Sechs Schritte zur Umsetzung der DSGVO

Die DSGVO erlegt den Datenverarbeitern umfangreiche Pflichten auf. Kenner der Materie wissen zugleich, dass das Ziel einer hundertprozentigen Befolgung aller Regeln illusorisch ist. Auch den Datenschutzbehörden ist bewusst, dass es kaum einem Verpflichtetem gelingen wird, das neue Recht lückenlos zu befolgen. Bei der Umsetzung des neuen Rechts empfiehlt sich daher eine ebenso gründliche wie pragmatische Herangehensweise. Zunächst sollten die wichtigsten Anforderungen des neuen Rechts nachweisbar erfüllt werden. Dies kann in fünf Schritten geschehen. Damit ist dann eine Basis gelegt für weitere Maßnahmen, mit denen sich nach und nach Schwachstellen schließen lassen, um den Erfordernissen der DSGVO in größtmöglichem Umfang zu genügen.

1. Erster Schritt: Betrieblicher Datenschutzbeauftragter
Filterfrage: 10-Personen-Regel
Wie nach dem bisherigen Recht gibt es auch nach Art. 37 Abs. 4 DSGVO in Verbindung mit § 38 Abs. 1 BDSG-neu eine 10-Personen-Regel: Sind mindestens zehn Personen im Verein mit der Datenverarbeitung beschäftigt, muss ein Datenschutzbeauftragter bestellt werden. Ist dies bislang nicht der Fall, sollte man die Bestellung schnellstmöglich nachholen. Bei der 10-Personen-Regel ist zu beachten, dass es allein um die Anzahl der Personen geht, die mit Datenverarbeitung ständig befasst sind. Ob es sich um den Schriftwart, den 1. Vorsitzenden oder um den Jugendwart, Kassenwart oder freie Mitarbeiter, Vollzeit- oder Teilzeitkräfte handelt, spielt keine Rolle. Es kommt allein auf die Kopfzahl an.

Aufgabe: Der Datenschutzbeauftragte im Verein
Der Datenschutzbeauftragte ist dem Vorstand direkt unterstellt, in der Wahrnehmung seiner gesetzlichen Aufgaben aber nicht weisungsgebunden (Art. 38 Abs. 3 DSGVO). Er überwacht die Datenverarbeitungsprozesse im Verein, unterrichtet und berät den Vorstand und wirkt auf die Einhaltung des Datenschutzrechts hin. Zudem soll er die an den Verarbeitungsvorgängen Beteiligten sensibilisieren und schulen. Gibt es eine Beschwerde, ist der Datenschutzbeauftragte die erste Anlaufstelle für die Datenschutzbehörde.

Tipp: Vereinsmitglied mit IT-Affinität. Auch die Bestellung eines externen Datenschutzbeauftragten ist möglich.

Warum handeln? Nichts ist leichter zu überwachen Für eine Datenschutzbehörde ist es leicht zu prüfen, ob ein Verein einen Datenschutzbeauftragten hat, da der Datenschutzbeauftragte in allen Datenschutzinformationen namhaft gemacht werden muss (Art. 37 Abs. 7 DSGVO). Jeder Verein, in der mindestens zehn Personen am Rechner tätig sind, sollte daher bis zum 25. Mai 2018 einen Datenschutzbeauftragten haben. Fällt die Auswahl schwer, sollte man beachten, dass ein schwach geeigneter Datenschutzbeauftragter allemal besser ist als kein Datenschutzbeauftragter.

2. Zweiter Schritt: Erstellung eines Verzeichnisses
Aufgabe: Erfassen der Verarbeitungstätigkeiten Art. 30 DSGVO schreibt die Führung eines Verzeichnisses aller Verarbeitungstätigkeiten vor. Das Verzeichnis dient dem Nachweis einer DSGVO-konformen Datenverarbeitung im Verein. Als Verarbeitungstätigkeiten gelten beispielsweise:
• elektronische Adressen- oder Mitgliederverzeichnisse
• Vereinssoftware
• elektronische Diktier- und Spracherkennungsprogramme
• Buchhaltungssoftware (Finanzbuchhaltung und Lohnbuchhaltung)
• Software zur Versendung und Verwaltung von E-Mails
• Software zur Terminverwaltung
• Vereins-Websites
• Vereinsseiten in Sozialen Netzwerken (z.B. Twitter, Facebook)

Für das Verzeichnis ist kein bestimmter Aufbau vorgeschrieben. Es muss schriftlich oder elektronisch (etwa als Word- oder Exceldatei) geführt werden. Für jede einzelne Verarbeitungstätigkeit sind folgende Angaben vorgeschrieben:

- den Namen und die Kontaktdaten des Vereins
- den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten (falls erforderlich)
- die Zwecke der Datenverarbeitung
- die Art der Personen, deren Daten verarbeitet werden (z.B. Mitglieder, Beschäftigte oder Lieferanten)
- die Art der verarbeiteten Daten
- die möglichen Empfänger der Daten, an die Daten übermittelt werden oder worden sind
- die Übermittlung von Daten in die USA oder in ein anderes Land außerhalb der EU (z.B. bei der Nutzung von Webmail-Diensten oder anderen Cloud-Diensten)
- Löschfristen
- Maßnahmen der Datensicherheit nach Art. 32 DSGVO.

Tipp: Der Lohn der Arbeit – Erkenntnisse für das Vereinsmanagement Die Erstellung des Verzeichnisses ist ein mühsamer Prozess, da es meist gar nicht so einfach ist, den Überblick darüber zu gewinnen, welche Datenverarbeitungsprozesse es im Verein gibt. Dies gilt umso mehr, wenn Vorstand und Funktionsträger vereinsbezogen Smartphones, Tablets und Laptops ortsungebunden nutzen. Auch die Arbeit auf derartigen Endgeräten kann als Verarbeitungstätigkeit gelten, für die die Pflicht zur Aufnahme in das Verzeichnis gilt. Wenn erstmalig ein Verarbeitungsverzeichnis angelegt wird, ist dies nach aller Erfahrung mit einem hilfreichen Klärungsprozess verbunden. Denn stets sind die Verarbeitungszwecke zu definieren, und die Festlegung von Löschfristen gibt Anlass, Daten nicht unüberlegt für alle Ewigkeit auf Datenträgern „verstauben“ zu lassen. Wenn ein umfangreiches Verzeichnis über die gesamte Datenverarbeitung im Verein erstellt wird, ist dies ein guter Anlass, über die Effizienz, Nachvollziehbarkeit und Sinnhaftigkeit der eigenen Datenverwaltung nachzudenken. Dies kann nicht nur dem Schutz von Mitgliederdaten und der Datensicherheit dienen, sondern auch der Effizienz der Arbeitsabläufe im Verein. Die Erstellung des Verzeichnisses erfordert eine Vielzahl von Entscheidungen:

- Wie werden Speicherfristen für die Datenbank mit den Mitgliederadressen (insbesondere nach deren Ausscheiden) definiert?
- Wer entscheidet in welchen zeitlichen Abständen, ob Adressdaten gelöscht werden?
- Wie verfährt man mit Bewerberdaten?
- Braucht man Einwilligungen für die Mitgliederfotos, die sich auf der Kanzlei-Website oder im Intranet finden?

Sonderaufgabe: Datensicherheit

Maßnahmen der Datensicherheit sind nach Art. 32 DSGVO im Verarbeitungsverzeichnis zu definieren. Hier ist IT-Sachverstand gefragt, an der Hinzuziehung entsprechender Fachleute führt kein Weg vorbei. Wie funktioniert die Datensicherheit? Wie sind die Zugriffsrechte auf Daten organisiert? Haben ausschließlich Personen Zugriff, die die Daten bei ihrer täglichen Arbeit benötigen, oder ist die gesamte Vereins-IT ein „offenes Buch“, in dem sich jedes Mitglied nach Belieben umschauen darf? Welche Maßnahmen gibt es zur Abwehr von Hackerangriffen und zum Virenschutz? Sollte es im Verein bislang eher mäßigen Aufwand bei der Datensicherheit gegeben haben, bietet die DSGVO einen willkommenen Grund, Versäumtes nachzuholen. Sind die Prozesse und Zwecke der Datenverarbeitung definiert, sind Löschroutinen und Maßnahmen der IT-Sicherheit im Verarbeitungsverzeichnis festgelegt, ist das Verzeichnis laufend zu pflegen. Ändern sich Verarbeitungsprozesse oder kommen neue hinzu, muss dies im Verarbeitungsverzeichnis festgehalten werden. Damit können Verarbeitungsprozesse auch in Zukunft Anlass geben,

regelmäßig die Rechtmäßigkeit der Datenverwaltung zu überdenken und dabei zugleich die Effizienz der vereinsinternen Arbeitsabläufe zu steigern.

Warum handeln?
Kontrolle ist Chefsache Das Verfahrensverzeichnis ist der Grundpfeiler der Dokumentation, zu der die DSGVO umfassend verpflichtet. Auf Anforderung der Aufsichtsbehörde muss der Verein jederzeit in der Lage sein, durch Vorlage des Verzeichnisses nachzuweisen, welche Verarbeitungsprozesse zu einem bestimmten Zeitpunkt aktiv waren. Für die laufende Pflege des Verzeichnisses sollte es daher klare Regeln geben. Zuständig hierfür kann der Datenschutzbeauftragte oder auch ein IT-Dienstleister sein. Die Kontrolle, ob alle Regeln eingehalten werden, sollte jedenfalls stets Chefsache sein.

3. Dritter Schritt: „Gap Analysis“
Aufgabe: Gut sein und besser werden Die Verarbeitungsverzeichnis ist der Ausgangspunkt für eine „Lückensuche“, die in den DSGVO-Umstellungsprozessen „Gap Analysis“ genannt wird.

Warum handeln? Maßnahmenplan Jede einzelne Verarbeitungsverfahren muss in der „Gap Analysis“ überprüft werden im Hinblick auf mögliche Schwachstellen. Zu diesen Schwachstellen zählen vor allem:
• Datensparsamkeit: Ist die Vorhaltung von Daten und deren Verarbeitung tatsächlich notwendig?
• Datenrichtigkeit: Ist gewährleistet, dass Mitgliederdaten stets auf dem neuesten Stand sind, Fehler berichtigt und unrichtige Daten gelöscht werden?
• Rechtmäßigkeit: Ist die Datenverarbeitung gem. Art. 6 Abs. 1 DSGVO rechtlich zulässig? Dient die Datenverarbeitung der Erfüllung eines Vertrages? Gibt es Einwilligungen der Betroffenen? Lässt sich die Datenverarbeitung durch eigene „berechtigte Interessen“ oder durch „berechtigte Interessen“ der Mitglieder legitimieren?
• Löschfristen: Werden Daten gelöscht, sobald sie nicht mehr benötigt werden? Gibt es eine Löschroutine, die eine rechtzeitige Löschung gewährleistet?
• Zugriffsrechte: Haben Mitglieder ausschließlich Zugriff auf Daten, die sie für ihre jeweiligen Aufgaben benötigen?
• Zugangskontrolle: Sind die Rechner im Verein ausreichend gegen den Zugang durch Unbefugte geschützt?
• Schutz gegen Hacker und Malware: Gibt es eine Firewall? Sind aktuelle Virenscanner installiert? Am Ende jeder „Gap Analysis“ steht ein Maßnahmenplan mit dem Ziel der möglichst umfassenden Datenschutzkonformität aller Verfahren.

4.Vierter Schritt: Datensicherheit
Aufgabe: TOMs kennen und ergreifen „Technische und organisatorische Maßnahmen“–abgekürzt TOMs – sind zu ergreifen, um die Sicherheit der im Verein verarbeiteten Personendaten zu gewährleisten (Art. 32 DSGVO). Die Vorschrift konkretisiert den Grundsatz der „Integrität und Vertraulichkeit“ gem. Art. 5 Abs. 1 lit. f DSGVO. Folgende Maßnahmen sind vorgeschrieben:
• Verschlüsselung: Soweit möglich, sollen personenbezogene Daten verschlüsselt werden. Es empfiehlt sich daher beispielsweise, die Verschlüsselung von E-Mails mit Verschlüsselungsprogrammen zu ermöglichen.
• Stabilität: Die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme ist auf Dauer sicherzustellen. Hierzu bedarf es einer fachkundigen Einschätzung einer IT-Fachfirma oder eines fachkundigen Mitarbeiters.
• Wiederherstellbarkeit: Verarbeitungsprozesse müssen gegen Datenverlust geschützt werden durch eine fachgerechte Datensicherung
• Regelmäßige Überprüfung: Eine regelmäßige Routineprüfung ist für die Datensicherheit gleichfalls vorgeschrieben. Die DSGVO schreibt keinen „optimalen Schutz“ vor, sondern ein „angemessenes Schutzniveau“, das anhand der bestehenden Risiken und des Stands der Technik zu bestimmen ist.

Investitionen, die außer Verhältnis zu der Größe des Vereins stehen, fordert die DSGVO nicht. Jedoch sollte jeder Verein überprüfen, ob die vorhandenen Maßnahmen bereits in die Jahre gekommen sind. Gab es bisher keine Unterstützung durch eine IT-Fachfirma, kann es ratsam sein, sich über eine zukünftige Beauftragung Gedanken zu machen. Das Durchdenken der Prozesse stellt keine kostenintensive Maßnahme dar und ist daher von jedem Verpflichteten zu fordern.

Warum handeln? Dokumentation zwingend
Dokumentationspflichten werden in der DSGVO groß geschrieben. Es sollte daher ein Papier geben, das die Bemühungen um „technische und organisatorische Maßnahmen" der Datensicherheit und deren Durchführung belegt. Auf dieses Papier kann im Verarbeitungsverzeichnis verwiesen werden, um der Verpflichtung Genüge zu tun, die Maßnahmen der Datensicherheit im Verzeichnis zu beschreiben.

5. Fünfter Schritt: „Papierform"
Erste Aufgabe: Verträge zur Auftragsdatenverarbeitung Soweit sich der Verein bei der Datenverarbeitung der Unterstützung durch Dienstleister aller Art bedient, dies können IT-Servicefirmen sein oder auch Cloud-Dienstleister für die Textverarbeitung, Terminverwaltung oder Spracherkennung, bedarf es entsprechender Verträge. Bestehende Verträge müssen an das neue Recht angepasst werden. Sofern noch keine Verträge existieren, sollte ein schriftlicher Vertragsschluss vor dem 25. Mai 2018 nachgeholt werden.

Zweite Aufgabe: Datenschutzinformationen
Zum notwendigen „Paperwork" gehören auch Datenschutzinformationen. Die Informationspflichten sind nach neuem Recht wesentlich umfangreicher als dies bisher der Fall war (Art.13 und 14 DSGVO). Die Datenschutzbestimmungen auf Vereins-Websites müssen überarbeitet werden. Zudem empfehlen sich allgemeine „Hinweise zur Datenverarbeitung", die jedem Mitgliedsantrag beigefügt werden sollten. Entsprechende Hinweise gehören zudem in Zukunft in jeden Arbeitsvertrag.

6. Weitere Schritte zur Datenschutzkonformität
Nach dem ersten „Maßnahmenpaket" gibt es noch weitere Schritte zur Datenschutzkonformität, die ratsam erscheinen:
• Betroffenenrechte: Die DSGVO gibt dem Betroffenen eine Palette von Rechten an die Hand. Im Verein sollte es daher klare Regeln geben, wie zu verfahren ist, wenn beispielsweise ein (früheres / ausgeschlossenes) Mitglied sein gesetzliches Recht auf „Datenübertragbarkeit" gem. Art. 20 DSGVO geltend macht und die Herausgabe aller Daten verlangt, die der Verein über ihn gespeichert hat. Auch für andere Betroffenenrechte, wie etwa das Auskunftsrecht (Art. 15 DSGVO) oder das Recht auf Löschung (Art. 17 DSGVO) sollten vereinsinterne Reglungen existieren.
• Meldepflichten: Jeder Datenschutzverstoß muss gem. Art. 33 DSGVO innerhalb von maximal 72 Stunden bei der zuständigen Datenschutzbehörde gemeldet werden. Verliert ein Funktionsträger sein Vereins-Handy und befinden sich auf dem Handy personenbezogene Daten, muss geprüft werden, ob eine Meldepflicht in Betracht kommt. Der bloße Verstoß gegen die Meldepflicht kann ein Bußgeld nach sich ziehen. Interne Arbeitsanweisungen sollten festlegen, wie bei einer Datenpanne vorzugehen ist.
• Datenschutzrichtlinien: In vereinsinternen Richtlinien sollten klare Regeln für die Datenverarbeitung aufgestellt werden mit dem Ziel des rechtskonformen Handelns. Art. 24 DSGVO legt die Erstellung derartiger Richtlinien nahe. Vereinsinterne Richtlinien geben Funktionsträgern Orientierung, wenn es darum geht, Datenschutzverstöße, Datenpannen und Datenlecks zu vermeiden. Zugleich lässt sich durch Datenschutzrichtlinien gegenüber der Aufsichtsbehörde dokumentieren, dass der Verein die gesetzlichen Pflichten zur Vorsorge gegen Datenschutzverstöße ernstgenommen hat.