DEUTSCHE DATENSCHUTZ KANZLEI

EU-Datenschutzgrundverordnung - Umsetzung bei Vereinen

Stefan Fischerkeller, Deutsche Datenschutzkanzlei
Diplomverwaltungswirt (FH)
Geprüfter Datenschutzbeauftragter (DESAG)
Lead-Auditor DIN ISO/IEC 27001

Inhalt

DEUTSCHE DATENSCHUTZ KANZLEI

- Kurzeinführung in die EU-DSGVO
- Herausforderungen in der Praxis / Rechenschaftsprinzip
- Beispiele aus der Vereinspraxis
- Umsetzung / Vorgehensweise
- Hilfsmittel

Kurzvorstellung DDSK

DEUTSCHE DATENSCHUTZ KANZLEI

Team (www.ddsk.de)

Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, IT-Fachanwälte, Security-Experten

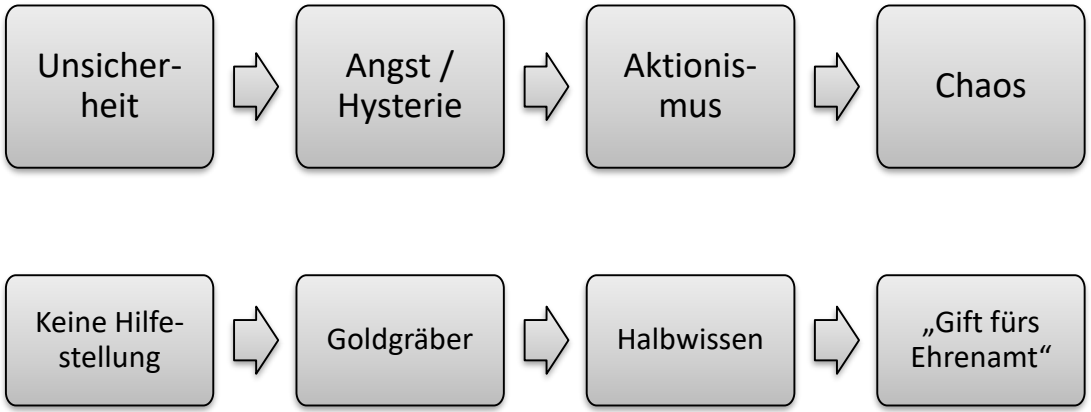
Portfolio

- **Externer Datenschutzbeauftragter**
- **Datenschutz-Managementsystem (Art. 5 Abs. 2 DSGVO)**
  - Konzeptionierung und Einführung, Betrieb und Überwachung
- **Informationssicherheits-Managementsystem (DIN 27001)**
  - Gap- und Risikoanalysen / Implementierung bis zur Zertifizierung
- **E-Learning-System** (www.schulungen-datenschutz.de)

Aktuelle Situation

DEUTSCHE DATENSCHUTZ KANZLEI

- EU-Datenschutzgrundverordnung: Umsetzungsfrist lief am 25.05.2018 ab
- Ab diesem Zeitpunkt „sollten“ alle Maßnahmen umgesetzt sein…



Mysterien…

DEUTSCHE DATENSCHUTZ KANZLEI

- Ja, wir dürfen auch zukünftig personenbezogene Daten erheben/verarbeiten!
  - Berechtigtes Interesse / Vereinssatzung als „Rechtsgrundlage“
- Nein, es kam keiner in den Knast am 26.05.18
  - Bisher…
- Ja, das (persönliche) Risiko steigt
  - aber die Sonne geht auch am 26.05.18 auf
- Ja, das bekommt man in den Griff
  - Ohne ein „Fass aufzumachen“
  - Wenn man vernünftig und praxisorientiert an das Thema heran geht

Was bedeutet Datenschutz?

DEUTSCHE DATENSCHUTZ KANZLEI

- Schutz von natürlichen Personen (Mitglieder, Beschäftigte, Ehrenamtliche, Lieferanten…)
- Personenbezogene Daten:
  - Telefonnummer, E-Mail-Adresse, Adressdaten (geringerer Schutzbedarf)
  - Sportliche Leistungen, Bild-/Videoaufnahmen (mittlerer Schutzbedarf)
  - Lebensläufe, Gesundheitsdaten (höherer Schutzbedarf)
- Betrifft jeden Verein!

Grundregeln des Datenschutzes (nichts Neues)

DEUTSCHE DATENSCHUTZ KANZLEI

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
  - vernünftig
- Zweckbindung
  - nur für den (Vereins-)Zweck
- Datenminimierung
  - nur erforderliche Daten
- Richtigkeit
  - korrekte und aktuelle Daten
- Speicherbegrenzung
  - so wenig wie möglich, so kurz wie möglich
- Integrität und Vertraulichkeit
  - Schutz der Daten
- Rechenschaftspflicht
  - Nachweisbarkeit

Der Einfachheit…
Datenverarbeitung erlaubt wenn…

1. Rechtsgrundlage
2. berechtigtes Interesse
3. Einwilligung

(Achtung bei unter 16 Jährigen)

Und dann…

1. Nur die „erforderlichen Daten“
2. Begründung dokumentiert!
3. Zweck entfallen: Löschung!

Was heißt das jetzt konkret? (ab 25.05.2018)

DEUTSCHE DATENSCHUTZ KANZLEI

- Bestellung eines Datenschutzbeauftragten (ab 10 Personen, die automatisiert pb. Daten verarbeiten – auch Ehrenamtler, Trainer etc.) ➔ Veröffentlichung auf Website
- Erstellen von Verfahrensbeschreibungen / „datenschutzrechtliche“ Prüfung
- Prüfen/Erstellen von Einwilligungserklärungen
- Infopflichten ableiten und sicherstellen
- Sicherstellung der Rechte der Betroffenen (Auskunft, Löschung etc.)
- Verträge zur Auftragsverarbeitung (bspw. Verwaltungssoftware, App, Newsletter etc.)
- Umgang mit Datenschutz-Verletzungen

RdB: Auskunft (Art. 15)

DEUTSCHE DATENSCHUTZ KANZLEI

- Grundsätzlich keine Neuerung zu § 34 BDSG-alt
- Auskunftsrecht über „ob“ und „Umstände der Verarbeitung“
  - Zweck
  - Datenkategorien
  - Empfänger
  - Dauer
- Hinweis auf Rechte
  - Löschung
  - Berichtigung
  - Beschwerde bei Aufsichtsbehörde
- Grundsätzlich unentgeltlich
- Frist: ohne Verzögerung, spätestens innerhalb eines Monats

RdB: Löschung („Vergessen“) (Art. 17)

DEUTSCHE DATENSCHUTZ KANZLEI

- Keine grundsätzliche Neuerung zum BDSG-alt
  - Pflicht zur Löschung, es sei denn es stehen Aufbewahrungspflichten-/Rechte entgegen
  - Bspw. Handels- und Steuerrecht (6, bzw. 10 Jahre)

- Recht auf Vergessen (Fokus: Social Media)
  - Löschung von Verknüpfungen / Einschränkung der Auffindbarkeit (bspw. Google-Suche)
  - Information an alle, die betroffene Daten verarbeiten
  - Fraglich: muss er das auch durchsetzen?

RdB: Datenübertragbarkeit (Art. 20)

DEUTSCHE DATENSCHUTZ KANZLEI

- Betrifft Daten, die der Betroffene bereitgestellt hat, bspw.
  - Zu Mitgliederverwaltung
  - Auf Basis einer Einwilligung
- Strukturiertes, gängiges, maschinenlesbares Format (bspw. .csv-Dateien)
- direkte Übermittlung, falls dies technisch möglich ist
- Hauptanwendungsfall:
  - Social Media
  - Aber auch:
    - Wechsel Stromanbieter
    - Wechsel Arbeitgeber
    - Vereinswechsel

Weitere Rechte der Betroffenen

DEUTSCHE DATENSCHUTZ KANZLEI

- Recht auf Berichtigung (Art. 16)
  - Anspruch auf Berichtigung unrichtiger personenbezogener Daten
- Recht auf Einschränkung (Art. 18)
  - Anspruch auf Sperrung
  - Verhinderung der weiteren Verarbeitung
  - Ersatz für Löschung, für den Fall das Aufbewahrungsfristen entgegenstehen
- Widerspruchsrecht (Art. 21)
  - Widerspruch zu werblichen Zwecken
  - Widerspruch gegen sonst zulässige Datenverarbeitung

Haftung (wirksam, verhältnismäßig, abschreckend)

DEUTSCHE DATENSCHUTZ KANZLEI

Bis zu 10 Mio. / 2 % des Umsatzes

Bis zu 20 Mio. / 4 % des Umsatzes

Grundsätze der Verarbeitung

Dokumentations-pflichten

Betroffenen-rechte

Aufgaben DSB

Übermittlung Drittland

Geldbuße nach Art. 83 DSGVO

Einführung

Datenschutz-Organisation
„light“

Kontrollen ab 25.05.2018

DEUTSCHE DATENSCHUTZ KANZLEI

- „Gießkannen“-Anfrage bei Datenschutzbeauftragten (Nachweispflicht!)
- Aufgrund fehlender Detailvorgaben: Prüfung der „**Datenschutz-Organisation**“ (Management-System)
- Stichproben
  - Unternehmen verarbeitet besonders schützenswerte Daten (z.B. Gesundheitsdaten)
  - Das Geschäftsmodell des Unternehmens basiert auf der Auswertung personenbeziehbarer Daten (BIG DATA, Auskunfteien etc.)
  - Es bestand in der Vergangenheit bereits Kontakt mit der Datenschutz-Aufsichtsbehörde
  - Unternehmen steht stellvertretend für eine bestimmte Branche oder genießt besondere Sichtbarkeit (z.B. Börsennotierung, Branchenführerschaft)

Beispiel: Hinweispflichten / „Bringschuld“

DEUTSCHE DATENSCHUTZ KANZLEI

Hinweis-/Informationspflichten gegenüber Betroffenen

- präzise
- transparent
- verständlich
- leicht zugängliche Form
- klare, einfache Sprache
- schriftlich oder elektronisch
- innerhalb eines Monats
- (grundsätzlich) kostenlos

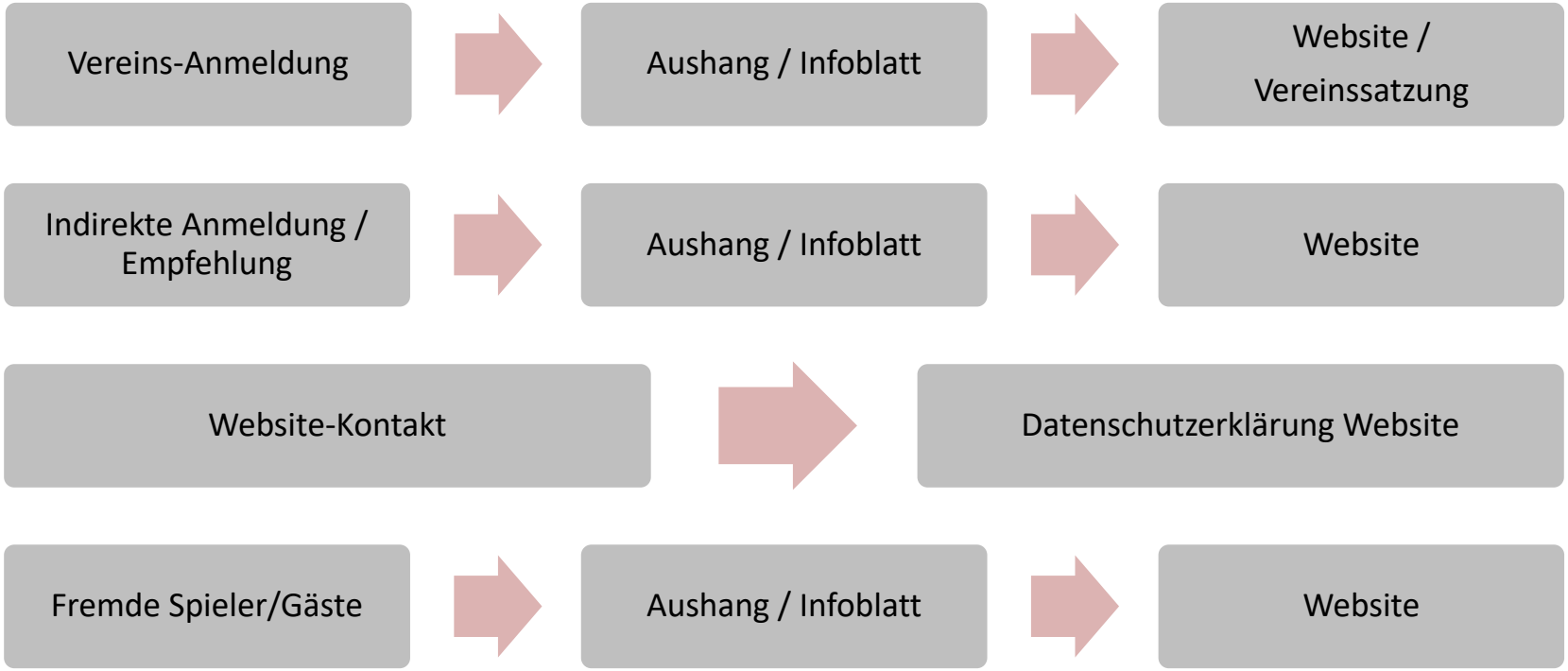
Inhalt einer Information

1.Firmenname- und Kontaktdaten, **Kontaktdaten des Datenschutzbeauftragten**
2.Verarbeitungen (Daten, Quellen, Dauer, Zwecke, Rechtsgrundlagen, Profiling)
3.Weitergabe (Empfänger, Zweck der Weitergabe)
4.Betroffenenrechte (Auskunft, Löschung, Widerspruch, Übertragbarkeit)
5.Möglichkeit zur Beschwerde bei einer Aufsichtsbehörde

Sanktionen: materieller Verstoß ➔ bis zu 20.000.000, – Euro bzw. 4% des Jahresumsatzes von Konzernen

Unklar: „rückwirkende Verpflichtung“ ab dem 25.05.2018

Beispiele im Verein



Einwilligungen

DEUTSCHE DATENSCHUTZ KANZLEI

Besteht kein ausreichender „Zweck“ bzw. berechtigtes Interesse, bleibt nur die Einwilligung

Anforderungen

- Freiwillig
- Informiert / transparent
- Schriftlich (ausnahmsweise elektronisch, mündlich)
- „hervorgehoben“ wenn gemeinsam bspw. mit Mitgliedsantrag

Achtung: Kinder/Jugendliche

- Keine starre Altersgrenze / Reifegrad entscheidend

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
Lohnabrechnung (über externen Dienstleister)	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	02.03.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name und Adressen der Beschäftigten • ggf. Religions-zugehörigkeit • Eindeutige Kennzahlen zur Steuer/ Sozialabgaben ...	Externer Dienstleister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)
Mitgliederverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	02.03.2018	Verwaltung der Vereinstätigkeiten	Mitglieder	• Name und Adressen • Eintrittsdatum • Sportbereiche ...	Keine	Keine	2 Jahre nach Beendigung der Vereinsmitgliedschaft
Betrieb der Webseite des Sportvereins (über Hosting-Dienstleister)	Max Meier 0981/123456-0 max@ waldmuehler-tsv.de	28.02.2018	Außendarstellung	• Mitglieder • Webseitenbesucher	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen
Veröffentlichung von Fotos der Mitglieder auf der Webseite	Max Meier 0981/123456-0 max@ waldmuehler-tsv.de	20.02.2018	Außendarstellung	Mitglieder	Fotos von Vereinstätigkeiten	Keine	Keine	Wenn Einwilligung widerrufen - unverzüglich
Beitragsverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	22.02.2018	Vereinsfinanzierung	Mitglieder	Bankverbindung	Steuerberater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)
...	...	...	...	...	...	...	...	...

Fallbeispiel

DEUTSCHE DATENSCHUTZ KANZLEI

Beim Verkauf von Eintrittskarten für ein Fußballspiel möchte der Verein Identifizierungsdaten erheben, um abzuklären, ob ein Stadionverbot für bestimmte, unbekannte Zuschauer ausgesprochen worden ist oder ob sie als gewaltbereit anzusehen sind.

Antwort:

- Berechtigtes Interesse des Vereins besteht nach Art. 6 Abs. 1f) DSGVO

Fallbeispiel

DEUTSCHE DATENSCHUTZ KANZLEI

Ein Verein möchte die Daten seiner Vereinsmitglieder für Spendenaufrufe und Werbung nutzen. Ist dies möglich?

Antwort:

- Gem. Art. 6 Abs. 1b) DSGVO ist die Nutzung für Spendenaufrufe und Werbung zur Erreichung der **eigenen Ziele** des Vereins möglich
- Die Nutzung zur **Werbung von Dritten** ist ohne Einwilligung der Mitglieder nicht zulässig

Fallbeispiel

DEUTSCHE DATENSCHUTZ KANZLEI

Ein Verein möchte Mitgliederdaten an die anderen Vereinsmitglieder übermitteln, z.B. über die Herausgabe von Mitgliederlisten oder einen Aushang im Vereinsheim o.ä. Ist die Übermittlung zulässig?

Antwort:

Zulässig wenn,

- der Verein ein berechtigtes Interesse hat und schutzwürdige Interessen der Mitglieder nicht entgegenstehen (Art. 6 Abs. 1f)
- Die Mitglieder eingewilligt haben
- oder der Vereinszweck darin besteht, die persönlichen oder geschäftlichen Kontakte zu pflegen, bspw. bei Selbsthilfe- oder Ehemaligenvereinen. Dieser Vereinszweck muss sich aber aus der Satzung ergeben. (Art. 6 Abs. 1b)

Herausgabe an Dritte

DEUTSCHE DATENSCHUTZ KANZLEI

- Mitgliederdaten können weitergegeben werden, wenn dies zur Erreichung des **Vereinszweck**, insbesondere zur **Verwaltung und Betreuung** erforderlich ist.

- Ansonsten ist eine Übermittlung nur möglich nach **Interessensabwägung** gem. Art. 6 Abs. 1f) DSGVO oder durch Abgabe einer **Einwilligung** der Mitglieder (Art. 6 Abs. 1a) DSGVO)

- **Wichtig:** zur Datenübermittlung gehört auch jede Art von **Veröffentlichung**, wie in einer **Zeitung**, im **Internet**, im Intranet, als Aushang oder die **Herausgabe einer Mitgliederliste an Sponsoren** oder **politische Parteien**

Gemeinde, KV, Arbeitgeber

DEUTSCHE DATENSCHUTZ KANZLEI

- Eine Übermittlung von Mitgliederdaten an die **Gemeindeverwaltung** ist zulässig. Es besteht sowohl ein **berechtigtes Interesse** des Vereins (Vereinsförderung durch die Gemeinde) als auch ein berechtigtes Interesse eines Dritten (die Gemeinde) und schutzwürdige Interessen der Vereinsmitglieder überwiegen grundsätzlich hierfür nicht.

- Bei Anfragen von **Krankenversicherungen** bzgl. erbrachter Leistungen wegen einer Verletzung, ist der Verein **berechtigt** den Namen des Schädigers mitzuteilen. Sollte dies nicht ausreichen, können auch weitere Angaben (z.B. über Spielverlauf) erfolgen. Um schutzwürdige Belange des Betroffenen zu berücksichtigen, sollte dieser vorher **angehört** werden.

- Dies gilt auch bei **Anfragen eines Arbeitgebers** (z.B. wenn er erfahren möchte, ob sein Arbeitnehmer an einer Vereinsveranstaltung teilgenommen hat, obwohl er krankgeschrieben ist)

Nächste Schritte

DEUTSCHE DATENSCHUTZ KANZLEI

DSB

- Beauftragter
- Ansprechpartner
- Evtl. gemeinsam mit anderen Vereinen

Verfahren

- Beschreibung
- Prüfung
- Maßnahmen

Einwilligungen

- Einführung
- Prüfung
- Optimieren
- Achtung: Jugendliche

Infopflichten

- Einführen
- Bekanntgeben

Rechte der Betroffenen

- Einführung
- Schulung

Vereinbarungen

- Dienstleister (bspw. Vereins-software)
- Datenschutz-Ordnung

Nächste Schritte

DEUTSCHE DATENSCHUTZ KANZLEI

- Prüfen wo welche (personenbezogenen) Daten vorliegen…
  - Zweck vorhanden?
  - Einwilligung vorhanden?
  - Sonst löschen!
- Technisch-organisatorische Maßnahmen treffen/beschreiben
  - Ist die Verfügbarkeit der Daten gesichert?
  - Sind Zugriffsrechte restriktiv vergeben?
  - Werden Daten „geschützt“ übermittelt (bspw. Verschlüsselung)?
  - Sind Daten getrennt (bspw. Angestellte, Mitglieder)?
- Schulung

Quellen

- https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-f%C3%BCr-Vereine.pdf
- https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf#
- https://www.lda.bayern.de/media/muster_1_verein.pdf
- https://www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf
- https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/OH-Datenschutz-im-Verein-Stand-1.-Mai-2017.pdf
- https://www.vereinswelt.de/dsgvo-fuer-vereine

DEUTSCHE DATENSCHUTZ KANZLEI

Herzlichen Dank für Ihre Aufmerksamkeit und

Viel Erfolg!

Stefan Fischerkeller

Dipl. Verwaltungswirt (FH)
Gepr. Fachkundiger Datenschutzbeauftragter (DESAG)
Lead-Auditor DIN/ISO/IEC 27001 (IRCA)

Deutsche Datenschutzkanzlei
Hauptverwaltung Bodensee
Richard-Wagner-Straße 2 - 88094 Oberteuringen
Tel.: +49 (0) 7544 / 904 96 91
fischerkeller@ddsk.de
www.ddsk.de