Datenschutz e.V.

Compliance bei FC, SV und Co.

Was sind Ihre Erwartungen?

Lernziel / Ziel der Veranstaltung

- Sie lernen, welche Anforderungen im Datenschutz und der Informationssicherheit Risiken in Ihrem Verein erhöhen
- Sie erfahren was Sie tun können, um diese Risiken für Ihren Verein zu minimieren

Agenda (1/2)

Warum ist Datenschutz so wichtig?

- Einheitliche Regelungen für die EU
- Rollen im Datenschutz

Welche Daten müssen geschützt werden?

- Welche Daten sind schützenswert?
- Unter welchen Voraussetzungen dürfen personenbezogener Daten (pbD) verarbeitet werden?
- Grundsätze zum Umgang mit personenbezogenen Daten
- Gibt es weitere schützenswerte Daten?

Agenda (2/2)

Was Sie tun können: Tipps für die Praxis

- Einstieg: Verzeichnis von Verarbeitungstätigkeiten
- Der Werkzeugkasten: Mit welchen TOM schütze ich die Daten?
- Pflicht der Vereine: Informationsrechte der Betroffenen
- Böhmische Dörfer: Brauche ich einen Datenschutzbeauftragten?

Diskussion

EU-DSGVO legt einheitliche Datenschutzregeln fest

Zweck der EU-DSGVO

- Sie schützt die Grundrechte und die Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf den Schutz ihrer personenbezogenen Daten.

Anpassungsgesetz zum Bundesdatenschutzgesetz

- Mitgliedsstaaten haben anhand von „Öffnungsklauseln“ die Möglichkeit, diese mit eigenen gesetzlichen Regelungen zu ergänzen. In Deutschland wurde daraufhin im August 2017 das BDSG-neu verabschiedet.

Anwendungsbereich für Vereine

- Für Vereine gilt die EU-DSGVO (fast) uneingeschränkt.
- Eine der wenigen Entlastungen bezieht sich auf die Verarbeitungsverzeichnisse, die nach Art. 30 Abs. 5 DSGVO nicht bei allen Vereinen geführt werden müssen und der Pflicht zur Bestellung eines Datenschutzbeauftragten unter gewissen Voraussetzungen.
- Haftung:
  - Vereinsvorstand, vertritt den Verein nach außen § 26 Abs. 1 Satz 2 Bürgerliches Gesetzbuch, BGB
  - Wer als Vorstand sein Pflichten schuldhaft schlecht erfüllt, muss den entstandenen Schaden ersetzen
  - Sind mehrere Mitglieder des Vorstandes für den Schaden verantwortlich, haften sie als Gesamtschuldner.

FAZIT **Jeder Verein ist betroffen, welcher personenbezogene Daten (Spieler, Mitglieder, Sponsoren, Kunden) verarbeitet**

Wer macht was? Rollen & Aufgaben

Betroffene Personen

- Natürliche Personen, deren Daten verarbeitet werden und deren Persönlichkeitsrechte Schutzobjekt des Gesetzes sind, bezeichnet die DSGVO als „betroffene Personen“.

Verantwortliche Stelle

- Sie als Vorstand eines Vereins sind verpflichtet, Sorge zu tragen, dass die Datenschutzprinzipien gewahrt werden und ihnen unterstellte Personen Daten nur nach Anweisung handeln. Sie sind die verantwortliche Stelle und zentrales Element der DSGVO.

Auftragsverarbeiter

- Dienstleister, die von Ihnen mit Datenverarbeitung beauftragt werden, sind Auftragsverarbeiter.

Aufsichtsbehörden

- Die Landesdatenschutz-behörden (LDSB) kontrollieren die Einhaltung der Datenschutz-Anforderungen.
- Die LDSB verhängen Bußgelder und stellen Strafanträge.

Datenschutzbeauftragter

- Der Datenschutzbeauftragte berät und unterrichtet den Verein hinsichtlich ihrer Datenschutzpflichten und überwacht deren Einhaltung.
- Er kann als Mitarbeiter des Vereins oder als externer Datenschutzbeauftragter bestellt werden.
- Er muss über eine hohe fachliche Qualifikation und über eine absolute Neutralität und Zuverlässigkeit verfügen.
- Bei Vereinen ist die Bestellung eines Datenschutzbeauftragten unter bestimmten Voraussetzungen nicht verpflichtend. In diesem Fall ist eine Beratung zur Sicherstellung von Datenschutz-Anforderungen sinnvoll.

Was sind personenbezogene Daten und welche sind besonders schutzwürdig?

Personenbezogene Daten

- Daten, die eindeutig einer bestimmten natürlichen Person zugeordnet werden können:
  - „Anna-Sophie Peters hat grüne Augen“
- Auch Daten ohne Namensangabe gelten als personenbezogen, wenn aus Ihnen auf die zugehörige Person geschlossen werden kann.
  - Der Vorstandsvorsitzende des FC Attacke ist Mitglied der Partei „Keine Alternative“

Beispiele (inkl. besonders schutzwürdige Daten)

- Folgende personenbezogene Daten sind zu schützen (Auszug)

	Art. 9
Name und Vorname	
Religiöse oder weltanschauliche Überzeugung	X
Adresse	
Festnetz- und Mobilrufnummer	
Rassische und ethnische Herkunft	X
Geburtsdatum	
Gewerkschaftszugehörigkeit	X
Haarfarbe	
Grundbesitz	
Politische Meinung	X
Kontonummer	
Einkommen	
Gesundheit	X
Genetische und biometrische Daten	X
Fotos und Videoaufnahmen	
Sexualleben oder sexuelle Orientierung	X
Leistungsmerkmale wie fleißig, redegewandt	

Was meinen Sie?

Sponsorenabend für die spendabelsten Mitglieder

- Der Vorstand eines Vereins die Analyse von Spendendaten. Er will wissen, welche 10 Mitglieder bisher am meisten gespendet hat. Diese sollen dann zu einem Sponsorenabend eingeladen werden.
- Der Kassenwart sieht die Auswertung kritisch. Sein Bauchgefühl sagt ihm, dass die Daten dazu nicht genutzt werden dürfen.

?

Dürfen die Daten verwendet werden?

1. Ja, da die Spendendaten nur intern und nur zu statistischen Zwecken verwendet werden. Die personenbezogenen Spenden geben wir nicht raus.
2. Ja, weil die Spender einen klar beschriebenen Nutzen davon haben.
3. Ja, wenn eine explizite Einwilligung der Spender zu dem genannten Verarbeitungszweck vorliegt.

Die Hürden für die rechtmäßige Verarbeitung personenbezogener Daten* durch die DSGVO steigen

Voraussetzungen

Einwilligungen bei Newsletter

- Die Kriterien einer wirksamen Einwilligungen bei Newsletter wurden in der Vergangenheit häufig vernachlässigt – einige kommen durch die DSGVO hinzu:
  - Ausdrücklich (Haken oder nicht)
  - Konkreter Zweck („Werbung“ reicht nicht)
  - Freiwillig (Kopplungsverbot)
  - Informationspflichten
    - „eigenes Kapitel“
    - Auftragsverarbeitung „Clever Reach“
    - Statistik-Tools/Analysen
  - Widerrufshinweis / Verarbeitung des Widerrufs
  - Double-Opt-In-Verfahren (DOI)
- Ausnahme: § 7 Abs. 3 UWG für bestehende Mitglieder mit weiteren Voraussetzungen

* Für die Verarbeitung „besonderer Kategorien“ personenbezogener Daten ist (fast) immer eine Einwilligung erforderlich.

Grundprinzipien der Datenverarbeitung (1/3)

Verbot mit Erlaubnis-vorbehalt

- Jede Verarbeitung personenbezogener Daten ist verboten außer es liegt ein Erlaubnistatbestand (siehe vorherige Folie) vor
  - Datenübermittlung an Auskunfteien und „Scoring“ fällt weg (ausdrückliche Einwilligung)
  - Beschäftigungsverhältnis (auch Bewerberdaten) weiterhin zulässig

Treu und Glauben

- Jede Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen
- Transparenzgebot ist umfassend gemeint und setzt voraus, dass setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind

Zweck-bindung

- Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, müssen eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen
- Eine Weiterverarbeitung zu anderen Zwecken ist nicht zulässig

Grundprinzipien der Datenverarbeitung (2/3)

Daten-minimierung

Daten-sparsamkeit

- Das Ziel einer Verarbeitung muss es sein, dass so wenig personenbezogene Daten wie möglich verarbeitet werden
- Erforderlichkeit : Nur die Daten erheben, die tatsächlich für die Verarbeitung notwendig sind
- Beispiel: Newsletter und Abgrenzung zu Bestellung
  - E-Mailadresse, Vorname, Nachname, Anrede

Richtigkeit

- Bei der Verarbeitung personenbezogener Daten ist sicherzustellen, dass sie richtig und auf dem neusten Stand sind
- Falsche personenbezogene Daten sind unverzüglich zu berichtigen oder zu löschen

Speicher-begrenzung

- Die Speicherfrist für personenbezogene Daten ist auf das unbedingt erforderliche Mindestmaß zu beschränken
  - Beispiel: Bewerberdaten sind zwei (§ 15 AGG) + drei (§ 61b Abs. 1 ArbGG) + einen (Toleranz) Monat nach Absage des Bewerbers aufzubewahren und dann zu löschen
  - Länger aufbewahrt werden dürfen nur für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke

Grundprinzipien der Datenverarbeitung (3/3)

Integrität und Vertrau-lichkeit

- Angemessene Sicherheit der personenbezogenen Daten gewährleisten
  - einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung,
  - vor unbeabsichtigtem Verlust,
  - unbeabsichtigter Zerstörung oder
  - unbeabsichtigter Schädigung
  - durch geeignete technische und organisatorische Maßnahmen

- Zu den technischen und organisatorische Maßnahmen (TOM) zählen zum Beispiel:
  - Richtlinie zur Vergabe und Nutzung von Passwörtern
  - Unbeaufsichtigte Geräte angemessen sichern
  - Nicht mehr benötigte Berechtigungen werden zeitnah entzogen (Ex-Vorstand)
  - Beschränkter Zugriff von Benutzern und Wartungspersonal auf Informationen, Applikationen und Dienste
  - Schriftlicher Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO
  - Backup- und Recoverykonzept mit regelmäßiger Sicherung
  - Regelmäßige Penetrationstest bei webbasierten Anwendungen
  - Unterbrechungsfreie Stromversorgung (USV) vorhanden

Verantwortliche Stelle ist für Einhaltung der Grundsätze verantwortlich und muss dies nachweisen können ("Rechenschaftspflicht")

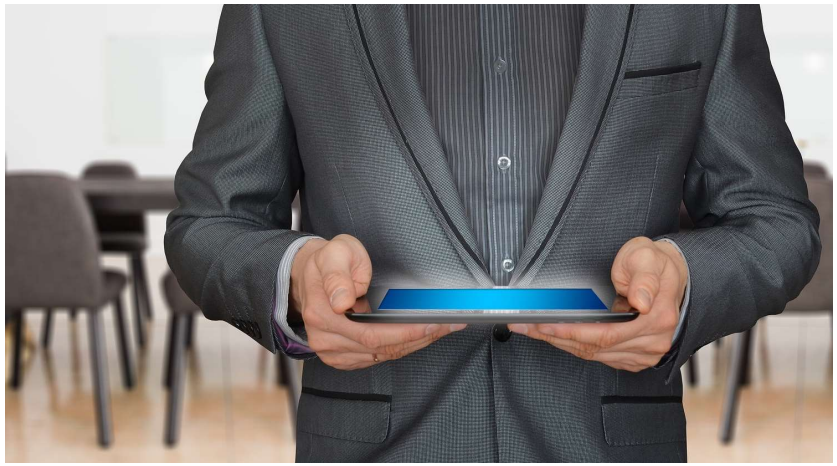
Wie Sie Datenschutz im Verein etablieren

1. Einstieg:
   Verzeichnis von Verarbeitungstätigkeiten
2. Der Werkzeugkasten:
   TOM für schützenswerte Daten
3. Pflicht der Vereine: Informationsrechte
4. Most wanted: Datenschutz im Verein

Der Einstieg: Verzeichnis von Verarbeitungstätigkeiten

Führen eines Verarbeitungsverzeichnisses

- Nicht mehr Pflicht zur Veröffentlichung
- Nicht mehr Meldung an die Aufsichtsbehörde
- Teilweise keine Pflicht
  - Vorteile überwiegen immer
  - Vereinfachungen an falscher Stelle
- Nur wer eigene Verarbeitungsprozesse kennt, kann gezielt Maßnahmen ergreifen, um eine rechtmäßige Verarbeitung personenbezogener Daten sicherstellen zu können



Vorteile

- Bewusstsein für personenbezogene Datenverarbeitung im Verein entsteht
- Grundlage für nachfolgende Arbeiten wie
  - Definition angemessener TOM
  - Vereinbarung von Auftragsverarbeitung
  - Auskunftsanfragen oder
  - Nachweispflicht (muss auf Anfrage der Behörde jederzeit vorgelegt werden können)
- Kann einfach geführt werden (z. B. Excel)
- Muster z. B. beim GDD e.V. und DSK abrufbar

Inhalt (vereinfacht)

- Namen und die Kontaktdaten des Verantwortlichen
- Zwecke der Verarbeitung
- Kategorien betroffener Personen und deren Daten
- Übermittlung an ein Drittland (Cloud!)
- Fristen für die Löschung
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (siehe vorne)
- Risikobewertung (für die Rechte und die Freiheit betroffener Personen) zur Identifizierung von TOM

Der Werkzeugkasten: TOM für schützenswerte Daten

Schritt für Schritt zu angemessenen TOM

1. Schutzbedarf feststellen
2. Risiko bewerten für die Rechte und Freiheiten natürlicher Personen
3. Geeignete TOM unter Berücksichtigung u. a. des Stands der Technik und der Kosten für die Implementierung
4. Nachweis der Konformität erbringen

Tipp: Alle Elemente prozessual verbinden

1. Jeder neue Verarbeitungsvorgang wird (im Rahmen einer Datenschutz-Folgenabschätzung) bewertet
2. Schutzbedarf, Risiken und TOM im Verzeichnis von Verarbeitungstätigkeiten dokumentieren
3. Verzeichnis ist Grundlage für regelmäßige Prüfung der Wirksamkeit der TOM
4. In Prüfungen erkannte Schwachstellen werden mit Maßnahmen hinterlegt und die Umsetzung nachgehalten
5. Verzeichnis, Prüf- und Maßnahmenliste sind die Grundlage der Nachweiserbringung nach Art. 5 (2)

TOM lassen sich unterteilen in

- Security-Maßnahmen
  - Schutzmaßnahmen der Informationssicherheit
  - Angepasst auf die Verarbeitung personenbezogener Daten
  - Fokus auf Vertraulichkeit, Integrität, Verfügbarkeit
- Privacy-Maßnahmen
  - Schutzmaßnahmen des Datenschutzes
  - Explizit: Pseudonymisierung, Verschlüsselung
  - Fokus auf Datenschutzgrundsätze (z.B. Datenminimierung, Zweckbindung, Transparenz,…)

Pflicht der Vereine: Informationsrechte

Kernelement der Transparenzanforderungen

- Basis für die Ausübung der Betroffenenrechte
- Gehen weit über die bisherige Rechtslage hinaus
- Daten direkt beim Betroffenen oder bei Dritten erhoben
- Verantwortliche Stelle: Nachweis erforderlich
- Bußgeldbewährt: Art. 83 Abs. 5 lit. B DSGVO

Erhebungsszenarien & denkbare Lösungen

- Videoüberwachung: Piktogramm, Verweis auf Aushang, detaillierter Aushang
- Gratis-WLAN (§8 TMG): Nutzungsbedingungen DSGVO-konform
- Telefonische Anfrage: Verweis auf Internetseite (Medienbruch: In der Literatur geteilte Meinung)
- Werbliche Nutzung: Vorab und Verweis auf Informationen als Textblock in jedem Brief/Rechnung
- Zeitpunkt beim Online-Shop: Gleichzeitig mit dem Aufruf des Online-Shops (wie bei Cookies)

Elemente der Information (verkürzt)

1. Name und Kontaktdaten des Verantwortlichen
2. Ggfs. Kontaktdaten Datenschutzbeauftragten
3. Zweck der Verarbeitung
4. Rechtsgrundlage der Verarbeitung
5. Ggfs. berechtigtes Interesse
6. Empfänger oder Kategorien von Empfängern
7. Übermittlung an Drittland
8. (Kriterien der) Speicherdauer
9. Betroffenenrechte
10. Bestehendes Widerrufsrecht
11. Beschwerderecht bei Aufsichtsbehörde inkl. Kontaktdaten
12. Grundlage der Bereitstellung der personenbezogenen Daten und mögliche Folgen die Nichtbereitstellung oder Quelle die personenbezogenen Daten (Daten von Dritten)
13. Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling inkl. Logik
14. Informationen über Zweckänderung

Exkurs: Bußgelder und Kontakt mit der Behörde

Woran wird die Bußgeldhöhe bemessen?

- DSGVO schreibt wesentlich höhere Bußgelder (20.000.000 Euro oder 4% Vorjahresumsatz, falls höher) als das BDSG (bis zu 300.000 Euro) vor
- Verhängte Bußgelder müssen eine abschreckende Wirkung entfalten und verhältnismäßig sein

Kriterien[1] für Höhe von Bußgeld

- Art, Schwere und Dauer des Verstoßes
- Vorsätzlichkeit oder Fahrlässigkeit
- Maßnahmen zur Schadensminderung
- Grad der Verantwortung unter Berücksichtigung der getroffenen TOM
- Einschlägige frühere Verstöße
- Umfang der Zusammenarbeit mit der Behörde
- Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind
- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde
- Finanzielle Vorteile oder vermiedene Verluste

Kontakt mit der Behörde (nach BDSG)

- Ein „Ja“ zum Servicegedanken des Kreditinstituts
- Vortäuschung ständiger Überwachung rechtswidrig
- Kameras für den Schiffsführer
- Selbstauskünfte bei Mietinteressenten
- Daten aufgrund der Anfrage unmittelbar gelöscht
- Nichtbestellung Datenschutzbeauftragten
- Hinweispflicht beim Reisebüro
- Unzulässig/vorsätzlich Daten für Werbung verarbeiten
- Betriebsöffentliche Fehlzeiten der Beschäftigten
- Abteilungsweite Geburtstagsliste / Geburtstage auf Vereins-Webseite
- Verbleib der Kundendaten nach Insolvenz
- Weitergabe der Mitgliederdaten an Dachverband
- Spende für den Kunstrasen
- Unterschriftensammlung gegen Windpark
- „Daten“schutz“container im öffentlichen Raum
- Schreddern? Aber richtig!

1 Auswahl an Kriterien nach Art. 83 Abs. 2 EU-DSGVO

Most wanted: Datenschutz-Risiken im Verein

Fotos von minderjährigen Spielern	Videoüberwachung des Vereinsgelände (inkl. DSB)	Geburtstagsliste auf Webseite oder Vereinsheft	Adressen von Trainern auf Webseite oder Vereinsheft
E-Mailverteiler ohne BCC	Kontaktformular online	Adressweitergabe an Sponsoren	Spendenliste
Diagnosen im Internet-Spielbericht	Verpflichtung auf Datengeheimnis	Sitzungsprotokolle online	Ergebnis- und Starterlisten

Handeln Sie jetzt – es lohnt sich mehrfach das Grundrecht auf informationelle Selbstbestimmung zu achten

Vermeiden Sie Haftungsrisiken mit astronomischen Bußgeldern

Verbinden Sie gesetzliche Pflichten mit vertrieblichen Chancen: Werben Sie mit Datenschutz

Eine gute Reputation aufzubauen dauert Jahre – sie zu verlieren dauert nur einen Klick

Seien Sie nicht angreifbar: Investieren Sie nicht in die Abmahnindustrie, sondern in Ihren Verein

Quick Wins: Priorisieren Sie die Maßnahmen und erkennen Sie sofort ihren Nutzen

Digestiv

Erste Regierungserklärung durch die Bundeskanzlerin in ihrer neuen Amtszeit (21.03.2018):

"[...] Europa und Deutschland (hat) durch die Erfahrung mit der sozialen Marktwirtschaft die einmalige Chance, hier wieder ein gerechtes, den Menschen in den Mittelpunkt stellendes System der Teilhabe an der Souveränität der Daten zu schaffen. Aber bis dahin haben wir noch einen weiten Weg zu gehen. Die Datenschutz-Grundverordnung **ist ein erster kleiner zaghafter Schritt**. Hier müssen wir weitergehen, wenn wir es gerecht machen wollen."

im Folgenden Thomas Jarzombek (CDU/CSU)

"Die Datenschutz-Grundverordnung ist ein Gesetzeswerk, das dieser Tage **viele Vereine und auch kleine Unternehmen in Aufruhr versetzt**, weil sie sich fragen: Welche Bedingungen müssen wir erfüllen?"

Hinweise in eigener Sache

Die vorliegenden Ausführungen von Datenschutz & Informationssicherheit Ingo Goblirsch LL.M. wurden im Rahmen einer Präsentation um mündliche Erläuterungen ergänzt. Sie sollten daher im Zusammenhang mit dem Vortrag gesehen werden.

Diese Schulung stellt keine Rechtsberatung dar und kann auch keine Rechtsberatung ersetzen. Die Kompakt-Schulung bietet einen Überblick über die Datenschutz-Anforderungen nach der EU-DSGVO - diese sind aufgrund der Kürze der Veranstaltung zu Teilen nicht vollständig dargestellt.

Die im Rahmen der Kompakt-Schulung zur Verfügung gestellten Informationen werden nach Möglichkeit vollständig und aktuell gehalten. Wir übernehmen jedoch keine Gewähr für die Richtigkeit, Vollständigkeit oder Aktualität der bereitgestellten Informationen.

Änderungen können sich insbesondere ergeben durch die ständige Rechtsprechung sowie die am laufenden Band neu erscheinenden und aktualisierten Ausführungsbestimmungen des Düsseldorfer Kreises/der Datenschutzkonferenz, der 18 unabhängigen Landes-Datenschutzbehörden, der Artikel-29-Datenschutzgruppe und den jeweiligen Branchenverbänden.