.

Das Verarbeitungsverzeichnis muss schriftlich oder in einem elektronischen Format geführt werden. Der Verantwortliche ist verpflichtet, der Aufsichtsbehörde das Verzeichnis auf deren Anfrage zur Verfügung zu stellen. Muster Anlage 2a



Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung

Auftragsdatenverarbeitung

Prüft, ob Ihr auch bei einer Auftragsdatenverarbeitung (Internet-Serviceprovider, etc.) die Datensicherheit gewährleisten könnt und diese vertraglich auf die Wahrung des Datengeheimnisses verpflichtet sind. Anlage 2b



Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung

Datenschutzordnung (Muster in Anlage 11)

Ein Verein ist verpflichtet, die Grundzüge der Datenerhebung, -verarbeitung und -nutzung schriftlich festzulegen. Falls dies nicht in der Satzung geregelt ist, kann auch ein gesondertes Regelwerk verfasst werden. Am gebräuchlichsten sind die Begriffe *Datenschutzordnung* oder *Datenschutzrichtlinie*. Die Datenschutzordnung kann vom Vorstand oder von der Mitgliederversammlung beschlossen werden und muss nicht die Qualität einer Satzung haben.

Es ist jeweils konkret festzulegen, welche Daten (z.B. Name, Vorname, Adresse, E-Mail-Adresse usw.) welcher Personen (z.B. Vereinsmitglieder, Teilnehmer an Veranstaltungen oder Lehrgängen, Besucher von Veranstaltungen) für welche Zwecke verwendet werden, ggf. auch, ob Vordrucke und Formulare zum Einsatz kommen.

Der Verein sollte insbesondere schriftlich festlegen, welche Daten beim Vereinseintritt für die Verfolgung des Vereinsziels und für die Mitgliederbetreuung und -verwaltung notwendigerweise erhoben werden. Auch sollte erkennbar sein, welche Angaben für Leistungen des Vereins erforderlich sind, die nicht erbracht werden können, wenn der Betroffene nicht die dafür erforderlichen Auskünfte gibt.

Der Verein sollte auch regeln, welcher Funktionsträger zu welchen Daten Zugang hat und zu welchem Zweck er Daten von Mitgliedern und Dritten verarbeiten und nutzen darf.

Des Weiteren sollte der Verein festlegen, zu welchem Zweck welche Daten von wem an welche Stellen (das können auch Vereinsmitglieder sein) übermittelt werden.

Der Kreis dieser Zugriffsberechtigten muss genau beschrieben sein.



Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung

Informationspflicht

Nur wenn die Betroffenen wissen, welche Daten zu welchen Zwecken verarbeitet werden und welche Rechte sie haben, lassen sich die Grundprinzipien der Transparenz und der Verarbeitung nach Treu und Glauben verwirklichen.

Daher sieht die DS-GVO die Verpflichtung vor, die betroffene Person umfassend zu informieren. Als Anlage 4 findet ihr ein Muster.

Einwilligungserklärungen nach der Datenschutz-Grundverordnung

Wenn keine Einwilligung vorliegt, müsst Ihr diese von Jedem einholen. (Anlage 5 und Muster Aufnahmeantrag)

- Es empfiehlt sich, schon beim Vereinsbeitritt in Form einer Erklärung zum Datenschutz darauf hinzuweisen, zu welchem Zweck und auf welcher Grundlage Sie welche personenbezogene Daten von Seiten des Vereins erheben und verarbeiten werden. In diesem Zuge ist es ratsam, bereits bei der Aufnahme von Mitgliedern, sich zur Verarbeitung von personenbezogenen Daten im Verein eine entsprechende schriftliche Einwilligung von den Betroffenen einzuholen, die den gesetzlichen Vorgaben zu Inhalt und Gestaltung von Einwilligungen, insbesondere den Betroffenenrechten, entspricht. Siehe Muster Aufnahmeantrag und Anlage 5

- Altmitgliedern könnt Ihr über die Vereinsmitteilungen eine allgemeine Information mit einer derartigen Einwilligungserklärung und dem Hinweis auf das jederzeitige Widerrufsrecht zukommen lassen. Für Altmitglieder ist eine Einwilligung nur erforderlich, wenn der Verein in weitergehendem Maße personenbezogene Daten als aus dem Vereinszweck begründet erhebt, verarbeitet und nutzt.



Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung

Auskunftsersuchen

Alle Personen, deren personenbezogenen Daten von Euch gespeichert wurden, können Auskunft über ihre persönlichen Daten verlangen. In Anlage 6 findet Ihr das Muster eines Antwortschreibens.

Löschen und Sperren von Daten

Ihr müsst in Eurem Verein die technischen und organisatorischen Voraussetzungen schaffen, damit alle betroffenen Daten auch tatsächlich komplett gelöscht bzw. gesperrt werden können, soweit noch nicht gelöscht werden kann oder darf.

Besonderheiten/Hinweise für die Vereinshomepage

- Überarbeitung Impressum
- Hinweise Telemediengesetz beachten, Homepage daraufhin überprüfen. Anlage 7b
- Beim Internet-Service-Provider (DTAG, 1&1, Strato,...) Auftragsdatenverarbeitungsvertrag anfordern.
- Eine Datenschutzerklärung kann sich jeder im Internet kostenlos mit einem DSGVO-Generator erzeugen,

z.B. <https://www.activemind.de/datenschutz/datenschutzhinweis-generator/>



Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung

Schutz der IT Systeme (technische und organisatorische Maßnahmen, TOM)

Geeignete Schutzmaßnahmen sind erforderlich (Passwort, Firewall, Zugangsberechtigungen, etc.)

Verpflichtung auf das Datengeheimnis

Alle Personen, die im Rahmen Ihrer Tätigkeit für den Verein personenbezogene Daten verarbeiten, sind zur Wahrung der Vertraulichkeit verpflichtet, dazu sind alle zu unterweisen und anschl. schriftlich zu verpflichten. Ein Muster findet ihr als Anlage 8a, Merkblatt Anlage 8b



Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung

Datenschutzbeauftragter (Anlage 9 und 10)

Ab 10 Personen, die ständig mit der automatisierten Datenverarbeitung zutun haben, muss ein Datenschutzbeauftragter bestellt werden.

Datenschutzbeauftragte können sowohl vereinsinterne (z.B. Vereinsmitglieder) als auch externe Personen oder Unternehmen (z.B. ein Rechtsanwalt oder ein auf datenschutzrecht spezialisiertes Unternehmen) werden. Um Interessenkonflikte zu vermeiden, sollte der Datenschutzbeauftragte jedoch nicht dem Vorstand angehören. Dabei muss der Datenschutzbeauftragte gem. Art 37 Abs. 5. DSGVO, § 5 Abs. 3 BDSG (neu) über eine ausreichende Qualifikation verfügen, um die Art. 39 DSGVO vorgeschriebenen Aufgaben erfüllen zu können.

Ihr seid verpflichtet, die Kontaktdaten Eures Datenschutzbeauftragten zu veröffentlichen (z. B. auf Eurer Homepage).

Außerdem müssen Ihr die Kontaktdaten der Landesbeauftragten für den Datenschutz Niedersachsen mitteilen. Bitte informiert Euch auf der Homepage der Landesbeauftragten für den Datenschutz Niedersachsen über das Meldeverfahren:

https://www.lfd.niedersachsen.de/themen/wirtschaft/meldepflicht_nach_bdsch/meldepflicht-nach-bdsch-56037.html



Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung

Vorgehen bei Datenpannen

In der Praxis kommt es auf vielfältigste Weise zu sog. Datenpannen, z. B. durch einen Hacker-Angriff, aber auch weil der USB-Stick des Kassenswirts mit den Mitgliederdaten verlorengegangen ist oder aufgrund eines Diebstahls des Laptops im Rahmen eines Einbruchs in die Geschäftsstelle. Liegt eine solche Verletzung des Schutzes personenbezogener Daten vor, müssen Sie diese innerhalb von 72 Stunden der zuständigen Datenschutzaufsichtsbehörde (LfD Niedersachsen) melden. Hierfür wird ein online-Meldeportal eingerichtet.

Videoüberwachung

Falls Ihr Vereinsgelände mittels Videokameras überwacht wird, müssen Sie entsprechende Hinweisschilder aufstellen. Übrigens, dies gilt auch, wenn Sie „nur“ Kamera-Attrappen installiert haben.



Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung

Backup

Hilfe im Internet:

dsb: [http://www.ziel-im-visier.de/inhalt/Finanzen, Steuern und Recht/](http://www.ziel-im-visier.de/inhalt/Finanzen,_Steuern_und_Recht/)

LSB: <https://www.lsb-niedersachsen.de/lsb-mitgliederservice/datenschutz-im-verein>

Anlagen:

1 EDV Verfahren

2a Verzeichnis von Verarbeitungstätigkeiten

2b Verarbeitungstätigkeit Auftragsbearbeiter

3 Muster Satzungseintrag Datenschutz

4 Informationspflichten

5 Einwilligung

6 Muster Auskunftersuchen

7a Verzeichnis von Verarbeitungstätigkeiten

7b Telemediengesetz

8a Verpflichtungserklärung Vorstand

8b Merkblatt zur Verpflichtungserklärung

9 Liste Mitarbeiter Datenverarbeitung

10 Qualifikation Datenschutzbeauftragter

11 Muster Datenschutzordnung



Leitfaden für den Datenschutz im Verein

Wesentliche Anforderungen nach der Datenschutz-Grundverordnung

**Vielen Dank für eure
Aufmerksamkeit**

