Verwaltung
im Verein

digital verein(t)

Mitgliederdaten: Schützen, verwalten und verwenden

Impressum

Herausgeber:
Deutschland sicher im Netz e.V. (DsiN)
Projekt digital verein(t)

Projektleitung:
Dr. Nils Weichert (DsiN)

Geschäftsführung:
Dr. Michael Littger (V.i.s.d.P.)
Albrechtstraße 10c
10117 Berlin
+49 (0) 30 767581-500
www.sicher-im-netz.de

Erscheinungsjahr: 2021

Redaktion:
Dr. Elisabeth Maria Hofmann,
Daniel Helmes (BBE), Petra Rollfing

Lektorat:
Lilian Misao Grote, Johanna Gabriel,
Franziska Groß

Gestaltung und Satz:
freistil grafik&design, München

Projektpartner:
Landesarbeitsgemeinschaft der Freiwilligenagenturen/
-Zentren/ Koordinierungszentren
Bürgerschaftliches Engagement Bayern (lagfa)

Projektleitung:
Lilian M. Grote (lagfa bayern e.V.)

Digital verein(t) in Bayern ist ein Landesprojekt im Bundesnetzwerk Digitale Nachbarschaft, das in enger Kooperation mit lagfa bayern e.V. durchgeführt wird. Das Projekt wird vom Bayerischen Staatsministerium für Digitales (StMD) gefördert. Es unterstützt ehrenamtliches Engagement und Vereine in ganz Bayern bei der sicheren und kompetenten Nutzung digitaler Angebote.

Dieses Handbuch berücksichtigt die Grundlagen der „Cyberfibel – Für Wissensvermittler:innen in der digitalen Aufklärungsarbeit“, ein Angebot von Deutschland sicher im Netz e.V. (DsiN) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Gefördert durch

Bayerisches Staatsministerium für Digitales

Ein Projekt von

DsiN Deutschland sicher im Netz

In Zusammenarbeit mit

lagfa bayern

Mitgliederdaten: Schützen, verwalten und verwenden

Handbuch von digital verein(t)

Die fünf Themenbereiche von digital verein(t) kommen direkt aus der Praxis des freiwilligen Engagements. Mit den digital verein(t)-Handbüchern zu den Themen „Öffentlichkeitsarbeit im Verein“, „Verwaltung im Verein“, „Zusammenarbeit im Verein“, „Finanzen im Verein“ und „Digitale Trends im Verein“ macht sich Ihr Verein fit fürs Netz.

Inhalt

Über dieses Handbuch **06**

1 Vereinssoftware & Datenschutz: **07**
Wie Mitgliederdaten digital verwaltet werden

2 Zugänge, Berechtigungen & Backups: **15**
Wie die Sicherheit personenbezogener Daten gewährleistet wird

3 Auftragsverarbeitung & Datenschutzbeauftragte: **20**
Wer bei der Datenverarbeitung unterstützt

Extra: Die wichtigsten Grundsätze der DSGVO auf einen Blick **26**

Checkliste: 16 Tipps: Mitgliederdaten verwalten – aber sicher! **28**

Über digital verein(t) und seine Partner:innen **30**

Mehr digitale Themen **31**

Über dieses Handbuch

Wenn der Tierschutzverein mehr Zeit für bedrohte Daten als für bedrohte Arten aufwendet, läuft etwas schief. Mitgliederdaten sind zwar auch eine sehr schützenswerte Art – anders aber als bei der Fürsorge für bedrohte Vierbeiner und Fellnasen kann hier die digitale Technik einen Beitrag zur Zeitersparnis und Sicherheit leisten. Mit einer Verwaltungssoftware kann der Verein Adressdaten aktuell halten, Mitgliedschaftsbeiträge einziehen und die Kommunikation organisieren. Dabei lässt sich mit ein paar einfachen Grundsätzen und Maßnahmen der Vereinsdatenschatz auf so viele Daten wie nötig und so wenige Daten wie möglich begrenzen. Denn beim Umgang mit den persönlichen Daten der Mitglieder spielt die Europäische Datenschutz-Grundverordnung (DSGVO) eine wichtige Rolle.

Digital verein(t) hat 16 Tipps formuliert, die helfen, die digitalen Chancen für den eigenen Verein sicher zu nutzen. Im ersten Kapitel geht es um digitale Hilfsmittel zur Datenverwaltung und welche Regeln bei der Verarbeitung von Mitgliedsdaten zu beachten sind. Das zweite Kapitel erläutert, mit welchen Maßnahmen ein Verein die Sicherheit von Daten gewährleistet. Und schließlich zeigt das dritte Kapitel, wer bei der Verarbeitung und beim Schutz personenbezogener Daten unterstützen kann. Am Ende des Handbuchs befinden sich dann noch einmal die wichtigsten Grundsätze der DSGVO auf einen Blick.

Dieses Handbuch ersetzt keine Rechtsberatung. Es dient als praxisnahe Orientierungshilfe und soll zur Umsetzung der DSGVO im Vereinsalltag ermuntern.

In den digital verein(t)-Kästen befinden sich kurze und praktische Hilfsmittel:

Informieren
Hier werden Fachbegriffe verständlich erklärt.

Machen
Hier werden digitale Werkzeuge vorgestellt, welche sofort verwendet werden können.*

Üben
Hier gibt es Übungsaufgaben, um das neue Wissen anzuwenden.

Weiterlesen
Hier werden Websites und digital verein(t)-Handbücher mit weiterführenden Informationen empfohlen.

* Die ausgewählten Werkzeuge sind bevorzugt frei zugänglich und zumindest in der Basisversion unentgeltlich. Sie arbeiten außerdem datensparsam, transparent und möglichst werbefrei. Die Aufzählung verschiedener Alternativen folgt keiner Rangfolge, sondern ist alphabetisch geordnet.

1 Vereinssoftware & Datenschutz

1

Vereinssoftware & Datenschutz: Wie Mitgliederdaten digital verwaltet werden

Was ist bei der Wahl einer Vereinsverwaltungssoftware zu berücksichtigen? Welche Regeln gibt es bei der Erhebung personenbezogener Daten? Und wie kann eine Organisation die Informations- und Auskunftspflichten erfüllen? Die Datenschutzgrundverordnung gibt diesen Aufgaben einen sicheren Rahmen. .

Tipp 1 / Eine sichere Software zur Datenverwaltung wählen.

Die Verwaltung von Mitgliedern, Förderer:innen und ehrenamtlichen Helfer:innen ist ein wichtiger Baustein des bürgerschaftlichen Engagements. Eine Vereinssoftware bietet eine Vielzahl von Funktionen, die solche Verwaltungsaufgaben vereinfachen. Mit den Programmen lassen sich unter anderem Mitgliedsdaten und Beitragszahlungen digital verwalten und Veranstaltungen planen. Außerdem beinhalten sie Vorlagen für Zahlungsverkehr und Korrespondenz und können sogar statistische Auswertungen liefern.

Vereinsverwaltungsprogramme können entweder als Onlinedienst oder als installierte Software genutzt werden. Dabei ist auf seriöse Quellen zu achten und die Bewertungen der Produkte zu berücksichtigen. Vorab sollte man sich in jedem Fall über die **Leistungsmerkmale** der jeweiligen Software und Dienste informieren und diese mit den individuellen Anforderungen abgleichen. Reicht eine kostenfreie Basisversion mit eingeschränkten Funktionen? Oder möchte der Verein gleich mit dem kompletten Leistungsumfang starten?

Bei der Suche nach dem richtigen Anbieter sind nicht nur die wichtigsten Funktionen zu prüfen, sondern auch die Einhaltung des **Datenschutzes**. In den Allgemeinen Geschäftsbedingungen (AGB) des Anbieters sollten die Antworten auf folgende Fragen zu finden sein:

> Wie werden eingegebene Daten von der Software oder dem Dienst gegen Diebstahl und Missbrauch gesichert?
>
> Ist eine verschlüsselte Datenübertragung möglich?
>
> Welche Möglichkeiten bieten Software oder Dienst für die sichere Verwaltung von Beitragszahlungen und Kassenbuchführung?
>
> Entsprechen die Sicherungsmaßnahmen der DSGVO und dem neuen Bundesdatenschutzgesetz (BDSG)?

Da gerade gemeinnützige Vereine neben der Sicherheit auf die Kosten achten müssen, bietet sich Software an, deren Nutzung ganz oder teilweise kostenfrei ist. Sogenannte **Open-Source-Software** darf kostenfrei kopiert, verbreitet und genutzt werden. Open Source heißt auf Deutsch „offene Quelle", da bei diesen Programmen der Quellcode offengelegt ist. Zu den erfolgreichsten Open-Source-Projekten gehören das Betriebssystem GNU/ Linux, der Internetbrowser Firefox und der Web-Server Apache. Auch **Freeware** (auf Deutsch: freie Ware) ist Software, die von den Urheber:innen oder Hersteller:innen zur kostenlosen Nutzung zur Verfügung gestellt wird.

Beliebte Open-Source-Programme

i

Ein Quelltext oder auch **Quellcode** ist der in einer Programmiersprache geschriebene Text eines Computerprogramms oder einer Website. Wer sich den Quelltext anzeigen lassen möchte, klickt mit der rechten Maustaste in einen freien Bereich der Seite und wählt dann „Seitenquelltext anzeigen" aus.

JVerein ist ein Open-Source-Angebot zur Erfassung von Mitgliedsdaten und Beiträgen. Der Zahlungsverkehr kann hierüber abgewickelt werden, inklusive dem Druck von Spendenquittungen. Es gibt sogar eine Anbindung an die ebenfalls quelloffene Homebanking-Software Hibiscus. JVerein kann in Java implementiert werden und arbeitet somit auf Windows-, Linux- und Mac-Geräten. Ein Datenexport ist zu Open-Office und LibreOffice möglich. Auf der Website der Software findet sich ein Handbuch, das die Anwendung des Programms erklärt. In einem eigenen Forum können sich Nutzer:innen über die Software austauschen.
> jverein.de

JoGoVerein ist eine Freeware für Windows und bietet Funktionen zur Mitgliederverwaltung, Kassenbuchführung und Abrechnung von beispielsweise Mitgliedsbeiträgen. Ein Datenexport zu Microsoft Excel, Word und als Nur-Text-Format ist möglich. Zusätzliche Funktionen für Microsoft Access und MySQL sowie das Drucken von Dokumenten sind kostenpflichtig. Auch hier gibt es auf der Website ein Handbuch und ein eigenes Forum.
> jogoverein.goeldenitz.org

Die kostenfreie Software **Vereinsverwaltung** ist ein Verwaltungsprogramm, mit dem alle wichtigen Daten der Vereinsmitglieder organisiert werden können. Außerdem liefern hilfreiche Statistikfunktionen einen Überblick über die Einnahmen und Ausgaben des Vereins und den aktuellen Vereinsetat. Mitgliederlisten oder Datensätze können als Textdokument exportiert und mit einem Textverarbeitungsprogramm weiterbearbeitet werden. Das Programm enthält außerdem eine E-Mail-Funktion, mit der Nachrichten direkt an Einzelne oder alle Mitglieder verschickt werden können.
> giga.de/downloads/vereinsverwaltung

Tipp 2 **Die Datenschutz-Grundverordnung ist eine Chance, vertrauensvoll mit den Personendaten umzugehen.**

Die Europäische Datenschutz-Grundverordnung (DSGVO) vereinheitlicht seit Mai 2018 die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Institutionen und gilt in der gesamten Europäischen Union. Die Verordnung findet überall dort Anwendung, wo mit personenbezogenen Daten gearbeitet wird. Darunter fallen Vorgänge wie das Anschauen, Erheben, Speichern, Übermitteln, Nutzen, Verändern, Anonymisieren und Löschen von Daten. Die DSGVO gilt für jede Art der Datenverarbeitung, unabhängig davon, ob die Daten automatisiert, digital oder analog verarbeitet werden. Die DSGVO hilft Vereinen dabei, die personenbezogenen Daten seiner Mitglieder zu schützen.

Alle Informationen, über die ein Bezug zu einer bestimmten Person hergestellt werden kann, fallen unter den Begriff der **personenbezogenen** Daten. Dazu gehören unter anderem Name, Adresse, Telefonnummer, Bankverbindung, Bewegungsdaten, IP-Adresse, Chat-Protokolle, E-Mail-Adresse und Fotos. Ein Verein verwaltet in der Regel personenbezogene Daten von Mitgliedern, Mitarbeiter:innen und Helfer:innen.

Tipp 3 **Personenbezogene Daten nur mit Rechtsgrundlage oder Einwilligung erfassen und verarbeiten.**

Mit der DSGVO gilt das grundlegende Prinzip des **Verbots mit Erlaubnisvorbehalt**. Das heißt, dass zunächst niemand mit personenbezogenen Daten von anderen umgehen darf, es sei denn, es gibt eine Erlaubnis dafür. Eine Verarbeitung von personenbezogenen Daten ohne Rechtsgrundlage oder Einwilligung ist unzulässig und kann zu Bußgeldern führen. Nach dem Grundsatz der Rechtmäßigkeit (Art. 6 EU-DSGVO) darf ein Verein oder der eine Organisation in folgenden Fällen personenbezogene Daten verarbeiten:

1. **Ausdrückliche Einwilligung der betroffenen Person**
   Ein Verein darf personenbezogene Daten verarbeiten, wenn er über eine ausdrückliche Einwilligung der betroffenen Person verfügt. Eine Einwilligung ist nur unter bestimmten Voraussetzungen wirksam: Sie muss freiwillig und für einen bestimmten Zweck abgegeben worden sein. Eine pauschale Einwilligungserklärung in mögliche zukünftige Datenverarbeitungen ist unzulässig. Die betroffene Person muss klar und verständlich darüber informiert worden sein, für welchen Zweck die Einwilligung gilt und dass sie jederzeit widerrufen werden kann. Die Einwilligung muss zudem durch eine eindeutige Handlung erfolgen, beispielsweise indem die betroffene Person ein Häkchen setzt. Ein bereits angekreuztes Kästchen beziehungsweise ein sogenanntes Opt-out, bei dem der Datenverarbeitung widersprochen werden muss, reichen nicht aus.

2. **Rechtliche Verpflichtung zur Vertragserfüllung**
   Personenbezogene Daten, die zur Erfüllung eines Vertragsverhältnisses erforderlich sind, dürfen ohne Einwilligung der betroffenen Person verarbeitet werden. Ein solches Vertragsverhältnis liegt zum Beispiel vor, wenn ein neues Mitglied in den Verein eintreten möchte. Für den Mitgliedsbeitritt dürfen alle Daten erhoben werden, die für die Verwaltung der Mitgliedschaft erforderlich sind. Dazu gehören der Name und die Adresse, aber auch das Geburtsdatum, wenn es zum Beispiel für die Altersklasseneinteilung in bestimmten Sportarten erforderlich ist. Wichtig ist, dass die erhobenen Daten nur zweckgebunden verarbeitet werden. Die Weitergabe der Informationen an Dritte für andere Zwecke wie zum Beispiel die Weitergabe von Adressen an befreundete Mitglieder oder andere Vereine zum Versand von Werbung ist nicht erlaubt.

3. **Wahrung berechtigter Interessen des Verantwortlichen**
   Neben der ausdrücklichen Einwilligung und der Erfüllung eines Vertragsverhältnisses dürfen personenbezogene Daten auch dann verarbeitet werden, wenn dies zur Wahrung berechtigter Interessen des Verantwortlichen erforderlich ist. Dies ist zum Beispiel der Fall, wenn der Verein auf seiner Website Fotos mit Vereinsmitgliedern veröffentlicht mit dem Ziel, seine Außendarstellung zu fördern und über die Veranstaltungen zu informieren. Dabei ist jedoch wichtig, dass die Interessen des Vereins die Interessen der betroffenen Person überwiegen. Dies nachzuweisen ist im Zweifelsfall nicht einfach. Daher ist es oft praktikabler, sich beispielsweise über die Satzung oder den Mitgliedsantrag die Einwilligung der Mitglieder einzuholen.

Verantwortliche sind im Sinne der DSGVO Personen, Behörden, Einrichtungen oder andere Institutionen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Das ist in diesem Fall der Verein. Betroffene sind Personen, deren personenbezogene Daten verarbeitet werden und die dadurch identifiziert werden können. Im Falle von Vereinen sind betroffene Personen vor allem die Vereinsmitglieder.

Der Landessportbund Berlin informiert auf seiner Website über das Thema Datenschutz im Vereinskontext. Ausführliche Hintergrundinformationen sowie ein kurzes und ein ausführliches Musterschreiben einer **Einwilligungserklärung** befindet sich am Ende des Artikels „Datenschutz im Verein“. Durch Eingabe „Einwilligungserklärung“ oben rechts im Suchfeld der Website, gelangt man direkt zu dem Artikel.
> lsb-berlin.net

Tipp 4 / Erhobene Daten nur zweckgebunden verwenden.

Ein weiterer Grundsatz der DSGVO ist die Zweckmäßigkeit (Art. 5 EU-DSGVO): Daten dürfen nur zu dem Zweck verwendet werden, zu dem sie erhoben wurden und das Ziel der Vereinssatzung verfolgen. Zu den Daten, ohne die ein Wirken des Vereins nicht möglich wäre, gehören beispielsweise:

- Name und Anschrift
- Geburtsdatum
- bei Lastschriftverfahren: Bankverbindung
- Funktion im Verein
- Übungsleiterlizenz
- Leitungsergebnisse
- Daten zum Abschluss von Versicherungsverträgen

Keinen konkreten Zusammenhang zum Vereinszweck gibt es bei der Telefonnummer und der E-Mail-Adresse. Darüber hinaus darf der Verein auch Daten von Nicht-Mitgliedern erheben, sofern er damit berechtigte Interessen des Vereins wahrnimmt und der Schutz der Einzelperson nicht beeinträchtigt wird (Art. 6 EU-DSGVO). Dazu können gehören:

- Name von Gästen, Besucher:innen, fremden Spieler:innen
- Teilnehmer:innen an Lehrgängen und Wettkämpfen
- Personendaten zur Umsetzung eines Stadionverbots beim Verkauf von Eintrittskarten

Tipp 5 / So viele Daten wie nötig und so wenige wie möglich.

Bei der Verarbeitung von personenbezogenen Daten gilt immer der Grundsatz der **Datenminimierung** (Art. 5 EU-DSGVO): So viel wie nötig, aber so wenig wie möglich. Das bedeutet: Um Mitglieder zu betreuen, Spenden zu sammeln oder Sponsor:innen zu akquirieren, darf ein Verein immer nur die Daten erheben, die für die Durchführung des einzelnen Zwecks tatsächlich erforderlich sind.

Eine weitere grundsätzliche Regel zum Datenschutz ist die **Speicherbegrenzung** (Art. 5 EU-DSGVO). Der Verein darf personenbezogene Daten nur so lange speichern, wie es für den Zweck, für den sie erhoben wurden, notwendig ist und wie es die gesetzliche Aufbewahrungsfrist für Geschäftsvorgänge vorsieht.

Zur Übung: Welche personenbezogenen Daten werden im eigenen Verein erhoben und zu welchem Zweck geschieht das?

Tipp 6 / Zur Unterstützung ein Datenverarbeitungsverzeichnis einführen.

Schon vor Einführung der DSGVO mussten Vereine die Grundregeln bei der Verarbeitung personenbezogener Daten einhalten. Durch die DSGVO ist die sogenannte **Rechenschaftspflicht** hinzugekommen: Vereine müssen in der Lage sein, die Einhaltung der Grundregeln bei der Verarbeitung personenbezogener Daten nachzuweisen. Das lässt sich in der Praxis unkompliziert mit einem Datenverarbeitungsverzeichnis lösen. Ein Verarbeitungsverzeichnis beinhaltet alle innerhalb des Vereins durchgeführten **Verarbeitungstätigkeiten** im Zusammenhang mit personenbezogenen Daten. Das Verzeichnis ist dabei nicht zu verwechseln mit einem Protokoll. Ein Protokoll über die einzelnen Verarbeitungstätigkeiten muss nicht geführt werden.

Das Bayrische Landesamt für Datenschutzaufsicht (BayLDA) hat ein exemplarisch ausgefülltes Datenverarbeitungsverzeichnis erstellt.
> lda.bayern.de/media/muster_1_verein_verzeichnis.pdf

Ein weiteres Verzeichnismuster stellt der Landessportbund Thüringen auf seiner Website zur Verfügung. Dieser befindet sich im Download-Bereich, wenn nach dem Stichwort „Verarbeitungsverzeichnis" gesucht wird.
> thueringen-sport.de/downloads

Zur Übung: Für den Überblick ist ein Verzeichnis hilfreich: Welche Verarbeitungstätigkeiten fallen im eigenen Verein an? Welche Personen und Daten sind von den Tätigkeiten betroffen?

Tipp 7 / Mit Erhebung und Verarbeitung personenbezogener Daten transparent umgehen.

Mit dem Grundsatz der DSGVO, die Rechte und Freiheiten natürlicher Personen zu schützen, geht das **Recht der Betroffenen** einher, zu wissen, wer welche Informationen über sie sammelt und nutzt. Vereine müssen daher verständlich, präzise und in leicht zugänglicher Form darüber informieren, welche personenbezogenen Daten sie erheben und was mit den Daten gemacht werden soll. Wichtig ist, dass dies vor der Erhebung der Daten geschieht. Konkret müssen die Betroffenen über folgende Punkte informiert werden:

Name und Kontaktdaten des/der Verantwortlichen;

Kontaktdaten des/der Datenschutzbeauftragten (falls vorhanden);

Zwecke, für die die personenbezogenen Daten erhoben werden, sowie die Rechtsgrundlagen für die Erhebung;

Interessen des Vereins, falls er die Daten auf Basis einer Interessensabwägung verarbeiten möchte;

Empfänger:innen der Daten, falls der Verein die erhobenen Daten weitergeben möchte;

Dauer der Speicherung der Daten oder Kriterien für die Löschung;

Hinweis auf die Betroffenenrechte (Auskunft, Berichtigung, Löschung usw.);

Hinweis auf Beschwerderecht bei der Aufsichtsbehörde.

Vereine können diese Informationen beispielsweise über eine zusätzlich zum Mitgliedsantrag gereichte **Datenschutzerklärung** vermitteln oder die Punkte mit in die Vereinssatzung aufnehmen. Theoretisch müssten die Informationen auch bereits bestehenden Mitgliedern zur Verfügung gestellt werden. Bei der Datenschutzaufsicht liegt die Priorität jedoch darauf, dass ab Einführung der DSGVO alle zukünftigen Mitglieder informiert werden.

Die Schwelle für die **Informationspflicht** sinkt bei direktem und unkompliziertem Kontakt mit Personen. Wenn eine Person beispielsweise nach dem Termin einer bevorstehenden Veranstaltung fragt und der Vereinsvorstand verspricht, diese Information per SMS zu schicken und in diesem Zusammenhang sich die Nummer der Person notiert, ist keine gesonderte Information über die Verarbeitung der Daten notwendig.

Tipp 8 / Die Datenschutzerklärung auf der Webseite ist ein Pflichtelement.

Betreibt ein Verein eine eigene Vereinswebsite und verarbeitet dort personenbezogene Daten, ist eine **Datenschutzerklärung** neben dem Impressum ein Pflichtelement auf der Homepage (Art. 13 Abs. 1 EU-DSGVO). Der Verein muss darin über folgende Punkte informieren:

- Zweck- und Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten;
- Dauer der Speicherung von personenbezogenen Daten beziehungsweise Kriterien für die Festlegung der Dauer;
- Hinweis auf das Bestehen der Betroffenenrechte (Recht auf Auskunft, Berichtigung, Löschung) und Widerspruchsrecht;
- Hinweis auf das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- Hinweis auf den Einsatz externer Dienste wie zum Beispiel Facebook und Google, sofern diese durch den Webseitenaufruf personenbezogene Daten erheben;
- Informationen über den Einsatz von Cookies;
- Kontaktdaten des/der Datenschutzbeauftragten (wenn verpflichtend bestellt).

Die Nutzer:innen werden mit der Datenschutzerklärung darüber informiert, welche Daten beim Besuch der Website erfasst und wie diese verwendet werden: Werden die Daten aus dem Kontaktformular inklusive der Anfrage gespeichert? Werden Kontaktdaten weitergegeben und wenn ja warum und an wen? Werden auf der Website sogenannte Cookies verwendet, die das Klickverhalten aufzeichnen? Je mehr Transparenz der Verein auf der Website zeigt, desto vertrauenswürdiger ist er.

Ausführliche Informationen zur sicheren Gestaltung einer Vereinswebsite sind im digital verein(t)-Handbuch „Homepage: Sicher gestalten, organisieren und pflegen“ zu finden.

In dem Artikel „Aufbau einer einfachen Datenschutzerklärung“ auf der Seite iRIGHTSinfo sind ausführliche Informationen zur einfachen Datenschutzerklärung auf Websites. Als Vorlage für eine entsprechende Erklärung auf der eigenen Vereinswebsite eignet sich die Datenschutzerklärung von iRIGHTSinfo.
> Irights.info/datenschutzerklaerung

Ein weiteres Muster für die Datenschutzerklärung auf Vereinswebsites können auf den Seiten des Bayerischen Sportschützenbund e.V. im Download-Bereich heruntergeladen werden. Das „Muster für eine Datenschutzerklärung auf der Homepage“ befindet sich im Ordner „Datenschutz“.
> bssb.de/downloads.html

Betroffenenrechte: Berichtigung & Löschung

Bei der Verarbeitung personenbezogener Daten gilt außerdem der Grundsatz der **Richtigkeit** (Art. 5 EU-DSGVO). Das bedeutet, dass die Daten sachlich richtig und aktuell sein müssen. Betroffene Personen haben daher auch einen Anspruch auf die Korrektur falscher Daten. Dies ist zum Beispiel der Fall, wenn sich durch einen Umzug die Adresse ändert oder bei irrtümlichen Dateneingaben. Wünscht die betroffene Person eine Löschung der Daten, muss dem gefolgt werden, wenn

- für die Erfüllung des ursprünglichen Zwecks die weitere Speicherung der Daten nicht mehr erforderlich ist;
- der/die Betroffene die Einwilligung widerrufen hat;
- es keine andere Rechtsgrundlage für die weitere Speicherung der Daten gibt.

Betroffenenrechte: Widerspruch

Betroffene Personen haben das Recht, der Verarbeitung ihrer personenbezogenen Daten zu widersprechen. Dies ist vor allem dann relevant, wenn sich der Verein oder die Organisation als Rechtfertigung für die Verarbeitung auf eine **Interessensabwägung** beruft. Für einen wirksamen Widerruf muss der oder die Betroffene plausible Gründe vorbringen. Die Verantwortlichen müssen dann unter Kenntnis der neuen Gründe eine erneute Interessensabwägung vornehmen und die Verarbeitung unter Umständen stoppen.

Zur Übung: Um allen Betroffenenrechten als Verein gerecht werden zu können, ist es ratsam, verschiedene Szenarien vorab festzuhalten und folgende Frage zu beantworten: Wer gibt nach welchem Vorgehen welche Informationen im Falle einer Anfrage raus?

2

Zugänge, Berechtigungen & Backups

2

Zugänge, Berechtigungen & Backups: Wie die Sicherheit personenbezogener Daten gewährleistet wird

Wer darf im eigenen Verein welche Daten verwalten? Welche technischen Sicherheitsmaßnahmen müssen unternommen werden? Und wie kann der Verlust von Daten vermieden werden? Damit die Daten der Mitglieder im Verein sicher sind, helfen ein paar grundsätzliche Regelungen.

Tipp 9 / **Zugriffsrechte auf vertrauliche Daten regelmäßig kontrollieren und korrigieren.**

Datenverlust ist nicht immer auf illegale Aktivitäten wie Datendiebstahl zurückzuführen. Das Risiko besteht vor allem bei der alltäglichen Arbeit, wenn beispielsweise Daten versehentlich an eine:n falsche:n Adressaten:in versendet werden. Mit einfachen Maßnahmen kann ein Verein solche Risiken vermeiden.

Dem Grundsatz der **Vertraulichkeit und Integrität** personenbezogener Daten (Art. 5 EU-DSGVO) zufolge muss die Verarbeitung in einer Weise erfolgen, die eine angemessene Sicherheit der Daten gewährleistet. Die IT-Struktur des Vereins muss so aufgestellt sein, dass sich Unbefugte nicht einfach Zugriff auf Daten verschaffen können. Der Verein muss außerdem sicherstellen, dass die Daten weder beabsichtigt noch unbeabsichtigt verändert beziehungsweise manipuliert werden können. Dies wäre beispielsweise der Fall, wenn ein unerfahrenes Vereinsmitglied mit dem Aufräumen der Datenbank beauftragt wird, dafür zu viele Zugriffsrechte erhält und versehentlich die Mitgliederliste löscht oder verändert.

Ein geeigneter Weg, um die Integrität sicherzustellen, ist ein funktionierendes **Berechtigungsmanagement**. Das bedeutet, dass im Verein festlegt wird, wer auf welche Daten für welchen Zweck in den jeweiligen Systemen zugreifen darf. Erhalten Personen jeweils nur die absolut erforderlichen Rechte, ist der eigene Verein auf der sicheren Seite. Dateiserver bieten die Möglichkeit, verschiedenen Nutzer:innen unterschiedliche Zugriffsrechte zuzuteilen. Nutzt ein Verein beispielsweise eine Buchhaltungssoftware, sollten nur die Personen einen Zugang zu der Anwendung erhalten, die mit der Buchhaltung des Vereins betraut sind (Art. 18 EU-DSGVO).

Wird nur mit persönlichen Computern gearbeitet, müssen auch hier Dateien und Programme unbedingt mit starken Passwörtern gesichert werden. Dabei sollte vermieden werden, dass mehrere Personen über einen Account und ein Passwort auf die Daten zugreifen können. Jedes Mitglied braucht einen eigenen Account und eigene Zugänge.

Ausführliche Anleitungen zu sicheren Passwörtern, Merkmethoden und Passwort-Verwaltungsprogrammen sind im digital verein(t)-Handbuch „Gemeinsam im Netz: Geräte absichern, Informationen sammeln und Netzwerke teilen“ zu finden.

Tipp 10 / **Daten mit Verschlüsselungsverfahren schützen.**

Die Verschlüsselung ist nach der DSGVO eine geeignete Maßnahme zur sicheren Datenverarbeitung. Es gibt eine Reihe von Verschlüsselungsmethoden, die im Alltag leicht anzuwenden sind:

E-Mail-Verschlüsselung: Wenn personenbezogene Daten über E-Mail verschickt werden, ist es ratsam, die E-Mails zu verschlüsseln.

Vereins-WLAN: Bietet der Verein oder die Organisation den Mitgliedern oder Gästen ein WLAN zur Nutzung an, sollte dessen Zugang nicht nur mit einem guten Passwort, sondern auch mit der WPA2-Methode gesichert sein.

Website: Sowohl die eigene Vereinswebsite als auch die Websites, die besucht wird, sollten mit dem sogenannten SSL-Zertifikat verschlüsselt sein. Dies ist erkennbar durch ein Schloss-Symbol neben der Websiteadresse (URL) als auch an dem Ausdruck „https://“ in der URL.

Dateien und Dokumente: Viele Dateien und Dokumente können mithilfe von Programmen wie den Office-Anwendungen Word, Excel oder PowerPoint mit einem Passwort versehen werden. Bietet das Programm selbst keine Möglichkeit an, ein Passwort zu erstellen, können die Dateien in einem verschlüsselten ZIP-Ordner verpackt und mit einem Passwort geschützt werden.

WPA2 (Wi-Fi Protected Access, auf Deutsch: Wi-Fi geschützter Zugang) ist die neueste Verschlüsselungsmethode für WLAN. Drahtlose Netzwerke werden dadurch vor dem unbefugten Zugriff geschützt, so dass ausgetauschte Daten nicht durch Dritte mitgelesen werden können.

Wie E-Mails verschlüsselt werden können, wird im digital verein(t)-Handbuch „Online-Kommunikation: Mailen, Messenger nutzen und Videokonferenzen veranstalten“ erklärt. Weitere Informationen zur Einrichtung und Administration einer sicheren Vereinswebsite sind im digital verein(t)-Handbuch „Homepage: Sicher gestalten, organisieren und pflegen“ zu finden.

Tipp 11 / Daten nur anonymisiert auswerten.

Die Analyse von Mitgliedsdaten ermöglicht es Vereinen, sich strategisch weiterzuentwickeln. Dabei können die Ergebnisse auch für die Kommunikation nach außen interessant sein. Die **Datenanalyse** liefert Erkenntnisse aus verschiedenen Bereichen:

Die **vergangene Entwicklung** eines Vereins lässt sich besser verstehen, beispielsweise mit der Frage: Welche Aktionen oder Maßnahmen haben sich auf die Mitgliederentwicklung positiv ausgewirkt?

Das **Beitragsengagement** lässt sich genau analysieren, unter anderem mit der Frage: Wie hoch ist der durchschnittliche Mitgliedsbeitrag?

Aus dieser Datenanalyse ergeben sich Hinweise auf die **Zielgruppen** eines Vereins. Dazu gehören Fragen wie: Sollte der Verein eher Personen ansprechen, die ihn mit einer hohen Einmalspende unterstützen oder mit einer kleineren regelmäßigen Summe? Wie sind die Geschlechterverteilung und das Durchschnittsalter?

Die Datenanalyse zeigt problematische Entwicklungen an und bietet **Erklärungsansätze**. Dadurch lässt sich beispielsweise ein Mitgliederschwund rechtzeitig erkennen und nachvollziehen. Ein anderer Weg, um interessante Daten für oder über die Vereinsarbeit zu gewinnen, ist eine Mitgliederumfrage zu einem aktuellen Thema. Wie auch immer Daten erhoben werden: Die betroffenen Personen sollten auf jeden Fall wissen, dass die Daten anonymisiert ausgewertet werden.

Kostenlose Online-Umfragen lassen sich beispielsweise mit der Anwendung Google Formulare erstellen. Dazu muss ein Google-Konto eingerichtet werden. Nachdem man sich in diesem Konto angemeldet hat, erhält man über die Funktion „Google Apps" Zugriff auf die Anwendung Google Formulare. Dort können dann individuelle Umfragen erstellt werden.
> www.google.com/forms/about

maQ-online.de bietet die Möglichkeit, Umfragen online zu erstellen. An den Umfragen können bis zu 600 Personen teilnehmen, die Laufzeit der Befragung kann auf 30, 60 oder 90 Tage festgelegt werden. Die Umfrageergebnisse lassen sich grafisch darstellen oder können zur Weiterbearbeitung in ein Tabellenkalkulations- oder Statistikprogramm exportiert werden.
> maQ-online.de

Für die Auswertung der erhobenen Daten kann zum Beispiel das Datenverarbeitungs- und Tabellenkalkulationsprogramm **Excel** genutzt werden. Dort lassen sich erhobene Daten anschaulich in Form von Tabellen und Diagrammen darstellen. Eine kostenlose Alternative zu Excel ist das Tabellenkalkulationsprogramm Calc von OpenOffice. Auch mit **Calc** lassen sich aussagekräftige Diagramme und Schaubilder erstellen, die die Umfrageergebnisse anschaulich zusammenfassen

Zur Übung: Drei Hypothesen überlegen, die mit einer Datenanalyse untersucht werden sollen. Zum Beispiel: In der Weihnachtszeit steigt das Spendenvolumen stark an – trifft das für auf den eigenen Verein zu?

Tipp 12 / Regelmäßige Backups der Dateien erstellen.

Sicherheitslücken in IT-Systemen werden von den Herstellern immer wieder durch Updates geschlossen. Vereine müssen sich daher regelmäßig über mögliche Lücken erkundigen und notwendige **Updates** für Software und Hardware installieren.

Für den Fall, dass es dennoch zu einem Datenverlust kommt – sei es durch Hacker oder selbstverschuldet – ist es wichtig, in regelmäßigen Abständen **Sicherheitskopien**, sogenannte Backups, der Dateien anzufertigen. Wenn ein Verein oder eine Organisation einen eigenen Server nutzt, bietet dieser häufig eine automatische, regelmäßige Sicherung der Dateien an. Diese müssen dann auf dem Server gespeichert werden und nicht lokal auf dem eigenen Computer.

Alternativ können die Daten auf einer externen Festplatte gespeichert und sicher verwahrt werden. Hier ist darauf zu achten, dass die Sicherung regelmäßig erfolgt. Es gibt auch die Möglichkeit, Daten in einer Cloud zu sichern. Dabei werden die Daten automatisch und kontinuierlich gesichert, wenn eine Cloud auf dem Rechner eingerichtet ist. Hierbei sollte auf jeden Fall ein vertrauenswürdiger Cloud-Anbieter genutzt werden, der die Vorgaben der DSGVO einhält.

AOMEI Backupper ist eine Backup-Software für den Schutz und die Notfallwiederherstellung von Dateien und Festplatten. Die Software verfügt über alle wichtigen Funktionen, die für eine umfassende Datensicherung notwendig sind. Möglich sind Backups ganzer Festplatten sowie von einzelnen Ordnern und Dateien. Die Standardversion von AOMEI Backupper ist kostenlos und für Windows 10, 8.1, 8, 7, Vista und XP verfügbar.
> backup-utility.com/de

Ebenfalls nutzbar für alle Windows-Geräte ab Windows 95 ist die Datensicherungssoftware **TrayBackup**. Die Freeware ermöglicht das Sichern von einzelnen Dateien sowie von ganzen Verzeichnissen. Außerdem können Dateien und/oder Verzeichnisse ausgewählt werden, die nicht gesichert werden sollen. Tray Backup benötigt keine Installation, sondern kann direkt von einem Wechseldatenträger (zum Beispiel von einem USB-Stick aus) gestartet werden. Für den privaten Einsatz und den Einsatz in öffentlichen Bildungseinrichtungen sowie gemeinnützigen Organisationen ist die Nutzung kostenlos.
> traybackup.de

Für die Sicherung von iOS-Geräten kann unter anderem die Software **SmartBackup** verwendet werden. Die Software ist kostenlos und ab macOS 10.10 verfügbar. Auch hier lassen sich entweder einzelne Dateien oder ganze Systeme sichern. Auf der Herstellerseite befindet sich ein Hilfe-Bereich, in welchem gängige Fragen zur Verwendung von SmartBackup nachgeschlagen werden können.
> solesignal.com/smartbackup4

Tipp 13 / **Nur Befugten den Zugang zu personenbezogenen Daten erteilen.**

Datensicherheit betrifft auch den physischen Zugang zu den Daten. Ob es sich um Ordner handelt, in denen Mitgliederinformationen abgelegt sind, oder einen Dateiserver, spielt dabei keine Rolle. Wichtig ist, dass Unbefugte keinen freien Zugang zu den Daten haben. Der Zugang zu den Räumen oder Schränken mit personenbezogenen Daten sollten daher immer gesichert sein, beispielsweise durch eine abschließbare Tür, einen abschließbaren Schrank oder eine Alarmanlage.

IT-Sicherheit als Vorstandssache

Das Thema Datenschutz betrifft viele unterschiedliche Bereiche und mehrere verantwortliche Personen im Verein. Zudem kann eine ganzheitliche Umsetzung der DSGVO gegebenenfalls Kosten verursachen. Gleichzeitig vertrauen Vereinsmitglieder darauf, dass sorgsam mit ihren Daten umgegangen wird. Aus diesem Grund müssen die IT-Sicherheit und der Datenschutz im Allgemeinen nicht nur von einzelnen Personen im Verein betrieben, sondern vom gesamten Vorstand unterstützt werden.

3

Auftragsverarbeitung & Datenschutzbeauftragte

3

Auftragsverarbeitung & Datenschutzbeauftragte: Wer bei der Datenverarbeitung unterstützt

Darf ein Verein Daten an Dienstleister weitergeben? Was steht in einem Auftragsverarbeitungsvertrag? Braucht ein Verein eine:n Datenschutzbeauftragte:n? Und was ist zu tun, wenn es doch mal zu einer Datenschutzverletzung kommt?

Tipp 14 / **Abschließen eines Auftragsverarbeitungsvertrag mit externen Dienstleistern.**

Manchmal können nicht alle im Verein anfallenden Arbeiten, die mit personenbezogenen Daten zu tun haben, selbst erledigt werden. Dann besteht die Möglichkeit, auf die Hilfe externer Dienstleister zurückzugreifen. Dies ist zum Beispiel der Fall, wenn ein externer Anbieter die Buchhaltung erledigt oder sich ein:e IT-Berater:in um eine funktionierende Serverstruktur kümmert.

Wenn externe Dienstleister Aufgaben für Vereine erfüllen und dabei mit personenbezogenen Daten arbeiten, handelt es sich um eine **Auftragsverarbeitung** (Art. 28 EU-DSGVO). Eine spezielle Einwilligung der Betroffenen ist dafür nicht notwendig, wenn allein der Verein über die Zwecke und Mittel der Verarbeitung entscheidet. Der Dienstleister führt also nur weisungsabhängig einen bestimmten Auftrag durch, ohne auf eigene Faust die Daten weiterzuverarbeiten. Dies gilt unter anderem für:

- Mitgliedsbeitragsabrechnung durch externe Buchhaltung;
- Lohn- und Gehaltsabrechnungen durch eine:n Steuerberater:in;
- Versand von Vereinszeitschriften über einen externen Versender.

Vor dem Auftrag ist zu prüfen, ob der Dienstleister garantiert, dass die Verarbeitung im Einklang mit den Vorschriften der DSGVO erfolgt. Für jede Auftragsverarbeitung muss dann zwischen dem Verein und dem Dienstleister ein Auftragsverarbeitungsvertrag geschlossen werden. Der Vertrag muss folgende vier Punkte enthalten:

- Beschreibung und Festschreibung des Weisungsrechts des Vereins;
- Inhalt des Auftrags;
- Verpflichtung zur Vertraulichkeit und Einhaltung der Sicherheit;
- Festlegung, was mit den Daten nach Abschluss der Auftragsverarbeitung geschehen soll.

Das Bayerische Landesamt für Datenschutzaufsicht stellt einen Muster-**Auftragsverarbeitungsvertrag** zur Verfügung.
> lda.bayern.de/media/muster_adv.pdf

Einen individuell anpassbaren Mustervertrag bietet auch der Bundesverband für Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) an.
> bitkom.org/Bitkom/Publikationen/Mustervertragsanlage.html

Bei der Beauftragung muss sich der Verein außerdem umfangreiche **Kontrollrechte** einräumen lassen. Es muss zum Beispiel ohne Vorankündigung möglich sein, Kontrollen beim Dienstleister vor Ort durchzuführen. Das gilt auch für die Heimarbeit von Privatwohnungen.

Für das **Ende der Auftragsverarbeitung** durch den Dienstleister sind entsprechende Reglungen zu treffen. So muss vor allem festgelegt werden, was mit den Daten nach dem Ende des Vertrags passiert. Das betrifft unter anderem die Frage, wie und ob sie gelöscht werden und welche Daten in welcher Form an den Verein zurückzugeben sind.

Die Mitgliederdaten eines Vereins sind nicht automatisch auch Daten eines Dachverbandes, dem der Verein angehört. Vielmehr ist der **Dachverband** datenschutzrechtlich wie eine fremde Stelle zu behandeln. Personenbezogene Daten der Vereinsmitglieder dürfen dem Dachverband nur zur Verfügung gestellt werden, wenn dieser eine Aufgabe erfüllt, die letztlich auch im berechtigten Interesse des übermittelnden Vereins liegt.

Zur Übung: Durchführung einer Überprüfung, mit welchen externen Dienstleistern der eigene Verein zusammenarbeitet und ob diese die Anforderungen der DSGVO einhalten. Falls noch nicht vorhanden, sollte ein Auftragsverarbeitungsvertrag mit den Anbietern abgeschlossen werden.

Handbuch von digital verein(t): Zusammenarbeit im Verein. Online-Zusammenarbeit: Projekte organisieren, erarbeiten und Wissen austauschen.

Mitgliederdatenverwaltung in einer Cloud

Cloud-Standorte in den USA sollten eine Zertifizierung durch den sogenannten EU-US Privacy Shield besitzen.

Wenn Cloud-Dienste für die Verwaltung oder Erhebung von personenbezogenen Daten genutzt werden, handelt es sich datenschutzrechtlich ebenfalls um eine Auftragsverarbeitung. Darum sollte, wie bei anderen externen Dienstleistern, darauf geachtet werden, dass der Cloud-Dienst die Vorschriften der DSGVO einhält. Eine Datenschutz-Zertifizierung nach DSGVO ist dabei sehr hilfreich. Der Cloud-Standort muss nicht innerhalb der EU liegen, aber es müssen die EU-Standardvertragsklauseln gelten.

Cloud Computing (auf Deutsch: Rechnerwolke oder Datenwolke) ist eine IT-Infrastruktur, die in der Regel aus Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung besteht. Diese Dienstleistungen werden über ein Rechnernetz zur Verfügung gestellt, also ohne Installation auf lokalen Geräten. Die Nutzung erfolgt über technische Schnittstellen, in den meisten Fällen über einen Webbrowser.

Weitere Informationen zur Nutzung von Cloud-Diensten sind im digital verein(t)-Handbuch „Online-Zusammenarbeit: Projekte organisieren, erarbeiten und Wissen austauschen“ zu finden.

Tipp 15 / Eine:n Datenschutzbeauftragte:n benennen.

Für den Schutz personenbezogener Daten ist in der Regel der Vorstand des Vereines verantwortlich. Ein:e Datenschutzbeauftragte:r kann den Vereinsvorstand dabei unterstützen und als Ansprechpartner:in für Betroffene oder die Datenschutzbehörde zur Verfügung stehen. Die Haftung trägt dabei weiterhin der Vereinsvorstand. Grundsätzlich kann jeder Verein selbst entscheiden, ob er eine:n Datenschutzbeauftragte:n ernennen möchte. Eine freiwillige Ernennung bietet sich insbesondere dann an, wenn dem Verein die nötigen Kapazitäten oder das Wissen fehlen, um alle Punkte der DSGVO richtig umzusetzen. Es gibt jedoch zwei Ausnahmen, bei denen ein Verein eine:n Datenschutzbeauftragte:n ernennen muss:

1 Die Benennung einer/eines Datenschutzbeauftragten ist Pflicht, wenn im Verein mindestens 20 Personen ständig mit der Verarbeitung von personenbezogenen Daten beschäftigt sind (§38 BDSG). Ständig heißt dabei nicht, dass eine Person Vollzeit arbeitet. Selbst wenn eine Person nur fünf Stunden pro Woche freiwillig im Verein aushilft, sich dann jedoch primär um die Pflege und Aktualisierung der Mitgliederdatenbank kümmert, zählt diese Person zu den zwanzig Personen.

2 Ein Verein muss außerdem eine:n Datenschutzbeauftragte:n ernennen, wenn es seine **Kerntätigkeit** ist, Daten der folgenden Art zu erheben:

   Gesundheitsdaten

   Daten zum Sexualleben oder zur sexuellen Orientierung

   genetische Daten

   Daten mit Bezug zur ethnischen Herkunft

   Daten mit Bezug zur politischen Meinung

   Daten zur religiösen Überzeugung oder Weltanschauung

   strafrechtlich relevante Daten.

Wichtig ist, dass es sich dabei um eine Kerntätigkeit des Vereins handelt. Werden zum Beispiel in der Lohnabrechnung – wie verpflichtend vorgeschrieben – Daten für die Ermittlung der Kirchensteuer erfasst, ist dies nicht als eine Kerntätigkeit zu werten.

Datenschutzbeauftragte können, müssen aber nicht Mitglied des Vereins sein und werden in der Regel durch den Vorstand bestellt. Ein Vereinsmitglied kann die Aufgabe auch neben anderen Pflichten wahrnehmen, wenn es dabei nicht zum Interessenskonflikt kommt. Die schriftliche **Benennung** ist nicht verpflichtend, aber empfehlenswert, um der Datenschutzbehörde im Zweifelsfall die Benennung nachweisen zu können. Die DSGVO sieht zudem vor, dass der Verein die Kontaktdaten des/der Datenschutzbeauftragten der Aufsichtsbehörde mitteilt, was mittels eines Onlineformulars der zuständigen Behörde erfolgen kann.

Datenschutzbeauftragte haben bestimmte **Aufgaben** zur Kontrolle und zur Unterstützung des Vereinsvorstands zu erfüllen:

- Unterrichtung und Beratung des Vereins und der Beschäftigten hinsichtlich ihrer Pflichten nach Datenschutzrecht;
- Überwachung der Einhaltung der Datenschutzvorschriften;
- Beratung im Zusammenhang mit Datenschutz-Folgeabschätzungen;
- Zusammenarbeit mit der Aufsichtsbehörde;
- Anlaufstelle für die Aufsichtsbehörde in Fragen, die mit der Verarbeitung personenbezogener Daten zusammenhängen;
- Beratung betroffener Personen.

Dabei sind für die Einhaltung der Richtlinien im Vereinsalltag immer die Mitarbeiter:innen beziehungsweise in letzter Instanz der Vorstand verantwortlich.

Die DSGVO gibt vor, dass Vereine die Kontaktdaten des/der Datenschutzbeauftragten veröffentlichen. Hier genügt die Veröffentlichung einer bestimmten E-Mail-Adresse wie zum Beispiel datenschutz@vereinx.de. Der Name oder die persönlichen Kontaktdaten des/der Datenschutzbeauftragten müssen nicht genannt werden. Wichtig bei der Nutzung einer solchen E-Mail-Adresse ist, dass die Eingänge des Postfachs regelmäßig, das heißt beispielsweise ein Mal pro Woche kontrolliert werden.

Datenschutzverletzungen und Sanktionen

Eine **„Verletzung des Schutzes personenbezogener Daten"** liegt vor, wenn dies negative Folgen für diese Daten haben kann. Darunter fallen die Vernichtung, der Verlust, die Veränderung, die unbefugte Offenlegung und der unbefugte Zugang zu personenbezogenen Daten. Es spielt dabei keine Rolle, ob die Verletzung der Sicherheit absichtlich oder unbeabsichtigt erfolgt. Mögliche Formen sind:

- Hacking des Servers durch Dritte;
- Datenverlust (zum Beispiel durch Verlust eines Laptops oder USB-Sticks);
- Diebstahl von Daten (zum Beispiel bei Einbruch in die Vereinsräume);
- Fehlversand von Daten (zum Beispiel durch Eingabe eines falschen E-Mail-Empfängers);
- Softwarefehler (zum Beispiel durch Fehler in der Datenbanksoftware);
- Schadcode (zum Beispiel durch einen Computervirus);
- Fehlentsorgung (zum Beispiel wenn eine defekt geglaubte Festplatte in den Müll geworfen wird).

Wenn die Daten der Mitglieder, Mitarbeiter:innen oder Dritter gut geschützt sind, gibt dies aktuellen und potenziellen neuen Mitgliedern ein zusätzliches Sicherheitsgefühl. Dementsprechend kann die Einhaltung und Umsetzung der DSGVO selbstbewusst über die eigenen Kanäle wie die Website oder den Newsletter kommuniziert werden.

Trotz aller Bemühungen kann es jedem Verein passieren, dass es zu Datenschutzverletzungen kommt, sei es unabsichtlich durch eigene Vereinsmitarbeiter:innen oder unrechtmäßig durch einen Eingriff von Dritten. Dies ist kein Grund zur Panik. Die Datenschutzbehörden sind nicht daran interessiert, kleine Vereine mit unverhältnismäßigen Strafen zu belegen. Oft wird sogar von Sanktionen abgesehen, vor allem wenn sich der Verein darum bemüht, die Regeln und Pflichten der DSGVO einzuhalten und umzusetzen. Wichtig ist jedoch, bei einer Datenschutzverletzung die richtigen Maßnahmen zu ergreifen.

Tipp 16 / Datenschutzverletzungen bei der zuständigen Aufsichtsbehörde melden.

Wenn der Schutz personenbezogener Daten verletzt wurde, ist dies unverzüglich der Aufsichtsbehörde zu melden, spätestens aber innerhalb von 72 Stunden nach Bekanntwerden der Verletzung. Dann wird gemeinsam geprüft, welches **Risiko für die Betroffenen** entstanden ist, und es werden weitere Schritte besprochen. Die Meldung kann bei den meisten Datenschutzbehörden über ein Onlineformular erfolgen. Zuständig ist immer die Datenschutzbehörde des jeweiligen Bundeslandes, in dem der Verein seinen Sitz hat.

Betroffene müssen nur dann über die Verletzung ihrer personenbezogenen Daten informiert werden, wenn die Schutzverletzung ein voraussichtlich hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person zur Folge hat. Da diese Einschätzung nicht so leicht ist, empfiehlt es sich, hier mit der Aufsichtsbehörde zusammenzuarbeiten.

Die **Benachrichtigungspflicht** entfällt, wenn der Verein im Vorfeld geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat wie zum Beispiel die Verschlüsselung risikobehafteter Daten. Sind Smartphone oder Laptop mit starken Passwörtern gesichert, durch die ein unbefugter Zugriff auf die Daten im Normalfall verhindert wird, müssen bei einem Verlust des Geräts die Betroffenen nicht benachrichtigt werden.

Die möglichen **Sanktionen** bei Verletzungen des Schutzes personenbezogener Daten schreiben Geldbußen in Millionenhöhe vor. Dabei geht es primär darum, größeren Unternehmen bei bewussten Datenschutzverletzungen wirksame Mittel entgegenzustellen. Denn die Verordnung legt ebenso fest, dass Geldbußen verhältnismäßig und abschreckend sein müssen. Vereine, die grundsätzlich auf den Datenschutz achten sowie organisatorisch und technisch gut aufgestellt sind, haben daher keine oder nur sehr geringe Sanktionen zu erwarten.

Ist dem Vereinsvorstand das Thema Datenschutz offenkundig egal und werden Vorschriften bewusst missachtet, muss mit hohen Strafen gerechnet werden.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfahlen hat eine umfangreiche **Handreichung „Datenschutz im Verein nach der Datenschutz-Grundverordnung“** veröffentlicht (Stand: November 2018). Unter den Suchbegriffen „Datenschutz Verein“ im Suchfeld oben rechts erscheint die Broschüre.
> ldi.nrw.de

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat eine Checkliste zu den wesentlichen Anforderungen der DSGVO an Vereine erstellt. In Verbindung mit den ergänzenden Hinweisen am Ende der Checkliste gibt das Dokument Vereinen eine Orientierung bei der Umsetzung der DSGVO.
> lda.bayern.de/media/muster_1_verein.pdf

Auch der Landesbeauftragte für Datenschutz und Informationsfreiheit des Landes Baden-Württemberg hat einen Praxisratgeber zum „Datenschutz im Verein nach DS-GVO“ herausgegeben. Diese Broschüre ist einsehbar, wenn auf der Website im Suchfeld oben rechts die Begriffe „Praxisratgeber DSGVO“ eingegeben werden.
> baden-wuerttemberg.datenschutz.de

In jedem Fall trägt der Vereinsvorstand die Verantwortung für die Umsetzung und muss die Haftung bei eventuellen Verstößen übernehmen. Um Datenschutzverletzungen frühzeitig zu erkennen und angemessen zu reagieren, helfen die folgenden Maßnahmen:

Es sollte sich vorab darüber informiert werden, welche Datenschutzbehörde für den eigenen Verein zuständig ist.

Es sollte geprüft werden, wie sich Datenschutzverletzungen im eigenen Verein erkennen lassen.

Es sollte festgelegt werden, wer bei einer aufgetretenen Datenschutzverletzung die notwendigen Schritte unternimmt.

Es sollten alle Vereinsmitglieder über Datenschutzverletzungen und die nötigen Schritte informiert werden.

Es sollte sich bei Datenschutzverletzungen mit der zuständigen Behörde abgestimmt werden, was zu tun ist.

Die wichtigsten Grundsätze der DSGVO auf einen Blick

Verbot mit Erlaubnisvorbehalt
Grundsätzlich ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten verboten.

Rechtmäßigkeit
Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn

- eine Einwilligung erteilt wurde,
- die Verarbeitung für die Erfüllung eines Vertrages erforderlich ist oder
- die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist.

Zweckbindung
Betroffene Person müssen darüber informiert werden, zu welchem Zweck die Verarbeitung der Daten erfolgt. Zudem dürfen die erhobenen Daten nur zu dem angegebenen Zweck genutzt werden.

Datenminimierung
Es dürfen nur die Daten erhoben werden, die für den angegebenen Zweck dringend benötigt werden.

Speicherbegrenzung
Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für den Zweck nötig ist, für den sie erhoben wurden.

Richtigkeit
Personenbezogene Daten müssen richtig und auf dem neuesten Stand sein. Falsche Daten müssen gelöscht oder berichtigt werden.

Integrität und Vertraulichkeit
Für personenbezogene Daten muss eine angemessene Sicherheit gewährleistet werden, so dass unbeabsichtigter Verlust, Zerstörung oder ähnliches durch technische oder organisatorische Maßnahmen weitestgehend ausgeschlossen werden.

Platz für Notizen

Checkliste

10 Tipps: Mitgliederdaten verwalten – aber sicher!

- **Tipp 1**
  Eine sichere Software zur Datenverwaltung wählen.
- **Tipp 2**
  Die Datenschutz-Grundverordnung ist eine Chance, vertrauensvoll mit den Personendaten umzugehen.
- **Tipp 3**
  Personenbezogene Daten nur mit Rechtsgrundlage oder Einwilligung erfassen und verarbeiten.
- **Tipp 4**
  Erhobene Daten nur zweckgebunden verwenden.
- **Tipp 5**
  So viele Daten wie nötig und so wenige wie möglich.
- **Tipp 6**
  Zur Unterstützung ein Datenverarbeitungsverzeichnis einführen.
- **Tipp 7**
  Mit Erhebung und Verarbeitung personenbezogener Daten transparent umgehen.
- **Tipp 8**
  Die Datenschutzerklärung auf der Webseite ist ein Pflichtelement.
- **Tipp 9**
  Zugriffsrechte auf vertrauliche Daten regelmäßig kontrollieren und korrigieren.

Tipp 10
Daten mit Verschlüsselungsverfahren schützen.

Tipp 11
Daten nur anonymisiert auswerten.

Tipp 12
Regelmäßige Backups der Dateien erstellen.

Tipp 13
Nur Befugten den Zugang zu personenbezogenen Daten erteilen.

Tipp 14
Abschließen eines Auftragsverarbeitungsvertrag mit externen Dienstleistern.

Tipp 15
Eine:n Datenschutzbeauftragte:n benennen.

Tipp 16
Datenschutzverletzungen bei der zuständigen Aufsichtsbehörde melden.

Weitere Themen und Informationen unter:
digital-vereint.de

Über uns und unsere Partner:innen

Gefördert durch
Bayerisches Staatsministerium für Digitales

Das **Bayerische Staatsministerium für Digitales** wurde im Zuge der Regierungsbildung am 12. November 2018 neu gegründet. Es ist Denkfabrik der Digitalisierung in Bayern und kümmert sich um Grundsatzangelegenheiten, Strategie und Koordinierung. Das Digitalministerium ist das erste dieser Art in Deutschland. Damit unterstreicht Bayern die fundamentale Bedeutung des digitalen Wandels.

Das Digitalministerium steht für die Entschlossenheit, den weltweiten digitalen Entwicklungen nicht nur zu folgen, sondern sie souverän mitzugestalten. Bayerns starke Wirtschaft, innovative Wissenschaft und Forschung und die engagierten Bürger werden dabei eng eingebunden.
> stmd.bayern.de

DsiN Deutschland sicher im Netz

Deutschland sicher im Netz e.V. (DsiN) wurde 2006 als Verein auf dem ersten Nationalen IT-Gipfel gegründet. Als gemeinnütziges Bündnis unterstützt DsiN Verbraucher:innen und kleinere Unternehmen im sicheren und souveränen Umgang mit der digitalen Welt. Dafür bietet der Verein in Zusammenarbeit mit seinen Mitgliedern und Partner:innen konkrete Hilfestellungen sowie Mitmach- und Lernangebote für Menschen im privaten und beruflichen Umfeld an. Schirmherr des Vereins ist der Bundesminister des Innern, für Bau und Heimat.
> sicher-im-netz.de

lagfa bayern

Die **lagfa bayern** versteht sich als Brückenbauer zwischen Zivilgesellschaft, Staat und Wirtschaft und handelt bedarfsorientiert als Partner und Berater von Organisationen, Initiativen, öffentlicher Verwaltung, Bildungseinrichtungen und Wirtschaft. Wir schaffen also Netzwerke im Bürgerschaftlichen Engagement.

Wir wollen Menschen begeistern und ermutigen, beraten und begleiten, sich mit ihren vielfältigen Fähigkeiten, Erfahrungen und Interessen für die Gesellschaft zu engagieren.
> lagfa-bayern.de

Digitale Nachbarschaft

Mit der **Digitalen Nachbarschaft (DiNa)** sensibilisiert Deutschland sicher im Netz e.V. Vereine, Initiativen und freiwillig engagierte Bürger:innen für die Chancen der Digitalisierung. Die DiNa wird in Kooperation mit dem Bundesnetzwerk Bürgerschaftliches Engagement (BBE) durchgeführt. Gefördert wird das Projekt durch das Bundesministerium des Innern, für Bau und Heimat, unterstützt von der Deutschen Telekom AG, Huawei Technologies Deutschland GmbH und der Deutschen Bahn AG.
> digitale-nachbarschaft.de

Mehr digitale Themen

Sie möchten sich aktuell zur digitalen Sicherheit informieren und mögliche Sicherheitsprobleme schnell beheben?

Laden Sie kostenlos die SiBa-App herunter:
> sicher-im-netz.de/siba

Starten Sie auf Ihrem Gerät den Computercheck von Deutschland sicher im Netz e.V., um Fehler im System zu erkennen und zu beheben.
> sicher-im-netz.de/dsin-computercheck

Sie möchten digitale Kompetenzen weitervermitteln?

#DABEI-Geschichten ist ein Angebot der Deutschen Telekom, sich leicht verständlich, innovativ und voller praktischer Tipps mit Themen der digitalen Welt zu beschäftigen, um sie zu verstehen: von Digitaler Demokratie über Digitale Freundschaft bis hin zu Datenschutz und Datensicherheit. Wer mit Lerngruppen arbeitet, findet hier Anregungen und Tipps. Die Unterlagen stehen auch in einfacher Sprache zur Verfügung.
> dabei-geschichten.telekom.com

Die **Cyberfibel für digitale Aufklärung** von Deutschland sicher im Netz e.V. und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ist ein Handbuch für Multiplikator:innen in Vereinen, Stiftungen, Bildungseinrichtungen, Volkshochschulen oder Verbänden über grundlegende Verhaltensstandards für sicheres und selbstbestimmtes Handeln in der digitalen Welt.
> cyberfibel.de

Der **Digital-Kompass** unterstützt engagierte Menschen, älteren Generationen die Chancen des Internets und ihrer sicheren Nutzung näher zu bringen. Im Mittelpunkt steht der Erfahrungsaustausch zur verständlichen Vermittlung für Senior:innen deutschlandweit.
> digital-kompass.de

Sie interessieren sich für aktuelle digital-politische und digital-gesellschaftliche Themen?

Das **Kompetenzzentrum Öffentliche IT (ÖFIT)** vom Fraunhofer-Institut für offene Kommunikationssysteme (FOKUS) beschäftigt sich mit der Entwicklung von Informationstechnologien im öffentlichen Raum, die gesellschaftliche Lebensbereiche und Infrastrukturen zukünftig beeinflussen.
> oeffentliche-it.de

Haben Sie noch Fragen?
Schreiben Sie eine E-Mail an:
kontakt@digital-vereint.de

Informationen zu aktuellen Veranstaltungen, Webinaren und weitere Materialien finden Sie unter:
> digital-vereint.de

BSI für Bürger ist ein kostenloses Informationsangebot des Bundesamtes für Sicherheit in der Informationstechnik zum sicheren Surfen im Internet.
> bsi-fuer-buerger.de

D3 – so geht digital ist die Plattform der Stiftung Bürgermut mit Informationen und Veranstaltungen rund um Digitalisierungsthemen für Vereine, Verbände, Initiativen und Social Start-ups.
> so-geht-digital.de

Die neue **browserbasierte Simon-App** klärt über digitale Sicherheit im Alltag auf. Sie bietet Schutz- und Sicherheitswissen in leicht verständlichen Themenbereichen. Ein Quiz motiviert dazu, die eigenen digitalen Kompetenzen zu testen und Wissenslücken zu schließen. Über die Soforthilfe erhalten Nutzer:innen Schritt-für-Schritt-Anleitungen zur Selbsthilfe bei den häufigsten Schadensfällen im Internet.
> simon-app.org

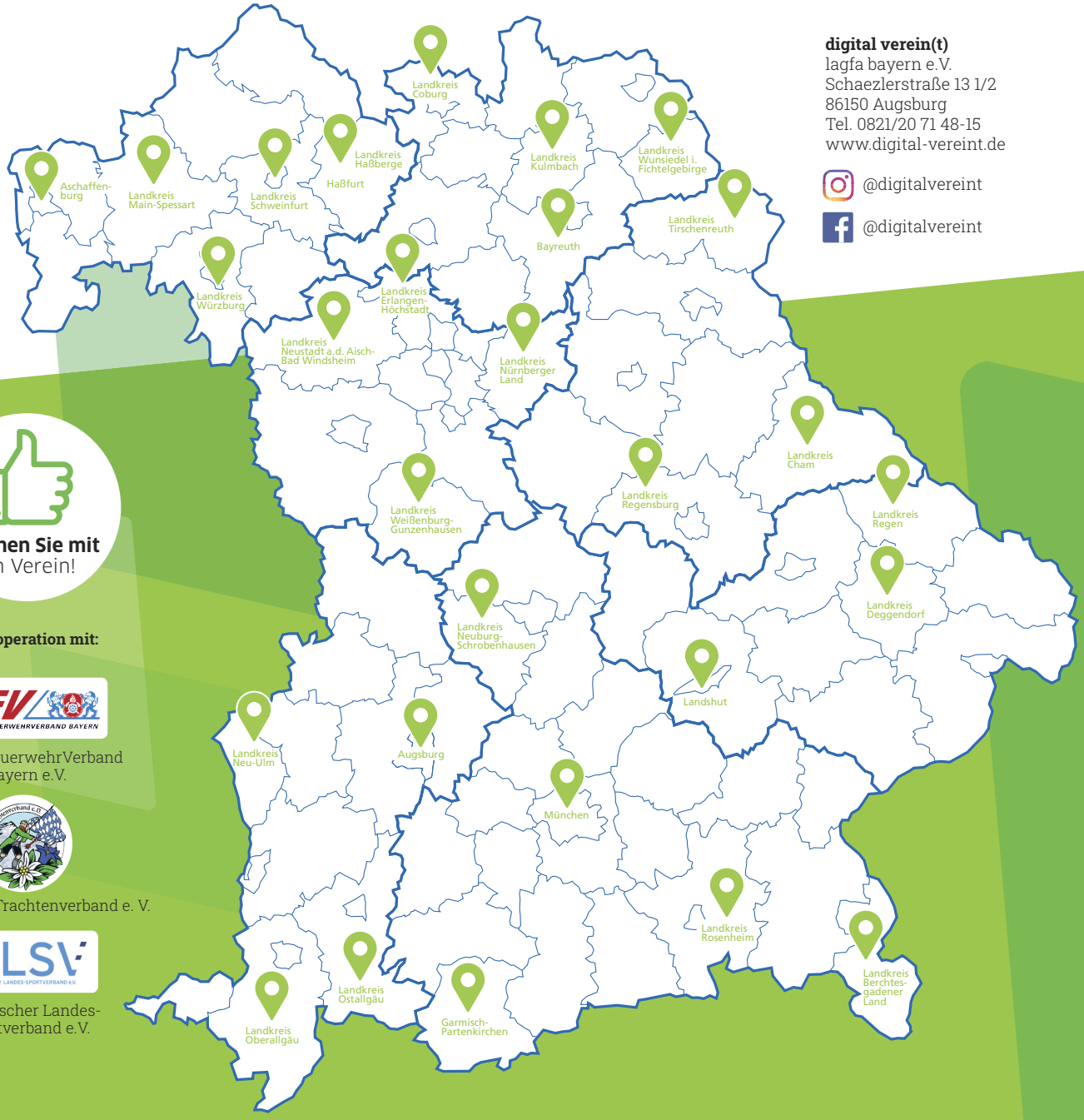
digital verein(t) vor Ort

digital verein(t)

digital verein(t)
lagfa bayern e.V.
Schaezlerstraße 13 1/2
86150 Augsburg
Tel. 0821/20 71 48-15
www.digital-vereint.de

@digitalvereint

@digitalvereint



Machen Sie mit
im Verein!

In Kooperation mit:

LandesFeuerwehrVerband Bayern e.V.

Bayerischer Trachtenverband e. V.

Bayerischer Landes-Sportverband e.V.

Freiwilligenagentur altmühlfranken
Landkreis Weißenburg-Gunzenhausen

Ehrenamtsagentur „Aschaffenburg aktiv!"

Freiwilligen-Zentrum Augsburg

Freiwilligen Zentrum Bayreuth

Freiwilligenagentur Berchtesgadener Land

Koordinierungszentrum Bürgerschaftliches Engagement „Treffpunkt Ehrenamt"
Landkreis Cham

Koordinierungszentrum Bürgerschaftliches Engagement
Landkreis Coburg

mach mit – Freiwilligenzentrum Landkreis Deggendorf

Ehrenamtsbüro Landkreis Erlangen-Höchstadt

„Auf geht´s" Das Freiwilligen-Zentrum Lebenslust Garmisch-Partenkirchen e.V.

Freiwilligenagentur Mehrgenerationenhaus Haßfurt

Koordinierungszentrum Bürgerschaftliches Engagement
Landkreis Kulmbach

Freiwilligen Agentur Landshut „fala"

EMiL, die Freiwilligen-Agentur Main-Spessart

Förderstelle für Bürgerschaftliches Engagement „FöBE" München

Koordinierungszentrum Bürgerschaftliches Engagement
Landkreis Neuburg-Schroben-hausen

Freiwilligenagentur „Hand in Hand"
Landkreis Neu-Ulm

Freiwilligenzentrum „mach mit"
Landkreis Neustadt a.d. Aisch-Bad Windsheim

Freiwilligenzentrum WinWin
Landkreis Nürnberger Land

Freiwilligenagentur
Landkreis Oberallgäu

Servicestelle EhrenAmt
Landkreis Ostallgäu

Ehrenamtsförderung ARBERLAND
Landkreis Regen

Koordinierungszentrum Bürgerschaftliches Engagement
Freiwilligenagentur
Landkreis Regensburg

Ehrenamtskoordination
Landkreis Rosenheim

Servicestelle Ehrenamt
Landkreis Schweinfurt

Ehrenamtsagentur
Landkreis Tirschenreuth

Koordinierungszentrum Bürgerschaftliches Engagement
Landkreis Wunsiedel

Servicestelle Ehrenamt
Landkreis Würzburg