

Was der Vereinsvorstand jetzt über die neue Datenschutzgrundverordnung DSGVO wissen muss

Das neue Datenschutzgesetz steht schon länger in den Startlöchern. Am 25. Mai 2018 ist es endlich soweit. Sie gilt!

Wann tritt die DSGVO in Kraft?

Die Regelungen stehen seit dem 25.5.2016 im Gesetz. Fassbare Gesetzeskraft erlangen sie jedoch erst ab dem 25.5.2018. Dann ist das Gesetz auch anwendbar.

Gilt die neue EU-DSGVO überhaupt für Vereine?

Auch Vereine müssen sich an die neue EU-Datenschutzgrundverordnung halten! Der Verein muss mit personenbezogenen Daten wie Mitgliederadressen, -Geburtstagen oder -Wohnorten vorsichtig umgehen. Sonst kann es leicht passieren, dass der Verein und Vorstand in die Haftungsfalle tappen. Deshalb ist es sehr wichtig, sich dem Datenschutz im Verein anzunehmen! Falls Sie es bisher noch nicht getan haben, ist jetzt der richtige Zeitpunkt.

Was ändert sich für konkret für meinen Verein?

DSGVO – das sind fünf Buchstaben, die angeblich alles sicherer machen sollen. Das neue Datenschutzgesetz bringt einige Neuerungen für den Datenschutz im Verein. Doch was bedeuten diese Änderungen für meinen Verein?

1. Rechenschaft ablegen!

Die größte Änderung betrifft eine zusätzliche Vereinspflicht – die **Pflicht zur Dokumentation**. Vereine müssen dokumentieren, dass sie die DSGVO einhalten. Sie müssen auf Nachfrage der Aufsichtsbehörde Nachweise in Form von

- einer Auflistung von nennenswerten Datenschutz-Zwischenfällen (DSGVO Art. 33)
- ein Verzeichnis, das die manuellen und automatisierten Verarbeitungsvorgänge personenbezogener Daten darstellt (DSGVO Art. 30)
- einer Datenschutzfolgenabschätzung bei Hochrisiko-Vorgängen (DSGVO Art. 35)

vorlegen können. Das heißt, ab dem Stichtag müssen Sie bei Hochrisiko-Vorgängen den Datenschutzbeauftragten des Vereins fragen, welche Folgen ein Datenschutzvorgang für Personenrechte hat. Das kann z.B. vorkommen, wenn Sie eine neue Technologie für die Datenspeicherung benutzen oder Kopiervorgänge vornehmen. Außerdem haben Sie ein Verzeichnis anzulegen, in denen Sie alle Vorgänge eintragen, bei denen Sie personenbezogene Daten verarbeiten – egal ob manuell oder automatisch.

Was muss das Verzeichnis für die personenbezogenen Daten enthalten?

Das Verzeichnis muss alle wichtigen Verarbeitungsmerkmale enthalten, z.B. Verarbeitungszwecke und eine Beschreibung der technischen und organisatorischen Maßnahmen. Was noch dazu gehört, können Sie im DSGVO Art. 30 nachlesen.

2. Einwilligungserklärung ohne Vertragsbindung!

Bei Einwilligungserklärungen gilt weiterhin, dass nachweisbar sein muss, dass die Person eingewilligt hat. Eine schriftliche Einwilligung muss in verständlicher Sprache verfasst sein. Außerdem gilt, dass die Person jederzeit widerrufen kann und dass der Widerruf so einfach wie die Annahme sein muss. Die widerrufende Person muss über den erfolgreichen Widerruf informiert werden.

3. Geldbuße beachten!

Dass die neuen Datenschutzvorschriften nicht zum Spaß da sind, merkt man an der neuen Geldbuße: **Bis zu 20 Millionen Euro kann es Institutionen kosten**, wenn sie gegen Anordnungen der Aufsichtsbehörde gemäß DSGVO Art. 58 verstoßen. **Es ist deswegen äußerst ratsam, den Datenschutz in Institutionen auf den neuesten Stand zu bringen**. Nur ein Beispiel: Eine Institution weigert sich, Datenschutzprüfungen durchführen zu lassen. Dann hat die Aufsichtsbehörde das Recht, eine Geldstrafe zu verhängen.

Auch wenn die Institution oder sein Vertreter gegen den Datenschutz verstößt und dadurch das Recht einer anderen Person verletzt, kann es zu Schadensersatzforderungen kommen – auch gegen den Vorstand!

4. Recht auf Datenübertragbarkeit beachten!

Die EU-DSGVO führt ein Recht auf Datenübertragbarkeit ein. Dadurch haben mit dem Verein in Beziehung stehende Personen das Recht

- ihre „personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“ (DSGVO Art. 20 Ab. 1) – z.B. auf Datenträgern wie USB-Sticks oder einer DVD.
- ihre personenbezogenen Daten anderen Mitgliedern bzw. Vereinsmitarbeitern zu übermitteln oder von einem Verantwortlichen an einen anderen Verantwortlichen übermitteln zu lassen (DSGVO Art. 20 Ab. 2).

sofern alle rechtlichen Voraussetzungen gegeben sind.

Der Verein muss sich so organisieren, dass er diese Rechte bieten kann. Regelungen zum Datenschutz im Verein müssen Sie auf aktualisieren

Wichtiges zum Datenschutz im Verein

Von der Datenschutzerklärung bis zum Datenschutzbeauftragten

1. Datenschutzerklärung des Vereins noch aktuell

Das neue Datenschutzgesetz sieht eine ganze Reihe neuer Pflichten vor (DSGVO Art. 13). Der Verein muss seiner Informationspflicht nachkommen und zum Zeitpunkt der Datenerhebung Folgendes mitteilen:

- Kontaktdaten des Vereins
- Kontaktdaten des Datenbeauftragten
- Zwecke der Verarbeitung
- „berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden“
- U.U. den Empfänger der Daten oder mindestens Kategorien von Empfängern, sofern nicht konkret nennbar

- U.U. Auskunft über Übermittlungen an Drittstaaten

Außerdem müssen diese Informationen bereit gestellt werden:

- Speicherdauer
- Auskunft über die gespeicherten Daten, eine Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung und Datenübertragbarkeit
- Widerrufbarkeit einer Einwilligung zur Datenverarbeitung
- Beschwerderecht bei der Aufsichtsbehörde
- Sind personenbezogene Daten gesetzlich oder vertraglich vorgeschrieben? Ist die Person zur Bereitstellung seiner Daten verpflichtet und welche Folgen hätte es, wenn die Person die Daten nicht bereitstellen würde?
- Besteht eine automatische Verarbeitung bzw. Entscheidungsfindung?
- Wo liegt die Datenquelle?

Vereine sollten nun prüfen, ob ihre Datenschutzerklärung noch ausreicht, und sie ggf. aktualisieren!

Satzungsüberprüfung

Auch die Satzung sollte überprüft werden, um den Datenschutz im Verein auf dem aktuellen Stand zu halten. Transparenz und Rechtssicherheit sollten dabei an erster Stelle stehen. Bedeutende Datenschutzregeln können eingefügt werden.

Überprüfung des Aufnahmeantrags

Auch der Aufnahmeantrag sollte überprüft werden. Bedeutende Datenschutzregeln können auch hier eingefügt werden.

2. Verzeichnis von Verarbeitungstätigkeiten notwendig?

Vereine mit weniger als 250 Mitarbeitern müssen kein Verzeichnis von Verarbeitungstätigkeiten anlegen (DSGVO Art. 30 Abs. 5), es sei denn

- die Verarbeitung bedroht die Rechte und Freiheiten der Personen
- die Verarbeitung wird nicht nur gelegentlich ausgeführt
- oder die Verarbeitung betrifft verbotene Bereiche wie ethnische Herkunft oder politische Meinungen (DSGVO Art. 10), oder Daten über Straftaten oder strafrechtliche Verurteilungen (DSGVO Art. 9).

Meistens empfiehlt es sich auch für kleinere Vereine, ein Verzeichnis von Verarbeitungsaktivitäten anzulegen, um dafür gewappnet zu sein, dass das Rechte einer Person bedroht werden – vor allem wegen Hacker-Angriffen.

3. Cookies abfragen?

Wir kennen es, dass immer mehr Webseiten eine Einwilligungserklärung für Cookies abfragen. Nach der neuen Datenschutzgrundverordnung ist dies nicht notwendig. Allerdings müssen Websitebetreiber, falls sie eigene Cookies oder Cookies von Drittparteien verwenden, **Änderungen in der Datenschutzerklärung** vornehmen: Es muss auf DSGVO Art. 6 Abs. 1 f hingewiesen werden (Grund der Verarbeitung). Außerdem muss klar gemacht werden, dass berechnete Interessen des Websitebetreibers vorliegen, die die Verwendung von Cookies notwendig machen, und dass die Nutzung von Cookies überwiegend im Interesse des Nutzers ist.

Weitere Änderungen zum Datenschutz im Verein bringt bald die ePrivacy-Verordnung. Diese Verordnung sieht neue Regelungen zu Cookies und Werbetoole vor. Sie kommt frühestens im Mai 2019.

4. Fristen beachten!

Stellt ein gespeichertes Mitglied einen Antrag und möchte sie gerne Auskünfte zu ihren personenbezogenen Daten, hat der Verein dem Mitglied unverzüglich (DSGVO Art. 12 Abs. 3) und spätestens innerhalb eines Monats, nachdem der Antrag eingegangen ist, zu informieren. Wenn komplexe Anträge oder zu viele Anträge vorliegen, kann die Frist verlängert werden, um einen Monat.

Wie oben schon erwähnt, müssen außerdem Datenschutz-Vorfälle wie z.B. Hacking-Angriffe, aufgelistet werden. Größere Datenschutz-Vorfälle sind der Aufsichtsbehörde 72 Stunden nach Erkennen des Vorfalls zu melden.

5. Regelungen für Kinder

„Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind.“ DSGVO Erwägungsgrund 38

Viele Vereine haben einen hohen Kinderanteil als Mitglied. Im BDSG gab es bisher keine besonderen Regelungen für Kinder betreffend Datenschutzrecht. Der Datenschutz im Verein ändert sich aber durch das DSGVO. Unter dem DSGVO (DSGVO Art. 8) ist die Verarbeitung von Daten von Kindern unter 16 Jahre nur erlaubt, wenn die Erziehungsberechtigten ihre Einwilligung geben, oder die Zustimmung zur Einwilligung geben.

6. ADV-Verträge und Dienstleistungsverträge prüfen!

Alte ADV-Verträge sollte man auf Einhaltung des Datenschutzes prüfen bzw. prüfen lassen.

Neuerungen:

Nach dem BDSG-Gesetz war der Verein für das Einhalten des Datenschutzes bisher alleinverantwortlich. Nach dem neuen DSGVO Art. 28 wird in manchen Fällen nun auch der Auftragnehmer der Datenverarbeitung haftbar gemacht.

Verträge mit Auftragsdatenverarbeitung können Sie zukünftig nicht nur schriftlich, sondern auch elektronisch abschließen (DSGVO Art. 28 Abschnitt 9).

Arbeitet der Verein mit Dienstleistern wie Newsletter-Versendern, Anbietern einer bestimmten Vereins-Software oder Paymentanbietern zusammen, müssen Sie ausreichend Beweise dafür geben, dass sie die DSGVO einhalten. Nach DSGVO Art. 28 Abschnitt 3 muss wenn dann **ein Vertrag** mit dem Dienstleister geschlossen werden, um den Datenschutz im Verein zu gewährleisten.

7. Braucht mein Verein plötzlich einen Datenschutzbeauftragten?

wenn mehr als neun Personen ständig mit der automatisierten Verarbeitung von Mitglieder- und Vereinsdaten beschäftigt sind oder diese nutzen, muss der Verein einen Datenschutzbeauftragten benennen (BDSG neu § 38). Auch wenn der Verein Datenschutzfolgenabschätzungen nach Art. 35 DSGVO bei Hochrisiko-Vorgängen vornimmt oder besondere Datenkategorien verarbeitet (DSGVO Art. 37 Abs. 1 b), die eine Vorab-Kontrolle benötigen, ist ein Datenschutzbeauftragter zu bestellen. Der Datenschutzbeauftragte ist durch den Vorstand oder durch Vereinsfunktionäre zu ernennen. Neu ist, dass der Datenschutzbeauftragte nach neuem EU-Recht nicht mehr schriftlich bestellt werden muss, sondern auch ohne Form ernannt werden kann. Außerdem entfällt die einmonatige Ernennungsfrist. Den Datenschutzbeauftragten muss man also umgehend ernennen. Die Kontaktdaten des Datenschutzbeauftragten müssen der Aufsichtsbehörde gemeldet werden (DSGVO Art. 37 Abs. 4).

8. Änderungen beim Datengeheimnis

Nach § 5 Absatz 1 BDSG war es den „bei der Datenverarbeitung beschäftigten Personen“ nicht erlaubt, „personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen“. Es bestand also die Pflicht, die Datenbearbeiter auf das Datengeheimnis zu verpflichten. Nach der neuen DSGVO-Regelung ist die Verpflichtung einer einfachen Anweisung gewichen (DSGVO Art. 32).

Sanktionen bei Verstoß!!

Wie oben schon erwähnt, können Verstöße gegen das neue Datenschutzgesetz Vereine bis zu 20 Mio. Euro kosten. Die Bußgelder sind spürbar gestiegen!

Unwissenheit schützt vor Strafe nicht! Mit der Mitgliedschaft im DEUTSCHEN EHRENAMT erhalten Sie von unseren Experten kostenfreie Rechtsberatung zum neuen EU-Datenschutzgesetz!

BITTE BEACHTEN! Im Schadenfall haftet der Verein mit seinem Vereinsvermögen und/oder es kann zu einer persönlichen finanziellen Haftung der rechtlichen Vertreter des Vereins „VORSTAND“ kommen!