

Die EU-DSGVO - der Countdown läuft !

Daten**S**chutz**G**rund**V**er**O**rdnung das neue Datenschutzrecht in Europa

Das neue Datenschutzrecht in Europa

- ▶ Ist ein großer Schritt in der Aktualisierung des europäischen Datenschutzrechts.
- ▶ Wurde am 04.Mai 2016 im EU Amtsblatt veröffentlicht.
- ▶ Sie gilt ab dem 25.Mai 2018 also in weniger als 30 Tagen.
- ▶ Sie gilt für alle Unternehmen, **Verbände** , **Vereine**, öffentliche Stellen, u.s.w innerhalb der EU
- ▶ Nur geringe Öffnungsklauseln können Nationalstaaten mit eigenen Regeln ausfüllen (ausnahmen sind nicht zulässig).
- ▶ Das derzeit gültige Bundesdatenschutzgesetz (BDSG) wird zu diesem Zeitpunkt aufgehoben

Was ist neu in der EU-DSGVO

- ▶ Die Dokumentationspflichten werden deutlich ausgeweitet (Art5 Abs.2 DSGVO)
- ▶ Die Betroffenenrechte werden deutlich ausgeweitet und es wird eine Reaktionspflicht verbindlich festgelegt (Art. 12-23 DSGVO)
- ▶ Es werden neue Bußgeldbestände eingeführt
- ▶ Die Bußgelder erhöhen sich drastisch auf bis zu 20 Mio € oder 4% des weltweiten Jahresumsatzes, je nach dem, welcher Betrag höher ist

Es besteht eine Rechenschaftspflicht

- ▶ Einhaltung der Datenschutzgrundsätze (Art5 Abs.2 DSGVO)
- ▶ Wirksamkeit von Einwilligungen (Art. 2 und 8 DSGVO)
- ▶ Datensicherungsmaßnahmen (Art. 24 und 32 DSGVO)
- ▶ Datenschutz durch Technik TOM's (Art. 25 DSGVO)
- ▶ Auftragsverarbeitung (Art. 28 DSGVO)
- ▶ Verzeichnis von Verarbeitungstätigkeiten (Art30 DSGVO)

Was ändert sich zum 25.05.2018

- ▶ Durch das Inkrafttreten der EU-Datenschutz-Grundverordnung (DS-VGO) werden die wesentlichen datenschutzrelevanten Bestimmungen vom Bundesdatenschutzgesetz (BDSG) in die DS-GVO verlagert.
- ▶ Das BDSG wird zukünftig zumindest für die Sportvereine nicht mehr die Bedeutung haben, die es bis zum 24.05.2018 hat
- ▶ Für Sportvereine werden im Wesentlichen nur noch die Regelungen zur Videoüberwachung und zur Bestellung eines Datenschutzbeauftragten im BDSG von Bedeutung sein
- ▶ Es wird eine Reaktionszeit von einem Monat eingeführt. Einmalig kann eine Frist um 2 Monate verlängert werden. Die betroffene Person ist hiervon innerhalb des ersten Monats unter Angaben der Gründe zu informieren.
- ▶ Eine **Herausforderung wird die Erfüllung der Informationspflichten darstellen**, die der Verein bei der Erhebung und Verarbeitung der Daten gegenüber den betroffenen Personen zu beachten hat

Typische Verfahren im Verein

Im Verein gibt es einige Verfahren, die in Unternehmen so nicht vorkommen und deswegen spezieller Dokumentation bedürfen. Diese werden im Folgenden kurz angerissen.

▶ Mitgliederverwaltung

- ▶ Die Mitgliederverwaltung umfasst die Aufnahme neuer, die Abrechnung bestehender und die Information von Mitgliedern. Hier werden regelmäßig persönliche Daten wie E-Mail Adresse, Kontodaten (falls die Beiträge per Bankeinzug eingezogen werden), Alter usw. erfasst. Die Rechtsgrundlage für die Verarbeitung kann z.B. eine Einwilligungserklärung sein oder aber berechnigte Interessen des Vereins können vorliegen.

▶ Turnier und Trainingsverwaltung

- ▶ Bei diesem typischen Verfahren geht es vor allem um Leistungsdaten und die Übermittlung dieser. So kann an bestimmten Turnieren nur teilgenommen werden, wenn eine bestimmte Leistung erbracht wurde. Es werden also persönliche Daten wie Bestzeiten, Gewicht, Name, Adresse usw. erfasst. Es findet regelmäßig eine Übertragung der Daten statt (z.B. zu anderen Vereinen), was einer besonderen Rechtsgrundlage bedarf.

▶ Personalverwaltung

- ▶ Dies ist eine Verarbeitung, die auch in regulären Unternehmen vorkommt. Sollte der Verein z.B. Angestellte beschäftigen, müssen bestimmte Daten erhoben werden, wie z.B. Name, Kontoverbindung, Familienstand usw.. Da das Gesetz den Beschäftigtendatenschutz besonders legitimiert ist die Rechtsgrundlage für die Verarbeitung. Es handelt sich um eine Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses §26 BDSG (neu).

Was müssen die Vereine/Verbände sicherstellen

- ▶ Erstellung eines Verarbeitungsverzeichnisses nach Art. 30 DSGVO.
- ▶ Überarbeitung von Einwilligungserklärungen gemäß den Vorgaben der DSGVO.
- ▶ Prüfung und Sicherstellung der TOMs (= technischen und organisatorischen Maßnahmen).
- ▶ Sicherstellung der Betroffenenrechte
- ▶ Erstellung eines Sicherheitskonzeptes
- ▶ Abschluss von Vereinbarungen zur Auftragsdatenverarbeitung mit externen Dritten gemäß Art. 28 DSGVO wenn vorhanden

Rechtmäßigkeit der Erhebung der Daten

- ▶ 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. Überarbeitung von Einwilligungserklärungen gemäß den Vorgaben der DSGVO.
- ▶ 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.

ULD Aufsichtsbehörde von Schleswig-Holstein

(April 2018 Auszug aus der: Praxis- Reihe Datenschutzbestimmungen praktisch umsetzen)

- ▶ Auch für Vereine (Vereine mit eigener Rechtspersönlichkeit, die im Vereinsregister eingetragen werden sowie nichtrechtsfähige Vereine) gelten ab dem 25.05.2018 die Datenschutz-Grundverordnung (DSGVO) und das Bundesdatenschutzgesetz (BDSG) in seiner neuen Fassung (BGBl. I, Nr. 44, vom 05.07.2017). Die Vorschriften gelten **ohne Einschränkung**. Es ist z. B. nicht von Bedeutung, ob etwa hauptamtliche oder ehrenamtliche Mitarbeiter für den Verein tätig sind, wie viele Mitglieder der Verein hat, ob der Verein in erster Linie eigenwirtschaftlichen Zwecken dient oder ob ausschließlich und unmittelbar gemeinnützige und mildtätige Zwecke verfolgt werden, welche Größe ein vorhandener Kundenstamm hat, ob der Verein mehr einen lokalen oder überregionalen Wirkungskreis hat und ob die personenbezogenen Daten des Vereins ganz oder teilweise bei einer übergeordneten Stelle wie einem Bundesverband verarbeitet werden.



Das Wichtigste zu personenbezogenen Daten

- ▶ Personenbezogene Daten sind Angaben, die bei Zuordnung zu einer natürlichen Person Einblicke ermöglichen in deren physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität (Artikel 4 Ziffer 1 DSGVO) und so **Rückschlüsse auf deren Persönlichkeit** erlauben.
- ▶ **Besondere personenbezogene Daten** umfassen Informationen über die ethnische und kulturelle Herkunft, politische, **religiöse** und philosophische Überzeugungen, **Gesundheit**, Sexualität und Gewerkschaftszugehörigkeit. Sie sind besonders schützenswert.
- ▶ Betroffene haben vor allem das Recht auf informationelle Selbstbestimmung.

Beispiele für personenbezogene Daten

- ▶ allgemeine Personendaten (Name, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer usf.) Kennnummern (Sozialversicherungsnummer, Steueridentifikationsnummer, Nummer bei der Krankenversicherung, Personalausweisnummer, Matrikelnummer usf.)
- ▶ Bankdaten (Kontonummern, Kreditinformationen, Kontostände usf.)
- ▶ Online-Daten (IP-Adresse, Standortdaten usf.)
- ▶ physische Merkmale (Geschlecht, Haut-, Haar- und Augenfarbe, Statur, Kleidergröße usf.)
- ▶ Besitzmerkmale (Fahrzeug- und Immobilieneigentum, Grundbucheintragungen, Kfz-Kennzeichen, Zulassungsdaten usf.)
- ▶ Kundendaten (Bestellungen, Adressdaten, Kontodaten usf.)
- ▶ Werturteile (Schul- und Arbeitszeugnisse , Leistungsnachweise, Ehrungen, usf.)
- ▶ u. v. m.

Umgang mit Daten im Besonderen die Betroffenenrechte

- ▶ Erfolgt eine Erhebung personenbezogener Daten direkt bei der betroffenen Person, so hat der Verein aus Gründen der Transparenz von Datenverarbeitungsprozessen zum Zeitpunkt der Datenerhebung eine entsprechende datenschutzrechtliche Unterrichtung vorzunehmen (Art. 13 Abs. 1 und Abs. 2 DS-GVO). Daraus folgt, dass der Verein **in jedem Formular, das er zur Erhebung personenbezogener Daten nutzt**, auf Folgendes hinweisen muss:.
- ▶ Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
- ▶ Kontaktdaten des Datenschutzbeauftragten
- ▶ Zwecke der Verarbeitung (bitte im Einzelnen aufzählen)
- ▶ Rechtsgrundlage der Verarbeitung
- ▶ berechnete Interessen i.S.d. Art. 6 Abs. 1 lit. f) DS-GVO
- ▶ Empfänger oder Kategorien von Empfängern (z.B. Weitergabe personenbezogener Daten an eine Versicherung, an den Dachverband, an alle Vereinsmitglieder, im Internet)
- ▶ Speicherdauer der personenbezogenen Daten
- ▶ Belehrung über Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht gegen Verarbeitung)
- ▶ Hinweis auf jederzeitiges Widerrufsrecht der Einwilligung
- ▶ Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde
- ▶ **Teilt der Verantwortliche die vorgesehenen Informationen nicht, nicht vollständig oder inhaltlich unrichtig mit, so verletzt er seine Informationspflichten. Das ist gemäß Art. 83 Abs. 5 lit. b) DS-GVO bußgeldbewehrt**

Erhebung von Personaldaten der Beschäftigten des Vereins

- ▶ Die Verarbeitung personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses ist in Art. 88 DS-GVO und § 26 BDSG-neu gesondert geregelt.
- ▶ Soweit ein Verein daher Personen in einem abhängigen hauptamtlichen Verhältnis beschäftigt (z.B. Mitarbeiter der Vereinsgeschäftsstelle, Trainer) ist § 26 BDSG-neu anwendbar.

Widerspruchs- und Auskunftsrecht

- ▶ Zentraler Punkt des Datenschutzes ist zudem das Recht des Betroffenen auf Auskunft Artikel 15 der DS-GVO
- ▶ Mitglieder haben ein Recht auf Vergessen (d.h. die Löschung der Daten) z.B.
 - ▶ Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
 - ▶ Die betroffene Person widerruft ihre Einwilligung
- ▶ Es besteht eine Benachrichtigungspflicht des Vereins bei der Verletzung datenschutzrechtlicher Verpflichtungen.
- ▶ Neu ist in der DS-GVO das Recht auf Datenübertragbarkeit (Art. 20). Die betroffene Person hat danach das Recht, die sie betreffenden personenbezogenen Daten, die sie dem Verein bereitgestellt hat, in einem gängigen und maschinenlesbaren Format zu erhalten. Das Recht auf Datenübertragbarkeit beinhaltet, dass diese Daten beispielsweise einem anderen Verein übermittelt werden.

Verarbeitungstätigkeiten und Auftragsverarbeitung

- ▶ Die DS-GVO verlangt in Art. 30, dass ein Verzeichnis aller Verarbeitungstätigkeiten erstellt werden muss. Das gilt auch für kleinere Vereine, da die Datenverarbeitung nicht nur gelegentlich erfolgt (Art. 30 Abs. 5 DS-GVO)..
- ▶ Wenn externe Dienstleister mit dem Verein zusammenarbeiten, bezeichnet die DS-GVO das als „Auftragsverarbeiter“ und es muss hier eine ADV vom Auftragsnehmer vorliegen.
- ▶ Insbesondere kleine Vereine bedienen sich zur Finanzierungs- und Adressverwaltung durch Sparkassen und sonstiger Dienstleister. Diese werden als Auftragsverarbeiter nach Weisung des Vereins tätig. Eine Datenverarbeitung im Auftrag ist auch dann gegeben, wenn ein Verein seine Mitgliederdaten nicht auf einer eigenen EDV-Anlage speichert, sondern hierfür über das Internet einen Datenbankserver nutzt

Schriftliche Regelungen zum Datenschutz: Datenschutzordnung

- ▶ Den Verein trifft die Pflicht, die Grundzüge der Datenerhebung, -verarbeitung und -nutzung schriftlich festzulegen. (In der Satzung aufnehmen oder in einer gesonderten Datenschutzrichtlinie)
- ▶ Der Verein sollte außerdem regeln, welcher Funktionsträger zu welchen Daten Zugang hat und zu welchem Zweck er Daten von Mitgliedern und Dritten verarbeiten und nutzen darf
- ▶ Der Verein sollte insbesondere schriftlich festlegen, welche Daten beim Vereinseintritt für die Verfolgung des Vereinsziels und für die Mitgliederbetreuung und -verwaltung notwendigerweise erhoben werden

Wer benötigt einen Datenschutzbeauftragten

Ferner besteht für Vereine und Verbände auch weiterhin die Pflicht, einen Datenschutzbeauftragten zu bestellen.

Ein Verein muss immer dann einen internen oder externen Datenschutzbeauftragten bestellen, wenn in der Regel **mindestens zehn Personen im Verein ständig** oder unregelmäßig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Dies ist in § 38 BDSG-neu geregelt worden.

Dabei sind sämtliche Personen mitzuzählen, die Umgang mit personenbezogenen Daten im Verein haben, soweit diese Daten aus einer automatisierten Verarbeitung stammen, und zwar unabhängig vom Status. Es sind Vorstandsmitglieder, Arbeitnehmer, Selbständige und sogar ehrenamtlich Tätige zu berücksichtigen. **Insofern sind auch Übungsleiter mitzurechnen, die Listen von Kursteilnehmern oder Mitgliederlisten aus der EDV-gestützten Verwaltung des Vereins erhalten**

Wie bisher ist es nicht möglich, dass der Vorstand im Sinne des § 26 BGB die Funktion des Datenschutzbeauftragten im Verein übernimmt

Neu hingegen ist jedoch, dass der Datenschutzbeauftragte gemäß Art. 37 Abs. 8 DSGVO der jeweiligen zuständigen Aufsichtsbehörde gemeldet werden muss.

Gemeinsam schaffen wir es !!!

► Fragen und Diskussion ?

