Amt der Tiroler Landesregierung
Abteilung Kultur
Michael-Gaismair-Straße 1 / 2. OG
A-6020 Innsbruck
Tel.: ++43 (0) 512/508-3752
kultur@tirol.gv.at
www.tirol.gv.at/kultur

Datenschutz für Vereine nach der Datenschutz-Grundverordnung (DSGVO)

Leitfaden / Checkliste **Info 10**

Allgemeines/Grundlagen

Der Schutz personenbezogener Daten ist ein Grundrecht und in Österreich gesetzlich als Verfassungsbestimmung verankert. Die Europäische Kommission hat mit der Datenschutz-Grundverordnung (DSGVO) eine umfassende EU-weit einheitliche Regelung des Datenschutzrechts geschaffen. Diese ist am 25.05.2018 in Kraft getreten.

Die DSGVO gilt für die „Verarbeitung personenbezogener Daten“. Darunter sind Daten zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (z.B. Name, Adresse, Geburtsdatum, SV Nummer, IP Adressen). Folglich verarbeitet de facto jeder Verein personenbezogene Daten und fällt in den Anwendungsbereich der neuen Bestimmungen.

Die Umsetzung der DSGVO ist eine erhebliche organisatorische, technische und juristische Herausforderung. Im Folgenden werden die wichtigsten Punkte in 9 Schritten zusammenfasst.

Schritt 1: Festlegen der Zuständigkeiten / Datenschutzbeauftragter

Vereinsintern sind die Zuständigkeiten für die Umsetzung der DSGVO festzulegen.

In bestimmten Fällen ist ein Datenschutzbeauftragter (DSB) zu bestellen, der die Organisation zu beraten hat, die Einhaltung der DSGVO überwacht und mit der Datenschutzbehörde zusammenarbeitet.

Nach der DSGVO ist die Bestellung u.a. zwingend vorgesehen,

- für Behörden und öffentliche Stellen

- wenn die Kerntätigkeit des Vereins in der Durchführung von Verarbeitungstätigkeiten besteht, die eine umfangreiche regelmäßige und systematische Überwachung erforderlich machen oder
- wenn die Kerntätigkeit in der umfangreichen Verarbeitung sensibler oder strafrechtlich relevanter Daten besteht.

Diese Voraussetzungen werden bei Vereinen zumeist nicht gegeben sein. Eine freiwillige Bestellung eines DSB ist immer möglich.

Info:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Der-Datenschutzbeauftragt.html

Schritt 2: Bestandaufnahme / Überblick verschaffen

Vor der Festlegung von Umsetzungsschritten sollte man sich einen Überblick über die DSGVO und die bestehenden Datenverarbeitungen verschaffen. Dabei sind Fragen zu klären wie z.B.:

- Welche Arten von IT Systemen werden genutzt
- Über welche personenbezogenen Daten verfügt der Verein
- woher kommen die Daten und auf welcher Grundlage wurden sie erhoben
- welche Verarbeitungstätigkeiten gibt es? (z.B. Mitgliederverwaltung, Lohnverrechnung, Buchhaltung etc.)
- Welche Gruppen von Betroffenen gibt es (z.B. Mitglieder, Angestellte, Kunden etc.)
- Wie sind Beitrittsverträge, Website, Statuten etc. in datenschutzrechtlicher Hinsicht ausgestaltet?

Info:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html

Schritt 3: Informationen über die Datenverarbeitungsprozesse erheben

Um ein Verzeichnis der Verarbeitungstätigkeiten zu erstellen und die Rechtsmäßigkeit der Verarbeitungstätigkeit beurteilen zu können, sind für jede einzelne Verarbeitungstätigkeit folgende Informationen zu erheben:

- Welche Datenkategorien werden verarbeitet?
- Zu welchem Zweck erfolgt die Verarbeitung?
- Erfolgt die Verarbeitung aufgrund einer Einwilligung? Liegt diese schriftlich vor?
- Werden Daten im Auftrag eines Dritten verarbeitet?

- Werden Daten von anderen im Auftrag des Vereins verarbeitet? Gibt es dazu Verträge?
- Werden Betroffene über die Datenverarbeitung informiert?
- Gibt es eine Datenschutzmitteilung?
- Durch welche technischen und organisatorischen Sicherheitsmaßnahmen werden die Daten geschützt?

Info:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Checkliste.html

Schritt 4: Verzeichnis der Verarbeitungstätigkeiten

Eine wesentliche Verpflichtung nach der DSGVO ist das Erstellen eines Verzeichnisses der Verarbeitungstätigkeiten. Die Mindestinhalte sind in Art. 30 DSGVO festgelegt.

- Kontaktdaten des Verantwortlichen, gegebenenfalls des Datenschutzbeauftragten
- Beschreibung der Verarbeitungstätigkeit
- Zwecke der Datenverarbeitung
- Kategorien betroffener Personen (z.B. Mitglieder, Kunden)
- Kategorien verarbeiteter Daten (z.B. Namen, Adresse)
- Kategorien von Empfängern, an die Daten weitergeleitet werden
- Aufbewahrungsfristen
- Technische und organisatorische Sicherheitsmaßnahmen

Info:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Dokumentationspflicht.html

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-verantwortliche.html

Schritt 5: Rechtmäßigkeit der Verarbeitungstätigkeiten

Nach der DSGVO ist für jede Datenverarbeitung eine Rechtsgrundlage erforderlich. Dabei kommen folgende Rechtsgrundlagen in Betracht:

- schlüssige und ausdrückliche Einwilligung
- Erfüllung eines Vertrages
- Erfüllung einer gesetzlichen Verpflichtung
- Erforderlichkeit zum Schutz lebenswichtiger Interessen

- Erforderlichkeit für eine Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt
- überwiegende berechtigte Interessen

Liegen Datenverarbeitungen vor, die von keiner gesetzlichen Verpflichtung oder vertraglichen Grundlage gedeckt sind und für die der Verein keine berechtigten Interessen geltend machen kann, ist eine Datenverarbeitung nur mit Einwilligung der betroffenen Person möglich.

Info:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Grundsaetze-und-Rechtmaes.html

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Einwilligungserklaerung-.html

Schritt 6: Auftragsverarbeitung

Auftragsverarbeiter sind Dienstleister, die Zugang zu personenbezogenen Daten haben und die Daten auf Anweisung und zu Zwecken des Vereins verarbeiten.

Es muss sichergestellt werden, dass der Verein in seiner Rolle als Verantwortlicher mit jedem Dienstleister eine Auftragsverarbeitervereinbarung abschließt, die den Anforderungen der DSGVO entspricht.

Info:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Pflichten-des-Auftragsver.html

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-auftragsverarbeitung.html

Schritt 7: Informationspflicht (Datenschutzmitteilung) und Betroffenenrechte

Eine Voraussetzung für die Rechtmäßigkeit der Datenverarbeitung ist, dass die Betroffenen über die Datenverarbeitung informiert werden. Die DSGVO sieht folgende Punkte vor, die in einer Datenschutzmitteilung enthalten sein müssen:

- Namen und Kontaktdaten des Verantwortlichen, gegebenenfalls des Datenschutzbeauftragten
- die Verarbeitungszwecke

- ob die Daten erforderlich oder verpflichtend sind und welche Folgen die Nichtbereitstellung hat
- die Rechtsgrundlage der Verarbeitung, sowie das Recht zum Widerruf bei Einwilligungen und die Bezeichnung des überwiegenden berechtigten Interesses als Rechtsgrundlage
- die Empfänger der Daten
- die Speicherdauer
- das Bestehen der Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragbarkeit)

Info:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Informationspflichten.html

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Betroffenenrechte.html

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/muster-informationspflichten-website-datenschutzerklaerung.html

Schritt 8: Datensicherheit

Angemessene Sicherheitsmaßnahmen umfassen technische (z.B. Sicherung der IT Systeme), organisatorische (z.B. Sicherheitstüren) und administrative Maßnahmen (z.B. Schulungen). Welche Maßnahmen getroffen werden müssen, hängt sowohl vom Risiko als auch von den Implementierungskosten ab.

Info:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Datensicherheit-und-Daten.html

Schritt 9: Datenschutz Folgenabschätzung

Für Datenverarbeitungen, die voraussichtlich ein hohes Risiko für die Betroffenen begründet, ist ein Datenschutz Folgenabschätzung durchzuführen.

Info:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Ablaufplan-Datenschutz-Fo.html

Weitere Vorgangsweise

Welche Aktivitäten in welchem Ausmaß zu setzen sind, hängt von den Geschäftsprozessen und den Verarbeitungstätigkeiten ab. Der sorgsame Umgang mit Daten verlangt neben der Durchführung der notwendigen Schritte zur Implementierung der DSGVO im Verein auch organisatorische Maßnahmen und Verantwortlichkeiten, um die Erfüllung der gesetzlichen Vorgaben laufend sicherzustellen.

Literaturauswahl:

Es gibt eine Vielzahl an Büchern, Artikeln und Praxisratgebern, z.B.

- Feiler/ Horn: Umsetzung der DSGVO in der Praxis. Wien 2018, Verlag Österreich
- Knyrim (Hrsg), (2016): Datenschutz-Grundverordnung. Wien 2016, Manz
- Unger: Grundzüge des Datenschutzrechts. Graz 2018, NWV
- Pachinger / Peham (Hrsg): Datenschutz-Audit. Wien 2018, LexisNexis