

## **Neues Datenschutzrecht in Kraft ab 01. September 2023**

### **Anleitung zur Umsetzung für Mitgliederverbände des ZKS – Zürcher Kantonalverband für Sport und für deren Vereine**

#### **Einführung und Vorgehen**

Die vorliegende Anleitung soll die Vereine und Verbände in die Lage versetzen, das neue Datenschutzrecht pragmatisch und mit einfachen Mitteln und ohne viel Technik umzusetzen.

Nach einer kurzen Übersicht für das neue Datenschutzrecht und einer kurzen summarischen Darstellung der Neuerungen, folgen die notwendigen Anpassungen in 13 Schritten. Am Schluss des Dokumentes findet sich ein Glossar für die wichtigsten Begriffe.

Bei der Bearbeitung dieser Schritte sollen stets das [Bundesgesetz über den Datenschutz vom 25.09.2020 \(DSG\)](#) und die [Verordnung über den Datenschutz vom 31. August 2022 \(DSV\)](#) konsultiert werden. Die einzelnen Bearbeitungsschritte sind gut zu dokumentieren, sei es in einem elektronischen oder in einem physischen Handbuch. Periodisch sind diese dann zu überprüfen und allenfalls neuen Gegebenheiten anzupassen.

Je besser schon das bisherige Datenschutzrecht umgesetzt ist, desto einfacher ist die Umsetzung des neuen Datenschutzrechtes. Wer bis jetzt für den Datenschutz nichts gemacht hat, soll jetzt das neue Datenschutzrecht umsetzen, denn dessen Verletzung könnte strafbar sein. Insbesondere «nichts tun» könnte zur Strafbarkeit führen.

Wer die EU Datenschutz Grundverordnung (DSGVO), die am 25. Mai 2018 in Kraft trat, umgesetzt hat, weil er im Ausland tätig ist, muss trotz Kompatibilität des Schweizer Rechts mit dem EU-Recht prüfen, ob er einzelne Bearbeitungsschritte dem neuen Schweizer Recht anpassen muss.

Wer keine sog. besonders schützenswerte Personendaten (Glossar, Ziff. 1) bearbeitet, kann von verschiedenen nachfolgend erwähnten Ausnahmen und Vereinfachungen Gebrauch machen. Insofern ist generell bei jeder bestehenden Datenbearbeitung zu überlegen, ob sie überhaupt notwendig ist.

Wo nachfolgend auf Muster verwiesen wird, sollen diese nicht tel quel, sondern wohl überlegt und angepasst auf die jeweiligen Verhältnisse übernommen werden.

*Quellenangabe: Die nachstehenden Ausführungen basieren auf Quellen, die auf dem KMU-Portal der Schweizerischen Eidgenossenschaft zu finden sind (Link: [Neues Datenschutzgesetz \(revDSG\) \(admin.ch\)](#))*

## Übersicht

Die Schweiz bekommt ein neues Gesetz für den besseren Schutz der Daten ihrer Bevölkerung. Die hiesigen Unternehmen und weitere natürliche und juristische Personen (wie bspw. Vereine, Verbände), die Daten bearbeiten müssen sich ab dem 01. September 2023 an die revidierten Regelungen anpassen.

- In seiner Herbstsession 2020 hat das Parlament das neue Bundesgesetz über den Datenschutz (revDSG) verabschiedet. Es verbessert die Bearbeitung persönlicher Daten und gewährt den Schweizer Bürgerinnen und Bürgern neue Rechte. Mit dieser wichtigen Gesetzesänderung gehen auch einige Verpflichtungen für Unternehmen, Vereine und Verbände, etc. einher.
- Das totalrevidierte Datenschutzgesetz (DSG) und die Ausführungsbestimmungen in der neuen Datenschutzverordnung (DSV) und der neuen Verordnung über Datenschutzzertifizierungen (VDSZ) treten am 01. September 2023 in Kraft.
- Das totalrevidierte Datenschutzgesetz und die Ausführungsbestimmungen sind ein notwendiges, neues Gesetz.
- Das erste Bundesgesetz über den Datenschutz stammte aus dem Jahr 1992. In der Zwischenzeit hat die Schweizer Bevölkerung die Nutzung von Internet und Smartphone in ihren Alltag integriert und auch soziale Netzwerke, Cloud-Dienste oder das Internet der Dinge finden immer mehr Zuspruch. Vor diesem Hintergrund ist eine vollständige Überarbeitung des Datenschutzgesetzes unverzichtbar, um der Bevölkerung einen angemessenen und an die technologischen und gesellschaftlichen Veränderungen unserer Zeit angepassten Datenschutz zu garantieren.
- Die Kompatibilität des Schweizer Rechts mit dem EU-Recht, insbesondere mit der Datenschutzgrundverordnung (DSGVO), ist das zweite grosse Anliegen des neuen Gesetzes. Das revDSG soll bewirken, dass der freie Datenverkehr mit der Europäischen Union erhalten werden kann, sodass die Schweizer Verbände und Vereine, die Sportveranstaltungen mit Teilnehmenden aus dem europäischen Ausland durchführen oder die im Ausland an Wettbewerben teilnehmen oder anderweitig gegen Entschädigung tätig sind, die entsprechenden Bestimmungen einhalten.

## Neuerungen - Was sind die wichtigsten Veränderungen?

1. Die Daten **natürlicher Personen** sind betroffen, diejenigen von juristischen Personen nicht mehr.
2. **Genetische und biometrische Daten** werden in die Definition der besonders schützenswerten Daten (Glossar, Ziff. 1) aufgenommen.
3. Die Grundsätze «**Privacy by Design**» und «**Privacy by Default**» werden eingeführt. Wie der Name bereits andeutet, bedeutet «Privacy by Design» (Datenschutz durch Technikgestaltung) für die Entwickler, den Schutz und den Respekt der Privatsphäre der Nutzerinnen und Nutzer in die Struktur der Produkte oder Dienstleistungen einzubauen, welche personenbezogene Daten sammeln werden. Der Grundsatz «Privacy by Default» (Datenschutz durch Voreinstellung) stellt sicher, dass schon beim Inverkehrbringen des Produktes oder der Dienstleistung die höchste Sicherheitsstufe vorhanden ist, indem standardmässig, also ohne Eingreifen der Nutzer, alle nötigen Massnahmen für den Datenschutz und die Einschränkung der Datennutzung aktiviert sind. Anders gesagt, müssen sämtliche Software, Hardware sowie die Dienstleistungen so konfiguriert sein, dass die Daten geschützt sind und die Privatsphäre der Nutzer gewahrt wird. Das gilt bspw. auch bei der Entwicklung von Internetanwendungen.
4. **Folgenabschätzungen** (Glossar, Ziff. 2) müssen durchgeführt werden, sofern ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht.

5. **Die Informationspflicht wird ausgeweitet:** Bei jeder Beschaffung von Personendaten – und nicht mehr nur von sogenannten besonders schützenswerten Daten – muss die betroffene Person vorgängig informiert werden. Und insbesondere diese Regel muss auch von Vereinen und Verbänden beachtet und umgesetzt werden. Dazu dienen die Datenschutzerklärungen.
6. Ein **Verzeichnis der Bearbeitungstätigkeiten wird obligatorisch.** Die Verordnung zum Gesetz sieht jedoch für diesen Grundsatz eine Ausnahme für Unternehmen und andere privatrechtlichen Organisationen (wie Verbände und Vereine) vor, wenn diese weniger als 250 Mitarbeitende beschäftigen und deren Datenbearbeitung nur ein geringes Risiko von Verletzungen der Persönlichkeit von betroffenen Personen mit sich bringt, weil besonders schützenswerte Personendaten (siehe oben Ziff. 2) nicht in grossem Umfange bearbeitet und Profiling (Glossar, Ziff. 3) nicht durchgeführt werden. Diese Ausnahme bietet sich für Vereine und Verbände an.
7. Eine **rasche Meldung ist erforderlich**, wenn die Datensicherheit verletzt wurde. Sie ist an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu richten.
8. Der **Begriff Profiling** (Glossar, Ziff. 3) wurde in das Gesetz aufgenommen.

### **Was ist zu tun? Welche Anpassungen sind nötig?**

Vereine und Verbände müssen die folgenden dreizehn Massnahmen umsetzen und in der Folge einhalten, um sich an das revDSG anzupassen:

1. **Datensammlungsinventar erstellen**  
Ein solches Inventar ist heute gesetzlich nicht mehr vorgeschrieben, aber praktisch noch notwendig, um die Auskunftsbereitschaft für Anfragen von betroffenen Personen sicherzustellen, um die weiteren Schritte einfach und korrekt umzusetzen und um insbesondere die Datenschutzerklärungen (vgl. unten Ziff. 2) korrekt abzufassen. Bei dieser Gelegenheit soll die Anzahl der Datensammlungen auf das Notwendige begrenzt und möglichst reduziert werden. Das Datensammlungsinventar hat alle Arten von Datensammlungen, wie bspw. physische Karteien, elektronische Speicherungen, etc., zu berücksichtigen. Für jede Datensammlung ist festzuhalten, welche Daten gespeichert werden, wo und bei wem diese Daten erhoben werden, wohin diese Daten allenfalls geliefert werden, ob und wie sie automatisiert bearbeitet werden und ob sie und gegebenenfalls durch wen sie extern bearbeitet werden.
2. **Datenschutzerklärung überarbeiten**  
Bestehende Datenschutzerklärungen auf der Basis von Schritt 1 und unter Berücksichtigung der Schritte 3 – 13 prüfen und ändern (Website, Statuten, Verträge, Werbeinhalte usw.) oder die Datenschutzerklärungen neu abfassen.  
(Muster für Datenschutzerklärungen: [Datenschutz Pfadibewegung Schweiz](#), [Datenschutzerklärungen von Swisscom](#), [Datenschutzerklärung von Swiss Olympic](#))
3. **Interne Datenschutzrichtlinien erstellen**  
Richtlinien für die Datenbearbeitung innerhalb des Verbandes / Vereines erstellen (oder ändern).
4. **Verzeichnis der Bearbeitungstätigkeiten erstellen**  
Ein Verzeichnis der Datenbearbeitung (Glossar, Ziff. 4) anlegen; es gibt eine Ausnahme zu dieser Regel für Verbände und Vereine mit weniger als 250 Beschäftigten und sofern kein hohes Risiko für Verletzungen der Persönlichkeit vorliegt (vgl. dazu oben Neuerungen, Ziff. 6).

5. **Betroffenenrechte sicherstellen**  
Eine Vorgehensweise für eine rasche Beantwortung der Anfragen betroffener Personen ausarbeiten, z.B. Ersuchen um Auskunft oder Löschung von Daten (gegebenenfalls inkl. elektronischer Lieferung der Daten).
6. **Vorgehen bei Datenschutzverletzungen definieren**  
Ein Meldeverfahren für Verletzungen des Datenschutzes einführen (vgl. dazu oben Neuerungen, Ziff. 7).
7. **Datenschutz-Risikomanagement**  
Einen Prozess für die Datenschutz-Folgenabschätzungen (Glossar, Ziff. 2) etablieren, die notwendig sind, wenn die Datenbearbeitung ein hohes Risiko mit sich bringt (z.B. bei systematischer Überwachung grosser Teile des öffentlichen Raums); bei Verbänden und Vereinen eher selten notwendig (aber Achtung: bei Profiling, Überwachungskameras, etc.).
8. **Datenbearbeitung durch Dritte**  
Verträge mit externen Datenbearbeitern und Lieferanten analysieren, um zu prüfen, ob die Sicherheit der ausgelagerten Daten gewährleistet ist, und allenfalls entsprechende Klauseln hinzufügen (insbesondere bezüglich der Meldung jeglicher Verletzungen des Datenschutzes).
9. **Löschpflicht einhalten**  
Dafür sorgen, dass alle personenbezogenen Daten gelöscht oder anonymisiert werden (sobald sie für den Zweck, der deren Bearbeitung rechtfertigte, nicht mehr benötigt werden).
10. **Datenübermittlungen ins Ausland**  
Prüfen, in welche Länder Daten übermittelt werden, auch für eine einfache Speicherung in der Cloud (diese Länder müssen in einer vom Bundesrat erstellten Liste aufgeführt sein. Ist dies nicht der Fall, gelten strengere Anforderungen). Aber Kompatibilität für EU-Raum ist gewährleistet.
11. **Datensicherheit sicherstellen**  
Die Datensicherheit ist durch geeignete technische und organisatorische Massnahmen zu garantieren; diese Massnahmen sind für jede Datenbank im Datensammlungsinventar zu festzuhalten.
12. **Daten-Portabilität**  
Die Herausgabe der Daten in einem elektronischen Format ist zu gewährleisten (bei automatisierter Bearbeitung der Daten und besonders im Zusammenhang mit dem Abschluss oder der Erfüllung eines Vertrags).
13. **Datenschutzberater/in**  
Einen Datenschutzberater oder eine Datenschutzberaterin (Glossar, Ziff. 5) benennen und die Kontaktdaten veröffentlichen (empfohlen wird die Meldung dieser Person beim Eidgenössischen Datenschutz- und Öffentlichkeits-beauftragten [EDÖB]).

Abschliessender Hinweis: Swiss Olympic stellt gute Unterlagen zum neuen Datenschutzrecht auf deren Wissensplattform [esi – elitesportinsights](#) zur Verfügung.

## Glossar

### 1. **Besonders schützenswerte Personendaten**

Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten; Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie; genetische Daten; biometrische Daten, die eine natürliche Person eindeutig identifizieren; Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen; Daten über Massnahme der sozialen Hilfe.

### 2. **Datenschutz-Folgenabschätzung**

Der Verantwortliche für die Datenbearbeitung erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann.

### 3. **Profiling**

Jede Art der automatisierten Bearbeitung von Personendaten um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen (bspw. Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben und Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel), zu bewerten.

### 4. **Verzeichnis der Datenbearbeitung**

Dieses umfasst u.a. die Identität des Verantwortlichen, Bearbeitungszweck, Beschreibung der Kategorien betroffener Personen, Kategorien der Empfängerinnen und Empfänger, Aufbewahrungsdauer der Personendaten, Kriterien zur Festlegung der Dauer, Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit, bei Bekanntgabe der Daten ins Ausland die Angabe des Staates und der Garantien für einen angemessenen Datenschutz.

### 5. **Datenschutzberaterin / Datenschutzberater**

Anlaufstelle für die betroffenen Personen und für die Behörden, die in der Schweiz für den Datenschutz zuständig sind.

- Ob Verantwortliche nach Datenschutzrecht, mithin ein Verband, ein Verein oder ein Unternehmen, eine Datenschutzberaterin / einen Datenschutzberater ernennt, ist jedem selbst überlassen.
- Wird eine Datenschutzberaterin / ein Datenschutzberater ernannt, dann ist sie / er Anlaufstelle für betroffene Personen und für Behörden des Datenschutzes. Im Weiteren hilft er bei der Umsetzung und Anwendung des Datenschutzes mit.
- Die / der freiwillige Datenschutzberaterin / Datenschutzberater muss mit dem neuen schweizerischen Datenschutzrecht gut vertraut sein und die IT-Infrastruktur im Unternehmen, Verband oder Verein kennen.
- Wer besonders schützenswerte Daten bearbeitet und/oder Profiling betreibt und bei der Datenschutz-Folgenabschätzung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen feststellt, muss zwingend vorgängig eine Stellungnahme des EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter) einholen und die von diesen angeordneten Massnahmen umsetzen.

Auf die Konsultation des EDÖB darf jedoch verzichten, wer eine(n) [qualifizierte(n)] Datenschutzberaterin / Datenschutzberater beschäftigt und dessen Weisungen und Anordnungen befolgt. Die / der qualifizierte Datenschutzberaterin / Datenschutzberater braucht von den Leitungsorganen des Verbandes, Vereines oder Unternehmens

fachliche Unabhängigkeit, darf von diesen Leitungsorganen im Bereich des Datenschutzes keine Weisungen entgegennehmen und muss über die erforderlichen Fachkenntnisse bzw. Ausbildung verfügen (Spezifische Ausbildungen werden im Markt angeboten). Im Weiteren müssen die Kontaktdaten der Datenschutzbeauftragten / des Datenschutzbeauftragten veröffentlicht und dem EDÖB bekanntgegeben werden.

## Weiterführende Informationen und Quellen

	<a href="#">Podcast Folge «Datenschutz im Fokus: Was Sportvereine über das neue Schweizer Datenschutzgesetz wissen sollten»</a>
	<a href="#">E-Learning von Swiss Olympic Datenschutz</a>
	<a href="#">Datenschutz-Schulung esi Swiss Olympic</a>

Version vom 07.05.2023  
Peter Höltschi (Finanzchef ZKS)