Dein Verein und seine Mitglieder

Digitale Nachbarschaft

Mitgliederdaten: Schützen, verwalten und verwenden

Impressum

Redaktion: Dr. Elisabeth Maria Hofmann, Daniel Helmes (BBE), Petra Rollfing
Gestaltung und Satz: wegewerk GmbH
Erscheinungsjahr: 2019
Auflage: 1.000

Herausgeber: Deutschland sicher im Netz e.V.
Projekt Nachbarschaft Digital >Ehrenamt >Sicher >Transformieren
Geschäftsführer: Dr. Michael Littger (V.i.s.d.P.)
Albrechtstraße 10c
10117 Berlin
+49 (0) 30 27576-310
www.sicher-im-netz.de

Bildnachweis: Deutschland sicher im Netz e.V.; S. 19 www.pexels.com

Dieses Handbuch berücksichtigt die Grundlagen der „DsiN-BSI-Cyberfibel für Verbraucheraufklärung", ein Angebot von Deutschland sicher im Netz e.V. (DsiN) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Ein Projekt von Deutschland sicher im Netz e.V.
Gefördert durch das Bundesministerium des Innern, für Bau und Heimat
Mit Unterstützung von Deutsche Telekom AG

Mitgliederdaten: Schützen, verwalten und verwenden

Handbuch der Digitalen Nachbarschaft

Die fünf Themenbereiche der Digitalen Nachbarschaft kommen direkt aus der Praxis des freiwilligen Engagements. Mit den DiNa-Handbüchern zu „Dein Verein macht sich bekannt“, „Dein Verein und seine Mitglieder“, „Dein Verein und das Geld“, „Dein Verein tauscht sich aus“ und „Dein Verein will’s wissen“ macht sich Dein Verein fit fürs Netz.

Inhalt

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.

Die Digitale Nachbarschaft hat 16 DiNa-Tipps formuliert, die Dir helfen, die digitalen Chancen für Dich und Deinen 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 Dein Verein die Sicherheit von Daten gewährleistet. Und schließlich zeigt Dir das dritte Kapitel, wer Dich bei der Verarbeitung und beim Schutz personenbezogener Daten unterstützen kann. Am Ende des Handbuchs findest Du 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 DiNa-Häuschen findest Du kurze und praktische Hilfsmittel:

Informieren

Hier werden Fachbegriffe verständlich erklärt.

Machen

Hier werden digitale Werkzeuge vorgestellt, die Du sofort verwenden kannst.*

Üben

Hier gibt es Übungsaufgaben, um das neue Wissen anzuwenden.

Weiterlesen

Hier werden Websites und DiNa-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

1

Vereinssoftware & Datenschutz: Wie Du Mitgliederdaten digital verwaltest

Was ist bei der Wahl einer Vereinsverwaltungssoftware zu berücksichtigen? Welche Regeln gibt es bei der Erhebung personenbezogener Daten? Und wie kann Dein Verein seine Informations- und Auskunftspflichten erfüllen? Die Datenschutzgrundverordnung gibt diesen Aufgaben einen sicheren Rahmen. Die Digitale Nachbarschaft zeigt Dir in diesem Kapitel, wie es geht.

DiNa-Tipp

DiNa-Tipp 1: Wähle eine sichere Software zur Datenverwaltung!

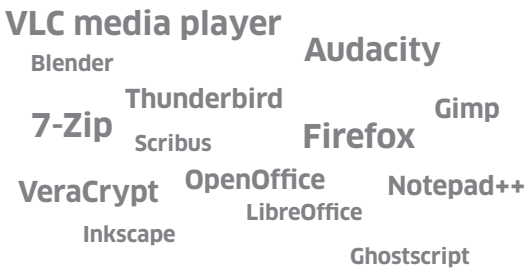
Die Verwaltung von Mitgliedern, Förderer*innen und ehrenamtlichen Helfer*innen ist ein wichtiger Baustein des bürgerschaftlichen Engagements. Eine Vereinssoftware bietet eine Vielzahl von Funktionen, die solche Verwaltungsaufgaben vereinfachen. Mit den Programmen lassen sich unter anderem Mitgliedsdaten 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. Achte dabei auf seriöse Quellen und berücksichtige die Bewertungen der Produkte. Vorab solltest Du Dich 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 Dein 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 solltest Du Antworten auf die folgenden Fragen finden:

- 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 Herstellern 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. Du kannst Dir den Quelltext einer Website anzeigen lassen, indem Du mit der rechten Maustaste in einen freien Bereich der Seite klickst und dann „Seitenquelltext anzeigen" wählst.

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 OpenOffice 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.
▸ www.giga.de/downloads/vereinsverwaltung

DiNa-Tipp 2: Nutze die Datenschutz-Grundverordnung als Chance, mit den Daten Deiner Vereinsmitglieder vertrauensvoll umzugehen!

Die Europäische **D**aten**s**chutz-**G**rund**v**er**o**rdnung (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 Deinem Verein 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.

DiNa-Tipp 3: Erhebe und verarbeite personenbezogene Daten nur mit Rechtsgrundlage oder Einwilligung!

DiNa-Tipp

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 Dein Verein in folgenden Fällen personenbezogene Daten verarbeiten:

1. **Ausdrückliche Einwilligung der betroffenen Person**

DiNa-Tipp

Dein 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 Dein 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** findest Du am Ende des Artikels „Datenschutz im Verein". Zu dem Artikel gelangst Du, wenn Du auf der Website im Suchfeld oben rechts den Suchbegriff „Einwilligungserklärung" eingibst.
▸ lsb-berlin.net

DiNa-Tipp

DiNa-Tipp 4: Verwende erhobene Daten nur zweckgebunden!

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 den Dein Verein entsprechend seiner Satzung verfolgt. 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 des Einzelnen 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

DiNa-Tipp 5: Erhebe 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 Dein 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). Dein 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.

Welche personenbezogenen Daten werden in Deinem Verein erhoben und zu welchem Zweck geschieht dies? Mache eine Liste.

DiNa-Tipp 6: Erstelle ein Datenverarbeitungsverzeichnis für Deinen Verein!

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.
▸ www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf

Ein weiteres Verzeichnismuster stellt der Landessportbund Thüringen auf seiner Website zur Verfügung. Du findest es im Download-Bereich, wenn Du nach dem Stichwort „Verarbeitungsverzeichnis“ suchst.
▸ www.thueringen-sport.de/downloads

Lege ein Verzeichnis von Verarbeitungstätigkeiten für Deinen Verein an. Welche Verarbeitungstätigkeiten fallen in Deinem Verein an? Welche Personen und Daten sind von den Tätigkeiten betroffen?

DiNa-Tipp

DiNa-Tipp

DiNa-Tipp

DiNa-Tipp 7: Gehe transparent mit der Erhebung und Verarbeitung personenbezogener Daten um!

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 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 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. Fragst Du zum Beispiel den Vereinsvorstand nach dem Termin einer bevorstehenden Veranstaltung und er verspricht, Dir diese Information per SMS zukommen zu lassen und notiert sich dazu Deine Nummer, ist keine gesonderte Information über die Verarbeitung Deiner Daten notwendig.

DiNa-Tipp

DiNa-Tipp 8: Gebe auf Deiner Vereinswebsite eine Datenschutzerklärung ab!

Betreibt Dein 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).

Mit der Datenschutzerklärung informierst Du die Nutzer*innen darüber, 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 Dein Verein hier zeigt, desto vertrauenswürdiger ist er.

DiNa-Handbuch „Homepage: Sicher gestalten, organisieren und pflegen“

Mehr Informationen zur sicheren Gestaltung einer Vereinswebsite findest Du im DiNa-Handbuch „Homepage: Sicher gestalten, organisieren und pflegen“.

In dem Artikel „Aufbau einer einfachen Datenschutzerklärung“ auf der Seite iRIGHTSinfo findest Du ausführliche Informationen zur einfachen **Datenschutzerklärung** auf Websites. Als Vorlage für eine entsprechende Erklärung auf Deiner Vereinswebsite eignet sich die Datenschutzerklärung von iRIGHTSinfo.
▸ irights.info/datenschutzerklaerung

Ein weiteres Muster für die Datenschutzerklärung auf Vereinswebsites kannst Du Dir auf den Seiten des Bayerischen Sportschützenbund e.V. im Download-Bereich herunterladen. Du findest das „Muster für eine Datenschutzerklärung auf der Homepage“ im Ordner „Datenschutz“.
▸ www.bssb.de/downloads.html

Betroffenenrechte: Recht auf Auskunft

Jedes Vereinsmitglied hat ein Recht auf Auskunft darüber, welche personenbezogenen Daten über ihn/sie erhoben werden. Um möglichen Auskunftsbegehren durch Vereinsmitglieder DSGVO-konform zu entsprechen, kann Dein Verein das **Datenverarbeitungsverzeichnis** nutzen. Dabei muss eine Auskunft nur dann erteilt werden, wenn ein konkreter **Antrag des Betroffenen** vorliegt.

Bevor eine Auskunft erteilt wird, muss zudem sichergestellt sein, dass es sich um den richtigen Antragsteller/die richtige Antragstellerin handelt. Kommt ein Mitglied, welches Du bereits mehrere Jahre kennst, persönlich vorbei oder ruft von einer bekannten Nummer aus an, reicht das natürlich vollkommen aus. Bei einer Anfrage per E-Mail von einer unbekannten Absenderadresse solltest Du jedoch vorsichtig sein und Dir die Identität nachweisen lassen.

Die Anfrage muss auch dann beantwortet werden, wenn keine Daten der Person erhoben werden. Falls Dein Verein Daten über die Person hat, musst Du diese nur als **Abschrift** zur Verfügung stellen. Die Abschrift kann sowohl schriftlich als auch elektronisch bereitgestellt werden und sollte folgende Informationen enthalten:

- Zweck der Verarbeitung
- Kategorien personenbezogener Daten
- Empfänger der Daten
- geplante Speicherdauer
- Hinweis auf sonstige Betroffenenrechte und Beschwerdemöglichkeit bei Aufsichtsbehörde

Die Auskunft darf nicht nur die Kategorien beschreiben, sondern muss auch die konkreten Daten selbst beinhalten (zum Beispiel Max Mustermann, Hauptstraße 1, 12345 Berlin). Denn nur so kann der Betroffene die Korrektheit der Daten prüfen. Die erste Auskunft muss kostenlos zur Verfügung gestellt werden und innerhalb eines Monats erfolgen. Werden weitere Kopien gewünscht, kann ein angemessenes Entgelt verlangt werden.

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 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 der Betroffene eine Löschung seiner Daten, muss dem gefolgt werden, wenn

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

Betroffenenrechte: Widerspruch

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

Um allen Betroffenenrechten als Verein rechtskonform nachkommen zu können, solltest Du Dich auf mögliche Fälle vorbereiten und verschiedene Szenarien üben, insbesondere das Szenario einer geforderten Auskunft.


2

2

Zugänge, Berechtigungen & Backups: Wie Du die Sicherheit personenbezogener Daten gewährleistest

Wer darf im Verein Daten verwalten? Welche technischen Sicherheitsmaßnahmen müssen unternommen werden? Und wie kannst Du vermeiden, dass Daten verloren gehen? Damit die Daten der Mitglieder in Deinem Verein sicher sind, helfen ein paar grundsätzliche Regelungen. Die Digitale Nachbarschaft zeigt Dir in diesem Kapitel, wie es geht.

DiNa-Tipp

DiNa-Tipp 9: Kontrolliere die Zugriffsrechte auf vertrauliche Daten!

Datenverlust ist nicht immer auf illegale Aktivitäten wie Datendiebstahl zurückzuführen. Das Risiko besteht vor allem bei der alltäglichen Arbeit, wenn beispielsweise Daten versehentlich an einen falschen Adressaten versendet werden. Mit einfachen Maßnahmen kann Dein 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 Deines Vereins muss so aufgestellt sein, dass sich Unbefugte nicht einfach Zugriff auf Daten verschaffen können. Dein 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 Dein Verein auf der sicheren Seite. Dateiserver bieten die Möglichkeit, verschiedenen Nutzer*innen unterschiedliche **Zugriffsrechte** zuzuteilen. Nutzt Dein 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 findest Du im DiNa-Handbuch „Gemeinsam im Netz: Geräte absichern, Informationen sammeln und Netzwerke teilen".

DiNa-Tipp

DiNa-Tipp 10: Schütze Deine Daten durch Verschlüsselungsverfahren!

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 Du personenbezogene Daten über E-Mail verschickst, ist es ratsam, Deine E-Mails zu verschlüsseln.
- **Vereins-WLAN:** Bietet Dein Verein seinen 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 Du besuchst, sollten mit dem sogenannten SSL-Zertifikat verschlüsselt sein.

Dies erkennst Du durch ein Schloss-Symbol neben der Websiteadresse (URL) als auch an dem Ausdruck „https://“ in der URL.

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

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 Du Deine E-Mails verschlüsselst, erfährst Du im DiNa-Handbuch „Online-Kommunikation: Mailen, Messenger nutzen und Videokonferenzen veranstalten“. Weitere Informationen zur Einrichtung und Administration einer sicheren Vereinswebsite findest Du im DiNa-Handbuch „Homepage: Sicher gestalten, organisieren und pflegen“.

DiNa-Tipp 11: Werte Daten nur anonymisiert aus!

Die Analyse von Mitgliedsdaten ermöglicht es Deinem Verein, 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** Deines 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** Deines Vereins. Dazu gehören Fragen wie: Sollte Dein 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 Du Daten erhebst: Lasse die Betroffenen auf jeden Fall wissen, dass Du die Daten anonymisiert auswertest.

Kostenlose Online-Umfragen lassen sich beispielsweise mit der Anwendung **Google Formulare** erstellen. Dazu musst Du Dir ein Google-Konto einrichten. Nachdem Du Dich in diesem Konto angemeldet hast, erhältst du über die Funktion „Google Apps“ Zugriff auf die Anwendung Google Formulare. Dort kannst Du dann individuelle Umfragen für Deinen Verein erstellen. ▸ 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

DiNa-Tipp

Für die Auswertung der erhobenen Daten kannst Du zum Beispiel das Datenverarbeitungs- und Tabellenkalkulationsprogramm **Excel** nutzen. 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.

Überlege Dir drei Hypothesen, die Du mit der Datenanalyse untersuchen möchtest, zum Beispiel: In der Weihnachtszeit steigt das Spendenvolumen stark an – trifft das für Deinen Verein zu?

DiNa-Tipp

DiNa-Tipp 12: Erstelle regelmäßig Backups Deiner Dateien!

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 Dein Verein 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. Nutze auf jeden Fall einen vertrauenswürdigen Cloud-Anbieter, 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. ▸ www.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. TrayBackup 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. ▸ www.traybackup.de

Für die Sicherung Deiner iOS-Geräte kannst Du unter anderem die Software **SmartBackup** verwenden. 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 dem Du gängige Fragen zur Verwendung von SmartBackup nachschlagen kannst. ▸ solesignal.com/smartbackup4

DiNa-Tipp 13: Stelle sicher, dass nur Befugte Zugang zu personenbezogenen Daten bekommen!

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: Wer Dich bei der Datenverarbeitung unterstützt

Darf Dein Verein Daten an Dienstleister weitergeben? Was steht in einem Auftragsverarbeitungsvertrag? Braucht Dein Verein eine*n Datenschutzbeauftragte*n? Und was ist zu tun, wenn es doch mal zu einer Datenschutzverletzung kommt? Die Digitale Nachbarschaft zeigt Dir in diesem Kapitel, wie es geht.

DiNa-Tipp 14: Schließe mit externen Dienstleistern einen Auftragsverarbeitungsvertrag ab!

DiNa-Tipp

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 weiter zu verarbeiten. Dies gilt unter anderem für

- Mitgliedsbeitragsabrechnung durch externe Buchhaltung;
- Lohn und Gehaltsabrechnungen durch einen Steuerberater;
- 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.
▸ www.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.
▸ www.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 aus.

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 Vereines liegt.

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.

Überprüfe, mit welchen externen Dienstleistern Dein Verein zusammenarbeitet und ob diese die Anforderungen der DSGVO einhalten. Schließe mit den Anbietern einen Auftragsverarbeitungsvertrag ab, wenn das noch nicht geschehen ist.

Weitere Informationen zur Nutzung von Cloud-Diensten findest Du im Handbuch „Online-Zusammenarbeit: Projekte organisieren, erarbeiten und Wissen austauschen".

DiNa-Tipp

Mitgliederdatenverwaltung in einer Cloud

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

Wenn Du Cloud-Dienste für die Verwaltung oder Erhebung von personenbezogenen Daten nutzt, handelt es sich datenschutzrechtlich ebenfalls um eine Auftragsverarbeitung. Darum solltest Du wie bei anderen externen Dienstleistern darauf achten, dass Dein 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. Im Falle eines Cloud-Standortes in den USA sollte eine Zertifizierung durch den sogenannten **EU-US Privacy Shield** vorliegen. Dieses „Datenschutzschild" garantiert die Einhaltung der DSGVO.

DiNa-Tipp 15: Benenne eine*n Datenschutzbeauftragte*n!

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

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.

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).

DiNa-Tipp

DiNa-Tipp 16: Melde Datenschutzverletzungen der zuständigen Aufsichtsbehörde!

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 und 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. 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:

- Informiere Dich vorab darüber, welche Datenschutzbehörde für Deinen Verein zuständig ist.
- Prüfe, wie sich Datenschutzverletzungen in Deinem Verein erkennen lassen.
- Lege fest, wer bei einer aufgetretenen Datenschutzverletzung die notwendigen Schritte unternimmt.
- Informiere alle Vereinsmitglieder über Datenschutzverletzungen und die nötigen Schritte.
- Stimme Dich bei Datenschutzverletzungen mit der zuständigen Behörde ab, was zu tun ist.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfahlen hat eine umfangreiche Handreichung „**Datenschutz im Verein nach der Datenschutz-Grundverordnung**“ veröffentlicht (Stand: November 2018). Du findest die Broschüre, wenn Du auf der Website in das Suchfeld oben rechts die Begriffe „Datenschutz Verein“ eingibst. ► www.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 Deinem Verein eine Orientierung bei der Umsetzung der DSGVO. ► www.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. Du findest die Broschüre, wenn Du auf der Website im Suchfeld oben rechts die Begriffe „Praxisratgeber DSGVO“ eingibst. ► www.baden-wuerttemberg.datenschutz.de

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 Deine Notizen

Platz für Deine Notizen

Dein Verein und seine Mitglieder

Checkliste

16 DiNa-Tipps: Mitgliederdaten verwalten – aber sicher!

1. Wähle eine sichere Software zur Datenverwaltung!
2. Nutze die Datenschutz-Grundverordnung als Chance, mit den Daten Deiner Vereinsmitglieder vertrauensvoll umzugehen!
3. Erhebe und verarbeite personenbezogene Daten nur mit Rechtsgrundlage oder Einwilligung!
4. Verwende erhobene Daten nur zweckgebunden!
5. Erhebe so viele Daten wie nötig und so wenige wie möglich!
6. Erstelle ein Datenverarbeitungsverzeichnis für Deinen Verein!
7. Gehe transparent mit der Erhebung und Verarbeitung personenbezogener Daten um!
8. Gebe auf Deiner Vereinswebsite eine Datenschutzerklärung ab!
9. Kontrolliere die Zugriffsrechte auf vertrauliche Daten!
10. Schütze Deine Daten durch Verschlüsselungsverfahren!
11. Werte Daten nur anonymisiert aus!
12. Erstelle regelmäßig Backups Deiner Dateien!
13. Stelle sicher, dass nur Befugte Zugang zu personenbezogenen Daten bekommen!
14. Schließe mit externen Dienstleistern einen Auftragsverarbeitungsvertrag ab!
15. Benenne eine*n Datenschutzbeauftragte*n!
16. Melde Datenschutzverletzungen der zuständigen Aufsichtsbehörde!

Weitere Themen und Informationen unter:
▸ **www.digitale-nachbarschaft.de**

Mehr digitale Themen

Du möchtest Sicherheitsinformationen tagesaktuell auf Dein Smartphone erhalten?

Lade kostenlos die SiBa-App herunter:
▸ www.sicher-im-netz.de/siba

Du möchtest digitale Kompetenzen weitervermitteln?

1001 WAHRHEIT ist eine Online-Plattform, um Themen der digitalen Welt zu verstehen: von Meinungsmache im Netz über digitalen Nachlass bis hin zu Datenschutz. Die Initiative des Projektpartners Deutsche Telekom eignet sich zum Selbststudium und für Multiplikator*innen im Umgang mit unterschiedlichen Lerngruppen. ▸ www.1001wahrheit.de

Die DsiN-BSI-**Cyberfibel für digitale Aufklärung** 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. ▸ www.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.
▸ www.digital-kompass.de

Du interessierst Dich für aktuelle digitalpolitische 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. ▸ www.oeffentliche-it.de

BSI für Bürger ist ein kostenloses Informationsangebot des Bundesamtes für Sicherheit in der Informationstechnik zum sicheren Surfen im Internet.
▸ www.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.
▸ www.so-geht-digital.de

Du hast noch Fragen?

Schreibe eine E-Mail an:
dina@digitale-nachbarschaft.de

Informationen zu aktuellen Veranstaltungen, Webinaren und weitere Materialien findest Du auf unserer Website:

▸ **www.digitale-nachbarschaft.de**

Über uns und unsere Partner

Deutschland sicher im Netz e. V.

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.

Die Digitale Nachbarschaft

Mit dem Projekt Nachbarschaft Digital >Ehrenamt >Sicher >Transformieren (DiNa) sensibilisiert Deutschland sicher im Netz e. V. (DsiN) Vereine, Initiativen und freiwillig engagierte Bürger*innen für die Chancen der Digitalisierung. Das Projekt verfügt über ein bundesweites Netzwerk von regionalen Anlaufstellen (DiNa-Treffs), das bedarfsgerechte Unterstützungsangebote für Bürger*innen im Ehrenamt bereitstellt. Die lokale Verankerung im vertrauten, ehrenamtlichen Umfeld fördert die nachhaltige Verbreitung von digitalen Themen im Alltag, bei denen IT-Sicherheit und Datenschutz grundlegend für ein erfolgreiches digitales Wirken im Ehrenamt sind. Mit zwei Infobussen (DiNa-Mobile) ist die DiNa auch mobil im Einsatz zu Fragen der Digitalisierung.

Das Bundesministerium des Innern, für Bau und Heimat

Die Aufgaben des Bundesministeriums des Innern, für Bau und Heimat (BMI) sind ebenso vielfältig wie verantwortungsvoll. Das Spektrum reicht von der Rolle als Hüter der Verfassung und Förderer des gesellschaftlichen Zusammenhalts über die Integration, Sportförderung des Bundes und die Informationstechnik bis hin zu den Sicherheitsaufgaben. Als „Verfassungs- und Kommunalministerium" ist das BMI für die Modernisierung von Staat und Verwaltung zuständig, aber auch für Kernfragen der staatlichen und föderalen Ordnung wie beispielsweise das Wahlrecht. Ziel der Digitalpolitik des Bundesministeriums des Innern ist es, die vielfältigen Chancen der Digitalisierung für möglichst viele Menschen zu ermöglichen und zugleich etwaige Risiken zu minimieren.

Die Deutsche Telekom AG

Die Deutsche Telekom ist eines der führenden integrierten Telekommunikationsunternehmen weltweit. Chancengleiche und aktive Teilhabe an der Informations- und Wissensgesellschaft ist der Telekom stets ein wichtiges Anliegen. Mit ihrem Angebot „Medien, aber sicher" leistet sie einen wichtigen Beitrag zur Gestaltung der Digitalisierung in der Gesellschaft, indem ein kompetenter, verantwortungsvoller und dadurch sicherer Umgang mit neuen Technologien ermöglicht werden soll. Ziel ist die Förderung von Medienkompetenz für Jung und Alt. So stellt die Deutsche Telekom AG zum Beispiel über die Plattform „1001 Wahrheit" gesellschaftlich relevante Themen wie Darknet, Meinungsmache im Netz oder Digitale Freundschaft vor und lädt zur kontroversen Diskussion zum jeweiligen Thema ein.

Das Bundesnetzwerk Bürgerschaftliches Engagement (BBE)

Das Bundesnetzwerk Bürgerschaftliches Engagement (BBE) ist ein Zusammenschluss von Akteuren (vorrangig Organisationen und Institutionen) aus Zivilgesellschaft, Wirtschaft und Arbeitsleben, aus Staat und Politik, Medien und Wissenschaft. Das übergeordnete Ziel des BBE ist es, die Bürgergesellschaft und bürgerschaftliches Engagement in allen Gesellschafts- und Politikbereichen nachhaltig zu fördern. In der Kooperation mit DsiN trägt das BBE im Projekt Digitale Nachbarschaft nachhaltig zur Förderung von Engagierten im Umgang mit den Chancen der Digitalisierung bei. Das Netzwerk versteht sich als Wissens- und Kompetenzplattform für bürgerschaftliches Engagement.

Ein Projekt von:

Deutschland sicher im Netz

Mit Unterstützung von:

Gefördert durch:

Bundesministerium des Innern, für Bau und Heimat

Deine DiNa ist nah dran ...

→ an Deinem Verein: Die DiNa-Treffs und DiNa-Mobile sind analoge Begegnungsorte für digitale Themen.

→ an Deinen Themen: Die DiNa-Angebote und Materialien entwickeln wir aus der Praxis des freiwilligen Engagements.

→ an Deiner Art zu lernen: Die DiNa-Workshops und Webinare zeigen die Chancen des Internets und wie Du sie sicher nutzt.

www.digitale-nachbarschaft.de