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.

Dokumentation der Einhaltung der Pflichten/Anforderungen
Rechenschaftspflicht gegenüber Mitgliedern und insbesondere Aufsichtsbehörden.
Als Grundlage kann dieser Leitfaden verwendet werden.

Für den Datenschutz **verantwortliches Vorstandsmitglied** (Name und/oder Funktion):

_____

Bestandsaufnahme aller **EDV-Verfahren** (siehe Anlage 1)

Bitte listen Sie alle EDV-Verfahren auf, die in Ihrem Verein genutzt werden, um personenbezogene Daten zu verarbeiten (z. B. Excel, Mitglieder-Verwaltungsprogramm).

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 Spielern, 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.

Risikoanalyse
Für Ihren Verein müssen Sie eine Risikoanalyse erstellen, d. h. Mängel und Defizite ermitteln und beheben. Bei der Verarbeitung personenbezogener Daten müssen Sie 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.

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 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.

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.
Weiter Informationen finden Sie im Kurzpapier Nr. 5 *Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO*

Verarbeitungsverzeichnis erstellen (siehe Anlagen 2a–c)
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.

Auftragsdatenverarbeitung
Prüfen Sie, ob Sie auch bei einer Auftragsdatenverarbeitung (Lohnbuchhaltung, IT-Wartungsfirmen, etc.) die Datensicherheit gewährleisten können und diese vertraglich auf die Wahrung des Datengeheimnisses verpflichtet sind.

Formulierungsvorschlag für eine Vereinssatzung (siehe Anlage 3)

Ein Formulierungsvorschlag für Ihre Satzung finden Sie in der Anlage 3.

Datenschutzordnung
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.

Informationspflicht (siehe Anlage 4)
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. Ein Muster für das Merkblatt zur Information finden Sie in Anlage 6.

Einwilligungserklärungen nach der Datenschutz-Grundverordnung (siehe Anlage 5)
Wenn keine Einwilligung vorliegt, müssen Sie diese von Jedem einholen. In Anlage 5 finden Sie ein entsprechendes Muster.

Auskunftsersuchen (siehe Anlage 6)
Alle Personen, deren personenbezogenen Daten von Ihnen gespeichert wurden, können Auskunft über ihre persönlichen Daten verlangen. In Anlage 7 finden Sie das Muster eines Antwortschreibens.

Löschen und Sperren von Daten
Sie müssen in Ihrem 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.

Datenschutzerklärung (u.a. Homepage) (siehe Anlagen 7a, 7b)
Das Muster der aktuellen Datenschutzerklärung auf der Homepage des LandesSportBundes ist als Beispiel als Anlage 7a beigefügt.
Erläuterungen zu den gesetzlichen Grundlagen sind als Anlage 7b beigefügt.

Schutz der IT Systeme (technische und organisatorische Maßnahmen)
Geeignete Schutzmaßnahmen sind erforderlich (Passwort, Firewall, Zugangsberechtigungen, etc.)

Verpflichtung auf das Datengeheimnis (siehe Anlagen 8a, 8b)
Alle Personen, die im Rahmen Ihrer Tätigkeit für den Verein personenbezogene Daten verarbeiten, sind zur Wahrung der Vertraulichkeit verpflichtet.
Hinweise dazu finden Sie in den Anlagen 8 a und 8b.

Datenschutzbeauftragter des Vereins (wenn notwendig, siehe Anlage 9):

_____

Qualifikation des Datenschutzbeauftragten (Hinweise siehe Anlage 10):

_____

Veröffentlichung des zuständigen Datenschutzbeauftragten
Sie sind verpflichtet, die Kontaktdaten Ihres Datenschutzbeauftragten zu veröffentlichen (z. B. auf Ihrer Homepage).

Außerdem müssen Sie die Kontaktdaten der Landesbeauftragten für den Datenschutz Niedersachsen mitteilen. Bitte informieren Sie sich auf der Homepage der Landesbeauftragten für den Datenschutz Niedersachsen über das Meldeverfahren:
https://www.lfd.niedersachsen.de/themen/wirtschaft/meldepflicht_nach_bdsg/meldepflicht-nach-bdsg-56037.html

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 Kassenwarts 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.