Ausgangslage

Am 01. September 2023 tritt das revidierte Schweizer Datenschutzgesetz (revDSG) in Kraft. Es verpflichtet dazu, notwendige Massnahmen zu ergreifen, um die Sicherheit von Personendaten sicherzustellen und den Datenmissbrauch möglichst zu verhindern. Bei Nichtbeachtung drohen empfindliche Strafen. Spätestens jetzt müssen sich Verbände und Vereine mit dem Thema auseinandersetzen. Wir haben hier für unsere Mitglieder die wichtigsten Informationen sowie Verweise auf nützliche Vorlagen sowie ein FAQ zusammengestellt.

Was ist Datenschutz?

Bereits heute gibt es Datenschutzbestimmungen, welche auch für Verbände und Vereine gelten. Der Datenschutz bezweckt in erster Linie den Schutz der Persönlichkeit und der Grundrechte von Personen. Es regelt was beachtet werden muss, wenn Personendaten bearbeitet werden. Als Personendaten gelten alle Angaben, welche einer Person zugeordnet werden können wie Kontaktangaben, Aufenthaltsorte aber auch Video- und Bildaufnahmen. Der Datenschutz schützt Personen vor dem ungerechtfertigten Beschaffen, Speichern, Bearbeiten und Verwenden von Daten. Das heisst, es dürfen nur Daten bearbeitet werden, die für den Zweck der Bearbeitung geeignet und erforderlich sind. Zentral ist dabei die transparente Information welche Daten für was gesammelt werden sowie eine Einwilligung der betroffenen Personen, insbesondere bei der Weitergabe von Daten. Daten dürfen weitergegeben werden, wenn die Zustimmung durch die Person selbst vorliegt, wenn die Daten öffentlich zugänglich sind oder wenn ein Gesetz die Weitergabe einräumt.

Darüber hinaus ist die Datensicherheit ein Grundsatz beim Datenschutz. Die Daten müssen sorgfältig und sicher verwaltet werden. Personenbezogene Daten müssen zudem vernichtet oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind. Dies gilt auch für Mitarbeitende und ehemalige Mitarbeitende. Alle Personen haben das Recht bei jedem Verband oder Verein anzufragen, ob und welche Daten über ihre Person gehalten werden.

Nichtpersonenbezogene Daten wie Finanzzahlen oder Produktedaten unterliegen nicht dem Datenschutz. Ebenfalls fallen auch anonymisierte Mitgliederdaten, welche für Statistikzwecke ausgewertet werden, nicht darunter.

Was ändert mit dem neuen Datenschutzgesetz?

Wenig! Am Kerngehalt des Datenschutzes ändert sich nicht viel. Die Prinzipien bleiben dieselben. Die Transparenz wird aber höher gewichtet. Darum müssen Datenschutzbestimmungen auf der Webseite aufgeführt und erläutert werden, was mit den Daten gemacht wird. Neu ist die Verpflichtung, Datenmissbrauchsvorfälle dem Eidgenössischen Datenschutzbeauftragten zu melden. Auch die Datenweitergabe an Lieferanten und Partner muss neu vertraglich geregelt werden.

Die Datenschutzerklärung auf der Webseite gewinnt mit dem neuen Gesetz an Bedeutung. Diese ist neu für alle verpflichtend. Darin muss informiert werden, welche Daten gesammelt und gespeichert werden, welche allfällige Programme genutzt werden und an wen man sich wenden muss, wenn man eine Auskunft möchte. Neu ist zudem, dass die Grundeinstellungen bei Formularen, Apps und Webseiten überall auf das Minimum eingestellt werden müssen, so dass nur die nötigen Daten gesammelt werden bzw. mitgeteilt werden müssen.

Ebenfalls wurde die Auskunftspflicht verschärft. Verlangt eine Person eine Auskunft darüber, ob und welche Daten über sie bearbeitet werden, so muss diese Auskunft nach gesetzlichen Vorschriften erfolgen, sofern keine Ausnahmen bestehen Unter https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/grundlagen/auskunftsrecht.html sind diese Vorschriften ausführlich nachzulesen. Auf derselben Seite gibt es auch eine Vorlage zum Auskunftsbegehren. Dabei muss auch informiert werden, unter welchen Bedingungen Daten an Dritte weitergegeben wurden.

Die wichtigsten Prinzipien beim Datenschutz

Der Wichtigste ist das Prinzip der Verhältnismässigkeit. Daten, die man zur Erledigung eines Auftrags benötigt, darf man erfassen.

Gleichzeitig gilt das Prinzip der Zweckmässigkeit. Die Daten dürfen nur dazu verwendet werden, wofür man sie erhalten hat. Wenn man zum Beispiel einer Autogarage seine Daten bekannt gibt, ist es klar, dass man Name, Vorname, Adresse, Kontrollschild, welches Fahrzeug und Kilometerstand der Garage mitteilt. Die Frage ist, ob der Garagist diese Daten an seinen Verband weitergeben darf, damit dieser ein Mailing machen kann. Dies muss wohl verneint werden. Der Garagist muss den Kunden fragen, ob er das darf.

Wesentlich ist ebenso die Transparenz. Jeder Kunde darf bei einer Unternehmung anfragen, welche Daten über ihn bearbeitet werden. Er besitzt von Gesetzes wegen ein Auskunftsrecht über seine Daten.

Das Gesetz verlangt zudem die Behandlung der Daten nach Treu und Glauben. Das heisst, dort nur dort und nur die Daten erfasst und bearbeitet werden, die für die konkrete Tätigkeit notwendig ist. Dazu gehören bei einem Musikverein namentlich die Kontaktdaten eines Mitglieds (Namen, Vorname, Postadresse, Mailadresse, Telefonnummer), das Instrument, die Dauer der Mitgliedschaft oder bekleidete Chargen.

Was muss geprüft oder geändert werden, um DSG-konform zu sein?

Betreffend: Allgemeine Mitgliederdaten

Vorstand und Mitarbeiter schulen	**Siehe Empfehlung Nr. 1**
Datenschutzerklärung erstellen	**Siehe Empfehlung Nr. 2**
Freiwillig ein Bearbeitungsverzeichnis erstellen	**Siehe Empfehlung Nr. 3**
Aufbewahrungsfristen prüfen	**Siehe Empfehlung Nr. 4**

Betreffend: Website

Datenschutzerklärung erstellen	**Siehe Empfehlung Nr. 2**
Prüfen, welche Tools eingesetzt werden	**Siehe Empfehlung Nr. 5**
Ausrichtung des Angebots innerhalb der Schweiz	**Siehe Empfehlung Nr. 6**
Auslanddatentransfer prüfen	**Siehe Empfehlung Nr. 7**

Betreffend: Social Media / WhatsApp

In Datenschutzerklärung darauf hinweisen	**Siehe Empfehlung Nr. 2**
Ggf. Einwilligung für Veröffentlichungen einholen	**Siehe dazu. "Gut zu Wissen"**
Auslanddatentransfer prüfen	**Siehe Empfehlung Nr. 7**

Betreffend: Hitobito

Datenschutzerklärung erstellen	**Siehe Empfehlung Nr. 2**
Aufbewahrungsfristen prüfen	**Siehe Empfehlung Nr. 4**

Bis wann muss man DSG konform sein?

Das DSG gilt ohne Übergangsfrist ab dem 1. September 2023. Wichtigstes To-Do dürfte ein, eine Datenschutzerklärung zu erstellen und zu publizieren, um der Informationspflicht zu entsprechen

1. Schulungen

- Vorstände und Personen, die mit Mitgliederdaten arbeiten, sind für das Thema Datenschutz zu sensibilisieren.
- Umsetzung: Teilnahme an Schulungen oder Informationen aus dem Internet

2. Datenschutz-erklärung

- Jeder Verein, der Personendaten verarbeitet, braucht eine Datenschutzerklärung. Diese sollte die Datenverarbeitung über die Webseite sowie über die Vereinsarbeit behandeln.
- Umsetzung: Datenschutzerklärung verwenden, Muster z.B. unter datenschutzmuster.ch

3. Bearbeitungs-verzeichnis

- Ein Verzeichnis der Datenverarbeitungsvorgänge muss der Verein (bei weniger als 250 Mitarbeitenden) nicht verpflichtend erstellen. Es ist aber gut zu wissen, welche Daten wie erhoben, gespeichert und gelöscht werden, damit der Vorstand sich datenschutzgerecht verhalten kann
- Umsetzung: Ein einfaches Verzeichnis erstellen

4. Löschungen

- Der Vorstand sollte überprüfen, welche Mitgliederdaten verarbeitet werden und welche Daten nicht mehr benötigt werden oder keine Aufbewahrungspflicht besteht, zum Beispiel weil die Mitglieder ausgetreten sind. Diese Daten sind dann zu löschen.
- Umsetzung: Aus Bearbeitungsverzeichnissen ergibt sich, welche Daten erhoben werden. Dies bildet die Grundlage, um Datenlöschroutinen einzuführen.

5. Cookie-Banner

- Mit dem neuen Datenschutzgesetz ist keine Pflicht für ein Cookie-Banner geschaffen worden. Im Einzelfall kann dies aber erforderlich sein, z.B. bei Datenübertragung ins Ausland. Bei dem Einsatz von Analyse-Tools (z.B. Google-Analytics) oder Social-Media-Plugins ist zu informieren und bei Auslandstransfer in die USA eine Einwilligung einzuholen
- Umsetzung: Prüfen, welche Analysetools eingesetzt werden und darüber in der Datenschutzerklärung informieren. Cookie-Banner sind meist nicht erforderlich.

6. DSGVO vermeiden

- Die Ausrichtung des Vereins (z.B. durch Darstellung auf der Webseite) sollte erkennbar nur innerhalb der Schweiz sein. Damit kann verhindert werden, der strengeren DSGVO zu unterliegen, selbst wenn einzelne Mitglieder EU-Bürger sind.
- Umsetzung: Auf der Webseite mitteilen, dass der Verein sein Angebot innerhalb der Schweiz ausrichtet.

7. Auslanddaten-transfer

- Der Transfer von Daten in die USA (z.B. bei Nutzung von MS365) oder über die Webseite gilt derzeit als unsicher, bis der Bundesrat einen Beschluss zur Angemessenheit des Datentransfers in die USA gefasst hat.
- Umsetzung: Bei MS365 kann ein Serverstandort in der Schweiz oder EU eingestellt werden. Bei Datenübertragungen in die USA bleibt zu hoffen, dass der Bundesrat im September oder Oktober den notwendigen Angemessenheitsbeschluss fasst. Ab dann ist der Datentransfer ohne vorherige Einwilligung zulässig.

Datenschutz im SBV

Der Schweizer Blasmusikverband (SBV) erfasst und bearbeitet lediglich Daten, die im Zusammenhang mit dem Verbandszweck stehen. So erfasst und verarbeitet der SBV insbesondere keine besonders schützenswerten Personendaten wie Konfession, politische Ausrichtung oder dergleichen. Für die Erfassung oder Verarbeitung solcher Daten bestünden höhere Anforderungen. Der SBV gibt auch keine bei ihm oder in von ihm benutzten Systemen (z. B. Hitobito) gespeicherten Personendaten ohne Einwilligung z.B. zu Werbezwecken an Dritte heraus. Wir treffen geeignete technische und organisatorische Massnahmen, um eine dem jeweiligen Risiko angemessene Datensicherheit zu gewährleisten. Der Zugriff auf unsere Website erfolgt mittels Transportverschlüsselung (insbesondere mit dem Hypertext Transfer Protocol Secure, abgekürzt HTTPS). Die meisten Browser kennzeichnen Transportverschlüsselung mit einem Vorhängeschloss in der Adressleiste.

Die Antworten auf diverse zum Datenschutz erhaltenen Fragen sind in einem FAQ-Sheet erfasst. Es wird auf der Seite des digitalen Unisono und auf der Webseite online zur Verfügung gestellt. Ebenfalls besteht die Möglichkeit, unter der Webadresse der Rechtsanwälte Wicki Partners AG weiterführende Informationen sowie Links zu Mustern, Vorlagen und einer Standard-Datenschutzerklärung zu beziehen: www.datenschutzmuster.ch

Datenschutzgesetz in Vereinen

Das neue Datenschutzgesetz enthält keine vereinsspezifischen Bestimmungen. Es verlangt auch nicht, Vereinsmitglieder proaktiv auf den 1. September 2023 zu informieren. Aber: Jeder Verein erfasst, bearbeitet und/oder verfügt über Personendaten, mit denen der Verein gesetzesgemäss umgehen muss. Der Vereinsvorstand trägt die Verantwortung für den datenschutzkonformen Umgang mit diesen Daten und die Einhaltung des DSG. Der Verein darf nur Personendaten erheben und bearbeiten, die mit dem Vereinszweck in direktem Zusammenhang stehen. Will der Verein weitere Daten erheben oder für andere als Vereinszwecke verwenden, muss er darüber vorgängig informieren und auch mitteilen, dass die Angabe der weitergehenden Daten verweigert werden kann.

Um der Informationspflicht zu entsprechen, wird üblicherweise eine Datenschutzerklärung (DSE) verwendet. Diese bedarf keiner Einwilligung, es muss jedoch die Möglichkeit der Kenntnisnahme bestehen. Am einfachsten geht dies mit der Platzierung der DSE auf der Website eines Vereins, vielfach erfolgt dies in der Fusszeile der Website (Footer).

Die Pflichtangaben einer DSE ergeben sich aus Art. 19 DSG. Der Umfang ist z.B. abhängig von den bearbeiteten Personendaten, Auslandstransfer und Social-Media-Einbindung. Der Entwurf einer einfachen DSE findet sich auf www.datenschutzmuster.ch.

Zu den Angaben einer Datenschutzerklärung zählen:

- Identität und Kontaktdaten des Vereins und des Vorstandes
- Aufzählung, welche Daten erhoben und bearbeitet werden
- Beschreibung, zu welchen Zwecken die Daten bearbeitet werden
- Nennung von Empfängern oder Kategorien von Empfängern, an die Daten weitergegeben werden (z.B. Tracking, Social-Media-Plugins und anderen Technologien im Zusammenhang mit der Nutzung der Website oder aber auch z.B. Treuhänder, Lieferanten und sonstige Dritte im Zusammenhang mit Vereinstätigkeit)
- gegebenenfalls Datenübermittlung ins Ausland
- Interne Ansprechperson
- Änderung der DSE (jederzeit und einseitig möglich)

Mit dem neuen Datenschutzgesetz ist keine Pflicht für ein Cookie-Banner geschaffen worden. Im Einzelfall kann dies aber erforderlich sein, z.B. bei Datenübertragung ins Ausland. Bei dem Einsatz von Analyse-Tools (z.B. Google-Analytics) oder Social-Media-Plugins ist zu informieren und bei Auslandstransfer in die USA eine Einwilligung einzuholen

Weitergabe von Personendaten

Der EDÖB1 weist auf seiner Webseite darauf hin, dass die Veröffentlichung von Personendaten in einem Magazin oder auf der Webseite nur zulässig ist, wenn diese zweckmässig ist, was der Vorstand vorgängig zu prüfen hat. Der Zugang zu Mitgliederdaten ist in einem geschützten Bereich und auf einen definierten Personenkreis zu beschränken.

Die Bekanntgabe von Mitgliederdaten (z. B. Abgabe der Mitgliederliste mit Adressen) an andere Mitglieder ist grundsätzlich nur zulässig, wenn zuvor die Einwilligung jedes einzelnen Mitglieds eingeholt wurde und klar definiert ist, zu welchem Zweck die bekanntgegebenen Daten verwendet werden (z. B., um miteinander Kontakt aufzunehmen; für Vereinsaktivitäten, aber nicht für Kundenwerbung). Bei elektronischer Versendung an Mitglieder ist die BCC «Blindkopie»-Funktion zu verwenden, um zu verhindern, dass Daten ohne Einwilligung an Mitglieder weitergegeben werden.

Die Bekanntgabe von Mitgliederdaten an Dritte ist nur zulässig, wenn die Mitglieder über den Zweck der Bekanntgabe in-formiert wurden und ausdrücklich zugestimmt haben oder die Möglichkeit hatten, im Vorfeld der Bekanntgabe zu wider-sprechen. Aus der Information muss hervorgehen, welche Daten (Adresse, Geburtsdatum, Telefonnummer usw.) weitergegeben werden, zu welchem Zweck (z. B. Werbung, Lizenzvergabe) und an welche Dritten (Sponsoren, Verband usw.). Wenn nötig kann die erwähnte Bekanntgabe in den Statuten oder in einer besonderen Vorschrift

vorgesehen sein. Die Bekanntgabe von Daten an Dritte ist auch denkbar, wenn dies gesetzlich vorgesehen oder vorgeschrieben ist (z. B. die Bekanntgabe von Daten in einem Strafverfahren).

(1 Quelle für diesen Absatz: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/freizeit_sport/datenbearbeitung_vereine.html)

Fazit

«Die Erfüllung und Einhaltung des revDSG ist nicht nur geboten, um die geltenden Gesetze einzuhalten, sondern auch, um der eigenen Reputation nicht zu schaden und gesetzestreu die Daten der Mitglieder zu bearbeiten. Die Um-setzung und Anpassung an die neue Rechtslage erfordert möglicherweise einen "kurzen Kraftakt", sodann ist der Verband bzw. die Mitgliedsverbände gut aufgestellt», so Rechtsanwalt und Datenschutzexperte Sven Kohlmeier im Gespräch mit Unisono.

Angesichts der erhöhten Bussen-Androhung, bei Verstössen zu verantworten durch die private Person, empfehlen wir, die Kardinalpflichten des neuen revDSG zwingend einzuhalten, insbesondere die Erfüllung der Informationspflichten sowie die Einhaltung der Anforderungen bei Auslandsdatentransfer in Staaten ohne angemessenes Datenschutzniveau; derzeit auch noch USA, siehe Beitrag: https://www.wickipartners.ch/news/eu-erlsst-angemessenheitsbeschluss-fr-us-datentransfer

Quellen:

https://www.kmu.admin.ch; https://www.windband.ch; RA und Fachanwalt für IT-Recht (DE) Sven Kohlmeier (Wicki Partners AG, Zürich); RA Dr. Roman Baumann Lorant (ALTENBACH BAUMANN BLOCH, Dornach SO)