Datenschutz-Grundverordnung (DSGVO)

WARUM??

- Mit 25. Mai 2018 wird die Datenschutz-Grundverordnung (DSGVO) im gesamten europäischen Raum nach einer zweijährigen Übergangsphase umgesetzt.
- In Österreich gibt es noch das Datenschutz-Anpassungsgesetz, das unter anderem bereits die Einwilligung von Kindern ab dem 14. Lebensjahr, die Bildverarbeitung, usw. regelt.
- Für Datenschutzbehörde kontrolliert in Österreich die Einhaltung des Datenschutzes. Bei jeder vorliegenden Beschwerde muss sie ein Prüfverfahren einleiten. Dieses ist für den Betroffenen (derjenige, der die Beschwerde einreicht und um dessen Daten es geht) kostenfrei.

WAS sagt die DSGVO genau:

- Regelt die Verarbeitung von Daten sowohl von natürlichen, als auch juristischen Personen. Die juristischen Personen sind im österreichischen Verfassungsgesetz verankert und kommen nicht aus der DSGVO.
- Verantwortliche sind diejenigen, die allein oder gemeinsam mit andern über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. In den Vereinen sind dies die Obmänner, bzw. das Präsidium. Die Auftragsverarbeiter sind diejenigen, die die Daten im Auftrag des Verantwortlichen verarbeiten. In den Vereinen sind das z.B. der Obmann, der Kassier oder der Schriftführer, bzw. diejenigen die die Daten der Mitglieder (Name, Adresse, etc.) verarbeiten. Ihre Pflichten sind:
    - Führen eines Verarbeitungsverzeichnisses (ersetzt alte DVR-Meldung), kann aus der DVR-Meldung generiert werden. Dieses muss folgende Informationen enthalten:
        - Zweck der Verarbeitung
        - Kategorien der betroffenen Personen
        - Kategorien der personenbezogenen Daten
        - Kategorien von Empfängern
        - Ggf. Übermittlung personenbezogener Daten an ein Drittland (z.B. Druckerei im Ausland)
        - Vorgesehene Speicherdauer
        - Allg. Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherheit der Datenverarbeitung
    - Notwendigkeit zur Verarbeitung der Daten muss gegeben sein. In den Vereinen z.B. zur Erfüllung eines Vertrages (Mitgliedschaft im Verein, dem Verband und daraus resultierende Zusendung der Verbandszeitschrift). Sonst muss die konkrete Einwilligung zur Verarbeitung bzw. der Weitergabe der Daten extra eingeholt werden.

In den Vereinen z.B. die Mitgliedschaft im Verband, das Angebot und der Besitz der Vereinscard.

- Es existiert ein Koppelungsverbot für Einwilligungen. D.h. jede Einwilligung muss extra eingeholt werden. In den Vereinen darf die Vereinscard nicht automatisch mit der Anmeldung der Mitgliedschaft beantragt werden.
- Generell dürfen bei Online-Formularen zum Ausfüllen keine Haken vorab gesetzt sein.
- Bei Datenschutzverletzungen (z.B. Verlust eines Datenträgers, etc.) muss binnen 72 Stunden eine Meldung des Verantwortlichen an die zuständige Aufsichtsbehörde erfolgen. Auch die betroffenen Personen müssen benachrichtigt werden, wenn ein hohes Risiko für die persönlichen Rechte und Freiheiten dieser besteht. Bemerkt der Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten, so muss er dies unverzüglich dem Verantwortlichen melden. Die Meldung an die Datenschutzbehörde hat zu enthalten:
  - Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten. Wenn möglich mit Angabe der im Verarbeitungsverzeichnis angegebenen Datenkategorien.
  - Namen und Kontaktdaten der Anlaufstelle für weitere Informationen.
  - Beschreibung der wahrscheinlichen Folgen.
  - Beschreibung der vom Verantwortlichen ergriffenen Maßnahmen zur Behebung der Datenschutzverletzung und zur Abmilderung der möglichen nachteiligen Auswirkungen.
- Jede betroffene Person hat das Recht kostenfrei Auskunft über seine personenbezogenen Daten zu bekommen. Dieser Antrag kann formlos gestellt werden. Die Identität des Antragstellers muss nur dann nachgewiesen werden, wenn der Verantwortliche berechtigte Zweifel daran hat. Nur der Verantwortliche hat Auskunft zu geben. Die Auskunft hat schriftlich binnen eines Monats nach Eingang des Antrags zu erfolgen und muss beinhalten:
  - Die konkret verarbeiteten Daten
  - Verarbeitungszwecke
  - Kategorien der Daten die verarbeitet werden
  - Empfänger weitergegebener Daten, ggf. Informationen über Verträge mit den Empfängern der Daten bzgl. Datensicherheit
  - Wenn möglich die geplante Speicherfrist der Daten
  - Alle verfügbaren Informationen über die Herkunft der Daten (z.B.: welcher Verein hat die Daten übermittelt)
- Betroffene Personen sind darüber in Kenntnis zu setzen, dass sie folgende Rechte haben:
  - Recht auf Berichtigung ihrer Daten
  - Recht auf Löschung ihrer Daten
  - Recht auf Einschränkung der Verarbeitung
  - Recht auf Widerspruch der Verarbeitung
  - Recht auf Datenübertragung
  - Recht auf Beschwerde bei der Aufsichtsbehörde

- Personenbezogene Daten dürfen nur in den notwendigen Mengen und nur so lange, wie für die Verarbeitung benötigt, gespeichert werden.
- Der Verantwortliche hat die Pflicht alle mit Daten arbeitenden Mitarbeiter hinsichtlich Datensicherheit zu schulen. Dies muss mit dokumentiert werden.
- Der Verantwortliche hat sicherzustellen das die Auftragsverarbeiter (z.B. für Versand) die DSGVO einhalten. Dies kann mittels eines diesbezüglichen Vertrages geschehen.

Mustervorlagen Verarbeitungsverzeichnis

Stammdatenblatt

Datenverarbeitungen/Datenverarbeitungszwecke

Datenverarbeitungszwecke – Detailangaben

Allgemeine Beschreibung organisatorischer Maßnahmen

Stammdatenblatt

Name(n) und Anschrift(en) des für die Verarbeitung Verantwortlichen:

Vor- und Nachname

Adresse

Weitere Kontaktdaten:

Emailadresse

Telefonnummer

Name(n) und Anschrift(en) der Vertreter des Verantwortlichen

Vor- und Nachname

Adresse

Datenverarbeitung/Datenverarbeitungszwecke

Zwecke und Beschreibung der Datenverarbeitung

1. Mitgliederverwaltung: *folgt Beschreibung*
2. Verbandszeitschrift: *folgt Beschreibung*
3. Kooperationen mit Geschäftspartnern usw.: *folgt Beschreibung*
4. Usw.

Wurde eine Datenschutz-Folgeabschätzung durchgeführt?

Ja oder Nein

Datenverarbeitungszwecke – Detailangaben

Kategorien der betroffenen Personen

Mitglieder, Kooperationspartner, usw.

Rechtsgrundlagen

DSGVO Art. 6 abs. 1b (durch Vereinsmitgliedschaft)

Verträge und Zustimmungserklärungen sind abgelegt (freiwillig)

Vereinbarungen für Vereinskarten, usw.

Kategorie der verarbeiteten Daten und Löschungsfristen

Kategorien der betroffenen Personengruppe	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO[1], strafrechtlich relevant iSd Art 10 DSGVO[2]	Empfänger[3]	Empfänger	Empfänger	Empfänger	Empfänger	Empfänger
1 ***(oder Angabe der Personenkategorie)***	1								
	2								
	3								
	4								
2	5								
	6								
	7								

Kategorien von Empfängern, speziell bei Empfängern in Drittländern

Verband, Druckerei, Kooperationspartner, usw.

Dokumentation der getroffenen Garantien im Falle einer Übermittlung in Drittländer

[1] Daten nach Art 9 DSGVO sind besondere Datenkategorien („sensible Daten): rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten zur Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung.
[2] Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln unter behördlicher Aufsicht.
[3] In der Rubrik „Empfänger“ sind nur die „Empfängerkategorien“ (zB „Gerichte“, „Banken“ oder „Sozialversicherungsträger“) einzutragen.

Allgemeine Beschreibung organisatorischer Maßnahmen

Vertraulichkeit

Zugriffkontrolle

Weitergabekontrolle

Verfügbarkeit und Belastbarkeit

Schutz gegen zufällig oder mutwillige Zerstörung bzw. Verlust

z.B. Backup-Strategie

Evaluierungsmaßnahmen

Regelmäßige Schulung aller Betroffenen

z.B. Datenschutz-Folgeabschätzung