**Mustervorlage für eine Verpflichtungserklärung zum Datenschutz**

**Herausgeberin:**

**Stiftung Datenschutz**

**Karl-Rothe-Straße 10-14
04105 Leipzig**

[**https://stiftungdatenschutz.org**](https://stiftungdatenschutz.org)

***Die Arbeit der Stiftung Datenschutz wird aus dem Bundeshaushalt gefördert (Einzelplan des BMJ).***

**Autorinnen der Arbeitshilfe:
Sofia & Katharina Vester, fix&fertig – Datenschutzhilfen für Zivilgesellschaft**

**Erstellt im Auftrag der Stiftung Datenschutz**

**Diese Arbeitshilfe wird ergänzend zum Praxisratgeber Verpflichtungserklärungen (**[**https://stiftungdatenschutz.org/ehrenamt/praxisratgeber/praxisratgeber-detailseite/verpflichtungserklaerungen-539**](https://stiftungdatenschutz.org/ehrenamt/praxisratgeber/praxisratgeber-detailseite/verpflichtungserklaerungen-539)**) des Angebotes „Datenschutz im Ehrenamt“ der Stiftung Datenschutz veröffentlicht.**

**Version 1.1 vom 16.01.2025**

Wichtige Hinweise für Vorstände/Verantwortliche im Verein
zur Mustervorlage für eine Verpflichtungserklärung zum Datenschutz

Was ist der Sinn und Zweck der Verpflichtungserklärung?

Als Vorstand eures Vereins seid ihr für die Verarbeitung von ***personenbezogenen Daten*** im datenschutzrechtlichen Sinn verantwortlich und habt die gesetzlichen Vorgaben wie die Datenschutzgrundverordnung zu beachten. Damit schützt ihr die Personen, deren Daten euer Verein verarbeitet, also zum Beispiel eure Vereinsmitglieder, aber auch andere Personen, die Angebote und Veranstaltungen eures Vereins wahrnehmen.

Eine „Verarbeitung personenbezogener Daten“ findet immer dann statt, wenn man etwas mit den Daten von Personen macht, also zum Beispiel Daten erhebt, speichert, nutzt, in welcher Form auch immer weitergibt bzw. zugänglich macht oder auch löscht. Beachtet also, dass die „Verarbeitung“ von personenbezogenen Daten bei ***sehr vielen eurer Vereinsaktivitäten*** eine Rolle spielen kann.

Darüber hinaus sind aber auch ***Vereinsinterna*** wie interne Abläufe oder Absprachen im Sinne des Gesetzes zum Schutz von „Geschäftsgeheimnissen“ schutzbedürftige Daten. Ein vertraulicher Umgang mit Vereinsinterna sollte daher – abhängig von euren Vereinsaktivitäten und den damit verbundenen Risiken – auch sichergestellt werden, falls das nicht schon in einem anderen Rahmen (etwa im Arbeitsvertrag von Hauptamtlichen) geregelt ist.

Als Vorstand müsst ihr dafür sorgen, dass schutzbedürftige Daten vertraulich behandelt werden, und sicherstellen, dass personenbezogene Daten weder unbefugt noch unrechtmäßig verarbeitet werden. Dazu müsst ihr alle Aktiven verpflichten, die bei ihrem Engagement für den Verein Zugang zu personenbezogenen Daten haben, **und ihr müsst auch die Voraussetzungen dafür schaffen, dass sie dieser Verpflichtung nachkommen können**. Mit dieser Verpflichtungserklärung könnt ihr gegenüber den Datenschutz-Aufsichtsbehörden bei Bedarf nachweisen, dass ihr eurer Pflicht nachgekommen seid.

Weitere Hintergrundinformationen und Tipps findet ihr im [Praxisratgeber „Verpflichtungserklärungen – Engagierte wirksam in den Datenschutz einbinden“](https://stiftungdatenschutz.org/ehrenamt/praxisratgeber/praxisratgeber-detailseite/verpflichtungserklaerungen-539).

Wer muss die Verpflichtungserklärung unterzeichnen?

Alle Personen, die im Zusammenhang mit der Tätigkeit für den Verein vertrauliche und insbesondere personenbezogene Daten verarbeiten, müssen die Erklärung unterzeichnen: Vorstandsmitglieder, ehrenamtlich Aktive und ggf. hauptamtliche Mitarbeitende.

Wann solltet ihr die Verpflichtungserklärung einholen?

Holt die Erklärung idealerweise zu Beginn des Engagements im Verein ein, bevor personenbezogene Daten für den Verein verarbeitet werden oder darauf zugegriffen wird.

Worauf wollt ihr eure Aktiven verpflichten?

Zunächst ist es sinnvoll, eure Aktiven zur Einhaltung der grundsätzlichen Datenschutzprinzipien und ggf. auf Vertraulichkeit zu verpflichten. Darauf aufbauend stellen konkrete Regelungen sicher, dass diese Prinzipien auch verstanden und im Vereinsalltag umgesetzt werden.

Wann und wie wird das Wissen zum Thema Datenschutz aufgefrischt? Wie werden Änderungen von Regelungen zum Umgang mit Daten mitgeteilt?

Sorgt dafür, dass ihr regelmäßig im Vereinsteam das Wissen über die wichtigsten Regelungen zum Datenschutz auffrischt und prüft, ob es Anpassungsbedarf gibt. Klärt auch, auf welchem Weg ihr im Vereinsteam über Änderungen von Regelungen informiert und wer die Ansprechperson für Fragen zum Thema Datenschutz ist.

Wie könnt ihr mit den folgenden Dokumenten arbeiten?

Im „Merkblatt zur Verpflichtungserklärung“ sind die grundsätzlichen Prinzipien erläutert. Darauf folgt ein Muster für die eigentliche Verpflichtungserklärung. In der „Anlage 1“ findet ihr im Baukastensystem ***Beispiele*** für Regelungen zum Datenschutz im Vereinsalltag und in der optionalen „Anlage 2“ findet ihr ***Beispiele*** für konkrete Regeln zum Thema Vertraulichkeit.

Geht die Dokumente sorgfältig durch und ***passt alle Texte unbedingt auf eure konkrete Vereinsarbeit an***. Die blau markierten Hinweise für den Vorstand könnt ihr anschließend löschen. An den gelb markierten Stellen könnt ihr ihr ggf. Zutreffendes auswählen oder Anpassungen vornehmen (das kann aber je nach euren Vereinsaktivitäten durchaus auch an nicht markierten Stellen sinnvoll sein). Die gelben Markierungen könnt ihr nach eurer Anpassung wieder entfernen.

Beachtet dabei, dass die Beispielregelungen euch eine möglichst praxisnahe Hilfestellung geben sollen, jeder Verein jedoch individuelle Anforderungen hat und die aufgeführten Regelungen ***nicht abschließend*** sind. Überlegt daher auch, ob über die angebotenen Bausteine hinaus weitere Bereiche für eure Arbeit wichtig sind, die hier geregelt werden sollten. Möglicherweise sind einige Regelungen für euren Verein aber auch gar nicht relevant oder sinnvoll umsetzbar – dann streicht solche Passagen. Letztlich sollten die Regelungen in einem angemessenen Verhältnis zu eurer konkreten Vereinsarbeit stehen.

Beachtet auch, dass für dieses Muster keinerlei Haftung übernommen werden kann, auch wenn wir es nach bestem Wissen und Gewissen erstellt haben, um euch möglichst praxisnah zu unterstützen.

***Tipp: Selbstcheck!***

Bevor ihr als Vorstand euren Aktiven das Merkblatt zur Verpflichtungserklärung mit Anlagen vorlegt und eine Unterschrift zu der Verpflichtungserklärung einholt, versetzt euch einmal in die Lage der anderen Person: Stellt euch vor, ihr selbst wärt gerade erst dabei, euch im Verein zu engagieren und hättet keinen Einblick in die Vorstandsarbeit.

Stellt euch dann die Kontrollfrage: Hättet ihr genügend Informationen, um die Erklärung wirksam unterschreiben zu können? Oder anders formuliert: Wüsstet ihr, was ihr warum beachten müsst, wie ihr die Vorgaben konkret bei eurem Engagement im Verein umsetzen könnt und an wen ihr euch bei Fragen dazu wenden könnt?

Falls ihr diese Frage mit „Nein“ beantworten würdet oder unsicher seid, schaut nochmal in den [Praxisratgeber „Verpflichtungserklärungen – Engagierte wirksam in den Datenschutz einbinden“](https://stiftungdatenschutz.org/ehrenamt/praxisratgeber/praxisratgeber-detailseite/verpflichtungserklaerungen-539) und klärt offene Fragen, bevor ihr die Verpflichtungserklärungen einholt. Falls ihr diese Frage mit „Ja“ beantworten könnt, kann es losgehen.

## Merkblatt zur Verpflichtungserklärung

1. **Sinn und Zweck der Verpflichtungserklärung**

Als Verein sind wir für die Verarbeitung personenbezogener Daten im datenschutzrechtlichen Sinn verantwortlich und haben die gesetzlichen Vorgaben wie die Datenschutzgrundverordnung zu beachten. Damit schützen wir die Personen, deren Daten wir verarbeiten, also zum Beispiel unsere Vereinsmitglieder.

Verstöße gegen die datenschutzrechtlichen Vorschriften können Bußgelder für unseren Verein bzw. den Vereinsvorstand (der für unseren Verein die Verantwortung übernimmt) zur Folge haben und nicht zuletzt zu einem großen Vertrauensverlust bei unseren Mitgliedern und Unterstützer\*innen führen. Unter Umständen können sich auch einzelne Aktive persönlich strafbar machen bzw. ordnungswidrig handeln, wenn sie gegen die Regelungen in dieser Verpflichtungserklärung verstoßen. (Nähere Informationen dazu finden sich in Art. 82 und 83 der Datenschutzgrundverordnung sowie in § 42 und 43 im Bundesdatenschutzgesetz.)

Unser Vorstand muss insbesondere sicherstellen, dass ***personenbezogene Daten weder unbefugt noch unrechtmäßig verarbeitet werden***. Hierzu müssen vom Vorstand alle Aktiven und Beschäftigten verpflichtet werden, die bei ihrem Engagement für den Verein Zugang zu personenbezogenen Daten haben. Mit dieser Verpflichtungserklärung kann der Vorstand bei Bedarf gegenüber den Datenschutz-Aufsichtsbehörden nachweisen, dass er seiner Pflicht nachgekommen ist.

[Falls es in eurem Verein Hauptamtliche gibt, können der folgende Abschnitt und der Verweis auf Anlage 2 bei der Verpflichtung der Hauptamtlichen gelöscht werden, sofern das Thema Vertraulichkeit bereits im Arbeitsvertrag geregelt ist. Auch wenn es in eurem Verein keine Vereinsinterna gibt, die eine Vertraulichkeitsverpflichtung erforderlich machen, können dieser Verweis sowie die Anlage selbst gelöscht werden. Falls nur wenige Personen Zugang zu vertraulichen Interna haben, so kann der Verweis samt Anhang 2 auch nur für diese Personen genutzt und für andere Personen ausgelassen werden.]

Darüber hinaus sind zum Schutz unseres Vereins auch interne Abläufe oder Absprachen schutzbedürftige Daten, auch wenn sie sich nicht unbedingt auf Personen beziehen. Mit dieser Erklärung wird daher auch zum ***vertraulichen Umgang mit Vereinsinterna*** verpflichtet, die man in einem Unternehmen als „Geschäftsgeheimnisse“ bezeichnen würde. (Nähere Informationen dazu finden sich im Gesetz zum Schutz von Geschäftsgeheimnissen.)

Für die Aktiven und Beschäftigten in unserem Verein soll diese Erklärung (insbesondere die konkreten Regelungen in Anlage 1 und Anlage 2) vor allem Handlungssicherheit schaffen und die nötigen Grundlagen vermitteln, damit wir gemeinsam vertrauliche Daten im Vereinsalltag effektiv schützen können.

2. Grundbegriffe des Datenschutzes

„Personenbezogen­e Daten“ umfassen alle Informationen über Personen, die digital erfasst wurden oder strukturiert in Papierform abgelegt wurden. Wichtig: Es muss kein Name vermerkt sein, damit es sich um personenbezogene Daten handelt – es reicht schon, dass jemand den Datensatz bzw. die Information einer Person zuordnen könnte.

Beispiele für personenbezogene Daten in unserem Vereinsalltag sind:

* Namen, Kontaktdaten, Bankverbindungen, Geburtstage, Mitgliedsnummern etc. unserer Mitglieder
* Namen und Kontaktdaten auf Teilnahmelisten unserer Veranstaltungen
* Foto-, Video- oder Tonaufnahmen von Personen, die zum Beispiel bei Vereinsveranstaltungen entstehen
* Daten, die beim Besuch unserer Website oder unserer Social-Media-Seiten (oft automatisch) verarbeitet werden
* ...

Eine „Verarbeitung personenbezogener Daten“ findet immer dann statt, wenn man etwas mit den Daten von Personen macht, also zum Beispiel Daten erhebt, speichert, nutzt, in welcher Form auch immer weitergibt bzw. zugänglich macht oder auch löscht.

In unserem Vereinsalltag verarbeiten wir zum Beispiel personenbezogene Daten, wenn wir:

* Mitgliederdaten für die Kontaktaufnahme nutzen (wie bei der Einladung zur Mitgliederversammlung oder beim Versand unseres Newsletters)
* Teilnahmelisten bei Veranstaltungen führen oder auch später wieder vernichten
* Fotos von Personen bei Vereinsaktivitäten machen
* …

3. Grundsätze des Datenschutzes

Wenn personenbezogene Daten verarbeitet werden, dann muss das gemäß der Datenschutz-Grundverordnung auf folgende Weise geschehen:

* rechtmäßig, fair und für die betroffene Person erwartbar und gut nachvollziehbar
(„Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“)
	+ **Wir brauchen also eine rechtliche Grundlage für jede Datenverarbeitung, müssen uns dabei an die rechtlichen Vorschriften halten und (möglichst im Vorfeld) darüber informieren, wie wir die Daten verarbeiten.**
* für festgelegte, eindeutige und legitime Zwecke, ohne dass die Daten in einer Weise weiterverarbeitet werden, die mit diesen Zwecken nicht zu vereinbaren ist
(„Zweckbindung“)
	+ **Wir müssen also vorher klar den Zweck (oder die Zwecke) benennen, für die wir Daten brauchen, und können diesen Zweck nicht einfach ändern oder erweitern.**
* für den Zweck angemessen und auf das notwendige Maß beschränkt
(„Datenminimierung“)
	+ **Wir dürfen also nur so viele Daten verarbeiten, wie es für diesen Zweck nötig ist, und auch nur jenen Personen Zugriff darauf ermöglichen, die den Zugriff für diesen Zweck brauchen.**
* sachlich richtig und aktuell
(„Richtigkeit“)
	+ **Wir müssen also dafür sorgen, dass wir unrichtige Daten möglichst löschen oder korrigieren.**
* in einer Form gespeichert, durch die ein Personenbezug nur so lange möglich ist, wie es für den Verarbeitungszweck nötig ist
(„Speicherbegrenzung“)
	+ **Wir müssen also regelmäßig Daten löschen, die nicht mehr für den Zweck gebraucht werden, für den wir sie erhoben haben.**
* unter Beachtung von Schutzmaßnahmen gegen eine unbefugte oder unrechtmäßige Verarbeitung und gegen einen unbeabsichtigten Verlust oder Beschädigung der Daten
(„Integrität und Vertraulichkeit“)
	+ **Unser Verein muss also Abläufe so gestalten, dass Unbefugte keinen Zugriff auf personenbezogen Daten erhalten und gespeicherte Daten geschützt werden. Und wir müssen bei unseren Tätigkeiten für den Verein die dazugehörigen Regeln kennen und befolgen.**

***Tipp: Selbstcheck!***
Auch wenn dies nicht das einzige Kriterium ist: Grundsätzlich sollten wir uns vor der Verarbeitung personenbezogener Daten immer die ***Kontrollfrage*** stellen: Wäre es für mich nachvollziehbar und in Ordnung, wenn meine Daten auf diese Weise verarbeitet werden? Wenn wir diese Frage nicht mit „ja“ beantworten können, müssen wir die Datenverarbeitung auf jeden Fall nochmal überdenken.

Konkrete Regelungen und Abläufe in unserem Verein

Die konkreten Regelungen zum Umgang mit personenbezogenen Daten sind dieser Erklärung als Anlage 1 beigefügt.

Die konkreten Regelungen zur Vertraulichkeit von Vereinsinterna sind dieser Erklärung als Anlage 2 beigefügt.

Falls sich die Regelungen ändern oder neue hinzukommen, werden alle Aktiven und Beschäftigten schriftlich per E-Mail darüber informiert.

Eine aktuelle Version der Regelungen ist auch immer hier abgelegt: [ggf. digitalen Speicherort oder physischen Aufbewahrungsort einfügen].

Hinweise und Ideen, wie wir unsere Regelungen zum Datenschutz im Verein verbessern können, sind jederzeit willkommen (siehe Abschnitt zu Ansprechperson(en) in Anlage 1).

Verpflichtungserklärung zum Datenschutz und zur Vertraulichkeit

Über meine Verpflichtung auf die Beachtung des Datenschutzes und zur Wahrung der Vertraulichkeit sowie auf die sich daraus ergebenden Regelungen im Zusammenhang mit meiner Tätigkeit für VEREINSNAME wurde ich unterrichtet.

Ich erkläre hiermit, dass ich diese Pflichten künftig gewissenhaft erfüllen und Daten nicht unbefugt oder unrechtmäßig verarbeiten werde. Diese Verpflichtung gilt auch über den Zeitraum meiner Tätigkeit für den Verein hinaus.

Das Merkblatt zur Verpflichtungserklärung und die Anlagen mit den konkreten Regelungen zum Datenschutz und zur Vertraulichkeit im Verein habe ich erhalten und gelesen. Ich hatte die Gelegenheit, mögliche Fragen zu klären. Ich weiß, an wen ich mich mit allen Fragen und Angelegenheiten zum Thema Datenschutz wenden kann.

……………. ……………………………………………………………. …………………………………………………………….

Datum Name, Vorname (Aktive\*r/Beschäftigte\*r) Unterschrift (Aktive\*r/Beschäftige\*r)

Anlagen:

Anlage 1 Regelungen zum Umgang mit personenbezogenen Daten in unserem Verein

Anlage 2 Regelung zur Vertraulichkeit zum Schutz von Vereinsinterna

Anlage 1:
Regelungen zum Umgang mit personenbezogenen Daten in unserem Verein

-----------------------------------------------------------------------------------------------------------------------------------

**ÜBERSICHT**

* Ansprechpersonen
* Melde- und Hinweispflichten zum Datenschutz
* Zugangs- und Nutzungsregelungen für unsere Vereinsräume
* Zum Umgang mit Passwörtern
* Zur Nutzung der Vereins-Cloud
* **Zur Nutzung von Vereinsgeräten und Datenträgern sowie zum Umgang mit Vereinsdokumenten**
* **Zur Nutzung von privaten Geräten und Datenträgern für die Vereinsarbeit sowie zum Umgang mit Vereinsdokumenten**
* Zur Nutzung von E-Mail-Kommunikation
* **Zum Umgang mit Fotos**

-----------------------------------------------------------------------------------------------------------------------------------

**Baustein Ansprechpersonen (für alle Vereine wichtig):**An wen können sich die Aktiven und Beschäftigten in eurem Verein bei Fragen und Hinweisen zu diesen Regelungen wenden?

🡪 Als Vorstand kümmert ihr euch um diese Voraussetzungen:

* Ihr klärt, wer in eurem Verein die Rolle der Ansprechperson(en) für Fragen zum Thema Datenschutz und ggf. auch Fragen zur IT übernimmt und stellt möglichst Ressourcen zur Fortbildung bereit oder informiert über Unterstützungsmöglichkeiten und kostenlose Angebote.

Ansprechpersonen

Unsere Ansprechperson(en) für Datenschutz ist/sind:

[Funktionsbezeichnung mit Kontaktdaten einfügen, zum Beispiel der Vorstand und/oder – wenn vorhanden – die\*der Datenschutzbeauftragte]

Unsere Ansprechperson(en) für Fragen zur IT (Umgang mit Geräten, Programmen und Passwörtern) ist/sind:

[ggf. Funktionsbezeichnung mit Kontaktdaten einfügen]

-----------------------------------------------------------------------------------------------------------------------------------

**Baustein Melde- & Hinweispflichten (für alle Vereine wichtig):**Wie geht ihr mit Datenpannen im Verein um und schließt Lücken im Datenschutz?

→ Als Vorstand kümmert ihr euch um diese Voraussetzungen:

* Ihr klärt, wer im Fall von verschiedenen Szenarien ggf. zusätzlich einbezogen werden sollte (zum Beispiel der ganze Vorstand im Fall einer schwerwiegenden Datenpanne).
* Ihr sorgt dafür, dass ihr regelmäßig im Vereinsteam das Wissen über die wichtigsten Regelungen zum Datenschutz auffrischt. So könnt ihr Datenpannen vorbeugen und sicherstellen, dass alle Aktiven im Verein über die Regelungen zum Datenschutz informiert sind.
* Ihr prüft regelmäßig, ob es Anpassungsbedarf bei euren Regelungen zum Datenschutz gibt.
* Ihr klärt, auf welchem Wege ihr im Vereinsteam über Änderungen von Regelungen informiert.

Melde- und Hinweispflichten zum Datenschutz

*Beispiele für Datenschutzverstöße oder Datenpannen sind:*

* Jemand schickt versehentlich eine E-Mail mit personenbezogenen Daten an einen oder mehrere falsche Empfänger\*innen.
* Passwörter für Vereins-Accounts, Geräte oder Ausdrucke mit vertraulichen Vereinsdaten darauf werden gestohlen oder gehen verloren.
* Auf einem Gerät mit vertraulichen Vereinsdaten wird ein Virus festgestellt oder vermutet.

*Beispiele für Verbesserungsmöglichkeiten oder Unklarheiten im Datenschutz sind:*

* Es bestehen Unsicherheiten bei der Wahl eines Programms, um eine Datenverarbeitung umzusetzen.
* Es ist unklar, wie Regelungen konkret umgesetzt werden können (zum Beispiel gibt es die Anforderung „sichere Datenübermittlung“ ohne dass klar ist, wie die Datenübermittlung konkret abgesichert werden soll).
* Wenn – ob willentlich oder unbeabsichtigt – gegen die Regelungen zum Datenschutz in unserem Verein verstoßen wird oder es zu Datenpannen kommt, muss das so schnell wie möglich an unsere Ansprechperson(en) für Datenschutz und im Falle technischer Datenpannen auch sogleich der Ansprechperson(en) für IT gemeldet werden (siehe Abschnitt zu Ansprechpersonen). So kann ein möglicher Schaden ggf. begrenzt werden. Eine unverzügliche Meldung ist auch deswegen wichtig, weil wir als Verein ab Bekanntwerden einer Datenpanne im Verein gegebenenfalls selbst dazu verpflichtet sind, diese innerhalb von 72 Stunden an die Datenschutzbehörde zu melden. Je früher wir also informiert werden, desto gründlicher können wir im Vereinsvorstand die Meldepflicht an die Behörde prüfen.
* Sollte sich eine Person bei jemandem aus unserem Verein mit einer Frage zu Datenschutz melden oder auch, weil sie ihre Datenschutzrechte in Anspruch nehmen möchte (Recht auf Auskunft, Berichtigung, Löschung etc.), so haben wir als Verein die Pflicht, diese Anfrage unverzüglich zu bearbeiten und schnellstmöglich zu beantworten. Dabei müssen wir auch formale Anforderungen beachten, weswegen Datenschutzanfragen immer erst nach Rücksprache mit unserer Ansprechperson für Datenschutz beantwortet werden dürfen. Auch hier gilt daher: Je früher eine solche Anfrage weitergegeben wird, desto besser.
* Außerdem sind alle, die sich für unseren Verein engagieren, ausdrücklich dazu aufgefordert, mögliche offene Fragen, Unklarheiten oder Verbesserungsmöglichkeiten bei der Datenverarbeitung zu melden. Gleiches gilt, wenn neue Abläufe nötig werden (zum Beispiel durch neue Vereinsaktivitäten, bei denen Daten verarbeitet werden). So können wir gemeinsam für klar geregelte Abläufe sorgen, bei denen wir personenbezogene Daten verantwortungsvoll und mit angemessenem Schutz verarbeiten.

-----------------------------------------------------------------------------------------------------------------------------------

**Baustein Büroräume (wenn euer Verein Büroräume hat):**Wie schützt ihr die personenbezogenen Daten, die im Büro aufbewahrt werden?

→ Als Vorstand kümmert ihr euch um diese Voraussetzungen:

* Ihr erstellt eine Liste über alle Personen, die einen Schlüssel zu den Vereinsräumen haben bzw. bekommen (und wenn eine Person den Verein verlässt, kümmert ihr euch darum, dass ihr den Schlüssel zurückbekommt).
* Ihr schafft einen Schredder/Aktenvernichter (mindestens Sicherheitsstufe 3) an oder organisiert regelmäßig eine professionelle Aktenvernichtung durch ein Dienstleistungsunternehmen und stellt in der Zwischenzeit einen möglichst abschließbaren Einwurf-Sammelbehälter dafür bereit.
* Ihr sorgt dafür, dass Räume oder Schränke zur Aufbewahrung sensibler Daten separat abschließbar sind.
* Nicht erforderlich, aber sehr zu empfehlen: Ihr erstellt eine Checkliste für das Verlassen der Vereinsräume am Ende des Tages (Sind die Fenster richtig zu? Sind die Kaffeemaschine/der Drucker/ggf. weitere Geräte ausgeschaltet? Abschließen nicht vergessen! etc.) und hängt sie innen an die Eingangstür.

Zugangs- und Nutzungsregelungen für unsere Vereinsräume

* Über alle Personen, die einen Schlüssel für die Vereinsräume erhalten, wird eine Liste geführt. Die Schlüssel werden nicht auf eine Weise beschriftet, die für Externe erkennen lässt, um welche Räume oder Adresse es sich handelt. Falls ein Schlüssel verloren geht, wird das sofort dem Vorstand mitgeteilt. Die Schlüssel werden nicht ohne Rücksprache mit dem Vorstand an Dritte weitergegeben oder ausgeliehen.

[Für Vereinsräume, in denen es Publikumsverkehr gibt oder in denen Mitglieder ein und aus gehen, die keinen Zugriff auf personenbezogene oder sonstige vertrauliche Daten brauchen:]

* Personenbezogene Daten oder sonstige vertrauliche Dokumente (zum Beispiel Mitgliederkontakte, Anmeldelisten für eine Veranstaltung, Honorarverträge etc.) dürfen nicht in öffentlich zugänglichen Räumen herumliegen, sondern nur in separat abschließbaren Räumen oder sicheren Aktenschränken aufbewahrt werden, die nicht unbeaufsichtigt offenstehen. Gäste dürfen in diese Räume nur in Begleitung. Das betrifft auch Personen, die Handwerksarbeiten oder Wartungen durchführen.

[Sollte es einen Serverraum geben:]

* Auch der Serverraum ist grundsätzlich abgeschlossen.

[Generell:]

* Werden personenbezogene Daten nicht mehr gebraucht, werden sie nicht einfach in den Papierkorb geworfen, sondern geschreddert oder kommen in den Sammelbehälter für die sichere Aktenvernichtung.
* Die Eingangstür zu den Vereinsräumen wird immer abgeschlossen, sobald die letzte Person die Räume verlässt.

[ENTWEDER: Wenn ihr keine Checkliste an der Innenseite der Tür angebracht habt, hier auflisten, was am Ende des Tages zu bedenken ist:]

* Vorher hat diese Person die Aufgabe zu kontrollieren, ob alle Fenster richtig geschlossen sind und ob die Kaffeemaschine und der Drucker [ggf. weitere Geräte einfügen] ausgeschaltet sind. Auf diese Weise werden die Räume gegen unbefugten Zutritt geschützt, aber auch gegen Regen, Sturm oder einen Brand durch defekte Geräte.

[ODER: Wenn ihr eine Checkliste an der Innenseite der Tür angebracht habt:]

* Vorher geht diese Person die Checkliste an der Innenseite der Eingangstür durch (Fenster schließen, Geräte ausschalten etc.). Auf diese Weise werden die Räume gegen unbefugten Zutritt geschützt, aber auch gegen Regen, Sturm oder einen Brand durch defekte Geräte.

-----------------------------------------------------------------------------------------------------------------------------------

**Baustein Passwörter (für alle Vereine sinnvoll, die auch digital arbeiten)**
Wie sorgt ihr für effektiven Passwortschutz im Rahmen eurer Vereinsarbeit? Welche Regeln gelten für die Einrichtung und Nutzung von Passwörtern sowie für die Nutzung von Zwei-Faktor-Authentisierung?

🡪 Als Vorstand kümmert ihr euch um diese Voraussetzungen:

* Ihr sorgt dafür, dass einzelne Engagierte möglichst individuelle Accounts und eigene Passwörter nutzen können. Dies gilt für E-Mail-Accounts ebenso wie im Hinblick auf Accounts für die Pflege der Webseite und der Social-Media-Kanäle oder für die Vereins-Cloud. So könnt ihr bei Beendigung des Engagements für den Verein durch das gezielte Abschalten einzelner Accounts einfach sicherstellen, dass Personen zu Vereinsaccounts keinen Zugang mehr haben. Außerdem könnt ihr so einzelnen Accounts gezielt nur die jeweils nötigen Berechtigung erteilen (siehe auch die Ausführungen zum Rechte- und Rollenkonzept im Abschnitt zur Vereins-Cloud).
* Ihr richtet – wenn möglich – einen Passwortmanager auf Vereinsgeräten ein oder stellt Engagierten eine Lizenz zur Nutzung auf privaten Geräten zur Verfügung oder sprecht eine klare Empfehlung für einen kostenfreien Passwortmanager aus, wenn im Verein für mehrere unterschiedliche Anwendungen Passwörter erforderlich sind und es schwierig wird, sich diese alle zu merken. Mehr Informationen zu sicheren Passwörtern als auch der Nutzung eines Passwortmanagers stellt zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereit unter: <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager_node.html>.
* Ihr entscheidet, ob ihr allgemein oder für bestimmte Programme (zum Beispiel die Vereins-Cloud) zur Nutzung von Zwei-Faktor-Authentisierung verpflichtet oder ermutigt. Das kann gerade bei besonders sensiblen Daten eine sinnvolle Maßnahme sein, um den Zugang zusätzlich abzusichern. Mehr Informationen zum Thema bietet bspw. das BSI: <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html>.

Zum Umgang mit Passwörtern

Passwörter haben den Zweck, ein Gerät oder ein Programm vor unbefugtem Zugriff zu schützen. Damit sie diesen Zweck erfüllen können, müssen Passwörter sicher und geheim sein.

* *Sicher* bedeutet, dass Passwörter bestimmte Sicherheitsstandards erfüllen (je länger und komplexer sie sind, desto sicherer sind sie).
Passwörter, die in unserem Verein genutzt werden, sollten daher (wenn technisch möglich):
* mindestens 8 Zeichen lang sein
* aus Groß- und Kleinbuchstaben bestehen
* Ziffern enthalten
* Sonderzeichen (!"§$%&/()=?`) enthalten

Zudem dürfen Passwörter:

* keinen persönlichen Bezug besitzen (wie Namen, Geburtstag, usw.)
* kein Wort sein, das in identischer Schreibweise in Wörterbüchern vorkommt

***Tipp für ein sicheres Passwort, das man sich gut einprägen kann:***Man überlegt sich einen Satz, z. B.: "Samstags fahre ich immer gut gelaunt um 10 Uhr ins Vereinsbüro & trinke erst mal Kaffee!" Die Anfangsbuchstaben, alle vorkommenden Zahlen und Satzzeichen sind nun das Passwort: Sfiiggu10UiV&temK!

* *Geheim* bedeutet, dass Passwörter nicht weitergegeben oder zugänglich gemacht werden dürfen (zum Beispiel dürfen sie nicht auf einem Zettel am Bildschirm oder an der Pinnwand notiert werden).

[Solltet ihr im Verein die Nutzung eines Passwortmanagers vereinbart haben:]

* Um den sicheren, geheimen und einfachen Umgang mit den zahlreichen Passwörtern für unsere Vereinszugänge zu ermöglichen, haben wir uns als Verein für die verpflichtende Nutzung eines Passwortmanagers entschieden, der auch automatisch komplexe und lange Passwörter generiert.

[Generell gilt:]

* Passwörter für Vereins-Accounts dürfen nicht im eigenen Browser (zum Beispiel Firefox oder Chrome) gespeichert werden.
* Es darf immer nur ein Passwort für je einen Account und eine Funktion genutzt werden (das E-Mail-Passwort darf zum Beispiel nicht auch für den Account zur Pflege der Webseite oder einen privaten Account genutzt werden).
* Um den Zugang zu unserer Vereins-Cloud und unseren E-Mail-Accounts zusätzlich abzusichern, ist hier eine Zwei-Faktor-Authentisierung erforderlich/sollte möglichst eine Zwei-Faktor-Authentisierung genutzt werden. Zwei-Faktor-Authentisierung bedeutet, dass zusätzlich zu einem Passwort zum Beispiel eine zusätzliche Anmeldebestätigung erteilt oder ein Zahlencode eingegeben werden muss.

-----------------------------------------------------------------------------------------------------------------------------------

**Baustein Vereins-Cloud (wenn ihr für eure Vereinsarbeit eine Cloud nutzt):**Wie schützt ihr eure Vereinsdaten in der Cloud? Stellt euch eure Vereins-Cloud als eure virtuellen Vereinsräume vor und prüft, wie ihr sie am besten gegen Einbruch und Diebstahl absichern könnt.

🡪 Als Vorstand kümmert ihr euch um diese Voraussetzungen:

* Es sollten keine privaten Cloud-Accounts für die Vereinsarbeit genutzt werden.
* Ihr legt also fest, welche Cloud für alle Vereinsaktivitäten genutzt wird, und schließt als Verein mit dem Anbieter einen Auftragsverarbeitungsvertrag ab (siehe Praxisratgeber „Auftrags­ver­arbeiter auswählen“: <https://stiftungdatenschutz.org/ehrenamt/praxisratgeber/praxisratgeber-detailseite/auftragsverarbeiter-auswaehlen-268> sowie das Webinar „Daten sicher in der Cloud speichern“ der Stiftung Datenschutz, das auch generell viele Hintergrundinformationen zum Thema Vereins-Cloud bereithält: <https://stiftungdatenschutz.org/ehrenamt/webinare/webinare-detailseite/datenschutz-im-ehrenamt-daten-sicher-in-der-cloud-speichern-231>).
* Ihr prüft die Grundeinstellungen in eurer Cloud (im Bereich „Administration“ oder „Nutzungsverwaltung“ oder ähnliches) und passt sie an: Vorgaben für sichere Passwörter (siehe Abschnitt zu Passwörtern), Standard-Einstellungen für Freigaben etc. (siehe auch die Sicherheitsempfehlungen des BSI: <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cloud-Computing-Sicherheitstipps/cloud-computing-verbraucher_node.html>).
* Ihr schreibt ein Rechte- & Rollenkonzept auf: Wer braucht für welche Tätigkeit im Verein Zugang zu welchen personenbezogenen Daten? Anhand dieser Frage legt ihr für die verschiedenen Rollen im Verein (Vorstand, Schatzmeister\*in, Mitgliederverwaltung, sonstige\*r Aktive\*r etc.) jeweils passende Zugangsberechtigungen in der Vereins-Cloud fest und weist sie den jeweiligen konkreten Personen zu, die diese Rollen derzeit ausfüllen. Zum Beispiel braucht eine ehrenamtliche Kursleitung in der Regel keinen Zugriff auf die Bankdaten der Mitglieder, die Mitgliederverwaltung hingegen schon. Diese Einstellungen könnt ihr in der Regel im Bereich „Administration“ oder „Nutzerverwaltung“ in der Cloud vornehmen.
* Ihr legt in der Cloud eine Ordnerstruktur an, die gut nachvollziehbar ist und die sich eignet, um euer Rechte- & Rollenkonzept praktisch umzusetzen (damit auf bestimmte Daten nur bestimmte Personen zugreifen können, müssen diese Daten in einem separaten Ordner gespeichert werden, damit der Zugriff auf diesen Ordner gezielt erteilt werden kann). Je nachdem, wie komplex eure Ordnerstruktur wird, kann es sinnvoll sein, ein paar Hinweise zur Nutzung aufzuschreiben (zum Beispiel zur Benennung von Dateien und zu den wichtigsten Speicherorten und der dazugehörigen Ablagelogik) und gut sichtbar in der Cloud zu speichern, damit sie jederzeit nachgelesen werden können und die Ordnerstruktur im Alltag nicht nach und nach unterlaufen wird.
* Ihr stellt als Verein für alle Aktiven entsprechend des Rechte- und Rollenkonzeptes und der dazugehörigen Ordnerstruktur die passenden individuellen und passwortgeschützten Zugänge bereit.
* Ihr kümmert euch darum, dass von den Daten in eurer Cloud regelmäßig eine Sicherungskopie (Backup) erstellt wird. Wie häufig ein Backup stattfindet, könnt ihr anhand der Frage entscheiden: Wie problematisch wäre es, wenn die Änderungen des letzten Tages/der letzten Woche/des letzten Monats verloren gingen? Backups können ggf. von eurem Cloud-Anbieter vorgenommen werden (fragt im Zweifel dort nach), es kann auch eine Person aus dem Vorstand regelmäßig eine Sicherungskopie der Cloud auf einer externen verschlüsselten Festplatte speichern und diese verschlossen aufbewahren. Wichtig ist, dass ihr wisst, wie ihr an die Sicherungskopie kommt und eure Daten möglichst schnell und ohne Verluste wiederherstellen könnt, falls in der Cloud Daten zum Beispiel versehentlich gelöscht oder auch bei einem Hacker-Angriff mutwillig zerstört werden.

Zur Nutzung der Vereins-Cloud

* Die individuellen Zugangsdaten zur Vereins-Cloud dürfen nicht an andere Personen weitergeben werden.
* Wenn auf die Vereins-Cloud zugegriffen wird, muss eine sichere Internetverbindung dafür genutzt werden (keine offenen WLANs wie zum Beispiel im Café oder im Zug ohne VPN-Verbindung nutzen).
* Die Ordnerstrukturen, die der Verein vorgibt, sollten eingehalten werden und personenbezogene Daten möglichst datensparsam gespeichert werden. Wenn außerhalb der Cloud an Dateien gearbeitet werden muss, die für die Vereinsarbeit wichtig sind, sollten diese so bald wie möglich in die Vereins-Cloud hochgeladen und lokal wieder gelöscht werden. Es sollten dauerhaft keine Vereins-Dateien außerhalb der Vereins-Cloud gespeichert werden. So lassen sich Parallelstrukturen vermeiden und die Daten können nicht verloren gehen (da der Vorstand organisiert hat, dass die Daten in der Cloud regelmäßig mit einem Backup gesichert werden).
* Wenn Daten aus der Cloud mit externen Personen geteilt werden, darf nur die relevante Datei (nicht der ganze Ordner, falls er nicht extra dafür angelegt wurde) für die Dauer der erwartbaren Zusammenarbeit freigegeben werden. Wenn eine Datei nur über die Cloud übermittelt werden soll (und nicht gemeinsam in der Cloud daran gearbeitet wird), sollte sich die Freigabe auf Leserechte bzw. das Herunterladen der Datei begrenzen.
* Private Daten dürfen grundsätzlich nicht in der Vereins-Cloud gespeichert werden.

-----------------------------------------------------------------------------------------------------------------------------------

**Baustein Vereinsgeräte (wenn ihr als Verein technische Geräte zur Verfügung stellt)**Wie sorgt ihr dafür, dass die personenbezogenen Daten auf Vereinsgeräten vor Angriffen geschützt werden?

🡪 Als Vorstand kümmert ihr euch um diese Voraussetzungen:

* Ihr dokumentiert, an wen Vereinsgeräte ausgegeben werden. Insbesondere behaltet ihr im Blick, dass ihr ausgegebene Vereinsgeräte bei Beendigung des Engagements für den Verein wieder zurückerhaltet.
* Ihr kümmert Euch um die Einrichtung von Standardprogrammen für eure Vereinsarbeit, Updates, ggf. einen VPN-Zugang für mobiles Arbeiten und eine Geräteverschlüsselung sowie einen Passwortmanager (siehe Abschnitt zu Passwörtern).
* Ihr überprüft, dass Firewall und Virenschutz des Betriebssystems aktiv sind oder installiert zusätzliche Programme hierfür.
* Ihr nutzt die Anpassung von Standardeinstellungen, um die Sicherheit zu erhöhen: zum Beispiel durch die Einstellung einer automatischen Sperrung des Bildschirms nach höchstens 10 Minuten Inaktivität und die weitestmögliche Aktivierung automatisierter Updates.
* Wenn euch im Verein die Kompetenzen für die Einrichtung und Absicherung der Geräte fehlen, gibt es neben externen Dienstleister\*innen auch Schulungen und Handreichungen, die – teils kostenlos oder mit Fördermöglichkeiten – zur Verfügung stehen (siehe zum Beispiel die Überblicksseiten des BSI <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html> und <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html>.

**Zur Nutzung von Vereinsgeräten und Datenträgern (Laptops, Smartphones, Tablets, USB-Sticks, Festplatten…) sowie zum Umgang mit Vereinsdokumenten**

* Die standardmäßigen Schutzmaßnahmen, die auf den Vereinsgeräten bei Erhalt voreingestellt sind, dürfen ohne Rücksprache mit dem Vorstand nicht deaktiviert oder deinstalliert werden. Ohne Genehmigung durch den Vorstand dürfen keine zusätzlichen Programme bzw. Handy-Apps installiert werden.
* Da sich Viren, Schadprogramme und Angriffsstrategien stetig ändern, müssen auch die Schutzmaßnahmen regelmäßig angepasst werden. Automatische Updates des Betriebssystems (z. B. Windows oder Android), des Virenschutzprogramms und anderer Programme müssen daher zeitnah zugelassen werden, damit die Sicherheit des Geräts nicht gefährdet wird.
* Festplatten oder USB-Sticks mit sensiblen Vereinsdaten oder Backups müssen verschlüsselt werden.
* Die Vereinsgeräte dürfen nur für Vereinszwecke verwendet werden. Eine Privatnutzung ist nur nach ausdrücklicher Genehmigung durch den Vorstand zulässig.
* Wenn Geräte in einem ungesicherten Netzwerk genutzt werden (zum Beispiel in offenen WLANs wie im Café oder im Zug), muss auf eine sichere Verbindung geachtet oder eine VPN-Verbindung genutzt werden. Wenn ein privates WLAN genutzt werden soll, dann muss das WLAN mit einem sicheren Passwort (siehe Abschnitt zu Passwortsicherheit) und einem aktuellen Verschlüsselungsstandard geschützt sein.
* Wenn in öffentlichen Räumen für den Verein gearbeitet wird (zum Beispiel im Café oder Zug), dann muss darauf geachtet werden, dass keine Bildschirmeinsicht für Unbefugte besteht und dass bei Gesprächen oder Telefonaten Dritte keine vertraulichen Informationen mithören können.
* Wenn Geräte wie Laptops unbeaufsichtigt gelassen werden, müssen sie gesperrt werden (bei Windowsrechnern z. B. mit der Tastenkombination Windowstaste + L für „Lock“) oder – vor allem bei längerer Abwesenheit – heruntergefahren werden, damit unbefugte Personen nicht auf Daten auf dem Gerät (oder in der Cloud, die über das Gerät zugänglich ist) zugreifen können.
* Damit Geräte nicht gestohlen werden, sollten sie möglichst verschlossen bzw. in verschlossenen Räumen aufbewahrt werden, wenn sie gerade nicht in Verwendung sind.
* Wenn Vereinsgeräte oder Dokumente trotzdem einmal gestohlen werden oder verloren gehen, muss das so schnell wie möglich dem Vorstand gemeldet werden (siehe Abschnitt zur Meldung von Datenpannen & Kontaktdaten).
* Ausdrucke von Vereinsdokumenten oder E-Mails sowie Notizen mit sensiblen Informationen zu Vereinsaktivitäten sind vertraulich zu behandeln, möglichst sicher aufzubewahren und – wenn sie nicht mehr benötigt werden – über das Vereinsbüro, eine Aktenvernichtung oder mithilfe eines Aktenschredders sicher zu entsorgen.
* Wenn das Engagement für den Verein beendet wird, müssen alle erhaltenen Vereinsgeräte und Vereinsdokumente zurückgegeben werden.

-----------------------------------------------------------------------------------------------------------------------------------

**Baustein Privatgeräte (wenn die Aktiven in eurem Verein (auch) ihre privaten Geräte für die Vereinsarbeit nutzen)**Wie regelt ihr, dass Vereinsdaten sicher und für die Aufgaben im Verein auffindbar bleiben?

🡪 Als Vorstand kümmert ihr euch um diese Voraussetzungen:

* Ihr unterstützt eure Aktiven bei Bedarf bei der Absicherung ihrer Geräte, die sie für die Vereinsarbeit nutzen, zum Beispiel bei der Einrichtung eines Passwortschutzes und ggf. Passwortmanagers (siehe den Abschnitt zu Passwörtern) und bei der Einrichtung einer Verschlüsselung des Geräts, einer Firewall, eines Virenschutzprogramms und von Standardprogrammen für eure Vereinsarbeit sowie ggf. eines VPN-Zugangs zum Schutz bei der Nutzung ungesicherter WLANs. Dies gilt auch für die Anpassung von Standardeinstellungen, um die Sicherheit zu erhöhen, zum Beispiel durch die Einstellung einer automatischen Sperrung des Bildschirms nach höchstens 10 Minuten Inaktivität und die weitestmögliche Aktivierung automatisierter Updates.
* Falls auf Vereinsdaten mittels einer Internetverbindung zugegriffen wird (und dies ist heutzutage sehr häufig der Fall, zum Beispiel, wenn ihr eine Cloud nutzt oder sich Aktive mit ihren Geräten in das Vereins-E-Mail-Postfach einloggen oder eure Webseite pflegen), stellt ihr dafür einen VPN-Zugang bereit oder verpflichtet eure Aktiven dazu, keine unsicheren Internetverbindungen (zum Beispiel offene WLANs im Zug oder im Café) zu nutzen und unterstützt sie ggf. dabei, ihr WLAN zuhause durch ein sicheres Passwort abzusichern.
* Wenn euch im Verein die Kompetenzen für die technische Unterstützung eurer Aktiven fehlen, gibt es neben externen Dienstleister\*innen auch Schulungen und Handreichungen, die – teils kostenlos oder mit Fördermöglichkeiten – zur Verfügung stehen (siehe zum Beispiel die Überblicksseiten des BSI <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html> und <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html>.
* Ihr trefft die Entscheidung, in welcher Struktur Vereinsdaten von euren Aktiven auf ihren Geräten verarbeitet werden, damit eine Trennung der Vereinsdaten von privaten Daten gewährleistet werden kann – ob ihr dafür zum Beispiel eine Vereins-Cloud einrichtet, was für die Zusammenarbeit in der Regel die sinnvollste Option sein wird (siehe Abschnitt zu Cloud), oder ob Aktive dafür separate geschützte Ordner auf ihren Geräten einrichten sollen. Bei der zweiten Option müsst ihr euch unbedingt überlegen, wie diese Vereinsdaten regelmäßig durch Backups gesichert werden können und wie ihr als Verein darauf zugreifen könnt, falls das Gerät gestohlen wird oder verloren geht oder das Gerät aus anderen Gründen nicht mehr zur Verfügung steht (zum Beispiel bei ungeplanter längerer Abwesenheit, plötzlichem Ausscheiden aus dem Verein oder auch Tod der Person, der das Gerät gehört).

**Zur Nutzung von privaten Geräten und Datenträgern (Laptops, Smartphones, Tablets, USB-Sticks, Festplatten…) für die Vereinsarbeit sowie zum Umgang mit Vereinsdokumenten**

* Private Geräte, die für die Vereinsarbeit zum Einsatz kommen, müssen grundsätzlich gegen Viren, Schadprogramme etc. abgesichert werden. Wendet euch für die aktuellen Anforderungen und eine Unterstützung bei der Umsetzung an unsere Ansprechperson für IT-Fragen (siehe Abschnitt zu Ansprechpersonen).
* Da sich Viren, Schadprogramme und Angriffsstrategien stetig ändern, müssen auch die Schutzmaßnahmen aktuell gehalten werden. Automatische Updates des Betriebssystems (z. B. Windows oder Android), des Virenschutzprogramms und anderer Programme müssen daher zeitnah zugelassen werden, damit die Sicherheit des Geräts und somit auch der Vereinsdaten darauf nicht gefährdet wird.
* Festplatten oder USB-Sticks mit sensiblen Vereinsdaten oder Backups müssen verschlüsselt werden.
* Wenn Geräte in einem ungesicherten Netzwerk genutzt werden (zum Beispiel in offenen WLANs wie im Café oder im Zug), muss auf eine sichere Verbindung geachtet oder eine VPN-Verbindung genutzt werden. Wenn ein privates WLAN genutzt werden soll, dann muss das WLAN mit einem sicheren Passwort (siehe Abschnitt zu Passwortsicherheit) und einem aktuellen Verschlüsselungsstandard geschützt sein.
* Wenn in öffentlichen Räumen für den Verein gearbeitet wird (zum Beispiel im Café oder Zug), dann muss darauf geachtet werden, dass keine Bildschirmeinsicht für Unbefugte besteht und dass bei Gesprächen oder Telefonaten Dritte keine vertraulichen Informationen mithören können.
* Wenn Geräte wie zum Beispiel Laptops oder Smartphones, die für die Vereinsarbeit zum Einsatz kommen, unbeaufsichtigt gelassen werden, müssen sie gesperrt werden (bei Windowsrechnern z. B. mit der Tastenkombination Windowstaste + L für „Lock“) oder – vor allem bei längerer Abwesenheit – heruntergefahren werden, damit unbefugte Personen nicht auf Daten auf dem Gerät (oder in der Cloud, die über das Gerät zugänglich ist) zugreifen können.
* Damit Geräte nicht gestohlen werden, sollten sie möglichst verschlossen bzw. in verschlossenen Räumen aufbewahrt werden, wenn sie gerade nicht in Verwendung sind.
* Wenn Geräte, über die ein Zugang zu Vereinsdaten möglich ist, oder Vereinsdokumente gestohlen werden oder verloren gehen, muss das so schnell wie möglich unserer Ansprechperson für Datenschutz gemeldet werden (siehe Abschnitte zu Ansprechpersonen sowie zu Melde- und Hinweispflichten zum Datenschutz).
* Ausdrucke von Vereinsdokumenten oder E-Mails sowie Notizen mit sensiblen Informationen zu Vereinsaktivitäten sind vertraulich zu behandeln, möglichst sicher aufzubewahren und – wenn sie nicht mehr benötigt werden – über das Vereinsbüro, eine Aktenvernichtung oder mithilfe eines Aktenschredders sicher zu entsorgen.
* Wenn das Engagement für den Verein beendet wird, müssen alle Daten zur Vereinsarbeit an den Verein übergeben und auf den eigenen Geräten gelöscht sowie alle Vereinsdokumente an den Verein zurückgegeben werden.

-----------------------------------------------------------------------------------------------------------------------------------

**Baustein E-Mails (wenn ihr E-Mail-Kommunikation im Rahmen eurer Vereinsarbeit nutzt)**E-Mails sind ein viel genutztes Einfallstor für Computervirenangriffe oder Versuche, sich Login-Daten für kriminelle Zwecke zu beschaffen (sogenanntes Phishing). Zudem besteht bei E-Mails ein erhöhtes Risiko, dass vertrauliche Daten versehentlich an falsche Empfänger\*innen geschickt werden. Wie geht ihr mit diesen Risiken um?

🡪 Als Vorstand kümmert ihr euch um diese Voraussetzungen:

* Wenn ihr auf eurer Webseite o. ä. eine Kontaktmöglichkeit per E-Mail anbietet, dann veröffentlicht nur so viele E-Mail-Adressen wie nötig, da diese leicht zugänglich und somit auch für kriminelle Zwecke automatisch auslesbar sind. Vermeidet die Veröffentlichung personalisierter E-Mail-Adressen (besser sind sogenannte Funktionspostfächer wie „mitgliederbetreuung@musterverein.org“ oder „info@musterverein.org“) und vermeidet insbesondere die Veröffentlichung privater E-Mail-Adressen.
* Auch wenn ihr die Veröffentlichung personalisierter E-Mail-Adressen vermeiden solltet: Richtet möglichst für alle, die im Zusammenhang mit ihrem Engagement für den Verein per E-Mail kommunizieren, personalisierte und mit individuellen Passwörtern geschützte Vereins-E-Mailadressen ein (zum Beispiel „b.beispielname@musterverein.org“). Somit ist sowohl intern als auch nach außen die Zugehörigkeit zum Verein erkennbar und eine gezielte Kommunikation zwischen einzelnen Aktiven möglich. Die Vereinskommunikation kann auf diese Weise zudem vom privaten E-Mail-Postfach getrennt stattfinden.
* Ihr sorgt dafür, dass insbesondere Personen, die sich um veröffentlichte Vereins-E-Mail Adresse(n) kümmern, für mögliche Risiken sensibilisiert und im Erkennen möglicher Phishing-E-Mails oder Virenquellen geschult werden.
* Ihr prüft, ob die Einrichtung eines zusätzlichen Backups für die Vereins-E-Mail-Postfächer sinnvoll ist.
* Ihr regelt im Verein welche zusätzlichen Schutzmaßnahmen für den elektronischen Versand besonders sensibler Informationen genutzt werden sollen und übt bspw. das Einrichten eines Passwortschutzes für angehängte Dateien oder das Freigeben von Dokumenten in der Vereins-Cloud.
* Ihr prüft, für welche Zwecke und auf welcher Rechtsgrundlage mehrerer Personen angeschrieben werden dürfen und klärt alle Aktiven darüber auf. Richtet ggf. einen Verteiler (bestenfalls mit automatisierter Widerrufmöglichkeit) ein oder nutzt ein Newsletter-Tool (siehe Praxisratgeber „Newsletter“), für das ein Auftragsverarbeitungsvertrag abgeschlossen wurde.

Zur Nutzung von E-Mail-Kommunikation

[Wenn ihr Vereins-E-Mail-Adressen nutzt:]

* Vereins-E-Mail-Adressen sind nur für die Vereinskommunikation zu nutzen. Eine private Nutzung – auch eine automatisierte Weiterleitung von Vereins-E-Mails an private E-Mail-Adressen – ist ausdrücklich untersagt.

[Wenn ihr die Nutzung privater E-Mail-Adressen für Vereinszwecke und interne Absprachen erlaubt:]

* Bei der Nutzung privater E-Mail-Adressen ist gründlich zwischen der Nutzung für Vereinszwecke und der privaten Nutzung zu unterscheiden: E-Mails, deren Inhalt sowie die dazugehörigen E-Mail-Adressen, die im Zusammenhang mit dem Vereins-Engagement erhalten werden, dürfen nur in diesem Rahmen und nicht für private oder anderweitige Zwecke verarbeitet werden.
* E-Mails dürfen grundsätzlich nur weitergeleitet werden, wenn dies erlaubt ist (wenn also die vereinsinterne Bearbeitung einer Anfrage es erfordert oder der Weiterleitung explizit zugestimmt wurde). Dies gilt auch für E-Mails, bei deren Beantwortung zusätzliche Empfänger\*innen angeschrieben werden.
* E-Mails an mehrere Personen, die nicht über eine Mailingliste oder ein Newsletter-Tool (auch) an externe Empfänger\*innen versendet werden, dürfen nur nach Absprache in mit sichtbaren Empfänger\*innen (als An/CC) verschickt werden, und sonst nur in Blindkopie (in BCC), so dass die Empfänger\*innen die E-Mail-Adressen der anderen Personen nicht sehen können.
* Sensible Daten dürfen nur zusätzlich abgesichert versandt oder anderen zugänglich gemacht werden: Es muss entweder eine Ende-zu-Ende-Verschlüsselung der E-Mail (bspw. via PGP), ein Passwortschutz für schützenswerte Dokumente im Anhang oder eine gezielte Freigabe einzelner Cloud-Dateien genutzt werden, die bestenfalls zeitlich begrenzt wird. Dazugehörige Passwörter sollten immer über einen anderen Kanal (zum Beispiel telefonisch) übermittelt werden.
* Beim Erhalt von E-Mails mit Anhängen oder Links ist Vorsicht geboten, da diese Viren oder Schadprogramme enthalten können. Besteht Unsicherheit, ob die Absende-Adresse vertrauenswürdig ist oder sich überhaupt wirklich die behauptete Quelle der Nachricht dahinter verbirgt, sollte unbedingt Rücksprache gehalten werden, bevor Anhänge geöffnet oder verlinkte Seiten aufgerufen werden (siehe Abschnitt zur Meldung von Datenpannen & dazugehörige Ansprechperson). Insbesondere ist äußerstes Misstrauen angebracht, wenn per E-Mail zum Login zum Beispiel ins Online-Banking oder in einen anderen Account des Vereins aufgefordert wird, ohne dass der Anlass dafür nachvollziehbar ist, da es sich hier um einen Versuch handeln kann, Zugangsdaten zu erbeuten.
* Bei aller Vorsicht: Fehler können passieren. Wenn ein vermutlich schadhafter E-Mail-Anhang geöffnet oder einer vermutlich trügerischen Handlungsaufforderungen gefolgt wurde (zum Beispiel Einloggen in Online-Banking des Vereins), muss dies unverzüglich gemeldet werden – nur so können wir den möglichen Schaden begrenzen und uns ggf. um die Entfernung von Computerviren/schadhafter Software kümmern (siehe Abschnitt zur Meldung von Datenpannen & dazugehörige Ansprechperson).

-----------------------------------------------------------------------------------------------------------------------------------

**Baustein Fotos im Vereinsalltag**Bei den meisten Vereinen werden zu verschiedenen Anlässen und für unterschiedliche Zwecke Fotos gemacht und teils veröffentlicht oder unter Vereinsaktiven geteilt. Fotos (sowie auch Video- und Tonaufnahmen), auf denen Personen erkennbar sind, sind personenbezogene Daten. Wie beachtet ihr beim Erstellen und Veröffentlichen oder Teilen solcher Aufnahmen im Rahmen eurer Vereinstätigkeiten die datenschutzrechtlichen Vorgaben?

🡪 Als Vorstand kümmert ihr euch um diese Voraussetzungen:

* Ihr verschafft Euch einen Überblick, zu welchen Anlässen, für welche Zwecke und auf welcher Rechtsgrundlage in eurem Verein üblicherweise Fotos gemacht werden und wie das Recht auf Widerspruch umgesetzt werden kann (siehe hierzu den Praxisratgebers „Fotos und Datenschutz“, der euch bei diesem komplexen Thema wertvolle Unterstützung bietet: <https://stiftungdatenschutz.org/ehrenamt/praxisratgeber/praxisratgeber-detailseite/fotos-und-datenschutz-275>).
* Ihr legt fest, wer im Namen des Vereins Fotos für mögliche unterschiedliche Vereinszwecke anfertigt und welche Regeln diese Personen dabei beachten müssen (eine separate Auflistung kann dabei sinnvoll sein, da sich die unten vorgeschlagenen Regeln an alle Vereinsaktiven wenden und nicht speziell an die „Vereins-Fotograf\*innen“). Mit diesen Personen geht Ihr auch gründlich die Informationspflichten und Voraussetzungen durch, die beim Fotografieren für den Verein relevant sind.
* Ihr sensibilisiert dafür, wo ggf. erhöhte Risiken eine Rolle spielen. Von erhöhten Risiken ist zum Beispiel bei Bildern von Kindern oder Jugendlichen auszugehen, aber auch dann, wenn Fotos Hinweise auf besonders schützenswerte Informationen geben können, wie etwa auf Gesundheitsdaten (gerade bei manchen Selbsthilfegruppen, in denen Anonymität gewünscht ist) oder auf religiöse oder weltanschauliche Überzeugungen (siehe auch den Praxisratgeber „Umgang mit besonderen Datenkategorien“: <https://stiftungdatenschutz.org/ehrenamt/praxisratgeber/praxisratgeber-detailseite/besondere-datenkategorien-272>).
* Ihr stellt sicher, dass auch alle Personen, die im Namen des Vereins Fotos veröffentlichen dürfen (zum Beispiel auf der Webseite, über Social-Media-Kanäle, in der Vereinszeitung etc.), über diese Datenschutzanforderungen und Regeln informiert sind.
* Ihr legt eine Person fest, an die sich Vereinsaktive wenden können, wenn sie im Namen des Vereins Fotos machen oder veröffentlichen möchten.
* Vergesst auch nicht, festzulegen, in welchem Rahmen und auf welchen Wegen (Messengergruppe, E-Mails, geschlossene Social-Media-Gruppen, Vereins-Cloud etc.) ***innerhalb*** des Vereins Fotos geteilt werden dürfen und welche Regeln dabei gelten. Denkt dabei auch daran, dass Aufnahmen nicht immer dauerhaft gespeichert werden sollten (und zum Beispiel ein Ablaufdatum und Löschfristen für einen Ordner zum Teilen von Fotos sinnvoll sein können).

Zum Umgang mit Fotos

[ENTWEDER: Wenn ihr das Anfertigen von Fotos bei euren Vereinsaktivitäten unter bestimmten Voraussetzungen erlaubt]

Es ist uns im Verein wichtig, dass wir verantwortungsvoll fotografieren und verantwortungsvoll mit Fotos (und ebenso mit Video- und Tonaufnahmen) umgehen:

* Auch wenn es im Verein freundschaftliche Verbindungen geben kann und sehr verständlich ist, dass gemeinsame Aktivitäten gern zur eigenen Erinnerung fotografiert oder gefilmt werden: ***Fotos im Rahmen einer Vereinstätigkeit sind keine privaten Fotos***. Es gilt hier keine sogenannte „Haushaltsausnahme“ wie zum Beispiel für Fotos bei Familienfeiern. Auch hier sind also datenschutzrechtliche Anforderungen zu beachten. Wichtig: Schon beim Aufnehmen von Bildern, auf denen Personen zu erkennen sind, werden deren Daten verarbeitet, auch wenn die Aufnahmen nicht veröffentlicht werden.
* Grundsätzlich gilt dabei: Jede Person hat das Recht auf ihr eigenes Bild. Wenn jemand also nicht fotografiert werden möchte und dies zum Ausdruck bringt, dann wird dies respektiert.
* Damit alle dieses Recht auch wahrnehmen können, werden Fotos nur gemacht, wenn dies deutlich sichtbar ist und die betroffenen Personen es erwarten können (zum Beispiel Fotos von Sport-Turnieren, Reden und Preisverleihungen). Heimliche Aufnahmen sind nicht erlaubt.
* Es muss nicht nur erwartbar sein, dass Fotos gemacht werden. Es muss auch erwartbar sein, wofür die Bilder genutzt werden sollen. Wenn Fotos gemacht werden, müssen die betroffenen Personen also vorher darüber informiert werden (also zum Beispiel, dass jemand ein Foto zur privaten Erinnerung oder zum Teilen in einer vereinsinternen Messenger-Gruppe machen möchte). Es dürfen ohne Einwilligung auch keine vereinsinternen Bilder an Dritte weitergeleitet werden.
* Kinder und Jugendliche dürfen nur mit Einwilligung der Eltern bzw. Sorgeberechtigten fotografiert werden, wenn sie auf den Bildern zu erkennen wären. Denn bei Kindern und Jugendlichen wird grundsätzlich von einem erhöhten Schutzbedarf ausgegangen.
* Bevor ein Foto gemacht, intern geteilt oder veröffentlicht wird, sollte man sich auch immer die einfache Kontrollfrage stellen: Wäre das für mich selbst in Ordnung, wenn ich auf diese Weise auf einem Foto zu sehen wäre? Denn es kann (zum Beispiel bei einer Vereinsfeier) durchaus zu Aufnahmen kommen, die den betroffenen Personen im Nachhinein peinlich sein könnten, selbst wenn diese vorher angekündigt wurden.
* Sollte einmal der Fall eintreten, dass im Nachhinein über die Verwendung eines Fotos für einen anderen Zweck nachgedacht wird (zum Beispiel, wenn ein Foto zu vereinsinternen Zwecken gemacht und in der internen Messenger-Gruppe geteilt wurde und nun für eine öffentliche Vereinschronik oder zum Teilen auf Social-Media-Kanälen interessant wäre), dann müssen die abgebildeten Personen und die Person, die das Bild gemacht hat, vorher um ihre Einwilligung gebeten werden.
* Personen, die auf Fotos zu sehen sind, haben das Recht, jederzeit gegen die Verarbeitung eines Fotos Widerspruch einzulegen oder eine erteilte Einwilligung zurückzuziehen. Wenn es im Vereinskontext zu einem solchen Widerspruch oder einem Widerruf einer Einwilligung kommt, nachdem ein Bild bereits veröffentlicht wurde, so muss die Ansprechperson zu Datenschutzfragen unverzüglich informiert werden, so dass das weitere Vorgehen gemeinsam geklärt werden kann.
* Im Rahmen unserer Vereinsarbeit haben einige Personen die Aufgabe übernommen, für den Verein die Bilder zu machen, die wir nutzen, um unsere Aktivitäten öffentlichkeitswirksam zu dokumentieren (Webseite, Social-Media-Kanäle, Vereinsberichte, Spendenaufrufe) oder um sie offiziell unter Mitgliedern zu teilen (zum Beispiel Pinnwand im Vereinsbüro, Vereinsheft, Mitglieder-Newsletter, Powerpoint auf der Mitgliederversammlung). Wenn Interesse daran besteht, Fotos ***im Namen des Vereins*** zu machen oder zu veröffentlichen, dann muss dies vorher mit PERSON X / VORSTAND abgesprochen werden.

[ODER: Wenn ihr das Anfertigen von Fotos bei euren Vereinsaktivitäten grundsätzlich untersagt (zum Beispiel sinnvoll bei Selbsthilfegruppen, in denen Anonymität gewünscht ist)]

* Aufgrund der sensiblen Informationen (wie zum Beispiel Gesundheitsdaten, die schon aus der Zugehörigkeit zu unserem Verein hervorgehen), die im Zusammenhang mit unseren Vereinsaktivitäten stehen, ist das Fotografieren von erkennbaren Personen im Vereinskontext grundsätzlich untersagt.

Anlage 2:

**Regelung zur Vertraulichkeit zum Schutz von Vereinsinterna**

🡪 Als Vorstand kümmert ihr euch um folgende Voraussetzungen:

* Ihr prüft, ob es im Rahmen eurer Vereinsarbeit vertrauliche Interna gibt, die nicht personenbezogen sind, und die daher eine gesonderte Vertraulichkeitserklärung erforderlich machen und wer ggf. darauf Zugriff hat. Sollte es vertrauliche Interna geben und nur wenige Personen Zugriff darauf haben, dann braucht ihr auch nur von diesen Personen die Verpflichtung zur Vertraulichkeit. Sollte es keine vertraulichen Interna geben, so braucht ihr diese Anlage nicht und könnt die Verweise darauf löschen.
* Ihr prüft, welche Informationen innerhalb des Vereins vertraulich behandelt werden müssen, da eine Offenlegung der Information zu einem möglichen Schaden für den Verein führen könnte (auch wenn es sich nicht um personenbezogene Daten handelt).
* Ihr legt fest, wie ihr entsprechende Informationen als vertraulich kennzeichnet oder interne Absprachen als solche erkennbar macht (zum Beispiel durch den Hinweis „VERTRAULICH“ in einem Protokoll). Ihr könnt eure Vereinsablage auch grundsätzlich als vertraulich einstufen und Ausnahmen wie das erforderliche Teilen von Dokumenten mit externen Vereinspartner\*innen regeln.

In unserem Verein gibt es vertrauliche Informationen (Vereinsinterna), die man in einem Unternehmen als „Geschäftsgeheimnisse“ bezeichnen würde. Über diese Informationen ist Stillschweigen zu bewahren, um einen möglichen Schaden für den Verein zu vermeiden. Vereinsinterna dürfen externen Personen also nicht unerlaubt in Gesprächen oder auf anderem Wege mitgeteilt werden.

Zu den Vereinsinterna in unserem Verein gehören:

* Protokolle nicht öffentlicher Sitzungen,
* nicht veröffentlichte Projektplanungen oder Projektberichte,
* nicht veröffentlichte Ideen für Fundraising-Aktionen,
* Details zu unserer technischen Infrastruktur,
* …

sowie

* alle weiteren Informationen, die schriftlich oder mündlich als vertraulich gekennzeichnet werden.

***Ausgenommen*** von der Verpflichtung zur Vertraulichkeit sind selbstverständlich Informationen, die zur Meldung möglicherweise strafrechtlich relevanter Vorgänge im Verein an die jeweiligen Behörden oder Meldestellen übermittelt werden. Weitere Ausnahmen finden sich in §5 des Gesetzes zum Schutz von Geschäftsgeheimnissen (<https://www.gesetze-im-internet.de/geschgehg/__5.html>).

[NUR WENN euer Verein Angestellte hat:]

***Ebenfalls ausgenommen*** von der Verpflichtung zur Vertraulichkeit ist die Offenlegung von Informationen durch Arbeitnehmer\*innen gegenüber der Arbeitnehmer\*innenvertretung, wenn dies erforderlich ist, damit diese ihre Aufgaben erfüllen kann.