INFORMATIONEN ZUM NEUEN DATENSCHUTZ-GESETZ

AB 1. SEPTEMBER 2023

swiss aquatics

INHALTSVERZEICHNIS

1. ALLGEMEINES

Beim Datenschutz geht es um den transparenten und verhältnismässigen Umgang mit Personendaten und deren Bearbeitung durch private (natürliche und juristische Personen) und Behörden.

Bearbeitung bedeutet jeden Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden, Auswerten, Bekanntgeben oder Vernichten. Auch wenn Personendaten auf einem Speichermedium ruhen, ohne dass Sie etwas damit anfangen, gilt das als Bearbeitung.

Personendaten sind Daten wie Name, Adresse, Telefonnummer, AHV-Nummer, Geburtsdatum, etc. die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

Besonders schützenswerte Personendaten:

- rassische und ethnische Herkunft
- politische Meinungen, Gewerkschaftszugehörigkeit
- religiöse oder weltanschauliche Überzeugungen
- genetische Daten
- biometrische Daten zur eindeutigen Identifizierung
- Gesundheitsdaten
- Daten zum Sexualleben oder zur sexuellen Orientierung
- In der Schweiz zusätzlich:
    - Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
    - Daten über Massnahmen der sozialen Hilfe

Bei besonders schützenswerten Personendaten muss zwingend beachtet werden, dass ein Bearbeitungsverzeichnis geführt wird und dass die ausdrückliche Einwilligung eingeholt wird – am besten schriftlich.

1.1. BEARBEITUNGSGRUNDSÄTZE

Datenbearbeitungen sind immer zulässig, solange die Bearbeitungsgrundsätze erfüllt sind:

1.1.1. RECHTMÄSSIGKEIT UND TREU UND GLAUBEN

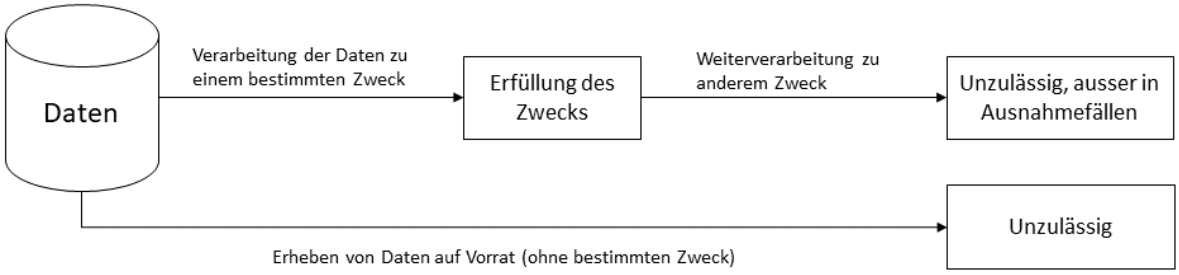
Datenbearbeitungen können nur dann zulässig sein, wenn sie rechtmässig sind und nicht gegen den Grundsatz von Treu und Glauben verstossen.

Rechtsmässig ist eine Datenbearbeitung wenn sie nicht gegen gesetzliche Vorschriften verstösst. Namentlich wenn die nachfolgend erläuterten Bearbeitungsgrundsätze eingehalten werden oder wenn ein Rechtfertigungsgrund für die Bearbeitung vorliegt.

Der Grundsatz von Treu und Glauben gilt als eingehalten, wenn das Verhalten des Verantwortlichen im Rechtsverkehr loyal und vertrauenswürdig ist. Ein Verstoss liegt bei rechtsmissbräuchlichem Verhalten des Verantwortlichen vor. Beispielsweise wenn der Verantwortliche eine Person täuscht, um dessen Daten zu erheben.

1.1.2. ZWECKGEBUNDENHEIT

Personendaten dürfen nur zu dem Zweck verwendet werden, für den sie erhoben wurden.



1.1.3. VERHÄLTNISMÄSSIGKEIT („DATENMINIMIERUNG“)

Personendaten dürfen nur bearbeitet werden, wenn ihre Bearbeitung verhältnismässig ist. Verhältnismässig ist eine Datenverarbeitung wenn sie **geeignet**, **erforderlich** und **angemessen** ist.

- **Eignung** – Die Bearbeitung ist geeignet, um den Bearbeitungszweck zu erreichen.
- **Erforderlichkeit** – Der Bearbeitungszweck kann nicht mit einer weniger umfangreichen Datenbearbeitung erreicht werden. Daten von ausgetretenen Mitgliedern müssen gelöscht werden, insofern diese nicht mehr benötigt werden.
- **Angemessenheit** – Die Bearbeitung ist angemessen, wenn ein angemessenes Verhältnis zwischen dem Bearbeitungszweck und der Bearbeitung vorliegt.

1.1.4. KORREKTHEIT DER DATEN

Personendaten müssen sachlich richtig und auf dem neuesten Stand sein. Zudem müssen sie vollständig sein.
Der Verantwortliche ist verpflichtet, die Daten regelmässig zu überprüfen und gegebenenfalls zu löschen oder zu korrigieren.

1.2. RECHTFERTIGUNGSGRÜNDE

Falls Bearbeitungsgrundsätze nicht eingehalten werden, ist die Datenbearbeitung dennoch zulässig, wenn ein Rechtfertigungsgrund vorgewiesen werden kann:

Einwilligung der betroffenen Person – Eine gültige Einwilligung erfordert, dass die betroffene Person unmissverständlich ihr Einverständnis mit der Datenbearbeitung erklärt. Dabei muss sich die Einwilligung auf bestimmte Zwecke beziehen
Bei besonders schützenswerten Personendaten muss die Einwilligung ausdrücklich erfolgen.

> Beispiel: Ein Patient willigt in die Bearbeitung seiner Gesundheitsdaten zu Forschungszwecken ein, indem er aktiv ein Kreuzchen bei der entsprechenden Frage auf dem Registrierungsformular im Spital setzt.

Erfüllung eines Vertrags – Teils sind Datenbearbeitungen für die Erfüllung eines Vertrags erforderlich. Erforderlich sind sie, wenn der Vertrag ohne die Datenbearbeitung nicht erfüllt werden kann.
Beispiel: Eine Person bestellt beim Verein einen Merchandise Artikel. Der Verein kann die Adresse der Person an die Post weitergeben, damit diese den Merchandise Artikel per Post zustellen kann.

Rechtliche Verpflichtung – Verantwortliche haben rechtliche Verpflichtungen zur Bearbeitung von Personendaten. Dies ist insbesondere bei Aufbewahrungspflichten oder der Pflicht zur Meldung von Lohndaten an Sozialversicherungen der Fall.
Beispiel: Der Verein meldet ihrer Vorsorgeeinrichtung den Jahreslohn eines Mitarbeiters.

Lebenswichtige Interessen – Dies ist ein Ausnahmefall und kommt dann zur Anwendung, wenn eine lebensbedrohte Person nicht in der Lage ist, in eine lebenswichtige Datenbearbeitung einzuwilligen.
Beispiel: Ein Athlet hat einen schweren Sportunfall und ist nicht mehr ansprechbar. Im Spital werden seine Personendaten dennoch bearbeitet, damit er behandelt werden kann.

Überwiegende Interessen – Wenn die Interessen des Privaten an einer Datenbearbeitung den Interessen der betroffenen Person überwiegen, liegt eine Rechtfertigung vor. Auf diesen Rechtfertigungsgrund kann man sich nur in begrenztem Rahmen berufen und fordert stets eine Interessenabwägung.
Beispiele:

- Ein Verein führt eine Bonitätsprüfung bei einem potentiellen Mitglied durch
- Ein Verein betreibt Direktmarketing bei seinen Mitgliedern

2. VERANTWORTUNG

2.1. ROLLEN

2.1.1. VERANTWORTLICHE (SOG. CONTROLLER)

- «Entscheidet» gemeinsam mit anderen oder allein über «die Zwecke und Mittel» (materielle oder automatisierte Bearbeitung, verwendete Software) der Bearbeitung von Personendaten.
- Muss dafür sorgen, dass eine Datenbearbeitung die gesetzlichen Vorgaben erfüllt und trägt die Verantwortung, wenn dies nicht der Fall sein sollte.

Der Controller ist verantwortlich für:

- Rechtmässigkeit der Bearbeitung

- Zweckbindung
- Informationspflichten bei der Beschaffung von Personendaten
- Datenminimierung
- Wahrung der Betroffenenrechte
- Auswahl von geeigneten Processors
- Grenzüberschreitende Bekanntgabe: Vorgaben beachten
- Informationssicherheit
- Meldung bei Datenschutzverletzungen
- Zusammenarbeit mit Aufsichtsbehörde (EDÖB)
- Rechenschaft und Beachtung der Aufbewahrungsvorschriften
- Ggf. Datenschutz-Folgenabschätzung
- Ggf. Führung des Bearbeitungsverzeichnisses
- Ggf. Ernennung eines Datenschutzberaters

2.1.2. AUFTRAGSDATENBEARBEITER (SOG. PROCESSOR)

- Führt Bearbeitung im Auftrag des Verantwortlichen aus.
- Muss Daten so bearbeiten, wie ihn sein Kunde dazu angewiesen hat.
- Auftragsdatenbearbeitungsvertrag (ADV)
    - Gegenstand und Umfang der Datenbearbeitung
    - Verantwortlichkeiten
    - Zweckbindung der Daten

2.2. INFORMATIONSPFLICHT

Der Verantwortliche informiert die betroffene Person angemessen über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei einem Dritten beschafft werden (vgl. Art. 19 revDSG).

In welcher Form und Frist erfolgt die Information? i.d.R. in einer Datenschutzerklärung spätestens einen Monat nach Erhalt der Daten von einem Dritten (bei Bekanntgabe früher)

Bspw. bei Adresskauf oder Übernahme von Adressdaten eines sich auflösenden Vereins.

3. DATENSICHERHEIT

Die Datensicherheit ist das Fundament für wirksamen Datenschutz. Sie schützt die Daten vor jeder Form von Verlust, Diebstahl oder Manipulation. Das Datenschutzgesetz stellt deswegen hohe Anforderungen an die Datensicherheit. Es sind folgende gesetzliche Schutzziele zu erreichen:

- Vertraulichkeit
- Verfügbarkeit
- Integrität
- Nachvollziehbarkeit

3.1. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Risikobasierter Ansatz
Um die Schutzziele zu erreichen müssen technische und organisatorische Massnahmen (sog. «TOMs») ergriffen werden. Die Anforderungen an die TOMs bestimmen sich nach dem Risiko, das mit der jeweiligen Datenbearbeitung verbunden ist und dem Schutzbedarf der bearbeiteten Daten.

- **Je höher das Risiko und der Schutzbedarf, desto höher die Anforderungen an die TOMs.**

Der aktuelle Stand der Technik und die Implementierungskosten, können bei der Festlegung der erforderlichen TOMs mitberücksichtigt werden.

3.2. DATENSICHERHEIT

- **Vertraulichkeit**

Die Personendaten dürfen nur **Berechtigten zugänglich** sein. Der Kreis der berechtigten Personen wird durch den **Kontext des Aufgabenbereichs** sowie den Inhalt und die Wichtigkeit der Daten bestimmt. Er kann sehr weit oder äusserst eng sein.

Unter Vertraulichkeit sind auch die **Authentifizierung**, die damit verbundenen Methoden sowie die Systeme zur **Verwaltung und Einschränkung des Zugriffs** zur Gewährleistung der Datensicherheit zu verstehen.

- **Verfügbarkeit**

Der Verantwortliche sorgt dafür, dass die Daten **jederzeit eingesehen werden** können. Diese Anforderung ist umso höher, wenn die Informationen für die Erfüllung wesentlicher oder sogar gesetzlicher Aufgaben ständig verfügbar sein müssen.

- Integrität

Die Richtigkeit der Daten muss gewährleistet sein. Es ist insbesondere dann von Bedeutung, wenn die Daten für die Öffentlichkeit bestimmt sind **oder weiterverwendet werden** sollen. Unter Integrität sind die Authentizität, die Zurechenbarkeit und die Nichtabstreitbarkeit der Daten zu verstehen.

- Systemsicherheit

Es wird nicht verlangt, dass jedes System- und Anwendungsupdate sofort installiert wird, sondern dass ein Prozess für die Aktualisierung vorhanden ist (sog. Vulnerability- und Patchmanagement).

Die entsprechende Sicherheitsaktualisierung kann zeitlich abgestuft, unter Berücksichtigung der Kritikalitätsstufen (hoch, mittel, tief), umgesetzt werden.

Bis zur Behebung von Schwachstellen müssen aber Massnahmen getroffen werden, damit die Datensicherheit dennoch gewährleistet bleibt.

Es geht nicht um reaktive Massnahmen, sondern die proaktive Behebung von Schwachstellen, für die im System bislang keine Verletzung der Datensicherheit festgestellt wurde.

- Nachvollziehbarkeit

Unbefugte Zugriffe oder sogar Missbräuche sollen identifiziert werden können. Darüber hinaus kann die Ursache eines Vorfalls ermittelt werden. Der Verantwortliche sorgt für die Aufzeichnung der Ereignisse und der Datenspuren und stellt sicher, dass diese nicht verändert werden können. Die Nachvollziehbarkeit der Bearbeitung kann für das Verfahren (Beweismittel) von Bedeutung sein und erleichtert die Kontrollen und Überwachung.

Eingabekontrolle – Welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden

Bekanntgabekontrolle – Wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekanntgegeben werden

Erkennung – Verletzungen der Datensicherheit sollen rasch erkannt werden

Beseitigung – Massnahmen zur Minderung oder Beseitigung der Folgen sollen ergriffen werden können

Umsetzen zweiter weiterer Massnahmen, wenn in grossem Umfang besonders schützenswerte Personendaten (bspw. Gesundheitsdaten) bearbeitet werden oder ein Profiling mit hohem Risiko durchgeführt wird:

- Protokollierung im System (Erfassen und Aufbewahren von Logs)
- Führen eines Bearbeitungsreglements

3.3. ALLGEMEINE MASSNAHMEN

Ferner gibt es noch einige Massnahmen, die - unabhängig von der konkreten Datenbearbeitung – stets sinnvoll sind:

- Regelmässige Updates von Software und Systemen vornehmen
- Sensibilisierung und Schulung von Mitarbeitenden, Organen und Hilfspersonen
- Berechtigungsmanagement
- Passwortmanager und Zwei-Faktor-Authentisierung
- Backups richtig aufsetzen, damit sie bei einem Cyberangriff nicht mit Ransomware infiziert werden können
- Verschlüsselung von besonders schützenswerten Daten bei der Übermittlung
- BYOD (Bring Your Own Device) nur restriktiv zulassen

4. MELDEPFLICHT

Bei einer Datensicherheitsverletzung ist eine Meldung an den EDÖB vornehmen, wenn ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person besteht. Die Information erfolgt auch an die betroffene Person, wenn es zu deren Schutz erforderlich ist oder der EDÖB es verlangt (vgl. Art. 24 revDSG).

Die Meldung hat so rasch wie möglich zu erfolgen.

Inhalt der Meldung: Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen

5. BETROFFENENRECHTE

5.1. AUSKUNFTSRECHT

Jede Person kann vom Verantwortlichen Auskunft darüber verlangen,

- ob Personendaten über sie bearbeitet werden
- und wenn ja, welche.

Das Gesetz nennt den Mindestinhalt der Auskunft:

- Angaben zur Identität und Kontaktangaben des Verantwortlichen
- Bearbeitungszwecke
- Aufbewahrungsdauer (oder deren Kriterien)
- Datenquelle (soweit verfügbar)
- automatisierte Einzelentscheide (und Logik)
- Kategorien von Empfängern (z.B. Behörden)
- Angaben zum Datenexport
- Generalklausel

5.1.1. ABLAUF

- Person muss schriftlichen Antrag stellen mit gültiger Ausweiskopie (ID / Pass)
- Interne Rücksprache mit Verantwortlichem
- Die Auskunft muss i.d.R. innert 30 Tagen erfolgen
- Bei unverhältnismässigem Aufwand ist dem Antragssteller CHF 300.00 zu verrechnen

Verweigerung, Einschränkung, Aufschiebung der Auskunft

Berufsgeheimnis, überwiegende Interessen Dritter, Gesuch ist offensichtlich querulatorisch, Gesuch verfolgt datenschutzwidrigen Zweck (Prozessvorbereitung). Grund muss angegeben werden.

5.2. LÖSCHUNG UND BERICHTIGUNG

Personendaten müssen vernichtet oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.

Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.

5.3. RECHT AUF DATENHERAUSGABE

Die betroffene Person kann ihre Personendaten beim Verantwortlichen herauszuverlangen oder einem Dritten übertragen zu lassen.

- Das Ziel der Datenherausgabe ist es, dass die betroffene Person ihre Daten unmittelbar an eine neue verantwortliche Person übertragen lassen kann
- So erhält die Person mehr Kontrolle über ihre Daten (bspw. bei Vereinswechsel).

6. DATENÜBERMITTLUNG INS AUSLAND

Datenexporte
Sobald Personendaten im Zusammenhang mit dem Ausland bearbeitet werden, liegt ein Datenexport vor.

Für Datenexporte gelten (je nach Empfängerland) besondere Regelungen, an die sich die Exporteure halten müssen.

Beispiel 1:
Ein Sportverein versendet eine E-Mail die Personendaten enthält, an einen ausländischen Veranstalter eines Wettkampfes.

- Es liegt ein Datenexport vor, weil die Personendaten ins Ausland weitergegeben werden.

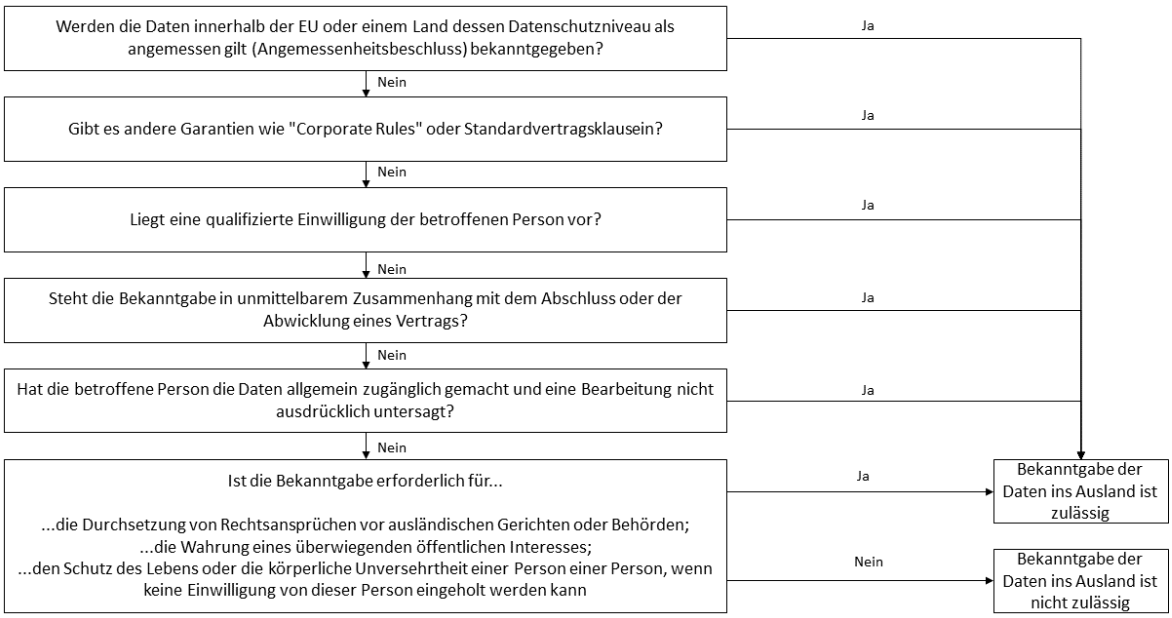
Beispiel 2:
Ein Sportverein speichert seine Mitgliederdaten auf einer Cloud, deren Server im Ausland stehen.

- Werden Personendaten im Ausland gespeichert, so gilt dies ebenfalls als Datenexport.
- Ein Export liegt auch vor, wenn aus dem Ausland auf die Daten zugegriffen werden kann (bspw. Im Supportfall)

In Staaten, welche ein angemessenes Datenschutzniveau aufweisen, können Daten ohne weiteres exportiert werden.

Die Liste der Staaten mit einem angemessenen Datenschutzniveau wird vom Bundesrat beschlossen und ist unter https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html#-2053327153 abrufbar.

Weist ein Land, in das Daten exportiert werden sollen, kein angemessenes Datenschutzniveau auf, können die Daten nur unter bestimmten Voraussetzungen exportiert werden (siehe Grafik).



Wenn Staaten, wie beispielsweise die **USA**, kein angemessenes Datenschutzniveau aufweisen, ist der Abschluss von Standardvertragsklauseln mit dem Datenimporteur die einfachste Lösung. Die Standardvertragsklauseln sind sowohl für den Datenexporteur, als auch für den Datenimporteur verbindlich. Sie stellen sicher, dass die Daten rechtmässig bearbeitet werden.

Die Standardvertragsklauseln verpflichten den Datenexporteur zur Erstellung eines «Transfer Impact Assessment» (TIA). Im TIA muss abgeklärt werden, ob die Personendaten im Empfängerland allfälligen Risiken durch die örtlichen Behörden ausgesetzt sind. Wird ein hohes Risiko festgestellt, muss dieses mittels technischer und organisatorischer Massnahmen neutralisiert werden.

Muster-TIA: https://iapp.org/resources/article/transfer-impact-assessment-templates/