Datenschutzreglement

Verein Swissdec

Swissdec, 6004 Luzern
www.swissdec.ch

Datenschutzreglement Version 1.0

Inhaltsverzeichnis

§ 1 Allgemeines

[1] Der Vorstand erlässt gestützt auf **§26 und § 27 Abs. 1 Ziff. 14 der Vereinsstatuen des Vereins Swissdec** das vorliegende Datenschutzreglement. Es regelt die datenschutzkonforme Bearbeitung von Personendaten und die insoweit im Verein Swissdec bestehenden Verantwortlichkeiten im Bereich des Datenschutzes.

[2]Bei der Bezeichnung von Organ- und Funktionsträgern des Vereins Swissdec sind stets Personen männlichen und weiblichen Geschlechts gleichermassen gemeint. Aus Gründen der einfacheren Lesbarkeit wird im Folgenden nur die männliche Form verwendet.

§ 2 Geltungsbereich

[1] Das Datenschutzreglement ist für alle Mitglieder des Vereins Swissdec verbindlich.

[2] Alle im Rahmen des Organisationsreglements aufgeführten Organe, Organisationseinheiten und Funktionen bzw. die Organträger und Funktionsträger des Vereins Swissdec sind verpflichtet, sich an das Datenschutzreglement zu halten (§1 Abs. 3 des Organisationsreglements).

[3]Die Mitglieder des Vereins Swissdec sind verpflichtet, ihre Mitarbeitenden bzw. externe Dritte, welche sie im Rahmen ihrer Mitarbeit gemäss §4 der Statuten in die Fachgruppen und Kommissionen entsenden, entsprechend zu informieren und vertraglich an die Einhaltung des Datenschutzreglements zu verpflichten.

[4]Dritte (z.B. Vertragspartner, Hilfspersonen, Subunternehmen), die Zugriff auf Personendaten erhalten oder an der Gestaltung von Datenbearbeitungsprozessen oder von Standards mitwirken, müssen vertraglich zur Einhaltung des Datenschutzreglements verpflichtet werden.

§ 3 Gesetzliche und andere verbindliche Grundlagen

[1] Der **Verein Swissdec** muss bei der Bearbeitung von Personendaten, bei der Gestaltung von Standards sowie zur Aufrechterhaltung der bestehenden Zertifizierung seines Datenschutz-Management-Systems (DSMS) verschiedene verbindliche Grundlagen beachten. Dies betrifft insbesondere die folgenden Grundlagen:

a) §1 Abs. 7 der Vereinsstatuten
b) Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1)
c) Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (VDSG; SR 235.11)
d) Verordnung über die Datenschutzzertifizierungen vom 28. September 2007 (VDSZ; SR 235.13)
e) Regulativ betreffend die Anforderungen an die Zertifizierung eines Datenschutz-Management-Systems des Datenschutz-Labels GoodPrivacy in der jeweils geltenden Version
f) Verträge mit den Datenempfängern betreffend die Datenübermittlung über den Distributor (AGB Distributor).

[2]Die **Vereinsmitglieder** sowie das **Bundesamt für Statistik** müssen bei der Bearbeitung von Personendaten zusätzlich ihre spezialgesetzlichen Grundlagen sowie allenfalls kantonale Datenschutzgesetze beachten. Diese verpflichten das jeweilige Vereinsmitglied bzw. das Bundesamt für Statistik direkt und haben auf die Gesetzeskonformität der Bearbeitung von Personendaten durch den Verein Swissdec sowie der Swissdec-Standards Einfluss.

§ 4 Begriffe

Zur besseren Lesbarkeit des Datenschutzreglements werden im Folgenden wichtige Begriffe definiert. Bei allfälligen Abweichungen gelten die Begriffsdefinitionen des Datenschutzgesetzes des Bundes.

a) Personendaten: Daten, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen. Bestimmbar ist die Person, wenn anhand von zusätzlichen Informationen auf ihre Identität geschlossen werden kann.
b) Besonders schützenswerte Personendaten: Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, 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 Massnahmen der sozialen Hilfe.
c) Bearbeiten: Jeder Umgang mit Personendaten wie das Erheben, die Übermittlung oder das Löschen der Daten. Auch das blosse Speichern von Personendaten, ohne dass diese dabei geändert werden, fällt unter den Begriff des Bearbeitens.
d) Verantwortlicher: Private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet.

e) Auftragsbearbeiter: Private Person oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.

§ 5 Datenschutz-Management-System

Der Verein Swissdec führt ein Datenschutz-Management-System, das nach der Verordnung über die Datenschutzzertifizierung (VDSZ, SR 235.13) und dem Datenschutzlabel GoodPriv@cy der Schweizerischen Vereinigung für Qualitäts- und Managementsysteme SQS zertifiziert ist.

§ 6 Verantwortung

[1] Die Vereinsversammlung ist als das oberste Organ des Vereins Swissdec im Rahmen der ihr zugewiesenen statutarischen Aufgaben für die Gesetzeskonformität des Handelns des Vereins Swissdec verantwortlich. Sie stellt im Rahmen der Beschlussfassung über das jährliche Vereinsbudget die für die systematische Gewährleistung des Datenschutzes und der Datensicherheit erforderlichen finanziellen Ressourcen zur Verfügung.

[2]Der Vorstand hat im Rahmen seiner statutarischen Pflichten vor allem die folgenden Kompetenzen und Verantwortungen im Zusammenhang mit der Gewährleistung der Datenschutzkonformität des Handelns des Vereins Swissdec:

a) Erlass und die Änderung des Datenschutzreglements;
b) Erlass und Änderung der Datenschutzpolitik;
c) Beurteilung der Risiken im Bereich Datenschutz und Datensicherheit und Festlegung von geeigneten Massnahmen zur Risikobehandlung;
d) Entgegennahme der Berichterstattung des Datenschutzbeauftragten;
e) Beurteilung des Datenschutz-Management-Systems im Rahmen eines jährlichen Management Reviews;
f) Kommunikation mit Dritten wie beispielsweise dem Eidgenössischen Datenschutz-und Öffentlichkeitsbeauftragten (EDÖB) sowie anderen Aufsichtsbehörden bei vermuteten oder tatsächlichen Datenschutz- oder Datensicherheitsverletzungen, sofern die Kompetenz nicht an die Geschäftsstelle oder den Datenschutzbeauftragten delegiert wird;
g) Beantragung der erforderlichen finanziellen Mittel für die Gewährleistung des Datenschutzes und der Datensicherheit zuhanden der Vereinsversammlung.

[3] Der Datenschutzbeauftragte übt für den Verein Swissdec die Funktion des Datenschutzverantwortlichen gemäss den Bestimmungen des DSG und des VDSG aus und ist beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet. Er berät den Verein Swissdec bei der Umsetzung des Datenschutzes. Seine organisatorische Einordnung und seine Pflichten sind in den §§ 17 – 19 des Organisationsreglements sowie in seinem Pflichtenheft detailliert festgelegt. Der Datenschutzbeauftragte stellt bei Bedarf Muster, Checklisten oder andere Hilfsdokumente zur Verfügung, die der Umsetzung der datenschutzrechtlichen Vorgaben sowie dieses Datenschutzreglements dienen.

[4] Die Geschäftsstelle und die Organisationseinheit Standardisierung arbeiten eng mit dem Datenschutzbeauftragten zusammen und haben insbesondere die folgenden Aufgaben:

a) Planung der regelmässig wiederkehrenden Aufgaben gemeinsam mit dem Datenschutzbeauftragten wie beispielsweise Schulungen, interne und externe Audits;
b) Führen des Datenschutz-Management-Systems;
c) Entgegennahme und Behandlung von Vorfällen im Bereich Datenschutz und Datensicherheit in Absprache mit dem Datenschutzbeauftragten und dem Vorstand;
d) Weiterleiten von Fragen im Zusammenhang mit dem Datenschutz an den Datenschutzbeauftragten;
e) Beizug des Datenschutzbeauftragten bei neu geplanten Projekten.

[5] Alle natürlichen und juristischen Personen im Geltungsbereich des Datenschutzreglements gemäss §2 sind verpflichtet, mit der Datenschutzbeauftragten zusammenzuarbeiten, sie bei Problemen und Fragen im Zusammenhang mit der Anwendung von Datenschutzrecht von sich aus zu kontaktieren und ihr auf ihre Anfrage hin Zugang zu Datenbearbeitungen und Systemen zu geben sowie Fragen zu Datenbearbeitungen zu beantworten. Sie sind zudem verpflichtet, an Datenschutz-Schulungen teilzunehmen.

§ 7 Datenschutzrechtliche Rollen

[1] Bei der Bearbeitung von Personendaten im Zusammenhang mit der Führung der Geschäfte des Vereins Swissdec handelt der Verein Swissdec in der datenschutzrechtlichen Rolle des Verantwortlichen. Dies betrifft insbesondere Angaben über Personen, die im Verein Swissdec vertreten sind oder an der Erledigung von Aufgaben des Vereins Swissdec als externe Personen mitwirken. Bei der Bearbeitung dieser Personendaten ist der Verein Swissdec direkt für die Erfüllung der datenschutzrechtlichen Pflichten gemäss DSG und den nachfolgenden Bestimmungen des Datenschutzreglements verantwortlich.

[2] Im Zusammenhang mit der Übermittlung von Personendaten über den Distributor an die angeschlossenen Datenempfänger sowie in deren Auftrag an die Kunden der Datenempfänger handelt der Verein Swissdec als Auftragsbearbeiter der Datenempfänger. Der Verein Swissdec bearbeitet dabei die Personendaten nur im Auftrag und für die Zwecke der Datenempfänger und ergreift angemessene Massnahmen zur Gewährleistung der Datensicherheit. Der Verein Swissdec wird zudem Subunternehmer nur mit Einwilligung der Datenempfänger beiziehen.

§ 8 Grundsätze für die Bearbeitung von Personendaten

[1] Der Verein Swissdec beachtet bei der Bearbeitung von Personendaten sowie bei der Erstellung und Weiterentwicklung von Swissdec-Standards die anwendbaren gesetzlichen Grundlagen.

[2] Der Verein Swissdec bearbeitet Personendaten rechtmässig. Dies bedeutet insbesondere, dass er

a) in der Rolle des Verantwortlichen Personendaten in der Regel auf der Basis der Statuten oder von Verträgen bearbeitet;

b) in der Rolle des Auftragsbearbeiters Personendaten auf der Basis eines Vertrages und für die Zwecke des Datenempfängers bearbeitet;

c) angemessene Massnahmen trifft, dass Datenempfänger nur die Personendaten über den Distributor erhalten, für welche diese über eine gesetzliche oder vertragliche Grundlage verfügen.

[2] Die Personendaten werden durch den Verein Swissdec über den Distributor nur an die vorgesehenen Empfänger weitergeleitet. Eine weitere Datenbearbeitung findet nicht statt (Zweckbindung).

[3] Der Verein Swissdec gestaltet seine IT-Systeme und die Datenbearbeitungen so, dass nur so viele Daten bearbeitet werden, wie es zur Zweckerreichung erforderlich ist (Privacy by Design).

[4] Personendaten werden vertraulich bearbeitet. Zugriff auf Personendaten haben nur jene Personen, welche diese für die Erfüllung ihrer Aufgaben benötigen.

[5] Der Verein Swissdec ergreift angemessene technische und organisatorische Massnahmen, um die Sicherheit der Datenbearbeitung zu gewährleisten.

[6] Werden Dienstleister zur Bearbeitung von Personendaten beigezogen, dann stellt der Verein Swissdec vertraglich sicher, dass diese die Daten ausschliesslich für die Zwecke des Vereins Swissdec und nur so bearbeiten, wie es der Verein Swissdec selbst darf. Zudem stellt er sicher, dass der Dienstleister die ausgelagerten Personendaten mit angemessenen technischen und organisatorischen Massnahmen schützt.

[7] Der Verein Swissdec betreibt den Distributor auf technischer Infrastruktur in der Schweiz.

[8] Der Verein Swissdec informiert die Öffentlichkeit sowie die betroffenen Personen über seine Datenbearbeitungen in geeigneter Weise, in der Regel mittels Publikationen über die Website.

§ 9 Datenschutz in Projekten

[1] Bei der Planung von Projekten, die die Bearbeitung von Personendaten zum Gegenstand haben oder diese steuern (z.B. bei der Erstellung neuer Standards), stellt der Verein Swissdec sicher, dass die Anforderungen des Datenschutzes und der Datensicherheit frühzeitig geklärt und mitberücksichtigt werden.

[2] Die Stellungnahme des Datenschutzbeauftragten wird bereits bei der Erstellung des Projektantrages eingeholt.

[3]Ist aufgrund der Stellungnahme des Datenschutzbeauftragten mit der geplanten Datenbearbeitung voraussichtlich ein hohes Risiko für die betroffenen Personen verbunden, muss durch die für das Projekt verantwortlichen Personen in Zusammenarbeit mit dem Datenschutzbeauftragten eine Datenschutz-Folgenabschätzung gemäss §10durchgeführt werden.

§ 10 Verzeichnisse und Datenschutz-Folgenabschätzungen

[1] Der Verein Swissdec dokumentiert seine Bearbeitungstätigkeiten, in denen Personendaten bearbeitet werden, in Verzeichnissen.

[2] Der Datenschutzbeauftragte unterstützt den Verein Swissdec bzw. die für eine Datenbearbeitung verantwortlichen Personen bei der Prüfung der Notwendigkeit sowie bei der Durchführung von Datenschutz-Folgenabschätzungen. Der Datenschutzbeauftragte stellt für diesen Zweck Muster und Checklisten zur Verfügung. Eine allenfalls gesetzlich erforderliche Information der zuständigen Datenschutz-Aufsichtsbehörde erfolgt durch den Datenschutzbeauftragten in Absprache mit dem Vorstand, der Organisationseinheit Standardisierung und der Geschäftsstelle.

[3] Der Verein Swissdec unterstützt die Verantwortlichen bei Bedarf bei der Erstellung von Verzeichnissen sowie bei den Datenschutz-Folgenabschätzungen, wenn er als Auftragsbearbeiter für diese Personendaten bearbeitet.

§ 11 Audits und Kontrollen

[1] Das Datenschutz-Management-System des Vereins Swissdec wird jährlich durch die externe Zertifizierungsstelle hinsichtlich der Erfüllung der Normanforderungen der VDSZ und von GoodPriv@cy geprüft.

[2] Der Verein Swissdec führt zusätzlich jährliche interne Audits durch. Diese werden unter Berücksichtigung der datenschutzrechtlichen Risiken des Vereins Swissdec und der betroffenen Personen sowie der Vorgaben der zertifizierten Normen über mehrere Jahre im Voraus geplant und durchgeführt.

[3] Der Datenschutzbeauftragte übt seine Kontrollfunktion wie folgt aus:

a) Präventiv durch den zwingenden Beizug in Projekten gemäss §9
b) Im Rahmen der Teilnahme an den Sitzungen der Fachkommission und der Technischen Kommission
c) Auf Anfrage eines Vereinsmitglieds, eines Organs oder eines Dritten bei einer vermuteten Verletzung des Datenschutzes oder der Datensicherheit
d) Durch die stichprobenartige Kontrolle von bestehenden Datenbearbeitungsprozessen.

§ 12 Abweichungen von gesetzlichen oder anderen Vorgaben (Nichtkonformität)

[1] Feststellungen, die sich aus den Audits und Kontrollen gemäss §11 ergeben, werden dokumentiert und hinsichtlich Handlungsbedarf für den Verein Swissdec sowie die Risiken für die betroffenen Personen bewertet.

[2] Eine Verletzung oder ein Verdacht einer Verletzung von Vorschriften zum Schutz von Personendaten oder zur Gewährleistung von Datensicherheit, die sich nicht aus einem Audit oder einer Kontrolle ergeben, sind der Geschäftsstelle zu melden, welche zusammen mit dem Datenschutzbeauftragten über den Vorfall und das weitere Vorgehen entscheidet.

[3] Betrifft die vermutete Datenschutzverletzung Personendaten eines Datenempfängers, die der Verein Swissdec im Auftrag bearbeitet, meldet er die vermutete Datenschutzverletzung so rasch als möglich dem zuständigen Datenempfänger.

[4]Der Datenschutzbeauftragte

a) empfiehlt Korrekturmassnahmen, wenn eine Verletzung der datenschutzrechtlichen Vorgaben vorliegt
b) klärt die Meldepflicht von Verletzungen der Datensicherheit und führt die gesetzlich vorgesehene Meldung in Absprache mit dem Vorstand durch
c) stellt Muster und Checklisten für die Bewertung und

[5] Die Verantwortung für die Kontrolle der Behebung von festgestellten und / oder gemeldeten Nichtkonformitäten liegt beim Datenschutzbeauftragten, der Geschäftsstelle und der Organisationseinheit Standardisierung.

[6] Alle Personen im Geltungsbereich des Datenschutzreglements sind verpflichtet, an der Klärung und Behebung von Nichtkonformitäten mitzuwirken.

§ 13 Betroffenenrechte

[1] Betroffene Personen sind natürliche Person, deren Daten bearbeitet werden. Sie haben insbesondere folgende Rechte:

- Auskunft zu erhalten, ob und welche Personendaten über sie bearbeitet werden;
- sie betreffende Personendaten berichtigen oder gegebenenfalls löschen oder deren Bearbeitung einschränken zu lassen.

[2] Stellt eine betroffene Person eine solches Gesuch an den Verein Swissdec, ist dieses an den Leiter der Geschäftsstelle weiterzuleiten. Dieser entscheidet, ob das Gesuch eine Datenbearbeitung des Vereins Swissdec oder eines Datenempfängers betrifft. Eine Anfrage betr. die Datenbearbeitung eines Datenempfängers wird an diesen weitergeleitet. Eine den Verein Swissdec betreffende Anfrage leitet der Leiter der Geschäftsstelle an den Datenschutzbeauftragten zur Bearbeitung weiter.

[3] Alle Personen im Geltungsbereich des Datenschutzreglements sind verpflichtet, den Datenschutzbeauftragten bei der Beantwortung von Gesuchen von betroffenen Personen zu unterstützen und ihm alle notwendigen Informationen zur Verfügung zu stellen.

§ 14 Schulungen

[1] Der Datenschutzbeauftragte schult alle Personen, welche im Verein Swissdec bei der Gestaltung von Datenbearbeitungsprozessen sowie an der Erstellung von Standards mitwirken.

[2] Ziele der Schulungen ist der Aufbau des für die datenschutzkonforme Vereinstätigkeit erforderlichen Grundwissens im Bereich Datenschutz und Datensicherheit. Bei Bedarf werden Schulungen für einzelne Interessensgruppen durchgeführt.

§ 15 Schlussbestimmungen

Dieses Reglement wurde vom Vorstand am 11.12.2019 erlassen und tritt am selben Tag in Kraft.

Luzern, 11.12.2019

Felix Weber
Vereinspräsident Verein Swissdec

Claudio Fischer
Vizepräsident Verein Swissdec

Genehmigt an Vorstandssitzung vom 11.12.2019