

30-03-2019
Hessischer Seglertag

Die neue DS-GVO
Datenschutz im Verein
- Ein Überblick -

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.lida.bayern.de/de/kleine-unternehmen.html>

Personenbezogene Daten

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

Beispiele für personenbezogene Daten



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

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

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
- z.B. Satzungszweck des Vereins

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) - .

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 -.



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



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



Datenübermittlung an „Dritte“: Was ist damit gemeint?

- Wer ist **Dritter**?
 - Personen außerhalb des Vereins
 - **unbefugte** Personen **innerhalb** des Vereins,
weil deren Kenntnis unnötig ist

Sonderfall Mitgliederliste



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

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 Gesangvereinen, Dichterlesungen, Ausstellungen bei Kulturvereinen usw. je nach Satzungszweck (etwa Ankündigungen, Verlaufsberichte, Spielberichte + -ergebnisse, Ergebnislisten, auch mit Fotos Teilnehmer + Zuschauer etc.)

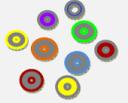
→ betrifft also Satzungszweck Öffentlichkeitsarbeit

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:.....

.....

Einwilligung

Einwilligung des Betroffenen (Art. 7 DS-GVO)



- freiwillige Entscheidung
- vorherige Aufklärung über Zweck der Erhebung, Verarbeitung, Nutzung
- Hinweis auf Folgen Verweigerung
- Einwilligung widerrufbar
- Verein ist beweispflichtig für Einwilligung

Technische und organisatorische Maßnahmen (Datensicherheit)

Sicherheit der Verarbeitung (Art. 32 DS-GVO)



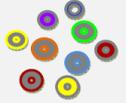
Berücksichtigung:

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

Ziel: ein dem Risiko angemessenes Schutzniveau

Wichtig: u.a. Verschlüsselung, Datensicherung

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



Praxisbeispiele (2)

- 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.)
- zeitnahe Datensicherung

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

Verzeichnis der Verarbeitungstätigkeiten (Art. 30)



Schriftlich oder elektronisch ist ein internes Verzeichnis anzulegen:

- Name und Kontaktdaten des Verantwortlichen (Verein), 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.)

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. 1 Jahr nach Beendigung der Mitgliedschaft, 3 Monate nach Volljährigkeit Löschung Elterndaten etc.)
- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Datensicherheit (Art. 32):
 - z.B. Geschäftsstelle wird abgeschlossen, wenn kein Mitarbeiter dort ist; Vorsitzender schließt zu Hause Zimmer mit PC ab; nur 3 Personen haben Zutritt zum PC und zu den Daten; techn. Zugriffsschutz durch Passwörter; automatische Updates; aktueller Virenschanner mit automat. Updates; Verfügbarkeit nach techn. Zwischenfall durch zeitnahe Datensicherung; Aktenvernichtung mit Standard-Schredder; Datenschutzerklärungen in Satzung und auf Website etc.

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



Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:

TSV Waldermühl e.V.
Steinbauerstr. 45a
98123 Sonsthausen

Tel. 0981/123456-0
E-Mail: team@waldermuehler-tsv.de
Web: www.waldermuehler-tsv.de

Vorstand: Dieter Eckbauer-Düppels, geb. 03.12.1952

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Herbert Bauer 0981/123456-1 herbert@waldermuehler-tsv.de	02.03.2018	<ul style="list-style-type: none"> Auszahlung der Löhne/Gehälter Abfuhr Sozialabgaben u. Steuern 	Beschäftigte	<ul style="list-style-type: none"> Name und Adressen der Beschäftigten ggf. Religionszugehörigkeit Eindeutige Kennzahlen zur Steuer/ Sozialabgaben 	Externer Dienstleister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Mitgliederverwaltung	Herbert Bauer 0981/123456-1 herbert@waldermuehler-tsv.de	02.03.2018	Verwaltung der Vereinstätigkeiten	Mitglieder	<ul style="list-style-type: none"> 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 0981/123456-0 max@waldermuehler-tsv.de	28.02.2018	Außendarstellung	<ul style="list-style-type: none"> 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 0981/123456-0 max@waldermuehler-tsv.de	20.02.2018	Außendarstellung	Mitglieder	Fotos von Vereinstätigkeiten	Keine	Keine	Wenn Einwilligung widerrufen - unverzüglich	Siehe IT-Sicherheitskonzept
Beitragsverwaltung	Herbert Bauer 0981/123456-1 herbert@waldermuehler-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 Virens Scanner/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 § 38 BDSG)

Informationspflichten

Ausnahme von Informationspflichten

- Die Informationspflichten bestehen **nicht**, wenn und soweit die betroffene Person bereits über die Informationen verfügt, also konkret Bescheid weiß.

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, Satzungszweck)
- Rechtsgrundlage für Verarbeitung (z.B. Art. 6 Abs. 1 b DS-GVO)
- Empfänger oder mögliche Empfänger, an welche die Daten (möglicherweise) weitergegeben werden (z.B. Öffentlichkeit, Fachverbände, Homepage, eventuell Steuerbüro XY, Minijob-Zentrale)
- Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung der Speicherdauer;

Information über „Pflichtdaten“

- z.B.: Welche Daten muss ich bereitstellen, um Vereinsmitglied zu werden (Pflichtangaben?)
- Welche Angaben sind freiwillig?

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 zuständige Aufsichtsbehörde

Ihnen steht ein Recht zur Beschwerde bei der zuständigen Aufsichtsbehörde zu. Zuständige Aufsichtsbehörde in datenschutzrechtlichen Fragen ist in Hessen der Hessische Datenschutzbeauftragte (Kommunikationsdaten).

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; bei Mitgliedern: Satzung
- Insbesondere auf die leichte Zugänglichkeit muss bei elektronischer Darstellung geachtet werden.
- Beim Verstoß gegen die Informationspflichten droht eine Geldbuße.

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, Homepage/Provider), 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 verlorengegangene Datenträger sind unverzüglich und möglichst innerhalb von 72 Stunden nach Bekanntwerden der Aufsichtsbehörde zu melden.

Datenschutzbeauftragter



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

ist vom Verein schriftlich zu bestellen,

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

oder

- Art. 37 DSGVO



- **beschäftigt in diesem Sinne:**

jede(r), der (die)

im Auftrag des Vereins

regelmäßig

mit Hilfe der EDV-Mitgliederverwaltung

personenbezogene Daten

automatisiert verarbeitet

- egal, ob als Ehrenamtler(in) oder gegen Vergütung im Verein tätig

Datenschutzbeauftragter



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

und ...

Datenschutzbeauftragter



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

Achtung neu:

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

Datenschutzbeauftragter



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



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?



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.

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



Wenn kein Datenschutzbeauftragter ...

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

Haftung des DSB



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

Datenschutzerklärung Homepage

Hilfen

zum Beispiel:

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

Weitere Infos

- 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!**



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