Checkliste zur EU-Datenschutz-Grundverordnung

10 Punkte, die Vereine bei der Umsetzung der Vorgaben aus der EU-Datenschutz-Grundverordnung (DSGVO) beachten müssen

Am 25. Mai 2018 treten die EU-Datenschutz-Grundverordnung (DSGVO) sowie das diese Verordnung ergänzende Bundesdatenschutzgesetz neu (BDSG) in Kraft. Damit verbunden sind Veränderungen der Rechtslage im Bereich des Datenschutzes, die es von Seiten von Vereinen und Verbänden, auch im Hinblick auf den erhöhten Sanktionsrahmen, zu beachten gilt.
Der Vorstand des Vereins, als „Verantwortlicher" im Sinne der DSGVO, muss somit prüfen, welche Maßnahmen in Abhängigkeit der Größe, Art und Struktur des Vereins ergriffen werden müssen, um den datenschutzrechtlichen Vorgaben aus der DSGVO und dem BDSG ausreichend Rechnung zu tragen.
Zur Klärung der Frage, welche Anpassungsprozesse im Verein hierzu im Einzelnen erforderlich sind und welche Aufgabenstellungen sich damit für den Verein ergeben, soll folgende Checkliste dienen.

1. **Wie können die Herausforderungen im Verein in Angriff genommen und welche Daten müssen eigentlich geschützt werden?**

   In einem ersten Schritt sollten die Vereinsgremien über die Notwendigkeit informiert werden, dass im Zuge des Inkrafttretens der DSGVO zum 25.05.2018 die bisherigen Prozesse in Zusammenhang mit der Verarbeitung von personenbezogenen Daten innerhalb des Vereins einer Prüfung unterzogen und Abläufe dokumentiert werden müssen.

   Evtl. ist es in Abhängigkeit des damit verbundenen Aufwands sinnvoll, über die Bildung einer Arbeitsgruppe im Verein zur Umsetzung der gesetzlichen Vorgaben und die Festlegung eines Ansprechpartners innerhalb des Vorstandes für das Thema „Datenschutz" nachzudenken.

   Der Datenschutz betrifft personenbezogene Daten. Das sind alle Einzelangaben über die persönlichen oder sachlichen Verhältnisse. In Vereinen betrifft das z.B. vor allem Mitglieder, daneben aber auch Spender, Klienten, Kunden. Typischer-

weise erhoben werden z.B. Name und Anschrift, Kommunikationsdaten, Geburtsdatum, Eintrittsdatum, Bankverbindung. All das sind personenbezogene Daten. Die Art der Erfassung (digital oder auf Papier) spielt keine Rolle.[1]

2. **Ist für alle personenbezogenen Daten die Zulässigkeit der Verarbeitung geprüft worden?**
   In vielen Fällen müssen die Betroffenen selbst aktiv in die Verarbeitung ihrer Daten einwilligen. Dies ist z.B. nicht erforderlich, wenn Daten im Rahmen einer vertraglichen Beziehung erhoben werden müssen. Bei Vereinen ist diese vertragliche Beziehung die Mitgliedschaft. Die für die Mitgliederverwaltung erforderlichen Daten (z.B. Name, Anschrift, Geburtsdatum, Bankverbindung) dürfen verarbeitet werden, da diese zur Erfüllung der Vertragsbeziehung erforderlich sind.[2]

3. **Gibt es im Aufnahmeantrag Hinweise auf den Umgang mit personenbezogenen Daten im Verein?**
   Es empfiehlt sich, schon beim Vereinsbeitritt z.B. in Form eines Merkblatts zum Datenschutz den Informationspflichten (z.B. Betroffenenrechte) nachzukommen und darauf hinzuweisen, zu welchem Zweck und auf welcher Grundlage welche personenbezogene Daten von Seiten des Vereins erhoben und verarbeitet werden sowie welche Rechte den Betroffenen zustehen. In diesem Zuge ist es ratsam, bereits bei der Aufnahme von Mitgliedern, sich zur Verarbeitung von personenbezogener Daten im Verein eine entsprechende schriftliche Einwilligung von den Betroffenen einzuholen, die den gesetzlichen Vorgaben zu Inhalt und Gestaltung von Einwilligungen, insbesondere den Betroffenenrechten, entspricht.[3]

4. **Gibt es in der Vereinssatzung bereits eine Regelung zum Datenschutz?**
   Eventuell gibt es bereits Regelungen in der Satzung zum Umgang mit personenbezogenen Daten bzw. zum Datenschutz allgemein. Eine weitere Möglichkeit, den Informationspflichten von Seiten des Vereins nachzukommen, besteht z.B. darin, in der Satzung auf eine Datenschutzrichtlinie des Vereins hinzuweisen. In einer Datenschutzrichtlinie kann z.B. neben den Betroffenenrechten festgeschrieben werden, welche Daten im Verein durch welche Funktionen erhoben und verarbeitet werden, wer Zugriff auf welche Kategorien von Daten hat und welche technischen Maßnahmen zum Schutz der Daten ergriffen werden. Die Regelungen in der Datenschutzrichtlinie können sich eng an das Verzeichnis der Verarbeitungstätigkeiten (s. Punkt 8) anlehnen.[4]

---

[1] Siehe hierzu auch Artikel 5 DSGVO und § 46 f BDSG neu
[2] Siehe hierzu auch Artikel 6 DSGVO und § 24; § 48 f BDSG neu
[3] Siehe hierzu auch Artikel 7, 12, 13, 14 DSGVO und § 32 f; § 51; § 55 f BDSG neu
[4] Siehe hierzu auch Artikel 13 DSGVO

5. Sind die Daten ausreichend geschützt?

Vereine müssen dafür Sorge tragen und überprüfen, ob die eigenen technischen und organisatorischen Maßnahmen der Datenverarbeitung geeignet sind, Datensicherheit zu gewährleisten. Bei allen Datenverarbeitungsvorgängen muss demnach überprüft werden, ob ausreichende Sicherheitsvorkehrungen getroffen worden sind. Dies reicht z.B. von Regelungen der Zutrittskontrolle, des Passwortschutzes und zu Anweisungen bezüglich der Eingabe und Löschung bis hin zur Sicherstellung der Verfügbarkeit von Daten.

Insgesamt spricht man von technischen und organisatorischen Maßnahmen, die den Schutz personenbezogener Daten sicherstellen sollen.[5]

6. Ist ein Datenschutzbeauftragter erforderlich?

Verantwortlich für den Schutz personenbezogener Daten ist der Vorstand. Wenn mindestens 10 Personen im Verein ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind, muss ein Datenschutzbeauftragter im Verein bestellt werden. Nach Bestellung eines Datenschutzbeauftragten muss dieser der zuständigen Aufsichtsbehörde namentlich gemeldet werden.

Der Datenschutzbeauftragte kontrolliert nicht nur die Einhaltung der datenschutzrechtlichen Bestimmungen, sondern unterstützt und berät den Vorstand und die Mitarbeiter/innen im Umgang mit personenbezogenen Daten.[6]

7. Gibt es ein Verzeichnis der Verarbeitungstätigkeiten?

Es ist davon auszugehen, dass auch Vereine ein Verzeichnis aller Verarbeitungstätigkeiten erstellen und regelmäßig aktualisieren müssen, da bereits die Mitgliederverwaltung im Verein in der Regel systematisch und nicht nur gelegentlich erfolgt. Ein solches Verfahrensverzeichnis kann z.B. in Form einer tabellarischen Auflistung erfolgen, in der neben den wichtigsten Eckdaten zum Verein und den Verantwortlichen z.B. auch Informationen darüber aufgeführt sind, von welchen betroffenen Personen welche personenbezogenen Daten zu welchen Zwecken auf welcher Grundlage von wem im Verein verarbeitet werden.[7]

---

[5] Siehe hierzu auch Artikel 24, 32 DSGVO und § 64; § 71 BDSG neu
[6] Siehe hierzu auch Artikel 37, 38, 39 DSGVO und § 38 BDSG neu
[7] Siehe hierzu auch Artikel 30, 35 DSGVO und § 70 BDSG neu

8. Sind alle Personen, die personenbezogenen Daten bearbeiten, auf das Datengeheimnis verpflichtet?

Jeder, der im Auftrag des Vereins mit personenbezogenen Daten in Berührung kommt, muss auf das Datengeheimnis verpflichtet werden. Eine Möglichkeit besteht z.B. darin, dass der Verein ein entsprechendes Formblatt vorbereitet und sich per Unterschrift die Inhalte bestätigen lässt. Die Verpflichtungserklärung sensibilisiert die Mitarbeiter im Umgang mit den personenbezogenen Daten.[8]

9. Gibt es einen Ablaufprozess bei Datenpannen und Zuständigkeiten hierzu?

Es besteht nun auch für Vereine die Pflicht, eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, der zuständigen Aufsichtsbehörde zu melden. Dies bedeutet, dass jeder Verein im Vorfeld einen Prozessablauf, ein Muster für die Meldung und die zuständige Person im Verein bestimmen sollte. In Abhängigkeit davon, ob z.B. besonders schützenswerte personenbezogene Daten (z.B. Gesundheitsdaten, ethnische Herkunft) im Verein verarbeitet oder Datenverarbeitungsprozesse durchgeführt werden, die eine hohe potentielle Gefährdung von Rechten und Freiheiten der Betroffenen mit sich bringen, ist ergänzend eine schriftliche Dokumentation darüber erforderlich, dass innerhalb des Vereins vorab eine Datenschutz-Folgeabschätzung durchgeführt wurde.[9]

10. Gibt es im Verein Vereinbarungen mit Dritten zur Auftragsdatenverarbeitung?

Wenn der Verein sich bei der Verarbeitung personenbezogener Daten externer Dienstleister bedient, ist hierzu eine Vereinbarung zur Auftragsdatenverarbeitung auf der Grundlage der gesetzlichen Bestimmungen zwingend erforderlich.[10]

Stand: 06.03.2018

[8] Siehe hierzu auch § 53 BDSG neu
[9] Siehe hierzu auch Artikel 9, 33, 34, 35 DSGVO und § 65 f BDSG neu
[10] Siehe hierzu auch Artikel 28 Abs. 4 DSGVO und § 62 f BDSG neu