Datenschutz-Grundverordnung im Verein – Ernstnehmen und Handeln, aber kein Grund zur Panik

Ab 25. Mai 2018 treten die neue Datenschutzgrundverordnung (DS-GVO) der Europäischen Union (EU) und das neugefasste Bundesdatenschutzgesetz (BDSG neu) nach 2-jähriger Übergangsphase in Kraft. Damit sollen die nationalen Gesetze innerhalb der EU weiter vereinheitlicht und personenbezogene Daten besser geschützt werden.

Grundsätzlich ändert sich am Schutz der personenbezogenen Daten nicht sehr viel, aber die Pflichten der Nutzer werden verschärft. Dies gilt vor allem für die Dokumentationspflichten, die die Kontrolle der Einhaltung des Schutzes personenbezogener Daten erleichtern und mehr Transparenz für die Betroffenen bieten soll.

Betroffene sollen leichter Zugang zu ihren Daten und Informationen über deren Nutzung erhalten. Außerdem wird es Pflicht, Daten, die nicht mehr genutzt werden zu löschen.

Für die Nutzer der Daten bedeutet das, dass eine Reihe von Dokumentationen erstellt und zukünftig gepflegt werden müssen und der Datenschutz verschärft wird.

Außerdem wird der **Bußgeldrahmen bei Verstößen erheblich erhöht und bei schwerwiegenden Verstößen besteht eine Meldepflicht.**

> Verantwortlich für Verstöße gegen die Datenschutzbestimmungen ist im Verein der Vorstand, egal ob ein Mitarbeiter oder Vereinsmitglied den Verstoß verschuldet hat.
>
> Sie können sich mit einer Vermögensschadenhaftpflicht und einer D&O-Haftpflichtversicherung gegen Schäden für Ihr eigenes Vermögen und das Vereinsvermögen absichern. Diese Versicherungen schützen Sie und Ihren Verein auch z.B. gegen Verstöße gegen das Urheberrecht, die aufgrund mangelnder Kenntnisse bei den Vereinen häufig vorkommen, wie eine Auswertung der abgelehnten Fälle bei der Rechtsschutzversicherung ergeben hat. Mit einer Cyberschutzversicherung schützen Sie Ihren Verein zusätzlich vor Schäden, die durch Hackerangriffe entstehen. Welchen Versicherungsschutz Ihr Verein tatsächlich benötigt, müssen Sie im Einzelnen abklären.

Was sind Verstöße gegen die DS-GVO:

Sie dürfen personenbezogene Daten nur denen zugänglich machen, die ein berechtigtes (d.h. vertraglich geregeltes Interesse daran haben), sie dürfen Ihnen nur die Daten zugänglich machen, die sie zur Ausübung benötigen und die Personen oder Unternehmen, die diese Daten erhalten, müssen ihrerseits auf die Einhaltung des Datenschutzes verpflichtet werden.

Ein Verstoß gegen die DS-GVO liegt vor, wenn z.B.

- Personenbezogene Daten nicht vor dem Zugriff durch Dritte gesichert sind und von unbefugten Dritten eingesehen werden können.

Beispiele: Die Mitgliederdaten werden auf dem PC des Vorstands gespeichert, sind nicht passwortgeschützt und können von den Mitgliedern seiner Familie eingesehen werden; personenbezogene Daten stehen frei zugänglich in offenen Regalen im Vereinsheim;

Ausdrucke von Rundschreiben an Mitglieder mit deren Adressen werden unvernichtet im Papierkorb entsorgt.

- Die Vorschriften der DS-GVO bezüglich der Dokumentation der Datenverarbeitungsprozesse und Zugriffsberechtigungen werden nicht eingehalten.

Beispiele: Sie haben nicht dokumentiert, welche Daten erfasst werden und zu welchem Zweck; Sie haben nicht dokumentiert, wer Zugriff auf die Daten hat. Diese Dokumente müssen griffbereit und für Dritte nachvollziehbar auf bewahrt werden und sie müssen gepflegt werden.

Welche Daten im Verein sind betroffen:

Grundsätzlich alle Daten die einer Person zugeordnet werden können. Damit sind nicht nur die zur Identifizierung einer Person erforderlichen Daten wie z.B. der Name und das Geburtsdatum gemeint, sondern auch Angaben wie Familienstand, Anschrift, Beruf, Telefonnummer, E-Mail-Adresse, Interessen, Mitgliedschaften in Organisationen, Wettkampfergebnisse etc., also z.B.

- Mitgliederdaten
- Mitarbeiterdaten
- Lieferanten und Kundendaten
- Daten von Spendern, Sponsoren, Unterstützern
- Daten von Mitarbeitern von Behörden
- Daten von Mitgliedern befreundeter Vereine/Kooperationspartnern

Welche Daten darf der Verein ohne ausdrückliche Zustimmung erheben:

Erlaubt ist eine Datenverarbeitung, wenn sie erforderlich ist, um ein Vertragsverhältnis zu bearbeiten. Das liegt immer vor, wenn Sie einen Vertrag schließen, z.B. einen Arbeits- oder Dienstleistungsvertrag. Ein solches Vertragsverhältnis ist auch die Mitgliedschaft ein einem Verein oder Verband (Art. 6, Absatz 1 Satz 1b DS-GVO).

> Sie dürfen aber nur die Daten speichern, die zur Erfüllung des Vertrags notwendig sind und sie müssen die Daten löschen, wenn der Vertrag erfüllt ist bzw. wenn die gesetzliche Aufbewahrungspflicht, z.B. bei Arbeitnehmerunterlagen, bei Spendern, Kunden und Lieferanten erloschen ist (z.B. 10 Jahre). Wenn Sie sich wegen der Aufbewahrungsfristen unsicher sind, fragen Sie Ihren Steuerberater.

Betroffen ist nicht nur die Speicherung von personenbezogenen Daten (elektronisch und in Papierform), sondern auch die Verarbeitung und Nutzung.

Verarbeitung bedeutet ändern, an andere versenden, abheften, speichern, ausdrucken …, also alles, was Sie mit den Daten machen.

Nutzung bedeutet, zu welchem Zweck sie genutzt werden. Die Nutzung für die satzungsgemäßen Zwecke, z.B. Beitragserhebung ist erlaubt, der Verkauf von Mitgliederadressen z.B. an Firmen für Werbezwecke nicht; es sei denn, Sie haben eine ausdrückliche, schriftliche Erlaubnis (Zustimmung/ Einwilligung) der betroffenen Personen.

Was müssen Sie tun, um die DS-GVO im Verein korrekt umzusetzen:

Für alle, die sich mit dem Thema bisher noch nicht auseinandergesetzt haben, ist zügiges Handeln geboten, denn **der 25. Mai 2018 ist Stichtag für die Umsetzung der DS-GVO.**

> *Das bayerische Landesamt für Datenschutzaufsicht stellt viele notwendige Dokumente zur Umsetzung der DSGVO für Vereine unter https://www.lda.bayern.de/de/kleine-unternehmen.html zum Download zur Verfügung. Außerdem finden Sie dort weitere Erläuterungen und Hinweise für die Umsetzung und eine Checkliste mit den wesentlichen Anforderungen der DS-GVO an Vereine. Die folgenden Erläuterungen nehmen auf die Checkliste Bezug; siehe alphabetische Gliederung von A-J.*
>
> *Der Datenschutzbeauftragte des Landesfischereiverbandes, die WGM Consulting GmbH, hat im Auftrag des LFV fehlende Musterdokumente entwickelt, die Sie im Anhang finden. Sie müssen alle Dokumente darauf überprüfen, ob Sie für Ihren Verein zutreffend sind, also bitte nicht blind übernehmen. Die hier getroffenen Ausführungen stellen keine Rechtsberatung dar. Die Vorlagen stellen lediglich Muster zur weiteren Prüfung dar.*

Schritt 1 Bestandsaufnahme

> *Alle Dokumente, die Sie zum Thema DS-GVO erstellen, sollten übersichtlich in einem Ordner (elektronisch und/ oder in Papierform) abgelegt werden. Dieser Ordner ist der Nachweis, dass Sie ihren Pflichten nachkommen!*

Erstellen Sie ein **Verfahrensverzeichnis (B).** In diesem wird erfasst, welche Daten gespeichert sind und wer Zugriff auf die Daten hat. Bei dieser Gelegenheit können Sie gleich überprüfen:

- Welche Daten gelöscht werden müssen, weil der satzungsmäßige oder geschäftliche Kontakt nicht mehr besteht bzw. die gesetzliche Aufbewahrungsfrist abgelaufen ist oder weil Daten erfasst sind, die nicht erfasst werden dürfen.
- Ob wirklich nur diejenigen Zugriff auf die Daten haben, die sie zur Aufgabenerfüllung im Verein benötigen.
- Benötigen Sie einen **Datenschutzbeauftragten (A)** (nur, wenn ständig mindestens 10 Personen mit der automatisierten Verarbeitung personenbezogenen Daten beschäftigt sind) – das sehen Sie, wenn mehr als neun Personen im Verfahrensverzeichnis als Ansprechpartner gelistet sind.

Die Aufgabe eines Datenschutzbeauftragten ist die Überwachung der Einhaltung des Schutzes personenbezogener Daten. Deshalb dürfen diejenigen, die die Daten verarbeiten bzw. für den Datenschutz verantwortlich sind (im Verein der Vorstand) nicht Datenschutzbeauftragter sein. Wenn Sie einen Angestellten des Vereins mit der Aufgabe betrauen, unterliegt er einem besonderen Kündigungsschutz und muss fachlich hierfür geeignet sein. Um Interessenkonflikte zu vermeiden, dürfen Vorstände und/oder IT-Verantwortliche, sowie Personal-Verantwortliche nicht zum DSB ernannt werden. Sie können auch einen externen Datenschutzbeauftragten engagieren. Der Datenschutzbeauftragte muss der Landesdatenschutzbehörde in Ansbach gemeldet werden.

Wenn Sie personenbezogene Daten vernichten, müssen die Daten müssen so vernichtet werden, dass sie nicht wiederherstellbar sind. Papierdokumente müssen geshreddert werden (siehe auch Schulung der Personen, die personengeschützte Daten verarbeiten); elektronische Speichermedien am besten von Profis entsorgen lassen, die eine entsprechende Bescheinigung ausstellen. **Dann brauchen Sie einen Vertrag zur Auftragsverarbeitung**.

Auftragsverarbeitung (G): Eine Formulierungshilfe und Erläuterungen finden Sie unter (G). Der Vertrag zur Auftragsbearbeitung ist notwendig, wenn Sie Verträge mit externen Dienstleistern besitzen oder in Zukunft abschließen, denen Sie personenbezogene Daten, die Sie erhoben haben, zur Ausführung des Auftrags zur Verfügung stellen, z.B. der Druckerei zur Auslieferung von Broschüren an Ihre Kunden; dem externen Lohnbuchhalter für die Lohnabrechnung Ihrer Mitarbeiter (auch 450-€-Kräfte). Ob dieser Schritt notwendig ist, entnehmen Sie dem Verfahrensverzeichnis.

Außenwirkung/ Homepage

Prüfen Sie Ihre Homepage auf folgende Inhalte/ Bestandteile:

- Rechtskonformes Impressum/ Impressum-Button auf der Startseite
- Aktuelle Datenschutzerklärung/ Datenschutz-Button auf der Startseite
- Cookie-Policy bei der Verwendung von Cookies auf der Startseite
- SSL-Verschlüsselung Ihrer Homepage (https) - Bitte Fragen Sie hierzu ggf. Ihren Web-Dienstleister

Sicherheit (F): Die Standardmaßnahmen zur Sicherung von Daten müssen eingehalten und jeweils dokumentiert werden **(TOMs):**

- Automatische Updates im Betriebssystem aktivieren
- Automatische Updates der Firewall, des Virenscanners/der Sicherheitssoftware, des Browsers aktivieren
- Gruppenverwaltung = Zugriffsrechte auf elektronische Ordner – siehe auch Verzeichnis von Verwaltungstätigkeiten, muss eingerichtet sein (Berechtigungskonzept)
- Backups müssen regelmäßig erfolgen und getestet werden
- Papieraktenvernichtung mit Standard-Shredder
- Passwortgeschützte Zugriffe auf Daten, auch auf Speichermedien wie Festplatten und USB-Sticks (Festplattenverschlüsselung)
- Regelmäßige Änderung der Passwörter, z.B. alle 3 Monate (am besten als automatische Aufforderung an den Nutzer in Form einer Passwortregelung)
- Personenbezogene Daten, egal auf welchem Träger, wegräumen und abschließen, wenn sie unbeaufsichtigt sind.

Anbei eine leere Vorlage der technisch-organisatorischen Maßnahmen (TOMs). Diese Vorlage sollte zur Dokumentation der 14 Punkte verwendet werden.

Schritt 2: Umsetzung der notwendigen Maßnahmen

Datenschutzverpflichtung von Beschäftigten (C): Sie müssen die Personen, die Zugriff auf personenbezogene Daten haben, informieren und auf die Einhaltung des Datenschutzes verpflichten. Ein Muster für die Verpflichtung auf den Datenschutz finden Sie unter (C). Ein

weiteres Muster unter:
https://www.bfdi.bund.de/SharedDocs/.../VerpflichtungDatengeheimnis1.pdf?

Besprechen Sie mit den Betroffenen im Verein, dieses Schreiben und seine Anhänge zur Information.

Der Landesfischereiverband Bayern veröffentlicht in seiner Mitgliederzeitschrift „Bayerns Fischerei + Gewässer“ und auf seiner Homepage sowohl Informationen als auch Schulungstermine der Bezirksfischereiverbände zum Thema. Schulungsbescheinigungen, schriftliche Informationen an die „Datenverarbeiter“ oder Teilnehmerlisten zu Treffen zum Thema im Ordner DS-GVO ablegen.

Informations- und Auskunftspflichten (D): In diesen drei Publikationen des Vereins sollte die Datenschutzverpflichtung des Vereins (Datenschutzerklärung) aufgenommen werden:

- Aufnahmeformular für Neumitglieder
- Homepage
- Satzung

Auf diese Weise sind alle Mitglieder darüber informiert, welche Daten zu welchem Zweck von ihnen gespeichert, verarbeitet und ggf. weitergegeben werden.

Es gibt keine „Basis-Datenschutzerklärung“. Unter folgendem Link können Sie sich eine individuelle DSE erstellen lassen; das ist kostenpflichtig und es gibt weitere Anbieter; dieser Link ist also nur eine Möglichkeit:

https://dsgvo-muster-datenschutzerklaerung.dg-datenschutz.de/

Aufnahmeformular für Neumitglieder:

Machen Sie die Zustimmungserklärung zum Bestandteil Ihres Aufnahmeformulars für Neumitglieder; damit setzen Sie die Mitglieder direkt über die von Ihnen erhobenen Daten in Kenntnis (**siehe Anhang Zustimmungserklärung für Mitglieder**).

Löschen von Daten (E): In den Informationen zum Datenschutz muss stehen, dass Daten gelöscht werden, wenn der Zweck der Speicherung, Verarbeitung und Nutzung weggefallen ist. Außerdem sollten die Mitglieder wissen, an wen Sie sich wegen Datenlöschung und Datenänderung wenden können (E-Mail-Adresse und Postadresse). Der Verantwortliche für die Datenlöschung muss sich die Fristen für das Löschen von Daten, für die Aufbewahrungsfrist besteht, auf Wiedervorlage legen. Tritt ein Mitglied aus und besteht keine Notwendigkeit, die gespeicherten Daten aufzuheben (z.B. weil noch Beiträge ausstehen oder es zu einem Rechtsstreit mit dem Mitglied gekommen ist), müssen die Daten unverzüglich gelöscht werden. Im Bestätigungsschreiben für den Austritt sollte mit einem Satz darüber informiert werden, dass alle Daten gelöscht wurden. Wenn die Daten an Dritte weitergegeben wurden, z.B. an den Bezirksfischereiverband für die Aussendung der Mitgliederzeitschrift, muss dieser parallel informiert und zur Löschung der Daten aufgefordert werden. – mit einem **Vertrag zur Auftragsverarbeitung**.

Datenschutzfolgeabschätzung (I): Die ist notwendig, wenn technisch-organisatorische Änderungen den Schutz personenbezogener Daten betreffen. In der Praxis z.B. Systemumstellungen im Unternehmen. Das betrifft Vereine in der Regel nicht. Denken Sie den Datenschutz aber auch bei kleineren Änderungen mit und sei es nur, dass sich Verantwortliche im Verein ändern und sie diese neu auf den Datenschutz verpflichten müssen und das Verzeichnis der Verarbeitungstätigkeiten ändern müssen.

Videoüberwachung (J): Falls z.B. Ihr Vereinsheim videoüberwacht ist, muss das durch Ausschilderung kenntlich gemacht werden. Verwenden Sie hierzu ein Kamerapiktogramm, welches in Augenhöhe anzubringen ist. Zudem muss hierauf die „Verantwortliche Stelle", also der Vereinsname, sowie eine Kontaktmailadresse genannt sein.

Und hier noch einige Hinweise, zu Vorfällen, die immer wieder nachgefragt werden:

Fotos von Mitgliedern und Mitarbeitern: Holen Sie sich die schriftliche Einwilligung der Positionsinhaber in ihrem Verein (Vorstand, Jugendleiter …) und der Mitarbeiter ein, dass sie fotografiert und diese Fotos unentgeltlich auf der Homepage, in Pressemitteilungen (geben Sie genau an, wofür genutzt werden soll und wie lange sie genutzt werden dürfen (während der Mitgliedschaft oder des Arbeitsvertrages, zeitlich unbeschränkt …). Die Mitglieder und die Mitarbeiter dürfen dies verweigern, dann haben Sie kein Recht die Fotos zu veröffentlichen.(**Anlage Einwilligungserklärung zur Nutzung von Fotoaufnahmen)**

Weitergabe von Mitgliederdaten an andere Vereinsmitglieder, z.B. Fischereiaufseher. Das ist nach §2, Art. 4, Nr. 2 DS-GVO erlaubt, denn die Weitergabe der Daten ist zur satzungsgemäßen Ausführung der Aufgaben des Vereins notwendig.
Verpflichtungserklärung zur Verschwiegenheit nach § 5 BDSG (s. Anlage)

Weitergabe von personenbezogenen Daten für den Verkauf von Erlaubnisscheinen durch Dritte, z.B. Kioskbesitzer am Gewässer, damit er Tageskarten verkaufen kann. Verkauft der Verein die Karten nur an Mitglieder oder zu vergünstigten Konditionen an Mitglieder, darf er die Daten weitergeben; er beauftragt einen Dritten mit der Ausführung der satzungsgemäßen Aufgaben. In dem Fall muss der Kioskbesitzer einen Vertrag zur Auftragsverarbeitung unterschreiben. Kann er die Erlaubnisscheine an jeden verkaufen, der einen Fischereischein besitzt, gibt es keinen Grund, die Daten weiterzugeben und es ist nicht erlaubt. **Verpflichtungserklärung zur Verschwiegenheit nach § 5 BDSG (s. Anlage)**