Erste Schritte EU-DSGVO

Da uns viele Vereine und Selbsthilfegruppen angesprochen haben, ob wir ihnen Tipps zur EU-DSGVO geben können, haben wir (rechtsunverbindlich!) erste Schritte zusammengestellt…

Vereine, die gesundheitsbezogene („sensible Daten“) von Personen verarbeiten, sind strengeren Regeln unterworfen, die wir hier nicht abdecken können.

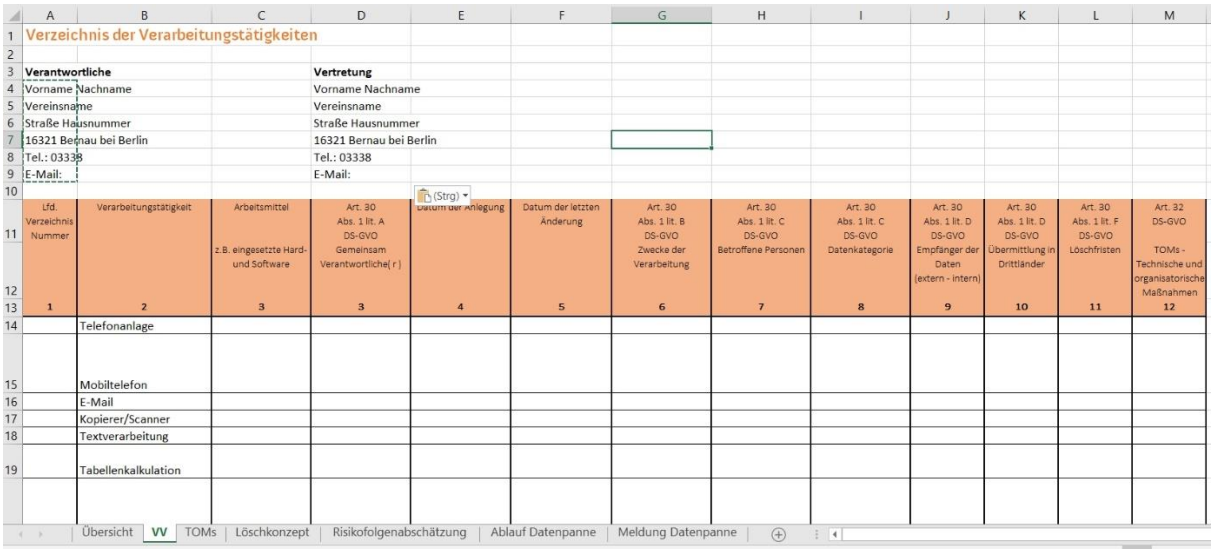
1) Klärung: Was ist Datenverarbeitung und welche Daten verarbeitet mein Verein?

- Unter **Datenverarbeitung** versteht man das Erheben, Erfassen, Organisieren, Ordnen, die Speicherung, Anpassung oder Veränderung, das Auslesen/Filtern, Abfragen, die Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, des Abgleichs oder der Verknüpfung, Einschränkung, Löschung, Vernichtung von Daten einer natürlichen Person.
- In der Regel verarbeiten Vereine folgende **Daten** ihrer Mitglieder:
    - Vor- und Zuname
    - Postadresse
    - E-Mail-Adresse
    - Telefon- und/oder Mobilnummer
    - Bankverbindung: Bei der Erteilung von Einzugsermächtigungen für Mitgliedsbeiträge werden auch Kontodaten verarbeitet
    - ggf. Geburtsdatum (nach EU-DSGVO mit Geburtsjahr schwierig, da ein berechtigtes Interesse zur Gratulation nur an Tag und Monat besteht…)
- Für diese Daten ist keine ausdrückliche (nachträgliche) Einwilligung erforderlich, da diese quasi mit dem Eintritt in den Verein erteilt wird! „Ein Verein darf aufgrund des Art. 6 Abs. 1 lit. b) DS-GVO beim Vereinsbeitritt (Aufnahmeantrag oder Beitrittserklärung) und während der Vereinsmitgliedschaft nur solche Daten von Mitgliedern erheben, die für die Begründung und Durchführung des zwischen Mitglied und Verein durch den Beitritt zustande kommenden rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich sind. Damit dürfen alle Daten erhoben werden, die zur **Verfolgung der Vereinsziele** und für die **Betreuung und Verwaltung der Mitglieder** (wie etwa Name, Anschrift, in der Regel auch das Geburtsdatum, ferner Bankverbindung, Bankleitzahl und Kontonummer) **notwendig** sind.“ (Zitat: Landesdatenschutzbeauftragte Baden-Württemberg, Datenschutz im Verein nach der DSGVO, S. 12, Link s.u.)

- Die Daten müssen in einem **maschinenlesbaren Format**, d.h. in Datenbanken oder Exceltabellen, gespeichert sein. (Nicht nur in Papierordnern!)
- Die Rechtsgrundlage für die Verarbeitung von Daten ergeben sich aus den Artikeln 6-9 der EU-DSGVO sowie aus der Vereinssatzung (und ggfs. den Mitgliederverträgen).

2) Verarbeitungsverzeichnis! (Dokumentation)

- Jeder Verein muss ein Verarbeitungsverzeichnis führen! Ziel ist die Dokumentation, wer, wann, welche Verarbeitung personenbezogener Daten durchgeführt hat und zu welchem Zweck. [Tipp: Excel-Tabelle!]
- Diese muss einmal angelegt und für alle Daten „durchgespielt" und ständig aktualisiert werden. [Tipp: Routine festlegen: alle x Monate, auf jeden Fall bei neuer Technik mit der personenbezogene Daten verarbeitet werden wie Telefone, PCs, Software… und bei „Personalwechsel"]
- Dieses Verzeichnis muss auf Anfrage den Aufsichtsbehörden zur Verfügung gestellt werden!



Verzeichnis der Verarbeitungstätigkeiten

Verantwortliche	Vertretung
Vorname Nachname	Vorname Nachname
Vereinsname	Vereinsname
Straße Hausnummer	Straße Hausnummer
16321 Bernau bei Berlin	16321 Bernau bei Berlin
Tel.: 03338	Tel.: 03338
E-Mail:	E-Mail:

Lfd. Verzeichnis Nummer	Verarbeitungstätigkeit	Arbeitsmittel z.B. eingesetzte Hard- und Software	Art. 30 Abs. 1 lit. A DS-GVO Gemeinsam Verantwortliche(r)	Datum der Anlegung	Datum der letzten Änderung	Art. 30 Abs. 1 lit. B DS-GVO Zwecke der Verarbeitung	Art. 30 Abs. 1 lit. C DS-GVO Betroffene Personen	Art. 30 Abs. 1 lit. C DS-GVO Datenkategorie	Art. 30 Abs. 1 lit. D DS-GVO Empfänger der Daten (extern - intern)	Art. 30 Abs. 1 lit. D DS-GVO Übermittlung in Drittländer	Art. 30 Abs. 1 lit. F DS-GVO Löschfristen	Art. 32 DS-GVO TOMs - Technische und organisatorische Maßnahmen
1	2	3	3	4	5	6	7	8	9	10	11	12
	Telefonanlage											
	Mobiltelefon											
	E-Mail											
	Kopierer/Scanner											
	Textverarbeitung											
	Tabellenkalkulation											

(Überschrift: Verzeichnis der Verarbeitungstätigkeiten
darunter (Haupt-)Verantwortliche*r mit Vorname Nachname, Vereinsname, Straße Hausnummer, PLZ Ort, Telefonnummer und E-Mail-Adresse
daneben Vertretung mit den entsprechenden Angaben

Tabelle mit folgenden Spalten:

1) Lfd. Verzeichnis-Nummer
2) Verarbeitungstätigkeit
3) Arbeitsmittel (z.B. eingesetzte Hard- und Software)
4) Art. 30 Abs. 1 lit. A DS-GVO Gemeinsam Verantwortliche(r)
5) Datum der Anlegung (der Daten)
6) Datum der letzten Änderung (der Daten)
7) Art. 30 Abs. 1 lit. B DS-GVO Zwecke der Verarbeitung
8) Art. 30 Abs. 1 lit. C DS-GVO Betroffene Personen
9) Art. 30 Abs. 1 lit. C DS-GVO Datenkategorie
10) Art. 30 Abs. 1 lit. D DS-GVO Empfänger der Daten (extern - intern)
11) Art. 30 Abs. 1 lit. D DS-GVO Übermittlung in Drittländer
12) Art. 30 Abs. 1 lit. F DS-GVO Löschfristen

13) Art. 32 DS-GVO TOMs - Technische und organisatorische Maßnahmen (Verschlüsselung, neuester Stand der Technik sofern möglich und angemessen, Berechtigungskonzept: wer darf auf welche Daten zugreifen, Löschkonzept, Konzept Ablauf Datenpanne…)

3) Informationspflichten, Zweckbindung und Speicherung (Löschfristen)

- Mitglieder und ggf. andere betroffene Personen (Besucher, sofern Daten erhoben werden) müssen umfassend über die Datenverarbeitungsvorgänge im Verein (Art. 12 - 14 DS-GVO) informiert werden, insbesondere z.B. darüber, **wer welche personenbezogenen Daten zu welchem Zweck und auf welcher Rechtsgrundlage über welchen Zeitraum verarbeitet**.
- **Neumitglieder**: Information zum Zeitpunkt der erstmaligen Erhebung der Daten, z. B. mit dem Mitgliedsantrag
- **Bestandsmitglieder**: Information nur wenn neue Daten erhoben werden, z.B. bei Änderungsmitteilungen
- **Informationspflichten**: ***Recht auf Auskunft*** (jederzeit kostenlos und umfassend Auskunft darüber erteilen, welche Daten gespeichert sind), ***Recht auf Widerruf*** (Einwilligung zur Datenverarbeitung kann jederzeit formlos widerrufen werden; Adresse, an die der Widerruf zu richten ist, muss mitgeteilt werden) und ***Recht auf Löschung*** (auf Wunsch teilweise oder vollständige Löschung der Daten einer Person)
  (i.d.R. 1 Monat Zeit, um diese Anfragen zu erfüllen)
- **Zweckbindung**: Nur personenbezogene Daten erheben und speichern, die für die Erfüllung des Vereinszweckes notwendig sind (Geburtsjahr, Religionszugehörigkeit, Anzahl der Kinder, Krankheiten…)
- **Speicherung**: nur solange, wie zur Zweckerfüllung erforderlich (z. B. bis zur Beendigung der Mitgliedschaft oder bis x Jahre nach Tod des Mitgliedes), es sei denn es gibt eine gesetzliche Verpflichtung Daten länger zu speichern (z. B. Unterlagen für das Finanzamt 10 Jahre…)

4) Datenschutzbeauftragte*r

- Muss nur ernannt werden, wenn **mehr als 10 Personen** im Verein ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. (Dabei ist es egal wie diese 10 Personen beschäftigt sind, also ehrenamtliche, Teil- und Vollzeitbeschäftigte zählen genauso wie andere „Hilfskräfte“. Tipp: Wenn 11 Personen damit beschäftigt sind auf 10 reduzieren!)
- Eine verantwortliche Person, ein*e Ansprechpartner*in muss in jedem Fall benannt werden.

5) Vertraulichkeitserklärung für Angestellte

- Angestellte eines Vereins (aber auch ehrenamtliche Mitglieder), die personenbezogene Daten verarbeiten sollten eine Vertraulichkeitserklärung unterschreiben, mit der sie sich verpflichten die datenschutzrechtlichen Bestimmungen einzuhalten.

6) Internetseite, Newsletter und Postversand

- **Datenschutzerklärung**:
  - muss individuell an die verwendete Technik auf der Internetseite (Cookies, Statistiktools etc.) angepasst sein
  - muss mit maximal zwei Klicks des Besuchers erreichbar sein (Tipp: sollte so wie Impressum und Kontakt von jeder Seite erreichbar sein – im Header oder Footer)
  - Dafür gibt es im Internet Generatoren, die für gemeinnützige Vereine kostenlos sind: z. B. https://datenschutz-generator.de
  - (Tipp: Verlinken Sie Ihre Datenschutzerklärung auch in der Signatur Ihrer E-Mails)

- **Veröffentlichung von Daten im Internet:**
    - Die Veröffentlichung von personenbezogenen Daten von Mitgliedern bedarf der expliziten Einwilligung der Mitglieder, außer die Veröffentlichung ist zur Erfüllung des Vereinszwecks notwendig (z. B. Vor- und Nachnamen in einer Mannschaftsaufstellung)
- **E-Mail-Newsletter:**
    - Einwilligung, den Newsletter zu empfangen muss mit Datum dokumentiert sein!
    - wenn nicht mit Datum dokumentiert werden kann, wann die Einwilligung von „Bestandsempfängern“ (mindestens zwei Klicks bzw. Double-Opt-In mit Link anklicken in E-Mail-Bestätigung) erfolgt ist, müssen alle Newsletter-Empfänger erneut ihre Einwilligung geben
      Tipp: senden Sie eine E-Mail an all Ihre Newsletter-Empfänger und informieren über ihre neue
    - Tipp: nutzen Sie ein kostenloses E-Mail-Newsletter-Programm mit Buttons zur An- und Abmeldung im Newsletter (z.B. Newsletter2Go mit Sitz in Deutschland oder MailChimp mit Sitz in den USA, aber Lizenz für die EU), die dokumentieren automatisch, wann die Anmeldung erfolgt ist
    - Für die Zusendung einer E-Mail muss eine vorherige Einwilligung erfolgen!
- **Postversand:**
    - „Kaltakquise“ (erstmalige Zusendung) eines Briefes ohne Einwilligung okay, danach Einwilligung notwendig
    - Zusendung von Einladungen zu Veranstaltungen per Post benötigen die Einwilligung des Empfängers

7) Datenverarbeitung durch Dienstleister

- Klärung: Verarbeiten Dritte (Dienstleister) für den Verein personenbezogene Daten? (Grafiker, Buchhaltungsservice, Webhoster!, E-Mailhoster!, Wartungsservice… **Ausnahme:** Rechtsanwälte, Steuerberatungsbüro, Bank)
- Mit diesen „Dritten“ müssen sogenannte AV- (oder auch ADV-)Verträge (**A**uftrags[-**d**aten-] **v**erarbeitungsverträge) abgeschlossen werden. (Die meisten dieser Dienstleister haben eigene AV-Verträge, die man dann nur noch ggfs. Kopieren und unterschreiben muss

8) weiterführende Links:

- DSGVO – 10 Tipps für Vereine: https://www.datenschutz-notizen.de/dsgvo-10-tipps-fuer-vereine-3720448/
- Datenschutz im Verein nach der Datenschutzgrundverordnung (PDF 602 KB): https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf
- Orientierungshilfe Datenschutz im Verein: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/Datenschutz_im_Verein__DS-GVO__-_Kompakt.pdf
- EU-DSGVO für Vereine: https://www.vereinswelt.de/dsgvo-fuer-vereine
- kostenlose Newslettersysteme:
    - http://www.newsletter2go.com
    - http://www.mailchimp.com
- AV-Vertrag: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/02/DSK_KpNr_13_Auftragsverarbeitung.pdf