

Tipps zur Anwendung der DS-GVO für Vereine

Die DS-GVO (Datenschutzgrundverordnung) kann das aktuelle Vereinsleben schwierig gestalten.

Für diesen Zweck haben die FREIEN WÄHLER versucht, Ihnen zentrale Inhalte der DS-GVO kurz, knapp und hoffentlich verständlich für Ihren Verein darzulegen.

Wir hoffen, dass wir Ihnen mit diesem Dokument ein wenig bei Ihrer Datenschutzarbeit im Verein helfen können.

1. Benennung eines Datenschutzbeauftragten

Ihr Verein muss **nur** dann einen **Datenschutzbeauftragten** benennen, **wenn** in dem Verein **mehr als zehn Personen mit personenbezogenen Daten arbeiten**.

Wichtig: Das bedeutet nicht, dass ein Verein, der mehr als zehn Mitglieder hat, einen Datenschutzbeauftragten benennen muss.

Es geht darum, dass nur maximal zehn Vereinsmitglieder mit personenbezogenen Daten arbeiten dürfen.

Tipp: Strukturieren Sie die Organisation Ihres Vereines so, dass die Zahl der Mitglieder, die mit personenbezogenen Daten arbeitet, die Zahl zehn nicht überschreitet.

2. Verzeichnis über die Verarbeitungstätigkeiten der personenbezogenen Daten

Sie sind leider gemäß DS-GVO gezwungen in einem Verzeichnis bzw. Dokument festzuhalten, wer, wann und mit welchen personenbezogenen Daten arbeitet.

Beispiele:

- a) Der Vorsitzende führt das Bestandsregister und erfasst die personenbezogenen Daten, die für die Mitgliedschaft im Verein unabdingbar sind. *Bsp. Name, Vorname, Adresse, Mobilfunknummer, Bankverbindung.*
- b) Der zweite Vorsitzende gratuliert den Mitgliedern zum Geburtstag und nutzt dazu die Geburtsdaten der Vereinsmitglieder.
- c) Der Kassenvwart zieht von den Mitgliedern die Mitgliedsbeiträge über die Daten der Bankverbindung ein.

Ein Muster für Vereine finden Sie hier:

https://www.lida.bayern.de/media/muster_1_verein_verzeichnis.pdf

(abgerufen: 28.06.2018)

3. Die Datenschutzverpflichtung von betroffenen Vereinsmitgliedern

Der Verein muss von seinen Mitgliedern, die mit personenbezogenen Daten umgehen, eine s.g. Datenschutzverpflichtung eingehen, bzw. diese von denen einfordern. In dieser Datenschutzverpflichtung müssen die Mitglieder, die mit personenbezogenen Daten arbeiten, versichern, dass sie bei der Verarbeitung der personenbezogenen Daten die Grundsätze der DS-GVO einhalten.

Tipp: Infos dazu finden Sie hier

https://www.lida.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf

(abgerufen: 26.06.2018).

4. Informationen und Auskunftspflichten gegenüber betroffenen Personen

Sie müssen betroffene Personen (z.B. Vereinsmitglieder) darüber informieren, in welcher Form Sie personenbezogene Daten verarbeiten und speichern.

Dieses gilt auch für die Website. Bereits auf der Website sollten Sie in der Datenschutzerklärung die entsprechenden Informationen zur Verfügung stellen. Hier wäre es sinnvoll, die Vereinssatzung abzubilden, die alle notwendigen Informationen enthält. Gleichzeitig müssen Sie, sofern Sie Google-Analytics oder ähnliche Analysetools (Besuchszahlenerhebung, etc. pp.) nutzen, diese Informationen über die Datenerhebung auf Ihrer Website in der Datenschutzerklärung darstellen.

Wenn Ihr Webhoster (z.B. 1und1, WIX, JIMDO, etc.) Daten der Besucher erfasst (z.B. IP-Adresse), dann müssen Sie die Seitenbesucher ebenfalls darauf hinweisen. Wenn von Dritten für Sie Daten erhoben werden (z.B. IP-Adresse) benötigen Sie sogar eine **Auftragsvereinbarung**. Siehe dazu Punkt 7.

Wir wissen, dass dadurch die betroffene Website der Datenschutzerklärung sehr lang werden kann. Das sollte Sie aber von der Informationsbereitstellung nicht abhalten, denn dann sind Sie rechtlich „auf der sicheren Seite“.

5. Löschen von Daten

Sie sind verpflichtet, Daten Ihrer Mitglieder oder anderen dritten Personen von den Sie Daten gespeichert haben, auf deren Verlangen hin zu löschen. ABER beachten Sie unbedingt gesetzliche Aufbewahrungsfristen.

Verlangt ein Mitglied z.B. nach Vereinsaustritt oder -ausschluss die Löschung aller seiner Daten, überprüfen Sie, ob Sie nicht zur zeitlich begrenzten Aufbewahrung (z.B. Vereinsbeiträge aufgrund steuerrechtlicher Begründung) bestimmter Daten verpflichtet sind. Löschen Sie also nur die Daten, deren Löschung Sie nicht in Konflikte mit geltenden Gesetzen bringt.

6. Sicherung der Daten

Die personenbezogenen Daten, die Sie erheben, müssen **angemessen** gesichert sein. Sie müssen Ihre EDV-Systeme und Aktenschränke vor dem Zugriff durch unberechtigte Personen sinnvoll sichern.

Papier als Datenträger personenbezogener Daten

Papiere müssen so aufbewahrt werden, dass unbefugte Dritte keinen Zugang zu den Papieren haben. Beispielsweise sollten Aktenschränke abgeschlossen sein bzw. Akten in verschließbaren Räumen aufbewahrt werden.

Computersysteme als Datenträger personenbezogener Daten

Für Computersysteme gilt:

1. Der Herausgeber des Betriebssystems (z.B. Microsoft, Apple, etc.) muss durch entsprechende Updates aktuelle Sicherheitsaktualisierungen durchführen.
2. Das Betriebssystem muss mit einer Antivirensoftware ausgestattet sein.
3. Das Konto des Betriebssystems muss mit einem Kennwort versehen sein.
4. Zu dem Konto des Betriebssystems, auf dem die Daten verarbeitet und oder gespeichert werden, dürfen nur berechtigte Personen Zugriff haben.
5. Datenbanken oder Dateien, in denen die betroffenen Daten gespeichert sind, sollten mit einem Passwort gesichert sein.

Die obigen fünf Punkte sind komplett kostenfrei realisierbar.

7. Auftragsverarbeitung mit dritten Personen

Wenn Sie personenbezogene Daten an Dritte Person zu Dienstleistungszwecken (z.B. Steuerberater) weitergeben, müssen Sie mit diesem eine s.g. Auftragsvereinbarung treffen, aus der hervorgeht, dass die rechtlichen Grundlagen der DS-GVO eingehalten werden.

Achtung: Auch das Erfassen von IP-Adressen bzw. erfassen von Webseitenzugriffe auf der Vereinswebsite ist eine Verarbeitung personenbezogener Daten durch Dritte. Auch in diesem Falle sollten Sie eine Auftragsverarbeitung mit Ihrem Webhoster (z.B. 1und1, WIX, JIMDO, etc.) treffen. Wichtig ist, dass die Verantwortung über die Datenverarbeitung sowie deren Einhaltung in Ihrer Verantwortung liegt.

Eine Formulierungshilfe für Vereine finden Sie hier:

https://www.lda.bayern.de/media/muster_adv.pdf (angerufen: 27.06.2018).

8. Datenschutzverletzung

Wenn es in Ihrem Verein zu Verletzungen der DS-GVO kommt, sind Sie verpflichtet, diese Verletzung nach Möglichkeit innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde zu melden.

Verletzungen können z.B. die folgenden Situationen sein:

1. Ein Fax wurde an den falschen Empfänger gesendet.
2. Es wurden personenbezogene Datenträger (Aktenordner, Festplatten, Computer) gestohlen oder diese sind verloren gegangen.
3. Daten sind durch Internetkriminalität (Hacking) in unbefugte Hände geraten.

Die Meldung hat hier <https://goo.gl/1tUAgL> (abgerufen: 28.06.2018) zu erfolgen.

Tipp: Senden Sie keine unverschlüsselten Emails mit personenbezogenen Daten Ihrer Vereinsmitglieder. Nutzen Sie dafür ein Verschlüsselungsprogramm. Der Hessische Datenschutz selbst nutzt aktuell (27.06.2018) das Verschlüsselungsprogramm PGP.

9. Datenschutz-Folgenabschätzung

Mittels einer Datenschutz-Folgenabschätzung muss abgeschätzt werden, welche Risiken für Persönlichkeitsrechte und Freiheit von Personen bestehen, wenn es zu einer Datenschutzverletzung kommt.

Wenn Sie **keine hochsensiblen Daten** (z.B. Gesundheitsdaten, strafrechtlich relevante Daten) Ihrer Mitglieder oder sonstigen Personen speichern und keine besondere Überwachung (z.B. Video oder Akustik) durchführen, müssen Sie keine Datenschutzfolgeabschätzung abgeben.

10. Videoüberwachung

Wenn Sie eine Video- und oder akustische Überwachung durchführen, sind Sie verpflichtet, Hinweisschilder aufzustellen.

Achtung: Solche Hinweisschilder sollten Sie auch aufstellen, wenn Sie künstliche Intelligenzen in Form von Cortana, Google, AMAZON-ALEXA, etc. betreiben, die das gesprochene Wort Dritter Personen aufzeichnen und oder überwachen.

Weiterführende Tipps:

1. Erfassen und speichern Sie nur die Daten, die Sie auch wirklich benötigen.
2. Wenn Sie Fotos von Mitgliedern oder sonstigen Personen aufnehmen, **muss** deren Einverständniserklärung dafür vorliegen. Holen Sie sich die Einverständniserklärung im eigenen Interesse schriftlich ein. Weisen Sie unbedingt darauf hin, was mit den Fotos geschehen soll. Lassen Sie Ihre Vereinsmitglieder unbedingt entscheiden, was mit den Fotos geschehen darf. Die abgebildete Person muss also ihr Einverständnis dafür geben, wenn die Fotos z.B.
 - a. im Vereinsheim aufgehängt werden.
 - b. in der Zeitung veröffentlicht werden.
 - c. auf der Website veröffentlicht werden.

Lassen Sie der abgebildeten Person die Wahl.

3. WhatsApp! Die Nutzung des Messenger-Dienstes WhatsApp ist rechtlich problematisch, denn wenn Sie WhatsApp im Standardmodus nutzen, wird jede Telefonnummer die Sie in Ihren Kontakten speichern automatisch an Facebook übertragen, denn WhatsApp gehört zu Facebook.
Diese Übertragung der Kontaktdaten stellt eine unberechtigte Datenweitergabe von personenbezogenen Daten dar. Wenn Sie also im Verein WhatsApp nutzen möchten, lassen Sie sich unbedingt eine Einverständniserklärung Ihrer Vereinsmitglieder geben, dass Sie damit einverstanden sind, dass Sie die Daten an Facebook weitergeben.

Quellen und weitere Hinweise

Bayrisches Landesamt für Datenschutzaufsicht. (2018). *Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc.* Abgerufen am 26. 06 2018 von https://www.lida.bayern.de/media/muster_1_verein.pdf