DATENSCHUTZ IM EHRENAMT

Datenschutz im Verein

KOMPAKT

Anleitungen und Tipps für eure Vereinspraxis

Ein Angebot der STIFTUNG DATENSCHUTZ

Datenschutz? IST DAS FÜR UNSEREN VEREIN RELEVANT?

Ja! Denn schon die Verwaltung der Mitgliederdaten unterliegt der EU-Datenschutzgrundverordnung (DSGVO). Dazu kommen Buchhaltung und eure Website, vielleicht nutzt ihr Social Media oder tauscht Daten über eine Cloud-Software aus, macht Fotos auf Veranstaltungen oder übermittelt Daten an einen Dachverband. Bei all diesen Tätigkeiten müssen die Datenschutzvorschriften eingehalten werden.

Die wichtigsten Aufgaben

- Datenschutz organisieren: **Wer ist wofür zuständig?**
- Verarbeitungsverzeichnis anlegen und pflegen: **Welche Daten werden wie verarbeitet?**
- Sichert personenbezogene Daten: **Wer hat Zugang zu und auf welche Daten?** Wie ist dieser Zugang gesichert?
- **Datenschutzbeauftragte** benennen, falls erforderlich

THEMENAUSWAHL

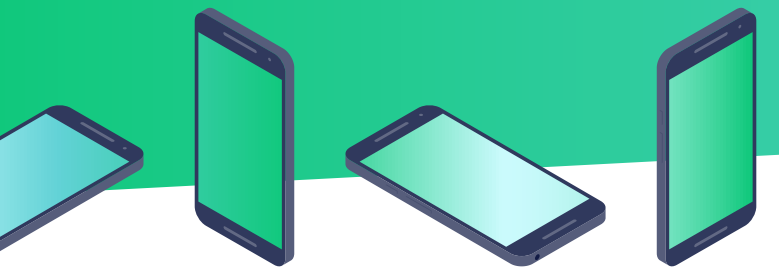
Wir haben uns bei der Zusammenstellung der Themen an den Fragen orientiert, die uns in der Praxis häufig erreichen. Einen Anspruch auf Vollständigkeit können wir natürlich nicht erfüllen.

Betroffenenrechte	Ehemalige Mitglieder	Datenpannen
Buchhaltung	Fotos	Veranstaltungen
Cloud-Tools	Gesundheitsdaten	Verantwortlichkeiten
Datenschutzbeauftragte	Newsletter	Website

Auf jeder Karte fassen wir das Wichtigste für die Umsetzung des Datenschutzes für euch zusammen. Ergänzend findet ihr Hinweise und QR-Codes zu weiterführenden Informationen.

WICHTIG

Aus Platzgründen können wir nicht bei jedem Thema alle Pflichten aufführen, die zu erfüllen sind. **So gelten z. B. Informationspflichten für Betroffene in jedem Fall** und unabhängig davon, ob wir die Informationspflichten auf einer Karte explizit erwähnen oder nicht.



BASISWISSEN

Einen allgemeinen **Einstieg in die Datenschutzpflichten** aus Sicht eines Vereins bieten wir auf unserer Website im Abschnitt „Basiswissen“.

sds-links.de/ehrenamt-basiswissen

Das Wichtigste im Überblick

PRAXISRATGEBER

Vertieftes Wissen zu **vereinstypischen Themen** gibt es im Abschnitt „Praxisratgeber“.

sds-links.de/ehrenamt-praxisratgeber

Anwendungsfälle und Beispiele aus der täglichen Arbeit anschaulich erklärt.

NEWSLETTER

Unser Newsletter informiert über unsere Angebote und Neuigkeiten zum Datenschutz im Ehrenamt.

sds-links.de/ehrenamt-nl-anmeldung

Wir bieten regelmäßig Webinare an und beantworten eure Fragen.

BETROFFENEN-ANFRAGEN

Nehmt Betroffenenanfragen ernst. Betroffene sind die Personen, deren Daten ihr verarbeitet.

Betroffenenrechte

Jeder Person, deren Daten ihr verarbeitet, hat das Recht zu erfahren, welche Daten über sie verarbeitet werden.

Sie haben ein Recht darauf, dass ihr eventuell falsche Daten berichtigt und dass ihr Daten löscht.

Dies betrifft nicht nur Mitglieder, sondern alle Personen, deren Daten ihr verarbeitet.

Wichtige Betroffenenrechte Art. 15 ff DSGVO

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch gegen die Verarbeitung

Wie geht ihr vor?

Kümmert euch zeitnah

Ansprüche aus Betroffenenrechten müssen **innerhalb eines Monats bearbeitet** werden. In begründeten Fällen kann die Frist um bis zu zwei Monate verlängert werden, dann muss aber die betroffene Person innerhalb des ersten Monats einen Zwischenbescheid erhalten.

Prüft, ob die Anfrage berechtigt ist

Dazu gehört auch, im Zweifelsfall zu prüfen, **ob die anfragende Person überhaupt die betroffene Person ist** und nicht unberechtigt versucht, sich Daten zu beschaffen.

Legt die Verantwortlichkeit fest

Auch wenn Auskunftsersuchen, Löschanträge und andere Anfragen in der Praxis selten sein mögen, wir empfehlen unbedingt, dass ihr euch überlegt, wie ihr damit umgehen wollt und festlegt, wer sich darum kümmert.

* pbD = personenbezogene Daten

BETROFFENEN-ANFRAGEN

Reagiert in jedem Fall

Auch wenn keine Daten verarbeitet werden, müsst ihr das der antragstellenden Person mitteilen.

Bearbeitet ihr Auskunftsersuchen, Berichtigungs- und Löschanträge nicht korrekt, könnten Beschwerden bei der Aufsichtsbehörde, Bußgelder oder Schadenersatzansprüche die Folge sein.

Muster für die Auskunfts-erteilung findet ihr über den QR-Code.

Löschen oder aufbewahren?

Zwar besteht grundsätzlich ein Anspruch auf Löschung, es kann aber sein, dass andere Vorschriften verlangen, die Daten dennoch aufzubewahren, z. B. für die Buchhaltung. Dann müssen diese für die Verarbeitung gesperrt, also getrennt von den anderen Daten aufgehoben werden.

„Ich verlange, dass alle meine Daten gelöscht werden!"

Immer informieren

Wann immer ihr pbD verarbeitet, müsst ihr die Betroffenen darüber informieren.
Die Datenschutzhinweise (oft auch „Datenschutz-erklärung") müssen ohne Nachfrage zugänglich sein, z. B. auf der Vereins-Website.

Streng genommen gehört die Informationspflicht über die Datenverarbeitung auch zu den Betroffenenrechten. Im Gegensatz zu den anderen Rechten muss aber immer informiert werden, egal, ob ihr danach gefragt werdet.

Datenschutz-hinweise: Art. 13 und 14 DSGVO

sds-links.de/ehrenamt-betroffenenrechte

Weiterführende Informationen findet ihr online.

BUCHHALTUNG

In der Buchhaltung müssen die Vorgaben der Abgabenordnung mit den Vorgaben der DSGVO in Einklang gebracht werden. Der Vorstand ist für die Einhaltung verantwortlich.

Zugriff auf eure Buchhaltung

Üblicherweise darf nur ein **beschränkter Personenkreis** auf die Buchhaltung zugreifen: Vorstand, Kassiererin, Kassenprüferin.

Wir empfehlen euch, diese Personen im Umgang mit pbD zu schulen oder schulen zu lassen. Verpflichtet sie zusätzlich schriftlich auf Verschwiegenheit, unabhängig davon, ob sie Mitglied im Verein, ehrenamtlich oder hauptamtlich tätig sind.

Korrekt aufbewahren, dann löschen

Manchmal ist ein Mitglied längst ausgeschieden und seine Daten, z. B. aus dem Mitgliederverzeichnis, sind gelöscht. In der Buchhaltung müssen sie jedoch noch einige Jahre aufbewahrt werden, z. B. als Bestandteil von Zahlungsbelegen.

- Diese Daten müssen dann **getrennt** von den Daten, die im Alltagsgeschäft verarbeitet werden, **abgelegt** werden.
- Am **Ende der Aufbewahrungsfrist** müssen die Daten endgültig gelöscht werden.
- Wir empfehlen, **regelmäßig zu prüfen**, zu welchen Daten die Aufbewahrungsfristen abgelaufen sind, und diese dann endgültig zu löschen bzw. sie sachgerecht zu vernichten.
- Dazu braucht es ein **Löschkonzept**. Ein Löschkonzept verhindert einerseits unzulässiges Speichern und andererseits willkürliches Löschen.

* pbD = personenbezogene Daten

BUCHHALTUNG

Rechtsgrundlagen

- **Abbuchung der Mitgliedsbeiträge, Zahlung von Rechnungen**: Art. 6 Abs. 1 S. 1 lit b. DSGVO.
- **Mitarbeiterdaten**: Art. 6 Abs. 1 c. DSGVO i. V. m. § 26 Abs. 1 Bundesdatenschutzgesetz (BDSG)
- **Aufbewahrung von Rechnungen usw.**: Art. 6 Abs. 1 c DSGVO in Verbindung mit Abgabenordnung (AO), ggf. Handels- und Steuerrecht

Auftragsverarbeitungsverträge

Der Auftragsverarbeitungsvertrag (AV oder AVV, englisch DPA) regelt im Kern, dass der Dienstleister nur auf Weisung des Vereins handelt, die Daten sicher verwahrt und sie nicht zu eigenen Zwecken nutzt.

Der Vertrag muss auch dann abgeschlossen werden, wenn die Dienstleistung kostenlos erbracht wird.

Wenn ein **Steuerberater** eure Buchhaltung macht, braucht es **keinen** Auftragsverarbeitungsvertrag. Steuerberater sind selbst Verantwortliche im Sinne der DSGVO.

Mit anderen Dienstleistern, wie den Betreibern der cloudbasierten Buchhaltungssoftware, muss dagegen ein AVV abgeschlossen werden.

Weiterführende Informationen findet ihr online.

sds-links.de/ehrenamt-buchhaltung

DATEN IN DER „CLOUD“

Cloud-Anwendungen erleichtern das digitale Vereinsleben. Datenspeicherung, Buchhaltung, Newsletterversand – für vieles gibt es komfortable Lösungen.

Nutzungsvertrag

Auch bei kostenlosen Werkzeugen: Mit Akzeptieren der Nutzungsbedingungen kommt ein Nutzungsvertrag zwischen Anbieter und Verein zustande.

Tipp!

Nutzerkonto immer im Namen des Vereins anlegen.

Auftragsverarbeitung

Wenn ihr pbD durch einen Dienstleister verarbeiten lasst, heißt das „Auftragsverarbeitung“: **Der Dienstleister handelt in eurem Auftrag**. Ihr bleibt dafür verantwortlich, dass die Datenschutzvorschriften beachtet werden.

Dabei spielt es keine Rolle, ob der Verein die Daten an den Auftragsverarbeiter übermittelt (z. B. die Mitgliederliste in einem Cloud-Speicher ablegt) oder ob der Dienstleister die Daten direkt erhebt (z. B. über ein Anmeldeformular).

Der Auftragsverarbeitungsvertrag

Ganz wichtig!

Der Auftragsverarbeitungsvertrag (AV oder AVV, englisch DPA) regelt im Kern:

- dass der Dienstleister nur auf Weisung des Vereins handelt,
- die Daten sicher verwahrt und
- sie nicht zu eigenen Zwecken nutzt.

Der Vertrag muss auch dann abgeschlossen werden, wenn die Dienstleistung kostenlos erbracht wird.

Tipp!

Die meisten Dienstleister haben vorgefertigte Verträge.

* pbD = personenbezogene Daten

DATEN IN DER „CLOUD“

Internationale Datentransfers

Sobald Daten den europäischen Wirtschaftsraum verlassen, kommen weitere Regeln ins Spiel. Viele Cloud-Anbieter betreiben ihre Server jedoch in den USA oder anderen Ländern. Dann wird es komplizierter und ist in bestimmten Fällen sogar unzulässig.

Am einfachsten ist es daher, wenn man Dienstleister in der EU nutzt.

In unserem Webinar „Daten sicher in der Cloud speichern" erklären wir, was alles zu beachten ist.

Das Video findet ihr über den QR-Code.

Praxistipp!

Auch wenn die US-Anbieter häufig bekannter sind – eine Recherche lohnt sich, es gibt fast immer EU-Anbieter mit vergleichbaren Funktionen.

Weiterführende Informationen findet ihr online.

sds-links.de/ehrenamt-cloud

DATENSCHUTZ-BEAUFTRAGTE

Weit verbreitet ist die Auffassung, dass Datenschutzbeauftragte sich um die Umsetzung der DSGVO kümmern. Verantwortlich für die Einhaltung der Vorschriften ist jedoch stets der Vorstand.

Was machen dann Datenschutzbeauftragte?

Die Datenschutzbeauftragte (DSB) berät den Vorstand, überwacht die Einhaltung der Vorschriften und ist Ansprechperson für die Datenschutzaufsichtsbehörde.

Wann braucht ihr eine DSB?

- Wenn mindestens 20 Personen in eurem Verein ständig pbD automatisiert (also digital) verarbeiten **oder**
- wenn häufig besonders sensible pbD verarbeitet werden (z. B. im Selbsthilfe-Verein) **oder**
- wenn euer Verein umfangreich, regelmäßig und systematisch Leute überwacht.

Besonders sensible Daten nach Art. 9 DSGVO

pbD, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,

genetischen Daten, biometrischen Daten, Gesundheitsdaten oder

Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

* pbD = personenbezogene Daten

DATENSCHUTZ-BEAUFTRAGTE

Wer kann DSB werden?

- Ein geeignetes Vereinsmitglied
- Ein geeigneter Vereinsmitarbeiter
- Ein externer Dienstleister

Und wer nicht?

Der Vorstand, weil er sich selbst kontrollieren müsste.

IT-Verantwortliche, Verwaltungsleute, die selbst häufig pbD verarbeiten, aus dem gleichen Grund.

Wichtig: Eignung und Sachkunde sind Voraussetzungen.

Was ist noch zu beachten?

- Veröffentlicht die Kontaktdaten der DSB, z. B. durch Angabe der E-Mail-Adresse der DSB auf der Vereins-Website
- Meldet die Benennung der DSB an eure zuständige Aufsichtsbehörde

Tipp! Auch wenn ihr keine DSB benennen müsst – wir empfehlen, dass sich eine Person des Themas annimmt und den Vorstand unterstützt. Diese Person sollte aber nicht Datenschutzbeauftragte, sondern z. B. Daten-schutzkoordinatorin genannt werden.

sds-links.de/ehrenamt-datenschutzbeauftragte

Weiterführende Informationen findet ihr online.

EHEMALIGE MITGLIEDER

Wie geht ihr mit pbD um, wenn Vereinsmitglieder ausgeschieden sind?

Verarbeitungszwecke vorab festlegen

Der Verarbeitungszweck der Vertragserfüllung entfällt sofort mit Ende der Mitgliedschaft. Möchte euer Verein Daten über das Ende der Mitgliedschaft hinaus für eigene Zwecke verwenden, müsst ihr dies aktiv planen und darüber informieren.

Als Rechtsgrundlage hierfür kommen dann eine Einwilligung oder das berechtigte Interesse in Betracht, z. B. für Fotos auf der Vereins-Website, auf denen Ehemalige zu sehen sind.

Löschen oder nicht löschen?

Generell müsst ihr pbD immer dann löschen, sobald der Verarbeitungszweck für diese wegfällt. Mitgliederdaten werden primär für die Mitgliederverwaltung erhoben. Dieser Zweck entfällt also mit Ende der Mitgliedschaft. Daher müssen die Daten überall dort gelöscht werden, wo keine gesetzliche Aufbewahrungspflicht dagegenspricht.

Aufbewahrungspflichten

Für Rechnungen, Zahlungsbelege und Ähnliches, gelten zahlreiche Aufbewahrungspflichten, die berücksichtigt werden müssen und daher **Ausnahmen von der Löschpflicht** begründen.

Fristen und Pflichten sind z. B. hier festgelegt.

- § 147 Abgabenordnung (AO)
- Handelsgesetzbuch (HGB)
- Arbeits- und Sozialrecht
- In der Regel sechs bis zehn Jahre

* pbD = personenbezogene Daten

EHEMALIGE MITGLIEDER

Aufbewahren, aber getrennt

Es kann also sein, dass die Daten des ausgeschiedenen Mitglieds längst aus dem Mitgliederverzeichnis gelöscht wurden, aber in der Buchhaltung noch viele Jahre aufbewahrt werden müssen, z. B. auf Zahlungsbelegen.

Zwischen den verschiedenen Verarbeitungszwecken muss unterschieden und die Daten müssen entsprechend getrennt aufbewahrt werden.

! Auf die Daten der Buchhaltung sollte nur ein sehr kleiner Personenkreis Zugriff haben.

Endlich doch löschen

Wir empfehlen: Prüft regelmäßig, zu welchen Daten die Aufbewahrungsfristen abgelaufen sind, und löscht diese dann endgültig bzw. vernichtet sie sachgerecht. Dazu braucht es ein Löschkonzept.

Ein **Löschkonzept** verhindert einerseits unzulässiges Speichern und andererseits willkürliches Löschen.

Weiterführende Informationen findet ihr online.

sds-links.de/ehrenamt-ehemalige-mitglieder

GESUNDHEIT!

Allergien, Behinderungen, Krankheiten, Süchte oder der Impfstatus – Daten zur Gesundheit werden in Artikel 9 der DSGVO besonders geschützt.

Einwilligung unabdingbar

Wenn euer Verein oder eure Selbsthilfegruppe mit solchen Daten arbeitet, braucht ihr dafür die Zustimmung der Betroffenen, bei Kindern die Zustimmung der Eltern.

Diese Einwilligung muss

- **freiwillig** sein – kein Zwang oder Druck, aber auch keine großen Vorteile
- informiert und **unmissverständlich** sein: Wie genau werden die Daten verarbeitet?
- **zweckbestimmt** sein: Wenn die Daten zu einem Zweck erhoben werden, dürfen sie auch nur dafür verwendet werden.
- **ausdrücklich** erfolgen
- einen Hinweis auf Möglichkeit enthalten, die Einwilligung **jederzeit zu widerrufen**.

! Wir empfehlen, die Einwilligung schriftlich einzuholen und zu dokumentieren.

* pbD = personenbezogene Daten

GESUNDHEIT!

Datenschutzbeauftragte gesucht!

Wenn die Verarbeitung von Gesundheitsdaten im Zentrum eurer Vereinstätigkeit steht, braucht ihr eine Datenschutzbeauftragte.

Beispiel: Selbsthilfegruppe von Betroffenen einer Krankheit

Der Vollständigkeit halber

Die Verarbeitung von Gesundheitsdaten ist in bestimmten Fällen auch ohne Einwilligung erlaubt.

In der Vereinspraxis dürften diese aber eher selten sein, z. B.

- zum Schutz lebenswichtiger Interessen (jemand ist bewusstlos und kann nicht einwilligen)
- in Einrichtungen der Gesundheitsvorsorge durch Angehörige eines Gesundheitsberufs

Weiterführende Informationen findet ihr online.

sds-links.de/ehrenamt-gesundheitsdaten

FOTOS VERÖFFENTLICHEN

Unter Datenschutz-Aspekten ist Einiges zu beachten, wenn ihr vereinsintern oder auf öffentlichen Veranstaltungen für den Verein fotografieren und die Bilder veröffentlichen wollt.

Zweck vorher festlegen

Überlegt euch vorher gründlich, was mit den Fotos geschehen soll, und dokumentiert eure Ergebnisse – das kann viel Arbeit und Ärger ersparen.

Es spielt dabei keine Rolle, ob die Fotografierten Vereinsmitglieder sind oder z. B. als Gäste an einer öffentlichen Veranstaltung teilnehmen.

Rechtsgrundlage prüfen

Jede Verarbeitung pbD braucht eine **Rechtsgrundlage**.

Hier ist das meist das **„berechtigte Interesse"** des Vereins oder die **Einwilligung**. Wichtig ist, welchen Zweck die Fotos erfüllen sollen.

§ 23 Kunst-urhebergesetz

Ohne Einwilligung dürfen Personen generell nur als **Teil einer größeren Gruppe oder „Beiwerk"** dargestellt werden.

Interessenabwägung

Werden die Fotos für die Information über das Vereinsleben oder für die Dokumentation von Veranstaltungen benötigt, besteht ein berechtigtes Interesse des Vereins.

Nun müsst ihr prüfen, ob dieses Interesse mehr Gewicht hat als das **Interesse der fotografierten Personen**, nicht fotografiert zu werden und die Fotos nicht veröffentlicht zu sehen.

Auch wenn das berechtigte Interesse des Vereins überwiegt, kann eine fotografierte Person dagegen **Widerspruch** einlegen, wenn sie Gründe dafür hat.

Dann müssen die Interessen des Vereins und die Interessen der Person erneut gegeneinander abgewogen werden.

* pbD = personenbezogene Daten

FOTOS VERÖFFENTLICHEN

Einwilligung der fotografierten Personen

Wenn das Interesse überwiegt, nicht fotografiert zu werden, könnt ihr euch nicht mehr auf das berechtigte Interesse als Rechtsgrundlage berufen und müsst die Person um ihre Einwilligung bitten. Das ist **bei Kindern und Jugendlichen fast immer notwendig** – hier braucht es also die Einwilligung der Eltern.

Einwilligung

Die Einwilligung ist hier die **Zustimmung** einer Person, fotografiert zu werden, und zur Veröffentlichung der Fotos. Eine **Einwilligung kann jederzeit widerrufen werden**; dann müsst ihr die Fotos löschen, was – bei Veröffentlichung im Internet – ziemlich aufwendig sein kann. Deswegen ist es so wichtig, dass ihr euch vorher überlegt, wofür ihr die Fotos verwenden und wo ihr sie veröffentlichen wollt.

Informationspflichten

Auf jeden Fall müsst ihr klar darüber informieren, dass Fotos gemacht werden und zu welchem Zweck. **Macht also deutlich, ob, wie und wo die Fotos veröffentlicht werden sollen** – im Vereinsblättchen oder auf eurem Social-Media-Profil.

Schreibt es am besten in die Einladung, auf die Veranstaltungs-Website, stellt Schilder an den Eingang oder hängt Zettel an die Wände.

sds-links.de/ehrenamt-fotos

Weiterführende Informationen findet ihr online.

Insbesondere findet ihr hier auch das Muster einer Einwilligungserklärung.

NEWSLETTER-VERSAND

Viele Vereine halten Mitglieder und Interessierte per Newsletter auf dem aktuellen Stand. Was ihr dabei beachten müsst.

Dürfen wir das einfach so?

Ja, wenn die Empfänger Mitglieder sind oder Personen, mit denen ihr auf anderen Wegen vernetzt seid. Dann hat euer Verein ein berechtigtes Interesse, das die Rechtsgrundlage für die Datenverarbeitung bilden kann.

Oder müssen wir fragen?

Ja, wenn die Person z. B. nur ein Ticket für eure Veranstaltung kaufen oder eine Broschüre bestellen möchte; dann solltet ihr eine Einwilligung einholen.

Tipp!

Mehr zu den Rechtsgrundlagen der Datenverarbeitung findet ihr über den QR-Code auf der Rückseite.

Versand per E-Mail-Programm

Beim Versand über das **eigene E-Mail-Programm**: Bitte nutzt für die Anschriften das BCC-Feld (**Blindkopie**), damit nicht alle E-Mail-Adressen für alle Empfängerinnen sichtbar sind.

Die Erfahrung zeigt allerdings, dass das fehleranfällig ist. Besser ist, ihr nutzt die **„Serienbrief"-Funktion**, die viele E-Mail-Programme mitbringen.

! Stellt sicher, dass alle E-Mails ein Impressum des Vereins enthalten. Ebenso müsst ihr auf eine Möglichkeit zum Abmelden hinweisen.

* pbD = personenbezogene Daten

NEWSLETTER-VERSAND

Versand per Cloud-Dienstleister

Es gibt auch spezielle Cloud-Dienstleister für Newsletter. Wenn ihr diese nutzen wollt, sind wichtige Aspekte zu beachten, von denen wir hier einige aufzählen.

- Auftragsverarbeitungsvertrag schließen
- Wenn der Anbieter nicht in der EU sitzt bzw. Server außerhalb der EU betreibt: Rechtsgrundlage für internationale Datentransfers klären
- An- und Abmeldeseiten datenschutzkonform gestalten
- Mails müssen immer Impressum und Abmeldelink enthalten
- Trackingfunktionen ausschalten oder Einwilligung einholen

Praxistipp!

Informationen zum Datenschutz können in die Datenschutzhinweise der Website integriert werden.

Oder ihr erstellt ein separates Dokument speziell für den Newsletter. Von der Anmeldeseite und in jedem Newsletter kann dorthin verlinkt werden.

Weiterführende Informationen findet ihr online.

sds-links.de/ehrenamt-newsletter

UMGANG MIT DATENPANNEN

Datenpanne“ , „Datenleck“ oder „Daten-schutzvorfall“: Hier ist geht es um eine Verletzung des Schutzes personenbezogener Daten.

Was ist ein Datenschutzvorfall?

Es besteht die Möglichkeit oder die Gewissheit, dass pbD unberechtigt offengelegt, verändert oder vernichtet wurden.

Dies kann im Alltag schnell passieren, denn praktisch jeder Verstoß gegen datenschutz-rechtliche Vorschriften kann als Datenpanne betrachtet werden. Dabei spielt keine Rolle, ob die Daten absichtlich oder versehentlich in die falschen Hände gelangt, verändert oder vernichtet worden sind (oder sein könnten).

Beispiele

- Tasche mit unverschlüsselten Speichermedien (z.B. USB-Stick, Smartphone, Laptop) wurde verloren.
- Eine E-Mail wurde an die falschen Empfänger geschickt.
- Ins Büro wurde eingebrochen, Laptops und Kameras gestohlen.

* pbD = personenbezogene Daten

UMGANG MIT DATENPANNEN

Was tun, wenn es passiert ist?

1. Soforthilfe

Maßnahmen ergreifen, um den Schaden zu begrenzen.

2. Information

Den Vorstand und die Datenschutzbeauftragte (wenn vorhanden) informieren.

3. Bewertung

Einschätzen, wie groß der potenzielle Schaden ist. Maßstab ist dabei die Gefahr für die Rechte und Freiheiten der betroffenen Personen.

Faustregel:
Je sensibler die Daten, umso größer die Risiken.

4. Meldung an die Aufsichtsbehörde

Wenn die Bewertung ergibt, dass die Datenschutzverletzung ein Risiko für die Betroffenen darstellt, muss der Vorstand die **Verletzung nach spätestens 72 Stunden** der zuständigen Aufsichtsbehörde melden. Zuständig ist die Aufsichtsbehörde des Bundeslands, in dem der Verein seinen Sitz hat.

Übersicht der Aufsichtsbehörden findet ihr über den QR-Code.

5. Information der Betroffenen

Wenn die Bewertung ergibt, dass das Risiko für die Betroffenen hoch ist (z. B. bei Gesundheitsdaten), müssen auch die Betroffenen informiert werden.

6. Dokumentation

Unabhängig davon, ob die Datenpanne meldepflichtig war, sollte diese intern dokumentiert werden.

Weiterführende Informationen findet ihr online.

sds-links.de/ehrenamt-pannenmeldung

VERANSTALTUNGEN

Euer Verein organisiert ein Turnier, einen Vortrag oder eine Spendensammlung? Auf Veranstaltungen treten mehrere Formen der Datenverarbeitung auf.

Betroffenengruppen und deren Datenverarbeitung

Wichtig ist, dass ihr die Gruppen der betroffenen Personen hinsichtlich der Datenverarbeitung unterscheidet und sie getrennt über die für sie jeweils relevante Verarbeitung informiert.

Teilnehmende und Zuschauende

Je nachdem, wie öffentlich die Veranstaltung ist, kommen Leute einfach vorbei, oder sie melden sich vorab bei euch an.

Die Daten, die ihr mit der **Anmeldung** erhaltet, dürfen nur für die Organisation der Veranstaltung verwendet und müssen danach gelöscht werden. Die Rechtsgrundlage ist die Vertragserfüllung.

! Mit der Anmeldung kommt eine Art Vertrag zustande. Die Schriftform ist nicht erforderlich.

Weiterverwendung von Kontaktdaten

Wollt ihr die Kontaktdaten auch nach der Veranstaltung noch nutzen, müsst ihr die Teilnehmenden vorab darüber informieren:

- was ihr auf Basis welcher Rechtsgrundlage mit ihren Daten macht
- und wann ihr diese wieder löscht.

Typischer Anwendungsfall Newsletter-Anmeldung

Ihr könnt die Person fragen, ob sie künftig Informationen über das Vereinsleben per E-Mail beziehen möchte. Wenn sie das bejaht, ist die Rechtsgrundlage die Einwilligung der betroffenen Person zur weiteren Datenverarbeitung.

* pbD = personenbezogene Daten

VERANSTALTUNGEN

Referierende und Spielende

Manche Personen stehen im Fokus der Veranstaltung, vielleicht als Rednerinnen oder Gastspieler. Meist werden ihre Namen schon vor der Veranstaltung bekannt gegeben, z. B. auf eurer Website, auf Werbeflyern oder auf Spieler-/Starterlisten.

Die Vereinbarungen zwischen eurem Verein und diesen Personen gelten als Vertrag. Dieser Vertrag kann verschiedene Formen haben und auch mündlich sein. Er ist die Rechtsgrundlage für die notwendige Datenverarbeitung.

Ihr seid verpflichtet, die Person vorab zu **informieren**, was ihr mit den Daten macht, und die Datenverarbeitung auf das Nötigste zu beschränken.

Fotos

Falls ihr auf der Veranstaltung fotografiert, ist auch das eine Form von Datenverarbeitung. Völlig unabhängig davon, ob ihr die Namen der Personen auf den Fotos kennt.

Üblicherweise wird die Nutzung der Fotos von Referierenden und Spielenden gesondert vereinbart.

Was zu beachten ist, wenn ihr die Fotos veröffentlichen wollt, findet ihr über den QR-Code.

sds-links.de/ehrenamt-veranstaltungen

Weiterführende Informationen findet ihr online.

VERANTWORT-LICHKEITEN

Wer ist eigentlich für den Datenschutz in eurem Verein verantwortlich? Die Datenschutzbeauftragte? Alle Aktiven? Hier wollen wir zeigen, wer wofür zuständig ist.

Im Verein

Vorstand

Muss dafür sorgen, dass der Datenschutz organisiert und eingehalten wird. Kümmert sich entweder selbst um die Umsetzung oder weist die Umsetzung einer anderen Person, der Datenschutzkoordinatorin, zu.

Datenschutzkoordinatorin

Kümmert sich um die Umsetzung von Datenschutzvorgaben und behält den Überblick. Berichtet dem Vorstand.

Datenschutzbeauftragte (DSB)

Berät den Vorstand und kontrolliert die Einhaltung von Datenschutzvorgaben. Brauchen nicht alle Vereine.

Ehrenamtlich Aktive

Handeln nach Weisung des Vorstands im Namen des Vereins und müssen Datenschutzvorgaben einhalten.

Beschäftigte, Angestellte, Hauptamtliche

Gleiche Rolle im Datenschutz wie ehrenamtlich Aktive.

Wann ihr eine DSB braucht und weitere Details sucht, findet ihr diese auf der Karte „Datenschutzbeauftragte"

* pbD = personenbezogene Daten

VERANTWORT-LICHKEITEN

Betroffene Personen

Alle, deren Daten verarbeitet werden. Dazu gehören alle Mitglieder und Beschäftigte des Vereins, Gastspieler, Spender, Besucher öffentlicher Veranstaltungen …

Auftragsverarbeiter

Dienstleister, die pbD der Betroffenen im Auftrag des Vereins, nach dessen Vorgaben und in dessen Verantwortung verarbeiten. Häufig bei technischen Dienstleistungen, wie z. B. Cloud-Tools.

Dritte

Organisationen, an die pbD auf Basis einer Rechtsgrundlage übermittelt werden und die keine Auftragsverarbeiter sind, z. B. Dachverbände.

Weiterführende Informationen findet ihr online.

sds-links.de/ehrenamt-verantwortlichkeiten

WEBSITE

Sicher hat auch euer Verein eine Website. Dort werden auf ganz unterschiedliche Weise pbD verarbeitet.

Die Datenschutzhinweise („Datenschutzerklärung")

Jede Website muss darlegen, welche pbD wie und von wem verarbeitet werden, und welche Rechte die betroffenen Personen haben. Weil die Anforderungen an die Datenschutzhinweise recht komplex sind, stellen wir dafür einen **Generator** zur Verfügung.

Der erzeugte Text ist eine gute Grundlage, die ihr an eure konkrete Datenverarbeitung anpassen könnt.

Den Generator findet ihr über den QR-Code auf der Rückseite.

Die Inhalte

Wenn es auf der Website Fotos oder andere pbD (z. B. Kontaktdaten von Mitgliedern) gibt:

- Habt ihr die Einwilligung, oder hat der Verein ein berechtigtes Interesse an der Veröffentlichung von Fotos?
- Wird regelmäßig überprüft, ob das Interesse noch besteht? Wer kümmert sich darum?
- Erhebt ihr Daten über Webformulare?
  Setzt im Formular einen Link zu den Datenschutzhinweisen; weist dort darauf hin, was mit den Daten passiert.
- Kein Datenschutzthema, dennoch wichtig: Immer, wenn ihr Inhalte (z. B. Fotos, Artikel) von Dritten veröffentlicht, beachtet und wahrt zudem das Urheberrecht.

✓ **BEISPIEL: ihr habt mit Fotos vom letzten Sommerfest um Sponsoren für das diesjährige Fest geworben. Die Rechtsgrundlage war das berechtigte Interesse. Nun ist das Sommerfest vorbei – die Fotos müssen gelöscht werden.**

* pbD = personenbezogene Daten

WEBSITE

Unbeliebt: Cookies und Cookie-Banner

Wenn eure Website Cookies verwendet, müsst ihr den Besuchern die Möglichkeit geben, die kleinen Textdateien mit maximal zwei Klicks abzulehnen.

Dazu braucht es ein sogenanntes Cookie-Banner – am besten mit einem Link zu den Datenschutzhinweisen. Oder verzichtet auf Cookies, wenn möglich.

Das Impressum

Kein Datenschutzthema, trotzdem wichtig

Die Website muss ein Impressum mit folgenden Angaben enthalten:

- Vollständiger Name des Vereins
- Name des Vorstands
  (oder sonst vertretungsberechtigte natürliche Personen)
- Adresse des Vereins
- E-Mail-Adresse
- Eingetragener Verein: Angabe Vereinsregister, Registergericht, Registernummer

Hosting, Auftragsverarbeitung, Sicherheit

Die IP-Adresse des Computers, mit der Besucher auf die Website zugreifen, gelten als pbD und müssen als solche behandelt werden. Deshalb müsst ihr mit dem Unternehmen, auf deren Rechnern die Website läuft, einen Auftragsverarbeitungsvertrag schließen.

Bestimmt, wer für die Sicherheit der Website zuständig sein soll. Das kann ein Dienstleister sein oder ein zuverlässiges, technisch versiertes Mitglied.

sds-links.de/
ehrenamt-website

Weiterführende Informationen findet ihr online.

DIE WICHTIGSTEN BEGRIFFE

Auftragsverarbeitung (AV)

Wenn euer Verein einen Dienstleister mit der Verarbeitung eurer Daten beauftragt, spricht man von Auftragsverarbeitung. Die DSGVO verlangt, dass ihr das in einem Vertrag regelt.

Artikel 9 DSGVO – besondere Datenkategorien

Einige Kategorien von Daten, wie z. B. Gesundheitsdaten oder politische Meinungen, werden durch Art. 9 DSGVO besonders geschützt.

Aufbewahrungspflichten

In einigen Fällen, wie bei der Buchhaltung, gibt es gesetzliche Fristen, wie lange Dokumente und personenbezogene Daten aufbewahrt werden müssen.

Aufsichtsbehörde

Das Bundesland in dem euer Verein seinen formellen Sitz hat, hat eine Aufsichtsbehörde für den Datenschutz. Diese ist für eure Datenschutzbelange zuständig. Insbesondere für die Meldung eurer Datenschutzbeauftragten.

Berechtigtes Interesse

Rechtsgrundlage für die Verarbeitung, alternativ zu Einwilligung oder Vertrag. Erfordert eine Abwägung zwischen den Interessen eures Vereins und den Risiken für die betroffene Person.

Betroffene

Personen, deren Daten ihr verarbeitet.

Cloud

Speicherplatz oder auch komplexere Anwendungen bei einem Dienstleister, über die ihr auf das Internet zugreift.

Cookie

Information, die eure Website auf dem Computer/Smartphone des Betrachters zwischenspeichert. Hierzu gibt es spezielle Regelungen im TTDSG.

Cookie-Banner

Abfrage beim Aufruf der Website, bei der um Einwilligung in die Verwendung von Cookies gebeten wird.

DSGVO

Europäische Datenschutz-Grundverordnung

Datenpanne

Unbeabsichtigte Veröffentlichung von Daten.

Datenschutzbeauftragte

Person, die euren Verein in der Umsetzung von Datenschutzvorgaben berät und dies überwacht.

Datenschutzkoordinatorin

Person, die sich vereinsintern um die Datenschutzumsetzung kümmert.

Datenschutzhinweise

Anderes Wort für Datenschutzerklärung. Ein Text, in dem ihr Betroffene darüber informiert, was ihr mit ihren Daten macht.

Drittstaatentransfer

Wenn Daten den europäischen Wirtschaftsraum verlassen, kommen zusätzliche Regeln hinzu.

Einwilligung

Zustimmung in eine bestimmte Form der Datenverarbeitung. Eine von mehreren Rechtsgrundlagen.

Hosting

Technischer Betrieb einer Website oder eines anderen Dienstes, häufig bei einem darauf spezialisierten Dienstleister.

IP-Adresse

Technische Kennung eines Internetanschlusses, der eine Website aufruft. Ist per Gesetzesdefinition ein personenbezogenes Datum.

personenbezogene Daten (pbD)

Alle Informationen über Personen, die digital erfasst wurden oder strukturiert in Papierform abgelegt wurden. Wichtig: Es muss kein Name mit vermerkt sein – es reicht schon, dass jemand von euch den Datensatz einer Person zuordnen kann.

Rechtsgrundlage

Personenbezogene Daten dürfen nur auf Basis einer Rechtsgrundlage verarbeitet werden. Hierfür gibt die DSGVO verschiedene Möglichkeiten vor – die Rechtsgrundlagen. z. B. Einwilligung, Vertrag oder gesetzliche Grundlage.

Technisch-organisatorische Maßnahmen (TOM)

Vorkehrungen, die dafür sorgen, dass Daten sicher geschützt sind und nur von den Personen und in der Art verarbeitet werden, wie es von euch beabsichtigt ist.

TTDSG

Telekommunikation-Telemedien-Datenschutz-Gesetz

Verantwortlicher

Rechtlich dafür zuständige Stelle, die für gesetzeskonforme Datenverarbeitung in einem bestimmten Bereich zuständig ist. Zum Beispiel euer Verein, vertreten durch den Vorstand.

Verarbeitungstätigkeit

Eine, zumeist regelmäßige, Aktivität in euren Verein, bei der ihr personenbezogene Daten benötigt, z. B. die Mitgliederverwaltung.

Verarbeitungszweck

Nachvollziehbarer Grund, warum euer Verein etwas Bestimmtes mit Daten macht.

Eine ganze Reihe dieser Begriffe definiert die DSGVO im Art. 4 „Begriffsbestimmungen"