Häufig gestellte Fragen zur Umsetzung der DSGVO in Vereinen

1. **Muss die Verarbeitung von personenbezogenen Daten in die Vereinsstatuten integriert werden?**

   Wie schon bisher, sollten die Statuten den Vereinszweck widerspiegeln. Daraus lässt sich ableiten, wofür die Daten genutzt werden (siehe Leitfaden 3.1). In den Statuten muss die Verarbeitung personenbezogener Daten nicht explizit angesprochen werden. Bei der Aufnahme neuer Mitglieder bietet es sich allerdings an, diese über die Verarbeitungen ihrer personenbezogenen Daten zu informieren (siehe Leitfaden 3.3).

2. **Ist bei bestehenden Mitgliedern eine (nachträgliche) Einwilligung zur Datenverarbeitung einzuholen?**

   Eine Einwilligung ist grundsätzlich nur notwendig, wenn keine andere Rechtsgrundlage (siehe Leitfaden 3.1) herangezogen werden kann.

3. **Wie und wie lange dürfen/müssen personenbezogene Daten aufbewahrt werden?**

   Es ist grundsätzlich unerheblich, ob personenbezogene Daten elektronisch gespeichert sind oder in einem analogen Dateisystem in Form von bedrucktem Papier abgelegt werden. Sobald der Zweck für den die Daten verarbeitet wurden entfällt, müssen die Daten gelöscht oder vernichtet werden.

4. **Welche Möglichkeiten der Online-Speicherung von personenbezogenen Daten gibt es? Wie sicher sind diese?**

   Grundsätzlich muss man sich bewusst sein, dass die Speicherung von Daten auf Cloud-Systemen (Dropbox, Drive o.ä.) bedeutet, dass diese auf fremden Systemen gespeichert werden. Wenn diese Dienste zum Speichern von personenbezogenen Daten verwendet werden, sind die Anbieter als Auftragsverarbeiter im Sinne der DSGVO zu betrachten. Es muss also ein Auftragsverarbeitungsvertrag mit den Anbietern abgeschlossen werden (siehe Leitfaden 5.2).

   Werden personenbezogene Daten hingegen verschlüsselt gespeichert, handelt es sich aus Sicht des Cloud-Anbieters nicht mehr um personenbezogene Daten, so dass die Regelungen der DSGVO nicht gelten. Die Daten können während der Übertragung zum Cloud-Server oder auf der eigenen Festplatte verschlüsselt werden und anschließend auf den Cloud-Dienst kopiert werden. Die Verschlüsselung von Daten ist bspw. durch die Software boxcryptor (https://www.boxcryptor.com) möglich, dessen Einsatz für die nicht kommerzielle Nutzung kostenlos ist.

5. **Dürfen/müssen personenbezogene Daten von nicht mehr aktiven und ausgetretenen Mitgliedern gelöscht werden?**

   Wenn die Führung des Mitgliederverzeichnisses der einzige Zweck für die Speicherung war, müssen die Daten von ausgetretenen Mitgliedern gelöscht werden. Anders ist es, wenn der Verein oder das Mitglied weitere Ansprüche geltend machen können (siehe Leitfaden 8).

6. **Wer muss bei einem Landesverband mit Mitgliedervereinen tätig werden?**

   Wenn ein Landesverband keine natürlichen Personen als Mitglieder hat, sondern nur andere Vereine, dann werden die Mitglieder der Mitgliedervereine nicht automatisch zu Mitgliedern des Landesverbandes. D.h. die Mitgliedervereine müssen „ihre" Mitglieder von geplanten oder tatsächlichen Verarbeitungstätigkeiten, wie zum Beispiel einer Übermittlung an den Landesverband, informieren (siehe Leitfaden 7.4).

7. **Was muss ein Verein beachten, der (auch) mit sensiblen Daten arbeitet?**

   Für sensible Daten nach Artikel 9 DSGVO gelten andere Rechtsgrundlagen. So dürfen diese Datenarten nicht auf Grundlage eines berechtigten Interesses des Vereins oder eines Dritten verarbeitet werden. Für die Verarbeitung von sensiblen Daten ist eine ausdrückliche Einwilligung erforderlich. Zudem gibt es in Artikel 9 Buchstabe d) DSGVO eine eigene Rechtsgrundlage, die Vereinen ohne Gewinnerzielungsabsicht die Verarbeitung dieser Daten erlaubt, wenn sie diese Daten zur Pflege regelmäßiger Kontakte für ihre rechtmäßigen Zwecke nutzt.

   Bei der Planung und Umsetzung der technischen und organisatorischen Maßnahmen sollte der Verein dem Risiko, das den Betroffenen aufgrund der Verarbeitung dieser Daten entsteht Rechnung tragen.

8. **Dürfen Ergebnislisten o.ä. in der Vereinschronik/Homepage/Facebook etc. veröffentlicht werden?**

   Im Normalfall, ja (siehe Leitfaden 7.3 bzw. 7.6).

9. **Sollte für Fotos prinzipiell immer das Einverständnis eingeholt werden? Falls ja, wie?**

   Im österreichischen Datenschutzumsetzungsgesetz § 12 ist die Bildverarbeitung genauer geregelt. Demnach ist die Verarbeitung von Bildmaterial (inkl. Ton, Ortsangabe, etc.) im überwiegenden berechtigten Interesse eines Vereins (also ohne Einwilligung) möglich, wenn der Verein ein *„… privates Dokumentationsinteresse verfolgt, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung solcher Personen eignen, gerichtet ist."*

Dies trifft insbesondere dann zu, wenn ein Verein z.B. bei Veranstaltungen fotografiert. In diesem Fall ist somit **keine** Einwilligung notwendig.

Die Rahmenbedingungen zur Veröffentlichung von Fotos in Vereinszeitungen/Homepage/Chroniken etc. wird im Leitfaden 7.3 und 7.6 behandelt. Zudem gibt es im Anhang des Leitfadens eine Mustereinwilligung für die Veröffentlichung von Fotos.

10. Wie ist die Handhabung von Daten (insbes. Fotos) bei Personen unter 14 Jahren?

Personen unter 14 Jahren genießen besonderen Schutz. Daher sollte bei der Information an Kinder auf eine entsprechend angepasste Sprache geachtet werden (Erwägungsgrund 58 und Artikel 12 Absatz 1 DSGVO).

Wenn ein sogenannter Dienst einer Informationsgesellschaft sich direkt an Personen unter 14 Jahren wendet, muss die Einwilligung durch Erziehungsberechtigte erfolgen.

11. Wie ist die datenschutzkonforme Handhabung von Newslettern?

Bei Newslettern handelt es sich meistens um eine Form der Direktwerbung. Diese kann gemäß Erwägungsgrund 47 DSGVO im berechtigten Interesse eines Verantwortlichen liegen und ist daher zulässig, wenn die Betroffenen entsprechend informiert wurden, vor allem über ihr Recht auf Widerspruch. Wird von diesem Recht Gebrauch gemacht, dürfen keine weiteren Nachrichten an diese Person gesendet werden.

Im Newsletter Verteiler können grundsätzlich zwei Arten von Adressen landen:

a) Personen, die sich für Dienste oder Leistungen des Verantwortlichen interessieren oder diese gekauft haben.
b) Personen, die sich z.B. über eine Website angemeldet haben.

Zur Beweissicherung empfiehlt es sich zu dokumentieren woher die Adressen stammen.

12. Wie ist der datenschutzkonforme Umgang mit E-Mails?

E-Mails stellen für sich keine eigene Verarbeitungstätigkeit dar, sondern sind meist Korrespondenz im Rahmen anderer Verarbeitungstätigkeiten.

Es empfiehlt sich daher folgendes einzuhalten:

- E-Mails immer zu einer konkreten Verarbeitungstätigkeit speichern.
- Personenbezogene Daten nur an berechtigte Empfänger übermitteln.
- Wenn nicht sichergestellt, ist, dass ausschließlich der legitime Empfänger Zugang zu einem E-Mail Account hat, keine personenbezogenen Daten an diese Adresse senden.
- Wenn eine E-Mail an mehrere Empfänger gesendet werden soll, sollen die Empfänger nicht sehen, wer aller diese Nachricht erhalten hat. Dies kann

durch Senden der E-Mail an BCC-Empfänger erreicht werden oder durch Einsatz von Mailinglisten oder einer Newsletter Software.

- Wenn E-Mails unverschlüsselt übermittelt werden, sollte bei der Übermittlung personenbezogener Daten den Risiken für die Betroffenen Rechnung getragen werden. Daten mit besonderem Schutzbedarf hinsichtlich der Vertraulichkeit, zum Beispiel Daten besonderer Kategorien gemäß Artikel 9 DSGVO, sollten grundsätzlich nicht unverschlüsselt gesendet werden.

13. Datenschutzkonformer Umgang mit WhatsApp?

Die Verwendung von WhatsApp im geschäftlichen Bereich wirft gewisse Fragen auf (Datensicherheit, Datenweitergabe ins EU-Ausland, Datenzugriff, etc.). Im Gegensatz zu E-Mails werden WhatsApp Nachrichten zwar standardmäßig Ende-zu-Ende verschlüsselt, wodurch es besser zur Übertragung vertraulicher Daten geeignet ist als unverschlüsselte E-Mails. Beachtet werden sollte aber jedenfalls, dass eine automatische Datenweitergabe ins EU-Ausland (lokales Adressbuch wird an WhatsApp übertragen) zumindest in den Datenschutz-Richtlinien des Anbieters selbst ausgewiesen wird (siehe whatsapp.com/legal) und diese Datenweitergabe ins EU-Ausland an gewisse datenschutzrechtliche Voraussetzungen gebunden ist, die der Verantwortliche selbst zu prüfen hat.

Empfohlen wird, dass auf dem Gerät des Verantwortlichen lediglich Adressen gespeichert sind, die in diese Form der Verarbeitung eingewilligt haben. Eventuell sollte die Nutzung eines WhatsApp business accounts geprüft werden.

Alternative datenschutzfreundlichere Anbieter für Kurznachrichten sind bspw. Telegram, Signal oder Threema.

14. Datenschutzkonformer Umgang mit Veranstaltungseinladungen?

Einladungen zu Veranstaltungen stellen eine Form der Direktwerbung dar, was ein berechtigtes Interesse eines Vereins sein kann und damit aus Datenschutzsicht zulässig ist. Kundendaten dürfen für die Zusendung von Information über ähnliche Produkte oder Dienstleistungen verwendet werden, wenn die betroffenen Personen bei der Erhebung über die geplante Verarbeitung und ihr Recht dieser zu widersprechen informiert wurden.