Vereine und die EU DSGVO

Was müssen Vereine beachten, bedenken und erledigen?

Grundzüge

Datenschutz ist Grundrechtsschutz, Art. 1 DS-GVO

- Das Grundgesetz garantiert jedem das Recht, über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen (Grundrecht auf informationelle Selbstbestimmung).
- Jeder soll frei entscheiden können, welche seiner personenbezogenen Daten er wann, wem und zu welchem Zweck zugänglich macht.

Grundzüge

Datenschutz ist Grundrechtsschutz, Art. 1 DS-GVO

- Der freie Verkehr personenbezogener Daten in der Union soll weder eingeschränkt noch verboten werden.
- Schutz des Einzelnen vor dem Missbrauch seiner personenbezogenen Daten.

Grundzüge

Wo ist der Datenschutz gesetzlich geregelt?

- Europaweit einheitlich in der Datenschutz-Grundverordnung (kurz: DS-GVO) geregelt.
- In Deutschland ergänzt das Bundesdatenschutzgesetz (kurz: BDSG) die DS-GVO. Ferner bestehen bereichsspezifische Sondervorschriften, etwa:
  - Strafgesetzbuch: §201 Vertraulichkeit des Wortes, §202 Briefgeheimnis
  - Kunsturhebergesetz: §§22 ff Recht am eigenen Bild
  - Sozialgesetzbücher

Grundzüge

Die DS-GVO

- gewährleistet ein einheitliches Datenschutzniveau innerhalb der EU
- gilt grundsätzlich sachlich für jede ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung von Daten, die gespeichert sind oder gespeichert werden sollen (vgl. Art. 2 DS-GVO);

Grundzüge

Die DS-GVO

- gilt räumlich für eine Verarbeitung durch Verantwortliche oder Auftragverarbeiter mit Niederlassung innerhalb der EU; unabhängig davon ob die Verarbeitung innerhalb der EU stattfindet, sowie für eine Verarbeitung personenbezogener Daten, sofern das jeweilige Angebot auf den europäischen Markt („Marktort“) gerichtet ist (vgl. Art. 3 DS-GVO).

Grundzüge

Auf wen findet die DS-GVO bzw. das BDSG Anwendung:

- öffentliche Stellen
- Unternehmen
- Vereine
- Verbände
- Privatpersonen, soweit sich der Umgang mit den personenbezogenen Daten nicht ausschließlich auf persönliche oder familiäre Zwecke beschränkt

Grundzüge

Welche Daten werden geschützt?

- Die DS-GVO findet bei sog. „personenbezogene Daten“ Anwendung.
- Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen (vgl. Art. 4 Nr. 1 DS-GVO).
- Der Datenschutz umfasst ausschließlich natürliche Personen, das heißt „Menschen aus Fleisch und Blut“. Juristische Personen werden nicht geschützt.

Grundzüge

Welche Daten werden geschützt?

- Die betroffene Person muss bestimmt oder bestimmbar sein, das heißt die Informationen sind unmittelbar oder mit verfügbarem Zusatzwissen der Person zuzuordnen.
- Geschützt werden alle Informationen, die etwas über die betroffene Person aussagen.

Grundzüge

Beispiele für „personenbezogene Daten“:

- Name, Vorname, Adresse, E-Mailadresse, Rufnummern
- Geburtsdatum, Familienstand, Religion, Bankverbindung
- Gesundheitsdaten
- IP-Adresse
- Mitgliedsnummer
- rassische/ethnische Herkunft

Grundzüge

besondere Kategorien personenbezogener Daten:

- Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie
- Genetische oder biometrische Daten
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

Grundzüge

Häufig treffen Sie folgende Datenarten an:

- Mitarbeiterdaten, etwa Vorstand, Geschäftsstelle, Übungsleiter: z. B. Adresse, Sozialdaten, Arbeitszeiten, Ausbildung, Fähigkeiten, Arbeitszeugnisse
- Mitgliederdaten: z. B. Adresse, Bankverbindung, Bonität, Vertragsverhältnisse, Zahlungsverhalten, Gesundheitsdaten im Reha Sport
- Daten Dritter, etwa Sponsoren, Schiedsrichter, Gastvereine, Besucher etc.

Grundzüge

In welcher Form kommen personenbezogene Daten vor?

- Papier, Akte
- gesprochenes Wort
- bildliche Darstellung (z. B. Video, Fotos)
- digitale Form (z. B. Word-/Excel-Dokumente)

Grundzüge

Was ist erfasst?

- Die DS-GVO und das BDSG finden Anwendung, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden - unabhängig davon, ob dies elektronisch oder in anderer Form erfolgt.

Grundzüge

Was ist erfasst?

- Verarbeitung meint dabei nach Art. 4 Nr. 2 DS-GVO 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**

Grundprinzipien der Datenerhebung

- Jede Erhebung und Verarbeitung von personenbezogenen Daten bedarf einer gesetzlichen Rechtfertigung. Bei der Erhebung der Daten ist außerdem der Zweck, für den die Daten verarbeitet werden sollen, konkret festzulegen (vgl. Art. 5 DS-GVO).
- Die Verarbeitung personenbezogener Daten ist nach der **DS-GVO** (Art. 6 DS-GVO) rechtmäßig:

Grundprinzipien der Datenerhebung

- wenn eine Einwilligung des Betroffenen vorliegt, welche freiwillig und nachweisbar sein muss. Ein Vertrag darf nicht von einer Einwilligung abhängig gemacht werden (Kopplungsverbot, etwa Ankreuzoption auf dem Anmeldeformular bezüglich des Newsletters).
- wenn die Verarbeitung zur Erfüllung eines Vertrages oder einer vorvertraglichen Maßnahme erforderlich ist (etwa Mitgliederverwaltung oder Teilnahme an Wettbewerben).
- wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist (etwa gesetzliche Meldepflichten, Führungszeugnis in der Kinder-/Jugendarbeit).

Grundprinzipien der Datenerhebung

- wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen der betroffenen Person überwiegen (etwa Mahnwesen des Vereins, Berichterstattung über die Vereinsarbeit; Einzelfallprüfung).
- Art. 6 Absatz 1 lit. d) (lebenswichtige Interessen) und e) (öffentliche Aufgaben) spielen kaum eine Rolle.

Grundprinzipien der Datenerhebung

Verarbeitung besonderer Kategorien personenbezogener Daten, Art. 9 DS-GVO

Grundsätzlich untersagt, es sei denn

- Betroffener hat in die Verarbeitung für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt,
- Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann

Grundprinzipien der Datenerhebung

Verarbeitung besonderer Kategorien personenbezogener Daten, Art. 9 DS-GVO

Grundsätzlich untersagt, es sei denn

- Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,
- die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich.

Grundprinzipien der Datenerhebung

- Das BDSG ergänzt die Erlaubnistatbestände der DS-GVO, etwa:
  - Verarbeitung im Beschäftigungskontext
  - Videoüberwachung
  - Datenübermittlung an Auskunfteien
  - Scoring
  - Verarbeitung bes. persönlicher Daten für Forschungszwecke
  - Verarbeitung zu anderen Zwecken

Grundprinzipien der Datenerhebung

- Andere Rechtsvorschriften:
  - Steuer-und Sozialversicherungsrecht für die Entgeltabrechnung.
  - Abgeschlossene Betriebs-oder Dienstvereinbarungen können ebenfalls einen Erlaubnistatbestand beinhalten und sind grundsätzlich vorrangig, soweit sie den Grundsätzen der DS-GVO entsprechen.

Grundprinzipien der Datenerhebung

Direkterhebung beim Betroffenen, Art 13 DS-GVO

Grundsatz, wobei darüber zu informieren ist:

- wer die verantwortliche Stelle ist, nebst den Kontaktdaten des Datenschutzbeauftragten,
- zu welchem Zweck die Daten erhoben, verarbeitet oder genutzt werden,
- auf welcher Rechtsgrundlage die Verarbeitung beruht,
- an wen die Daten weitergegeben werden,
- wie lange diese aufbewahrt werden,
- welche Rechte der betroffenen Person zustehen.

Die Einwilligungserklärung, Art. 7 DS-GVO

- Die Einwilligung ist nur wirksam, wenn …
  - sie auf der freien Entscheidung des Betroffenen beruht,
  - sie widerrufbar ist (Widerruf muss genauso simpel wie Einwilligung selbst sein),
  - sie jede Phase der beabsichtigten Datenverarbeitung umfasst,
  - der Betroffene auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hingewiesen wurde.

Die Einwilligungserklärung, Art. 7 DS-GVO

- Die Einwilligung bedarf grundsätzlich keiner besonderen Form, zu empfehlen ist jedoch die Schriftform. Nachweispflicht des Verantwortlichen.
- Darüber hinaus ist die Einwilligung gegenüber anderen Textpassagen besonders optisch hervorzuheben.
- Liegt keine wirksame Einwilligung vor, ist die auf die Einwilligung gestützte Datenverarbeitung unzulässig. Bereits gespeicherte Daten müssen gelöscht werden.

Zweckbindung, Art. 5 DS-GVO

Personenbezogene Daten müssen:

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (**„Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“**);
- für **festgelegte, eindeutige und legitime Zwecke** erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Art. 89 Absatz 1 DS-GVO nicht als unvereinbar mit den ursprünglichen Zwecken;

Zweckbindung, Art. 5 DS-GVO

Personenbezogene Daten müssen:

- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung **notwendige Maß beschränkt** sein;
- **sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein**; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;

Zweckbindung, Art. 5 DS-GVO

Personenbezogene Daten müssen ferner:

- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen **nur so lange** ermöglicht, **wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist**; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Art. 89 Absatz 1 DS-GVO verarbeitet werden;

Zweckbindung, Art. 5 DS-GVO

Personenbezogene Daten müssen ferner:

- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete **technische und organisatorische Maßnahmen**.

Datenvermeidung und Datensparsamkeit, Art. 5 DS-GVO

Datenverarbeitungen sind an diesen Zielen auszurichten:

- keine oder so wenig wie möglich personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen.
- Soweit möglich, sind personenbezogene Daten zu
  - anonymisieren, das heißt die Daten können nicht oder nur mit einem unverhältnismäßig großen Aufwand einer Person zugeordnet werden, oder zu
  - pseudonymisieren, das heißt das Identifikationsmerkmal (z. B. Name) wird durch ein anderes Kennzeichen ersetzt.

Rechte der betroffenen Person

Jeder, dessen personenbezogene Daten erhoben, verarbeitet oder genutzt werden hat folgende Rechte:

- Recht auf Benachrichtigung
- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Vergessen werden
- Recht auf Einschränkung der Verarbeitung
- Recht auf Widerspruch
- Recht auf Datenübertragung

Welche Folgen können bei Datenschutzverstößen eintreten?

- Meldepflicht des Verantwortlichen gegenüber Betroffenen und der Aufsichtsbehörde bei unrechtmäßiger Kenntniserlangung von „Risiko“-Daten (z. B. Daten zu Bank-und Kreditkartenkonten, besondere Arten personenbezogener Daten)

- Vertrauensverlust bei Mitgliedern, Geschäftspartnern, Mitarbeitern und Behörden

Welche Folgen können bei Datenschutzverstößen eintreten?

- Daneben können Datenschutzverstöße
  - Bußgelder (Geldbußen bis zu 20.000.000 Euro oder 4% des Umsatzes aus dem Vorjahr)
  - Geldstrafen, Freiheitsstrafen
  - eine Schadensersatzpflicht gegenüber den Betroffenen sowie
  - arbeitsrechtliche Sanktionen (von der Abmahnung bis zur Kündigung)

  nach sich ziehen.

Was ist durch wen konkret zu tun?

Wer ist verantwortlich?

Im Verein ist der Vorstand i. S. d. § 26 BGB für die Umsetzung der gesetzlichen Anforderungen verantwortlich und muss daher entsprechende Veranlassungen treffen. Alle Mitarbeiter sind wiederum für die Einhaltung des Datenschutzes und der Informationssicherheit bei der Erfüllung ihrer Aufgaben verantwortlich.

Soweit ein Datenschutzbeauftragter bestellt ist, überwacht dieser zwar die Einhaltung des Datenschutzrechts, ist jedoch selbst nicht für die Umsetzung der sich daraus ergebenden Anforderungen zuständig.

Was ist durch wen konkret zu tun?

Was ist zu tun? (nicht abschließend)

Datenschutzerklärung auf der Homepage, Datenschutzhinweise, Einwilligungserklärungen, Bestellung Datenschutzbeauftragter, Erstellung Verzeichnis der Verarbeitungstätigkeiten, Erstellung der sog. TOMs, Beschäftigtendatenschutz, Verträge über die Auftragsverarbeitung, Datenschutzordnung, etc.

Was ist zu tun?

Handlungsempfehlung

Differenzieren Sie danach, welchen Maßnahmen Außenwirkung zukommt, und sodann, welche Maßnahmen mit welchem Aufwand umgesetzt werden können.

1. Bestellung eines Datenschutzbeauftragten, sofern 10 oder mehr Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, § 38 BDSG; es werden alle Personen mitgezählt, die tatsächlich auf die automatisierte Datenverarbeitung zugreifen. Nicht entscheidend ist, wie häufig oder intensiv auf die Daten zugegriffen wird; Kurzpapier Nr. 12 der DSK, FAQ zu Datenschutzbeauftragten der LDI NRW, Stand 11/2018 (intern/extern; Meldung gegenüber der Aufsichtsbehörde (online)

Was ist zu tun?

Handlungsempfehlung

2. Datenschutzerklärung für die Homepage (ggfls. mittels Datenschutzgenerator online); Einsatz von sog. cookies und social media plugins prüfen, vgl. Positionsbestimmung der DSK vom 26.04.2018, Einwilligung sowie Vertrag über Auftragsverarbeitung erforderlich; Abmahnrisiko wegen eines Verstoßes gegen § 4 Nr. 11 UWG bzw. jetzt § 3 a UWG, LG Würzburg, Beschluss v. 13.09.2018, Az. 11 O 1741/18

Was ist zu tun?

Handlungsempfehlung

3. Datenschutzhinweise ggü. Mitgliedern, Geschäftspartnern, etc.; ggfls. Einwilligungserklärung, sofern kein Rechtfertigungsgrund nach Art. 6 Abs. 1 lit b. ff. DS-GVO gegeben ist, etwa Lichtbilder, Newsletter etc., oder Gesundheitsdaten erhoben werden(Vorlagen bspw. unter https://www.vibss.de/vereinsmanagement/recht/datenschutz). Vorsicht ist bei der Einwilligung Minderjähriger geboten. Zur Presseberichterstattung: KUG weiterhin anwendbar, vgl. OLG Köln, Beschluss v. 08.10.2018, Az. 15 U 110/18; v. 18.06.2018, Az. 15 W 27/18

Was ist zu tun?

Handlungsempfehlung

4. Datenschutzordnung in Ergänzung der Vereinssatzung (Vorlage etwa unter https://www.vibss.de/vereinsmanagement/recht/datenschutz/
5. Beschäftigtendatenschutz, insbesondere Verpflichtung auf das Datengeheimnis, ggfls. Verpflichtung auf das Telekommunikationsgeheimnis, Datenschutzhinweise ggü. den Beschäftigten, vgl. Kurzpapiere Nr. 14 und 19 der DSK; datenschutzrechtliche Eingliederung von freien Mitarbeitern prüfen, etwa Übungsleiter auf Honorarbasis; Verpflichtung des (ehrenamtlichen) Vorstands auf das Datengeheimnis

Was ist zu tun?

Handlungsempfehlung

6. Verträge über die Auftragsverarbeitung (etwa Vereinssoftware, Hosting Vereinsseite, etc.), vgl. Kurzpapier Nr. 13 der DSK; prüfen, ob eine Datenübermittlung in Drittländer erfolgt; Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
7. Verzeichnis der Verarbeitungstätigkeiten („Datenschutzbibel“ oder Inhaltsverzeichnis),etwa nach dem Muster des BayLDA: https://www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf, ergänzt durch das Muster des LSB NRW: https://www.vibss.de/vereinsmanagement/recht/datenschutz/

Was ist zu tun?

Handlungsempfehlung

8. TOMs (Darstellung der technischen und organisatorischen Maßnahmen zur Datensicherheit), etwa Zugangs-/Benutzerkontrolle, Datensicherung, Virenschutz, Firewall etc.
9. Löschkonzept (wann wird wie gelöscht)

10. Sonderfall Videoüberwachung, vgl. Kurzpapier Nr. 15 der DSK
11. Grundsätzlich nicht erforderlich: Datenschutzfolgenabschätzung, vgl. „Blacklist“ der DSK, Stand 10.07.2018

Weiterführende Informationen

- https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf
- https://www.lfd.niedersachsen.de/themen/vereine/datenschutz-im-verein-56043.html
- https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/Datenschutz_im_Verein__DS-GVO__-_Kompakt.pdf
- https://www.engagiert-in-nrw.de/datenschutz_vereinsarbeit
- https://www.vibss.de/vereinsmanagement/recht/datenschutz/
- https://www.lsb-niedersachsen.de/fileadmin/user_upload/LSB-Leitfaden_DSGVO_5_2018.PDF

Vielen Dank für Ihre Aufmerksamkeit!

Bei Rückfragen stehe ich Ihnen gerne im Anschluss oder unter

Stein & Partner Rechtsanwälte mbB
Rechtsanwalt Sebastian Hinze, LL.M.
Bischof-Hemmerle-Weg 9
52076 Aachen
Telefon: 0241 / 510 55 207
E-Mail: hinze@steinundpartner.de

zur Verfügung.