

10.11.2018
SK Groß-Gerau e.V.

Die neue DS-GVO: Datenschutz im Verein

Dr. Frank Weller

Ihr Referent

Dr. Frank Weller

- Rechtsanwalt + Mediator in Hohenahr
 - Vereinsrecht, Ehrenamts- und Freiwilligenrecht
 - Datenschutz, Internet und Social Media
- Vorsitzender Landesausschuss Recht, Steuern, Versicherungen
Landessportbund Hessen e.V. (lsbh) von 2009 – 2018
- Vizepräsident Vereinsmanagement lsbh seit 2018
- Vereins-(Vorstands-)mitglied
- Mitautor der Bücher
 - Datenschutz für Vereine
 - Erfolgreiches Fundraising für Kitas
 - Gutes einfach verbreiten – Handbuch für erfolgreichen Projekttransfer (E-Book) <https://opentransfer.de/e-book-gutes-einfach-verbreiten/>

Arbeitshilfen

- <http://www.lsbh-vereinsberater.de/datenschutz/neues-datenschutzrecht/>
- <https://datenschutz.hessen.de/datenschutz/vereine>
- <https://www.lda.bayern.de/de/kleine-unternehmen.html>

Ausgangspunkt

Die „Erfindung“ des Datenschutzes



- 1983: „Volkszählungsurteil“ des Bundesverfassungsgerichts
- **Grundrecht auf informationelle Selbstbestimmung** als Teil des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 GG)
 - ➔ maßgeblich: Grundsatz der Verhältnismäßigkeit
 - ➔ **Datenvermeidung + -sparsamkeit**

www.ehrenamt-europa.eu

Roter Faden



- Datenverarbeitung immer zu einem bestimmten Zweck
- ➔ um diesen Zweck zu erreichen:
 - nur so viele Daten wie nötig
 - so wenige Daten wie möglich verarbeiten

www.ehrenamt-europa.eu

Begrifflichkeiten

Begriffsbestimmungen (Art. 4 DS-GVO)



personenbezogene Daten:

alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen

Datenschutz gilt für personenbezogene Daten

- Informationen, die einen
- bestimmten oder bestimmbaren (identifizierbaren)
- lebenden
- Menschen (nicht: juristische Person wie z.B. Verein, GmbH, AG)
- näher beschreiben

www.ehrenamt-europa.eu

Beispiele für personenbezogene Daten

Name, Adresse, Familienstand,
Geburtsdatum, Staatsangehörigkeit,
Vertrags- und Besitzverhältnisse,
Beruf, Partei- + Vereinsmitgliedschaften,
Überzeugungen, Aussehen,
Eigenschaften, Krankheiten, ...

www.ehrenamt-europa.eu

Begriffsbestimmungen



Verarbeitung:

jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

www.ehrenamt-europa.eu

Rechtsgrundlage für DV

Gesetze

- Europäische Datenschutz-Grundverordnung (DS-GVO) ab 25.05.2018
 - ➔ unmittelbar geltendes Recht in Ländern der EU
- Bundesdatenschutzgesetz (BDSG) neue Fassung
 - ➔ der DS-GVO untergeordnet, darf nur Regelungen in Bereichen treffen, in denen die DS-GVO das erlaubt oder lückenhaft ist
- Telemediengesetz (TMG) für Angebote im Internet
 - Verhältnis zu DS-GVO strittig!

Art. 2 DS-GVO i.V.m. § 2 BDSG (neu)

Diese Verordnung gilt für die ganz oder teilweise **automatisierte** Verarbeitung personenbezogener Daten sowie für die **nichtautomatisierte** Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

„**Dateisystem**“ ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird (Art. 4 Nr. 6 DS-GVO)

§§ 1 Absatz 2, 2 Abs. 4 BDSG (neu)

Für **nichtöffentliche Stellen** gilt dieses Gesetz für die ganz oder teilweise **automatisierte** Verarbeitung personenbezogener Daten sowie die **nichtautomatisierte** Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

Rechtsgrundlage für Datenverarbeitung nach DS-GVO (Art. 6 DS-GVO)

Datenverarbeitung ist rechtmäßig, wenn ...

- ... die Einwilligung der betroffenen Person vorliegt
- Art. 6 (1) a) - oder
- ... die Verarbeitung für die Erfüllung eines **Vertrags [Mitgliedschaft im Verein]** mit der betroffenen Person erforderlich ist - Art. 6 (1) b) - oder
- ... die Verarbeitung zur Durchführung **vorvertraglicher** Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist - Art. 6 (1) b) – oder ...

DV ist rechtmäßig, wenn ...

- ... die Verarbeitung zur Wahrung der **berechtigten Interessen des Vereins** erforderlich ist,
- **sofern nicht** die Interessen oder Grundrechte und Grundfreiheiten der **betroffenen Person** überwiegen,
- insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt - Art. 6 (1) f -.

Erwägungsgrund 47

Bei der Abwägung „sind die **vernünftigen Erwartungen** der betroffenen Personen, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen.

²Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht.

³.....,wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, **vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird.**

⁴Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise **nicht mit einer weiteren Verarbeitung rechnen muss**, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen.

Was ist im Verein erlaubt?

Grundsatz

Erlaubt ist

Datenverarbeitung, die
für den
Vereinszweck
unbedingt erforderlich ist,
ohne die ein
geregeltes Funktionieren des Vereins
also nicht möglich ist



Auf welche Daten kann ein Verein nicht verzichten?



- Name und Anschrift des Mitglieds
- Eintrittsdatum
- Funktionen im Verein
- TelNr/E-Mail Vorstandsmitglied
- Bankverbindung bei SEPA-Einzug gem. Satzung
- Geburtsdatum
(Satzung fragen: z.B. für Stimmrecht bei Volljährigkeit oder Altersklasse im Sport)
- E-Mail-Adr. allgemein, wenn Satzung E-Mail zulässt oder verlangt

www.ehrenamt-europa.eu

Wozu werden Daten gebraucht (Zweck der Datenverwendung) ?



Wichtige Unterscheidung:

- **interne Vereinsverwaltung, -organisation!**
 - Funktionieren des Vereins nach innen
 - *Erheben + Speichern* von Daten
- oder
- **Übermittlung** an „Dritte“, z.B.
 - ➔ Vereinszeitung, lokale Presse
 - ➔ Webseite
 - ➔ Verband

www.ehrenamt-europa.eu

Datenübermittlung an „Dritte“: Was ist damit gemeint?



- Wer ist **Dritter**?
 - Personen außerhalb des Vereins
 - **unbefugte** Personen **innerhalb** des Vereins, weil deren Kenntnis unnötig ist
- Übermittlung an Dritte weitaus problematischer als interne Nutzung, weil Personen Kenntnis erlangen, die ursprünglich keine Kenntnis hatten bzw. unbefugt waren

www.ehrenamt-europa.eu

www.ehrenamt-europa.eu

Datenübermittlung: Wann erlaubt?



Zulässig bei Daten (Texte und Fotos) im Zusammenhang mit öffentlichen Vereinsveranstaltungen

- soweit für Öffentlichkeitsarbeit/Außendarstellung notwendig
- weil Teilnehmer/Besucher damit rechnen müssen
 - Berichte im Zusammenhang mit Sportfesten, Wettkämpfen bei Sportvereinen, Chorauftritten von Gesangsvereinen, Dichterlesungen, Ausstellungen bei Kulturvereinen usw. je nach Satzungszweck (etwa Ankündigungen, Verlaufsberichte, Spielberichte + -ergebnisse, Ergebnislisten, auch mit Fotos Teilnehmer + Zuschauer etc.)

→ **betrifft also Satzungszweck Öffentlichkeitsarbeit**

Hinweis: Auf dieser Veranstaltung werden Fotos gemacht. Möglicherweise sind Zuschauer und Teilnehmer auf diesen Fotos erkennbar. Es ist beabsichtigt, die Fotos im Internet zu veröffentlichen (z.B. Homepage, Facebook und andere soziale Medien). Zuständig:.....

Datenübermittlung/-veröffentlichung: Wann erlaubt?

- **zulässig** meist bei Sportvereinen:
 - Teilnehmerlisten, Aufstellungen (am besten passwortgeschützter/interner Bereich)
 - Meldungen an Verband (am besten passwortgeschützter/interner Bereich)
 - Spielergebnisse, Torschützen etc.
 - Daten im Zusammenhang mit Sport- und anderen öffentlichen Vereinsveranstaltungen (Ankündigungen, Verlaufsberichte)
- **betrifft also Satzungszwecke:**
Mitgliederverwaltung, Sportbetrieb,
Öffentlichkeitsarbeit für Sportbetrieb

Besonderheit: Fotos und Persönlichkeitsrecht

- schützt die Privat- und Intimsphäre
- Stichwort „**Recht am eigenen Bild**“
(§§ 22 f. Kunsturhebergesetz, KUG)

Frage:

- Gilt das KUG vom 09. Januar 1907 weiterhin neben der DS-GVO?
- unterschiedliche Meinungen
 - KUG besteht auch nach DS-GVO fort, zumindest im Rahmen der Abwägung nach Art.6 (1) f) weiter zu berücksichtigen (wohl überwiegende Auffassung)

Kunsturhebergesetz

- Grundsatz: für Verbreitung/Veröffentlichung von Fotos immer **Einwilligung der fotografierten Person** erforderlich,
- wenn keine Ausnahme greift ...

Fotos: Keine Einwilligung erforderlich,
wenn ...

- Foto **zeitgeschichtliche Bedeutung** hat
(auch örtlich/regional);
es genügt **aber** nicht, wenn allein die Person/en
(z.B. Bürgermeister) zeitgeschichtlich interessant
ist/sind, vielmehr muss das Ereignis mit dieser/n
Person/en zeitgeschichtlich von Interesse sein
ja: Bgm besucht Vereinsjubiläum
nein: Bgm kauft privat Schuhe

Keine Einwilligung , wenn ... (2)

- **Person = TeilnehmerIn an Versammlung, Aufzug;**
Veranstaltung muss im Vordergrund stehen,
keine zufällige Gruppenbildung
- öffentliche Vereinsveranstaltungen?
 - unter zeitgeschichtliches Ereignis oder Versammlung
einzuordnen (Sportveranstaltung),
 - soweit für Öffentlichkeitsarbeit/Außendarstellung notwendig
 - zumal Teilnehmer/Besucher damit rechnen müssen

Noch zu beachten:

- Rechtsprechung betrachtet satzungsgemäße Vereinsveranstaltungen meist als zeitgeschichtliche Ereignisse.
- Ausnahme von der Ausnahme: Es darf in keinem Fall **ein berechtigtes Interesse** der abgebildeten Person oder, falls diese verstorben ist, ihrer Angehörigen verletzt werden, insbesondere darf man Personen nicht in herabwürdigender Weise fotografieren (siehe folgende Folie)
- Gerichte: Abwägung auf mehreren Ebenen

Abwägung gemäß Art. 6 (1) f DS-GVO führt zum gleichen Ergebnis:

- Datenverarbeitung (Foto, Bericht, Ergebnisliste) zur Wahrung der **berechtigten Interessen des Vereins** erforderlich (Öffentlichkeitsarbeit)
- Interessen, Grundrechte und Grundfreiheiten der **betroffenen Personen** überwiegen nicht, auch weil sie mit Fotos etc. rechnen müssen, wenn sie öffentl. Veranstaltg. besuchen
- Rechte von Kindern?

Einwilligung bei Bezahlung und nach dem Tod

- Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, dass er sich abbilden ließ, eine Entlohnung erhielt (§ 22 KunstUrhG)
- nach dem Tod des Abgebildeten bedarf es bis zum Ablauf von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten (§ 22)

Der Hessische Datenschutzbeauftragte (1):

Was ist beim **Umgang mit Bildern** zu beachten?

„ ... Über Veranstaltungen darf auch ohne ausdrückliche Einwilligung textlich und bildlich berichtet werden, wenn dabei die Veranstaltung im Vordergrund steht und Einzelpersonen nicht abgebildet werden. Ohne Einwilligung dürfen auch Ergebnisse veröffentlicht werden.“

Der Hessische Datenschutzbeauftragte (2):

Einwilligung erforderlich? Veröffentlichung im Internet?

Nein, wenn „ ... Berichterstattung über öffentlichen Wettkampf oder öffentliche Veranstaltung. Für die Bekanntgabe von Wettkampfergebnissen ist dann auch in der Regel keine Einwilligung erforderlich.“

Der Hessische Datenschutzbeauftragte (3):

Dürfen **Wettkampfergebnisse** veröffentlicht werden?

Ergebnisse von öffentlichen Wettkämpfen dürfen in der Regel auch ohne die ausdrückliche Zustimmung der Teilnehmer veröffentlicht werden. ... Im Einzelfall kann ein Teilnehmer begründen, welches besondere schutzwürdige Interesse einer Veröffentlichung seiner personenbezogenen Daten (Name und Vereinszugehörigkeit) entgegenstehen könnte. Dem sollte dann gefolgt werden.

„Datenschutz im Verein“

https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/20180613_Datenschutz%20im%20Verein_3.pdf

Datenübermittlung/-veröffentlichung:



Nur mit Einwilligung/Satzungsregelung:

- Ehrungen,
- Gratulationen
- Übermittlungen aus wirtschaftlichen Gründen (Sponsoring)
- nicht-öffentliche Veranstaltungen (Fotos!)

www.ehrenamt-europa.eu

Sonderfall Mitgliederliste



- Mitglied kann Herausgabe **zur Wahrnehmung Mitgliedsrechte** verlangen
(z.B. Minderheitenrechte wie Sammlung von Stimmen für a.o. MV, auch Teilnahmerecht)
 - ➔ Daten an Treuhänder zwecks Nutzung?
 - ➔ Papierform oder Datei?
 - ➔ welche Daten genau? Für den Zweck notwendige D.
 - ➔ Erklärung abgeben: zweckgemäße Verwendung und spätere Löschung

Dr. Frank Weiler
Rechtsanwalt

www.ehrenamt-europa.eu

... Mitgliederliste



Weiteres Beispiel:

BGH 21.06.2010, II ZR 219/09:

Opposition verlangt Herausgabe an
Treuhand, der Positionspapier versenden soll
→ Teilnahmerecht der Mitglieder

Näheres: <http://www.weller-hilft.de/index.php?id=118>

Dr. Frank Weller
Rechtsanwalt

www.ehrenamt-europa.eu

Verarbeitung besonderer Kategorien von Daten



Art. 9 DS-GVO

Die **Verarbeitung personenbezogener Daten**, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person **ist untersagt**.

www.ehrenamt-europa.eu

Verarbeitung besonderer Kategorien von Daten

ausnahmsweise erlaubt u.a.:

- Einwilligung der betroffenen Person
- DV bezieht sich nur auf Mitglieder oder ehemalige Mitglieder eines gemeinnützigen Vereins und die personenbezogenen Daten werden nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt
- die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat
- DV zur Geltendmachung, Ausübung von Rechtsansprüchen erforderlich

www.ehrenamt-europa.eu

Einwilligung

Einwilligung des Betroffenen (Art. 7 DS-GVO)



- freiwillige Entscheidung
- vorherige Aufklärung über Zweck der Erhebung, Verarbeitung, Nutzung
- Hinweis auf Widerrufsmöglichkeit + Folgen d. Verweigerung
- Einwilligung widerrufbar (Form wie Einwilligung)
- Verein ist beweispflichtig für Einwilligung
- Schriftliche Einwilligung und Belehrung: Ersuchen um Einwilligung muss in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

www.ehrenamt-europa.eu

Technische und organisatorische Maßnahmen (Datensicherheit)

- Art. 32 DS-GVO

Sicherheit der Verarbeitung (Art. 32 DS-GVO)

Berücksichtigung:

- Stand der Technik
- Kosten
- Art, Umfang, Umstände + der Zwecke der Verarbeitung
- Welches Risiko besteht?

Ziel: ein dem Risiko angemessenes Schutzniveau

Beispiele von Zielsetzungen + Maßnahmen:

- **Verschlüsselung** personenbezogener Daten
- Fähigkeit, die Verfügbarkeit der personenbezogenen Daten bei einem **physischen oder technischen Zwischenfall** rasch **wiederherzustellen**

www.ehrenamt-europa.eu

Praxisbeispiele

- Möglichst wenige Personen sollten Zugang zu Daten bzw. PC haben.
 - ➔ konkrete Benennung des Personenkreises mit jeweiliger Zugangsberechtigung (Wer darf auf welche Daten zugreifen? Wer darf an den PC?)
- Verhinderung des körperlichen Zugangs durch Abschließen des jeweiligen Raums, in dem sich die DV-Anlagen befinden.
- Verhinderung des technischen Zugangs durch passwortgeschützte Bereiche

www.ehrenamt-europa.eu

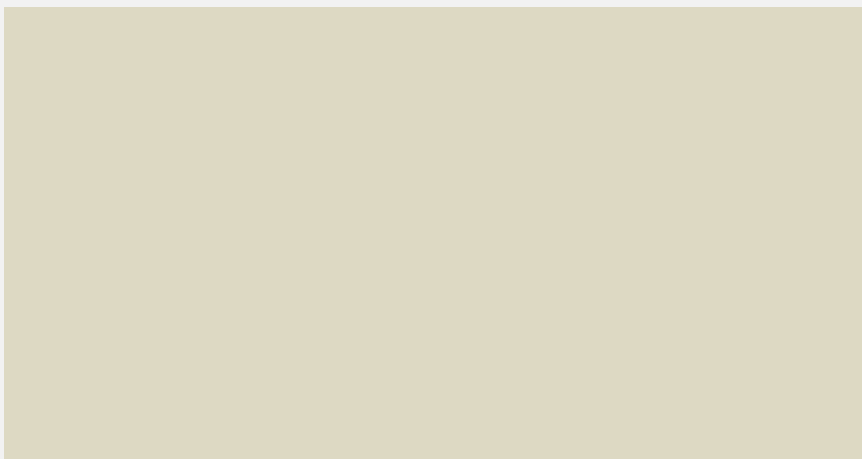
Praxisbeispiele (2)



- möglichst sichere Kommunikation wenigstens innerhalb des Vorstands (E-Mails nur über Vereins-Account, End-zu-End-Verschlüsselung)
- Bei Webseiten mit Kommunikation mit dem Nutzer: Hypertext Transfer Protocol Secure (**HTTPS**, englisch für „sicheres Hypertext-Übertragungsprotokoll“) verwenden (Kommunikationsprotokoll im World Wide Web, um Daten abhörsicher zu übertragen.)
- keine veraltete Software, regelmäßig Updates aufspielen
- zeitnahe Datensicherung

www.ehrenamt-europa.eu

Verzeichnis der Verarbeitungstätigkeiten



Verzeichnis der Verarbeitungstätigkeiten (1)



- Diese Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn die Verarbeitung erfolgt nicht nur gelegentlich.
- Genau dies tun jedoch Vereine in aller Regel: Sie verarbeiten ständig (also nicht nur gelegentlich) Daten der Mitglieder.

➔ Vereine müssen das Verzeichnis anlegen

www.ehrenamt-europa.eu

Verzeichnis der Verarbeitungstätigkeiten (2)



Schriftlich oder elektronisch ist ein internes Verzeichnis anzulegen:

- Name und Kontaktdaten des Verantwortlichen (Verein) und ggf. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- Verarbeitungszwecke (Mitgliederverwaltung, Satzungszweck - z.B. Sportbetrieb -, Öffentlichkeitsarbeit, eventuell Erfüllung vertraglicher Zwecke, eventuell Durchführung Arbeitsverhältnis, Newsletterbestellung)
- Von wem stammen die Daten (Kategorien betroffener Personen)? (Mitglieder, Eltern, Teilnehmer an Schnupperkursen, Übungsleiter, eventuell Arbeitnehmer etc.)
- Was für Daten sind dies? (Adressdaten, Geburtsdatum, Bankverbindung, Eintrittsdatum, event. Daten aus Führungszeugnis etc.)

www.ehrenamt-europa.eu

Verzeichnis (2)



- An wen werden die Daten weitergegeben? (intern: Vorstand, Abteilungsleiter, Geschäftsstelle; extern: Fachverbände, Isbh, Homepage, Öffentlichkeit, eventuell Steuerbüro XY etc.)
- vorgesehene Lösungsfristen für die jeweiligen Daten (z.B. 2 Jahre nach Beendigung der Mitgliedschaft, 3 Monate nach Volljährigkeit werden Daten der Eltern gelöscht, 1/2 Jahr nach Beendigung ÜL-Vertrags), soweit keine gesetzlichen, vertragsmäßigen oder satzungsmäßigen Aufbewahrungsfristen entgegen stehen
 - Regelung in Satzung möglich
 - Einzelfallvereinbarung möglich

www.ehrenamt-europa.eu

Verzeichnis (3)



- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Datensicherheit (Art. 32):

z.B.: Zutritt zur Geschäftsstelle nur dann, wenn autorisierte Mitarbeiter sich dort aufhalten; Passwortschutz für PC und Laptop; nur 3 Personen haben Zutritt zum PC und zu den Daten; regelmäßiges Aufspielen von Software-Updates; Verfügbarkeit nach techn. Zwischenfall durch Backup-System; Datenschutzerklärungen in Satzung oder auf Website etc.
- Muster:

https://www.lida.bayern.de/media/muster_1_verein_verzeichnis.pdf

www.ehrenamt-europa.eu

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einblick in das Thema „Verzeichnis von Verarbeitungstätigkeiten“ gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.bayern.de/media/061_muster_vov_verantwortlicher.pdf abrufbar.



Bayerisches Landesamt für
Datenschutzaufsicht

Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
TSV Waldemühl e.V.
Steinbaust. 45a
98123 Sordshausen

Kontakt:
Tel. 0961/123456-0
E-Mail: team@waldemueller-tsv.de
Web: www.waldemueller-tsv.de

Vorstand: Dieter Eckbauer-Düppels, geb. 03.12.1952

Verarbeitungstätigkeit	Anspruchspartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personalisierten Daten	Kategorie von Empfänger	Drittlands-Transfer	Löschrufen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Herbert Bauer 0961/123456-1 herbert@waldemueller-tsv.de	02.03.2018	- Auszahlung der Löhne/Gehälter - Abfuhr Sozialabgaben u. Steuern	Beschäftigte	- Name und Adressen der Beschäftigten - ggf. Religionszugehörigkeit - Einmalige Kennzahlen zur Steuer-/Sozialabgaben	Externer Dienstleister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Mitgliederverwaltung	Herbert Bauer 0961/123456-1 herbert@waldemueller-tsv.de	02.03.2018	Verwaltung der Vereinstätigkeiten	Mitglieder	- Name und Adressen - Eintrittsdatum - Sportbereiche	Keine	Keine	2 Jahre nach Beendigung der Vereinsmitgliedschaft	Siehe IT-Sicherheitskonzept
Betrieb der Webseite des Sportvereins (über Hosting-Dienstleister)	Max Meier 0961/123456-0 ma@waldemueller-tsv.de	28.02.2018	Außenanstellung	- Mitglieder - Webseitenbesucher	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept + HTTPS-Verschlüsselung
Veröffentlichung von Fotos der Mitglieder auf der Webseite	Max Meier 0961/123456-0 ma@waldemueller-tsv.de	20.02.2018	Außenanstellung	Mitglieder	Fotos von Vereinstätigkeiten	Keine	Keine	Wenn Einwilligung widerrufen - unverzüglich	Siehe IT-Sicherheitskonzept
Betragsverwaltung	Herbert Bauer 0961/123456-1 herbert@waldemueller-tsv.de	22.02.2018	Vereinsfinanzierung	Mitglieder	Bankverbindung	Steuerberater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)

- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virenschutz/Sicherheitssoftware

- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder

Ansprüche des Mitglieds

Ansprüche des Betroffenen (Mitglied) auf ...



- Auskunft (Art. 15 DS-GVO)
- Berichtigung (Art. 16 DS-GVO)
- Löschung (Recht auf Vergessenwerden; Art. 17 DS-GVO)
- Einschränkung der Verarbeitung (Art. 18 DS-GVO; siehe auch § BDSG)

www.ehrenamt-europa.eu

Auskunft



Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und u.a. auf folgende Informationen:

- Verarbeitungszwecke
- Art der Daten
- etwaige Empfänger
- Herkunft
- Dauer Speicherung
- 1 Kopie oder gängiges elektr. Format kostenlos

www.ehrenamt-europa.eu

Berichtigung



Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die **Berichtigung** sie betreffender unrichtiger personenbezogener Daten zu verlangen. ²Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die **Vervollständigung** unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

www.ehrenamt-europa.eu

Anspruch auf Löschung, wenn ...



- Verarbeitung **nicht rechtmäßig**
- Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind
- Widerspruch gegen die Datenverarbeitung rechtmäßig erhoben wurde
- Einwilligung widerrufen wurde
- etc.

- **Einschränkung der Verarbeitung** statt Löschung unter bestimmten Voraussetzungen (z.B. gesetzliche, vertragliche oder satzungsmäßige Aufbewahrungsfristen)
 - ➔ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken (Art. 4 Nr. 3)

www.ehrenamt-europa.eu

Ansprüche des Betroffenen (Mitglied) auf ...



- Mitteilung der Berichtigung, Löschung etc. (Art. 19 DSGVO)

Der Verantwortliche teilt allen Empfängern, denen personenbezogenen Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

www.ehrenamt-europa.eu

Auftragsverarbeitung

Auftragsverarbeitung Art.28 DS-GVO

- Sofern der Verein personenbezogene Daten im Auftrag verarbeiten lässt (beispielsweise Mitgliederverwaltung in der Cloud, Aufbau und Wartung der EDV, Buchhaltung, Gehaltsabrechnung), muss zwischen dem Verein und dem Auftragnehmer ein **Auftragsverarbeitungsvertrag** geschlossen werden (Art. 28 Abs. 3 DS-GVO)

Vertragsinhalt

- Welche Daten von welchen Personen sollen wie verarbeitet werden?
- Weisungsbefugnisse des Vereins
- Verpflichtung zur Vertraulichkeit und Gewährleistung der Sicherheit
- Kontrollrechte des Vereins, etwa unangemeldete Kontrollen vor Ort
- Regelungen zur Beendigung des Vertrages, Rückgabe oder Löschung von Daten
- etc.

Pannenmeldung

Meldung von Pannen (Art. 33 Abs. 1 DSGVO)

- Datenschutzpannen wie Datenlecks, Hacking, gestohlene oder verlorengangene Datenträger sind unverzüglich und möglichst innerhalb von 72 Stunden nach Bekanntwerden der Aufsichtsbehörde zu melden.

Informationspflichten

Informationspflichten nach Art. 12 EU-DSGVO - allgemein

- Der für die Verarbeitung Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen [...] die sich auf die Verarbeitung personenbezogener Daten beziehen, in **präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.**

Informationspflichten nach Art. 13 EU-DSGVO - konkret

- Vereinsname und Kontaktdaten des Verantwortlichen im Verein und seines Stellvertreters;
- Kontaktdaten des Datenschutzbeauftragten, wenn vorhanden;
- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen (z.B. Mitgliederverwaltung, Sportbetrieb)
- Rechtsgrundlage für Verarbeitung (z.B. Art. 6 (1) b oder f DSGVO)
- Empfänger oder mögliche Empfänger, an welche die Daten (möglicherweise) weitergegeben werden (z.B. Verband)
- Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung der Speicherdauer;

Information über „Pflichtdaten“

- ... ob Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte
 - Abgrenzung Pflichtdaten > < freiwillige Angaben
 - z.B.: Welche Daten muss ich bereitstellen, um Vereinsmitglied zu werden (Pflichtangaben?)
 - Welche Angaben sind freiwillig?

Information über „unsichere Staaten“

- Art. 45 ff.: Übermittlung von Daten nur zulässig,
 - in ein Land der EU
 - ein Land mit angemessenem Schutzniveau gemäß Beschluss der Kommission oder
 - aufgrund Einwilligung unter Hinweis auf Risiken

- Problemfall USA
 - „Privacy Shield“ (Vertrag mit EU)
 - Unternehmen können sich nach diesem Vertrag zertifizieren lassen
 - <https://www.datenschutz-notizen.de/ist-das-privacy-shield-bald-geschichte-3020811/>

Informationspflichten - Belehrungen

Ihre Rechte:

Sie haben im Rahmen der geltenden gesetzlichen Bestimmungen das Recht auf Auskunft über Ihre gespeicherten personenbezogenen Daten (Art. 15 DS-GVO) sowie auf Berichtigung (Art. 16 DS-GVO), Löschung (Art. 17 GS-DVO), Einschränkung der Verarbeitung (Art. 18 GS-DVO), Widerspruch gegen die Verarbeitung (Art. 21 DS-GVO) und Datenübertragbarkeit (Art. 20 DS-GVO). Diese Rechte können Sie schriftlich oder per E-Mail bei dem oben genannten Verantwortlichen geltend machen.

Belehrungen über Rechte

Sie können eine bereits erteilte Einwilligung jederzeit widerrufen. Der Widerruf kann schriftlich oder per E-Mail an den oben genannten Verantwortlichen gesandt werden.*

Die Rechtmäßigkeit der bis zum Widerruf erfolgten Datenverarbeitung bleibt vom Widerruf unberührt.

* Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein (Art. 7 Abs. 3 Ds-GVO).

Belehrungen über Rechte

Beschwerderecht bei der zuständigen Aufsichtsbehörde

Falls Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten gegen die DS-GVO verstößt, steht Ihnen das Recht zur Beschwerde bei einer Aufsichtsbehörde zu, insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes.

Das Beschwerderecht besteht unbeschadet anderweitiger verwaltungsrechtlicher oder gerichtlicher Rechtsbehelfe.

Zuständige Aufsichtsbehörde im Land ist:

.....

[weitere Kommunikationsdaten]

Ausnahme von Informationspflichten

- Die Informationspflichten bestehen **nicht**, wenn und soweit die betroffene Person bereits über die Informationen verfügt (Art. 13 Abs. 4 DS-GVO).

Form der Information

- Art. 12 DS-GVO verlangt, dass die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache unentgeltlich mitgeteilt werden.
- Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch, z. B. per E-Mail und/oder auf der Homepage, soweit damit alle Anforderungen erfüllt sind.
- Insbesondere auf die leichte Zugänglichkeit muss bei elektronischer Darstellung geachtet werden.
- Beim Verstoß gegen die Informationspflichten droht eine Geldbuße.

Datenschutzbeauftragter

Datenschutzbeauftragter (Art. 37 ff. DS-GVO,
§ 38 BDSG neu) ...



ist vom Verein zu benennen,

- wenn in der Regel **mindestens 10** Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten **beschäftigt** werden

Datenschutzbeauftragter



- **beschäftigt in diesem Sinne:**
jede(r), der (die)
im Auftrag des Vereins
regelmäßig
personenbezogene Daten
automatisiert verarbeitet
- egal, ob als Ehrenamtler(in) oder gegen Vergütung
im Verein tätig

www.ehrenamt-europa.eu

Datenschutzbeauftragter



- also z.B.:
 - Vorstandsmitglieder
 - Abteilungsleiter
 - Webmaster
 - externe Dienstleister

und ...

www.ehrenamt-europa.eu

Datenschutzbeauftragter



... auch: Schreibkräfte, Kursleiter
Übungsleiter etc.,
die lediglich aus DV stammende Angaben
nutzen (z.B. Adressen, Teilnehmerlisten)

www.ehrenamt-europa.eu

Achtung neu:

- „Datenverarbeiter“ müssen im Rahmen der automatisierten Datenverarbeitung tätig sein,
 - ➔ also Daten in elektronischer Form
erfassen, speichern, verändern, auslesen, abfragen,
verwenden, übermitteln, offenlegen,
verbreiten, abgleichen, löschen etc.
- Übungsleiter z. B. „beschäftigt mit DV“, wenn sie Daten
über Mitglieder in elektronischer Form erhalten (etwa per
E-Mail), nicht aber, wenn sie papiernen Ausdruck
bekommen

Datenschutzbeauftragter



- **nicht** bestellt werden dürfen
 - Mitglieder des Vorstands oder
 - für die Datenverarbeitung des Vereins verantwortliche Personen/EDV-Leiter

www.ehrenamt-europa.eu

Datenschutzbeauftragter



Der Datenschutzbeauftragte wird auf der Grundlage insbesondere des **Fachwissens** benannt, das er **auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis** besitzt (Art 37, 39 DS-GVO)

- ➔ abhängig von Art und Umfang der DV
 - welche Daten?
 - besonders sensible?
 - wie viele?
 - welche Risiken?

www.ehrenamt-europa.eu

Stellung des DSB (Art. 38 DS-GVO)



- Vereinsvorstand unterstützt den DSB (Ressourcen werden gestellt, Zugang zu allen DV-Vorgängen etc.).
- DSB erhält im Zusammenhang mit seinen Aufgaben keine Weisungen.
- DSB berät Vorstand und berichtet diesem.
- Betroffene können DSB zu Rate ziehen; DSB ist zur Vertraulichkeit verpflichtet.
- DSB hat keine Entscheidungsbefugnisse bei Ausübung seiner Aufgaben.

www.ehrenamt-europa.eu

Aufgaben des DSB (Art. 39 DS-GVO)



- Beratung des Vorstands und der mit DV Beschäftigten
- Überwachung der Einhaltung der Datenschutzgesetze
- Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter
- Zusammenarbeit mit der Aufsichtsbehörde

www.ehrenamt-europa.eu

Haftung des DSB



- wenn unentgeltlich (höchstens € 720/Jahr):
 - ➔ § 31 b BGB (Haftung für Vorsatz und grobe Fahrlässigkeit)
- Verpflichtung zur korrekten Beratung

www.ehrenamt-europa.eu

Wenn kein Datenschutzbeauftragter ...



- benannt werden muss,
hat der Vereinsvorstand
die Aufgaben des Datenschutzbeauftragten
sicherzustellen

t

www.ehrenamt-europa.eu

Datengeheimnis

Früher: Datengeheimnis (§ 5 BDSG alte Fassung)

- Mit Datenverarbeitung befasste* Personen dürfen Daten nicht unbefugt verarbeiten (**Datengeheimnis**).
*wie vorher bei DSB
- Sie waren bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten!
- Belehrung + Abgabe Bestätigung, dass man das Datengeheimnis kennt und beachtet

Heute: Keine Regelung mehr für nicht öffentliche Stellen (Vereine), aber dennoch unbedingt zu empfehlen:

https://www.lida.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf

(Bayerisches Landesamt für Datenschutzaufsicht; mit Muster)

Datenschutzerklärung Homepage

Hilfen

zum Beispiel:

- <https://datenschutz-generator.de/>
- <https://www.wbs-law.de/it-recht/datenschutzrecht/datenschutzerklaerung-generator/>

Weitere Infos

- www.ehrenamt-europa.eu oder
- www.weller-hilft.de
 - ➔ jeweils **Forum Ehrenamt**
 - dort Magazin/Datenschutz** oder ...



- Infos zu(m)
 - Vereins- + Freiwilligenrecht
 - Datenschutz + Telemediengesetz
 - Fundraising
 - Fördermittel u.v.m.

- Kostenlos registrieren - anmelden - **loslegen!**

www.ehrenamt-europa.eu

Herzlichen Dank!

THE
END!



- Europäisches Institut für das Ehrenamt
Inhaber: Dr. Frank Weller
www.ehrenamt-europa.eu

- Rechtsanwalt | Mediator Dr. Weller
www.weller-hilft.de
- Ser-Ve Organisationsberatung
Inhaberin: Karin Buchner
www.ser-ve.de

www.ehrenamt-europa.eu