



Datenschutz in der IMV

Checkliste für die Umstellung auf die Datenschutzgrundverordnung

Die Rechtsgrundlage in Kurzfassung:

Die Datenschutz-Grundverordnung (DS-GVO) wird ab dem 25. Mai 2018 unmittelbar in den Mitgliedsstaaten der EU anwendbar sein und das bis dahin geltende Bundesdatenschutzgesetz (BDSG) ablösen.

Einige Regelungen in der DS-GVO enthalten sog. Öffnungsklauseln, die es den nationalen Gesetzgebern ermöglichen, länderspezifische Regelungen zur Konkretisierung der EU-Vorschriften zu erlassen. Hiervon hat auch der deutsche Gesetzgeber durch eine Neufassung des BDSG Gebrauch gemacht und dabei den Regelungsspielraum u.a. genutzt, um die Pflicht zur Benennung von betrieblichen Datenschutzbeauftragten dem bisher in Deutschland bestehenden „Status quo“ anzupassen.

Inhaltlich schreibt die DS-GVO im Wesentlichen die bisherigen datenschutzrechtlichen Grundprinzipien fort und entwickelt sie weiter. Die Grundsätze des „Verbots mit Erlaubnisvorbehalt“, der „Datenvermeidung und Datensparsamkeit“, der „Zweckbindung“ und der „Transparenz“ prägen auch die DS-GVO.

Zusätzlich werden mit der DS-GVO neue Transparenzanforderungen eingeführt: Stärkung der Rechte auf Information, Zugang und Löschung („Recht auf vergessen werden“). Für die verantwortlichen IMV'en bedeutet die DS-GVO erweiterte Dokumentations- und Nachweispflichten, um der Rechenschaftspflicht des Art. 5 Abs. 2 DS-GVO zu genügen.

Die Artikel der DS-GVO sind zusammen mit den Erwägungsgründen (EG) zu lesen. Diese erläutern die damit verfolgten Ziele und sind hilfreich für die Interpretation der Rechtsnormen.



Verwenden Sie zur Umstellung auf die DS-GVO die folgende Checkliste:

1. **Verzeichnis von Verarbeitungstätigkeiten,**
Art. 30 DS-GVO, Dieses löst das bisherige Verfahrensverzeichnis ab.
Wegen der regelmäßig bzw. immer wieder kehrend erfolgenden Mitgliederverwaltung (z.B. Aktualisierung des Mitgliederverzeichnisses aufgrund von Vereinsbeitritten) ist grundsätzlich das Erstellen eines Verzeichnisses von Verarbeitungstätigkeiten geboten. Dies entspricht auch der bisherigen Rechtslage, d.h. es bedarf ggf. nur einer Anpassung.

2. **Datenschutzbeauftragte,**
Art. 37 DS-GVO und § 38 BDSG, wie bisher hat ein Verein auch nach § 38 Abs. 1 BDSG einen Datenschutzbeauftragten zu benennen, wenn er in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt. Dabei zielt der Wortlaut nicht darauf ab, ob die zehn Personen in einem bezahlten Arbeitsverhältnis stehen, auch Ehrenamtliche zählen dazu. Maßgeblich ist zudem die Zahl der Köpfe, nicht die Zahl der Stellen. Sofern in einem Verein also zehn Vorstandsmitglieder oder Beauftragte die personenbezogenen Daten ihrer Mitglieder in einer Datei auf dem PC verarbeiten, ist ein Datenschutzbeauftragter zu bestellen. Überlegen Sie, inwieweit Sie sich mit vergleichbaren Vereinen zusammenschließen und auf eine Person zurückgreifen, die von jedem Verein selbst bestellt wird. Sprechen Sie ggf. Personen aus ihrem Vereinsumfeld an, die aufgrund entsprechender Ausbildung oder Berufstätigkeit in besonderer Weise dafür geeignet sind. Nach Art. 37 Abs. 7 DS-GVO haben Sie als Verein die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen (z.B. auf Ihrer Internetseite) und diese dem/der Landesbeauftragten ihres Bundeslandes als zuständiger Aufsichtsbehörde mitzuteilen (per Post oder über das noch zu errichtende online-Meldeportal).

3. **Information,** Art.12 ff. DS-GVO, Zukünftig müssen Vereine ihre Mitglieder / Kunden / Nutzer / Beschäftigten umfassender gem. Art. 13 und 14 DS-GVO zur Erhebung personenbezogener Daten informieren. Einwilligungen müssen den Anforderungen des Art. 7 ff. DS-GVO genügen.
Darüber hinaus stehen den von einer Datenverarbeitung betroffenen Personen (z.B. Vereinsmitgliedern) umfassende Auskunftsrechte und Hinweise zu. Dabei sind teilweise Fristen zu beachten. Implementieren Sie daher Verfahren, um Ihren Pflichten frist- und formgerecht zu genügen. Betroffenenrechte, Art. 15 ff. DS-GVO. Die Rechte der von einer Datenverarbeitung betroffenen Personen auf Auskunft, Berichtigung, Löschung und Widerspruch werden umfangreicher. Neu hinzugekommen ist das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO). Auch hier sollten Sie Verfahren entwickeln, um den Rechten der Betroffenen frist- und formgerecht nachkommen zu können. Eine gute Basis bildet das Verzeichnis von Verarbeitungstätigkeiten.



Sie müssen als Verein sicherstellen, dass die personenbezogenen Daten gelöscht werden, wenn die Notwendigkeit der Verarbeitung zur Zweckerreichung entfallen ist. Dies ist beim Austritt aus dem Verein der Fall und entspricht der bisherigen Regelung im BDSG.

Es sind die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen, damit z.B. die Daten ehemaliger Vereinsmitglieder, Kunden und Beschäftigten nicht mehr im aktuellen Dateibestand vorhanden sind. Sprechen Sie in dem Zusammenhang ggf. auch Ihren IT-Dienstleister oder den Anbieter des verwendeten Software-Verwaltungsprogramms an. Die DS-GVO will diese mit Art. 25 Abs. 1 DS-GVO dazu ermutigen, das Recht auf Datenschutz bei der Entwicklung und Gestaltung ihrer Produkte, Dienste und Anwendungen zu berücksichtigen.

4. **Auftragsverarbeitung,**

Art. 28 DS-GVO, wie bislang (§ 11 BDSG), so besteht auch unter der DS-GVO eine Sonderregelung für Verarbeitungen von personenbezogenen Daten durch Beauftragung eines anderen. Bestehende Verträge können fortgelten, sofern sie den Anforderungen der DS-GVO entsprechen, andernfalls sind diese anzupassen. Eine Auftragsverarbeitung liegt aber nicht nur vor, wenn ein Verein seine personenbezogenen Daten an jemand von außerhalb abgibt, sondern auch, wenn z.B. der Verein seine Rechner durch einen externen Dienstleister (IT-Firma) warten lässt und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Zur rechtssicheren Gestaltung des Vertrags wird die Verwendung der Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO empfohlen.

5. **Verletzung des Schutzes personenbezogener Daten,**

Art. 33 DS-GVO und 34 DS-GVO. Die Regelungen in Art. 33 und 34 DS-GVO lösen jene aus § 42a BDSG ab. In der Praxis kommt es auf vielfältigste Weise zu sog. Datenpannen, z.B. durch einen Hacker-Angriff, aber auch weil der USB-Stick des Kassenwirts mit den Mitgliederdaten verloren gegangen ist oder aufgrund eines Diebstahls des Laptops im Rahmen eines Einbruchs in die Geschäftsstelle. Liegt eine solche Verletzung des Schutzes personenbezogener Daten vor, müssen Sie diese innerhalb von 72 Stunden mit den in Art. 33 Abs. 3 DS-GVO genannten Mindestinformationen der zuständigen Datenschutzaufsichtsbehörde melden.