Schweizerisches Rotes Kreuz
Kanton Solothurn

Datenschutz-Reglement des SRK Kanton Solothurn

Ziel und Zweck

Dieses Reglement legt verbindliche Regeln für die Bearbeitung von Personendaten innerhalb des SRK Kanton Solothurn fest. Das Reglement bildet die Grundlage für den Schutz von Personendaten im Sinne von verbindlichen internen Datenschutzvorschriften.

Geltungsbereich

Das Reglement gilt für alle Mitarbeitenden, Ehrenamtlichen und Freiwilligen des SRK Kanton Solothurn sowie für durch das SRK Kanton Solothurn beauftragte Personen.

Datenschutzverantwortliche

Ursina Pally Hofmann ist die Datenschutzverantwortliche für das SRK SO.

Verlauf
1. September 2023, Inkrafttreten
1. Januar 2025, Ergänzung in Ziffer 6.2.

Inhalt

1. Einleitung

Das SRK Kanton Solothurn (SRK SO) sammelt und bearbeitet aufgrund seiner Vielzahl an Tätigkeiten eine bedeutende Anzahl an Personendaten. Wir schützen das individuelle Recht der betroffenen Personen auf Schutz ihrer Privatsphäre und Persönlichkeit. Die Vorschriften zum Datenschutz kommen immer dann zur Anwendung, wenn bei einer Bearbeitungstätigkeit Personendaten betroffen sind.

Alle Mitarbeitenden, Ehrenamtlichen und Freiwilligen des SRK SO sind verpflichtet, sich an die Inhalte dieses Reglements zu halten. Dessen bzw. deren Einhaltung wird regelmässig überprüft. Im Falle von Missachtung oder Missbräuchen werden die erforderlichen Massnahmen ergriffen. Notwendige Abweichungen und Ausnahmen von diesem Reglement sind schriftlich zu begründen und zu dokumentieren.

Verhältnis zu den gesetzlichen Anforderungen: Für das SRK SO gelten grundsätzlich die Bestimmungen des neu revidierten Bundesgesetzes über den Datenschutz und dessen Verordnung sowie allfällige datenschutzrelevante Regelungen in anderen Gesetzen (DSG, DSVO). Werden Personendaten von Personen aus dem EU-Raum bearbeitet, gelten zudem die Bestimmungen der EU (Datenschutzgrundverordnung, DSGVO). Dieses Reglement führt die einschlägigen gesetzlichen Bestimmungen näher aus.

2. Verantwortlichkeiten

Für die Einhaltung und Umsetzung des Datenschutzes gelten in der GS SRK die nachfolgenden Verantwortlichkeiten.

- Die Datenschutzverantwortliche koordiniert die Umsetzung und Durchsetzung des Datenschutzes im SRK SO. Im Rahmen von neuen Projekten und bei geplanter Zusammenarbeit mit externen Dienstleistern wird die Verantwortliche vorgängig konsultiert.
- Sämtliche Mitarbeitenden, Ehrenamtlichen, Freiwilligen und durch das SRK SO beauftragten Personen sind in ihrem Tätigkeitsbereich für den Datenschutz verantwortlich. Kritische Aufmerksamkeit und eigenverantwortliches Verhalten von ihnen werden vorausgesetzt. Sie werden hinsichtlich ihrer Verantwortung für den Datenschutz entsprechend ihrer Funktion sensibilisiert und ausgebildet.
- Die Bereichsleitenden sind verpflichtet sicherzustellen, dass die Vorschriften dieses Reglements durch organisatorische, personelle und technische Massnahmen eingehalten werden.
- Verstösse gegen die schweizerische Datenschutzgesetzgebung können zukünftig zu hohen Bussen für Mitarbeitende, Ehrenamtliche und Freiwillige führen, die Personendaten bearbeiten. Das SRK SO als Arbeitgeberin kann zudem Sanktionen bis hin zur fristlosen Auflösung des Arbeitsverhältnisses aussprechen.

3. Allgemeine Grundsätze für die Bearbeitung von Personendaten

Alle Mitarbeitenden, Ehrenamtlichen und Freiwilligen halten sich an die folgenden, im Bundesgesetz über den Datenschutz festgelegten allgemeinen Grundsätze.

Grundsatz	Beschreibung
Rechtmässigkeit	Personendaten müssen auf rechtmässige Weise bearbeitet werden. Die Datenbearbeitung darf nur dann und soweit erfolgen, wie eine ausreichende Rechtsgrundlage für den jeweiligen Verarbeitungsvorgang vorhanden ist.
Transparenz, Treu und Glauben	Die Datenbearbeitung nach Treu und Glauben verlangt ein ehrliches, faires, verantwortliches und rechtlich korrektes Verhalten im Umgang mit Personendaten. Die Betroffenen erhalten präzise und leicht verständliche Informationen über die Datenerhebung, deren Umfang sowie den Bearbeitungszweck.
Zweckbindung	Jede Erhebung und Bearbeitung von Personendaten muss einen bestimmten und für die betroffene Person erkennbaren Zweck verfolgen. Daten dürfen nur dann für einen anderen als den ursprünglichen Zweck verwendet werden, wenn ein Rechtfertigungsgrund dafür vorliegt und die betroffene Person informiert worden ist.
Verhältnismässigkeit	Es dürfen nur diejenigen Personendaten erhoben und bearbeitet werden, die für die Erfüllung der Aufgaben bzw. die Erreichung des Bearbeitungszwecks unbedingt notwendig und dafür geeignet sind. Nicht mehr benötigte Personendaten müssen zeitnah vernichtet oder anonymisiert werden, sofern keine Archivierungs- oder Aufbewahrungsfristen bestehen.
Datenrichtigkeit	Die bearbeiteten Personendaten müssen jederzeit richtig und aktuell sein. Es müssen deshalb angemessene Massnahmen getroffen werden, um dies zu ermöglichen.
Datensicherheit und Vertraulichkeit	Personendaten müssen während des gesamten Bearbeitungs- und Aufbewahrungsprozesses geschützt und durch angemessene Massnahmen gesichert werden. Personendaten sind vertraulich zu behandeln.

Datenschutz / Privacy by Design und by Default	Systeme sollen so entwickelt und programmiert werden, dass sie von Grund auf datenschutzfreundlich gestaltet sind (Privacy by Design) und die enthaltenen Voreinstellungen stets standardmässig den grösstmöglichen Datenschutz ermöglichen (Privacy by Default).

4. Rechtmässigkeit der Bearbeitung von Personendaten

Jede Bearbeitung oder Erhebung von Personendaten verlangt einen «Rechtfertigungsgrund», der die Rechtmässigkeit der Bearbeitung begründet. Es gibt die folgenden Rechtfertigungsgründe:

- Einwilligung der betroffenen Person
- Erfüllung eines Vertrags
- Überwiegendes privates oder öffentliches Interesse
- Gesetzliche Grundlage
- Forschung, Planung oder Statistik

Bevor mit einer neuen Bearbeitung von Personendaten begonnen wird, muss sichergestellt werden, dass ein Rechtfertigungsgrund vorliegt. Dieser muss entsprechend dokumentiert sein.

4.1. Einwilligung der betroffenen Person

Wo notwendig wird die Einwilligung der betroffenen Person für die Bearbeitung ihrer Personendaten eingeholt.

Vor der Einwilligung muss die betroffene Person umfassend über die Datenbearbeitung, deren Umfang und Zweck informiert werden. Die Einwilligung ist an keine Formvorschrift gebunden, sie muss jedoch freiwillig und eindeutig erteilt werden. Aus Beweisgründen empfiehlt sich eine schriftliche oder elektronische Erklärung.

Eine ausdrückliche Einwilligung ist für die Bearbeitung von besonders schützenswerten Personendaten und für das Profiling mit hohem Risiko erforderlich. Diese kann schriftlich (analog oder digital) erfolgen, aber auch durch eine mündliche Äusserung gegeben werden, wobei eine beweisbare Erklärung vorzuziehen ist. Eine Einwilligung ist auch durch das Ankreuzen eines Kästchens oder das Anklicken einer Schaltfläche auf einer Website (z.B. «Weiter») gültig. Nicht zulässig sind vorangekreuzte Kästchen oder Blankoeinwilligungen. Keine Einwilligung liegt vor, wenn die betroffene Person gänzlich untätig bleiben muss.

4.2. Erfüllung eines Vertrags

Personendaten von Leistungsbeziehenden, Geschäftskundinnen oder Vertragspartnern dürfen zur Begründung, Durchführung und Beendigung eines Vertrags ohne Einwilligung erhoben und bearbeitet werden. Die Datenbearbeitung umfasst auch das Beziehungsmanagement zu diesen Personen, sofern dieses im Zusammenhang mit dem Vertragszweck steht (z.B. die Verdankung einer Spende).

4.3. Überwiegendes privates und öffentliches Interesse

Für die Erfüllung seines Mandats muss das SRK SO Personendaten bearbeiten können. In diesem Zusammenhang ist es dem SRK SO erlaubt, für die Durchführung einer Bearbeitungstätigkeit die Daten einer betroffenen Person zu bearbeiten, auch wenn dies in gewissem Widerspruch zu den Interessen der betroffenen Person steht (daher das «überwiegende» private Interesse des SRK). Ein überwiegendes öffentliches Interesse liegt zum Beispiel vor, wenn die innere Sicherheit der Schweiz bedroht ist oder wenn aus humanitären Gründen Daten ins Ausland bekannt gegeben werden, um bei der Suche von Personen zu helfen, die in einem Konfliktgebiet oder nach einer Naturkatastrophe vermisst werden.

Die Interessensabwägung muss stets unter Einbezug der Datenschutzverantwortlichen vorgenommen werden. Diese informiert die Geschäftsleitung.

4.4. Gesetzliche Grundlage

Die Bearbeitung von Personendaten ist zulässig, wenn eine gesetzliche Grundlage dies vorsieht. Viele Bundesgesetze haben eigene datenschutzrechtliche Vorschriften erlassen, so z.B. für die Anerkennung ausländischer Ausbildungsabschlüsse, die Einholung eines Strafregister- oder Betreibungsauszugs, Daten im Rahmen von Sozialversicherungsabklärungen oder Einträge in Personenregistern etc. In einem solchen Fall muss grundsätzlich keine Einwilligung eingeholt werden, da die Datenbearbeitung aufgrund der gesetzlichen Vorschrift erlaubt ist.

4.5. Forschung, Planung oder Statistik

Die Bearbeitung von Personendaten für nicht personenbezogene Zwecke im Rahmen von Forschung, Planung oder Statistik kann ebenfalls notwendig sein. Vorausgesetzt ist, dass die Personendaten anonymisiert werden, sobald der Bearbeitungszweck dies zulässt, besonders schützenswerte Personendaten nur anonymisiert an Dritte weitergegeben werden und auch die Publikation der Resultate so erfolgt, dass kein Rückschluss auf die betroffenen Personen möglich ist.

5. Rechte der betroffenen Person

5.1. Recht auf transparente und umfassende Information

Im Rahmen des Grundsatzes der Transparenz hat die betroffene Person ein Recht auf umfassende Information bzw. der Verantwortliche eine Pflicht zur Information. Ohne die entsprechende Information kann die betroffene Person nicht erkennen, dass und/oder wie ihre Personendaten bearbeitet werden und kann entsprechend ihre Rechte nicht wahrnehmen.

Die betroffene Person muss mindestens über die Identität des Verantwortlichen, den Bearbeitungszweck, Empfänger, denen Personendaten bekannt gegeben werden, sowie bei einer Weitergabe der Personendaten ins Ausland über den Staat oder das internationale Organ informiert werden. Die Information kann individuell oder kollektiv erfolgen, beispielsweise über Allgemeine Geschäftsbedingungen oder eine auf einer Website veröffentlichte Datenschutzerklärung.

5.2. Weitere Rechte

Daneben gelten für die betroffene Person, deren Personendaten vom SRK SO bearbeitet werden, die folgenden Rechte:

- das Recht auf unentgeltliche Auskunft über die Herkunft, den Erhebungs- und Verwendungszweck, die geplante Dauer der Speicherung sowie die Art der Bearbeitung ihrer Personendaten, sowie an welche Drittpersonen ihre Personendaten weitergegeben werden;
- das Recht auf Berichtigung und/oder Ergänzung ihrer Daten, sollten diese unrichtig oder unvollständig sein;
- das Recht auf Widerspruch und Einschränkung der Bearbeitung der für den Zweck benötigten Personendaten;
- das Recht auf Löschung, soweit nicht zwingende gesetzliche Gründe die Speicherung und Bearbeitung erfordern. Je nachdem kann die Löschung auch in der Inaktivierung bzw. Anonymisierung der Daten bestehen;
- das Recht auf Datenportabilität in einem elektronischen Format für automatisierte bearbeitete Personendaten, die das SRK mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem SRK als Verantwortlichen und der betroffenen Person bearbeitet;
- das Recht, eine Beschwerde bei der zuständigen Aufsichtsbehörde einzureichen, wenn es zu datenschutzrechtlichen Verstössen gekommen ist.

Entsprechende Anträge sind an die Datenschutzverantwortliche weiterzuleiten. Diese informiert die Geschäftsleitung.

6. Weitergabe von Personendaten

6.1. Weitergabe an interne Empfänger

Grundsätzlich dürfen Personendaten an interne Empfänger, das heisst an andere Bereiche innerhalb des SRK SO, weitergegeben werden, wenn dies zur Erfüllung des Auftrags notwendig ist. Wenn die Personendaten jedoch für einen neuen Zweck bearbeitet werden sollen, dann sind die Information der betroffenen Person sowie ein Rechtfertigungsgrund notwendig.

6.2. Weitergabe an externe Empfänger

Werden Personendaten an Dritte wie Vertragspartner, Behörden usw., weitergeben, muss ein Rechtfertigungsgrund vorliegen. Beispielsweise besteht das überwiegende Interesse daran, dass allfälligen Lösch- oder Auskunftsbegehren unserer Kundinnen und Kunden über alle Rotkreuzorganisationen hinweg in einem auch für die Kundin und den Kunden einfachen Prozess nachgekommen werden

kann. Deshalb werden Name, Adresse und Telefonnummer unserer Kundinnen und Kunden entsprechend bekanntgegeben.

Bearbeitet ein Dritter im Auftrag des SRK SO Personendaten, muss mit diesem vereinbart werden, dass er dieselben datenschutzrechtlichen Grundsätze wie das SRK SO einhält. Gilt es das Berufsgeheimnis zu wahren, ist der Beauftragte verpflichtet, sich ebenfalls daran zu halten.

Der Beauftragte verpflichtet sich, die gesetzlichen und vertraglich vereinbarten Pflichten einzuhalten, insbesondere darf er Personendaten nur gemäss den Anweisungen des SRK SO bearbeiten.

Im Falle einer Verletzung der Datensicherheit muss der Beauftragte das SRK SO unverzüglich informieren, sodass dieser über das weitere Vorgehen entscheiden kann.

- Organisation A beauftragt Organisation B Spendenbriefe zu drucken und zu verschicken und gibt ihr deshalb Zugang auf die Spendendatenbank.
- Organisation A speichert seine Dokumente auf den Servern von Organisation B.

Der / die Verantwortliche hat dabei die folgenden drei Pflichten:

- Sorgfalt bei der Auswahl: Ein Auftragsbearbeiter muss sorgfältig ausgewählt werden. Es muss sichergestellt werden, dass er die gesetzlichen Anforderungen an Datenschutz und -sicherheit erfüllen kann.
- Sorgfalt bei den Anweisungen: Dem Auftragsbearbeiter müssen alle für die Aufgabenerfüllung notwendigen Anweisungen in vertraglicher Form gegeben werden. Das gilt auch für die Grundsätze betreffend Datenschutz und Wahrung des Berufsgeheimnisses.
- Sorgfalt bei der Überwachung: Der / die Verantwortliche muss die Einhaltung der datenschutzrechtlichen Pflichten und des vertraglich vereinbarten Auftrags überwachen, um jegliche Verletzungen zu vermeiden.

Der Auftragsbearbeiter verpflichtet sich die gesetzlichen und vertraglich vereinbarten Pflichten einzuhalten, insbesondere darf er Personendaten nur gemäss den Anweisungen des Verantwortlichen bearbeiten.

Im Falle einer Verletzung der Datensicherheit muss der Auftragsbearbeiter den Verantwortlichen unverzüglich informieren, sodass dieser über das weitere Vorgehen entscheiden kann.

6.3. Weitergabe von Personendaten ins Ausland oder an internationale Organe

Wenn Personendaten ins Ausland (d.h. ausserhalb der Schweiz) oder an ein internationales Organ (wie z.B. das IKRK) übermittelt werden, muss das Empfängerland über ein angemessenes Datenschutzniveau verfügen. Wenn dies der Fall ist, ist im Prinzip eine Übermittlung möglich.

Der Bundesrat führt mit Anhang 1 der Datenschutzverordnung eine Liste von Staaten mit deren Stand des Datenschutzes.

Wenn kein angemessenes Schutzniveau besteht, können unter bestimmten Bedingungen dennoch Personendaten ins Ausland bekannt geben werden, beispielsweise:

- wenn die betroffene Person ausdrücklich in die Auslandbekanntgabe eingewilligt hat;
- wenn die Auslandbekanntgabe notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es nicht möglich ist, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen;
- wenn die Auslandbekanntgabe in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht.

7. Verzeichnis und Dokumentation der Bearbeitungstätigkeiten

Das SRK SO führt ein Verzeichnis über alle Bearbeitungstätigkeiten. Dies bedeutet gleichzeitig, dass alle neuen Bearbeitungstätigkeiten vor Einführung geprüft und anschliessend im Verzeichnis dokumentiert werden müssen.

7.1. Verzeichnis der Bearbeitungstätigkeiten

Bei diesem Verzeichnis handelt es sich um eine allgemeine Beschreibung der Bearbeitungstätigkeiten. Die wichtigsten Inhalte des Verzeichnisses sind der Bearbeitungszweck, der Rechtfertigungsgrund, Kategorien betroffener Personen sowie von Personendaten, interne und externe Empfänger sowie Massnahmen zur Datensicherheit.

7.2. Neue Bearbeitungstätigkeiten

Bei der Planung neuer Vorhaben wie Projekte, Applikationen, Prozesse usw. muss die Datenschutzverantwortliche frühzeitig einbezogen werden, damit die notwendigen Massnahmen berücksichtigt werden können (Datenschutz by Design and by Default). Diese legt bei Bedarf geeignete Massnahmen fest und prüft die Konformität mit dem vorliegenden Reglement sowie den gesetzlichen Bestimmungen, die Notwendigkeit einer Datenschutzfolgeabschätzung sowie Massnahmen für die Gewährleistung der Sicherheit sowie allfällige vertragliche Vereinbarungen.

Beispiele für neue Bearbeitungstätigkeiten: Einführung von Google Analytics, Beschaffung einer Applikation für die digitale Patientenadministration, Outsourcing des Call Centers.

7.3. Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (DSFA) ist ein Instrument, um mögliche Risiken bei Bearbeitungstätigkeiten frühzeitig zu erkennen und zu bewerten. Auf Basis dieser Einschätzung sollen bei Bedarf angemessene Massnahmen definiert werden, um die erkannten Risiken für die Persönlichkeit oder Grundrechte der betroffenen Person zu senken.

Eine DSFA muss für durchgeführt werden, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Das hohe Risiko ergibt sich aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Es liegt in den folgenden Fällen vor:

- bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten
- bei einem Profiling

In der DSFA wird eine dokumentierte Interessenabwägung zwischen den Interessen des Verantwortlichen und denen der betroffenen Person vorgenommen. Wenn man trotz der geplanten Abhilfemassnahmen zum Schluss kommt, dass für die betroffene Person weiterhin ein Risiko besteht, muss die Datenschutzverantwortliche in Absprache mit der Geschäftsleitung den EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter) informieren.

8. Datensicherheit

Personendaten müssen vertraulich und in einer Weise bearbeitet werden, die eine angemessene Sicherheit gewährleistet. Dies beinhaltet auch den Schutz vor unbefugter oder unrechtmässiger Bearbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Die Sicherheit der Personendaten lässt sich mit technischen und organisatorischen Massnahmen (TOMs) erhöhen. Technische Massnahmen hängen direkt mit dem Informationssystem bzw. der Applikation zusammen, welche bestimmten Kriterien genügen müssen, um die Sicherheit der Personendaten gewährleisten zu können. Organisatorische Massnahmen hingegen betreffen das Umfeld des Informationssystems, insbesondere die Personen, die es nutzen und ihr Umfeld. Nur ein Zusammenspiel beider Arten von Massnahmen verhindert den nicht datenschutzkonformen Umgang mit Personendaten.

Das Ziel ist die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit der Datenbearbeitung. Die wichtigsten technischen und organisatorischen Massnahmen sind:

- Pseudonymisierung und Verschlüsselung der Personendaten bei Aufbewahrung und Austausch

- Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Applikationen
- Sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten gemäss Need-toKnow-Prinzip
- Privacy by Design und by Default
- Nur berechtigter Zugang zu Räumlichkeiten, in denen Personendaten bearbeitet werden
- Regelmässige Überprüfung und Bewertung der Wirksamkeit der getroffenen technischen und organisatorischen Massnahmen

Die technischen und organisatorischen Massnahmen müssen dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie den Risiken, welche die Bearbeitung für die Persönlichkeit und Grundrechte der betroffenen Personen mit sich bringt, angemessen sein. Je höher das Risiko, je grösser die Eintrittswahrscheinlichkeit und je umfangreicher die Datenbearbeitung ist, umso höher sind die Anforderungen an die technischen und organisatorischen Vorkehrungen, damit sie als angemessen gelten können.

9. Aufbewahrung und Löschung von Personendaten

Personendaten müssen während ihres gesamten Lebenszyklus geschützt werden. Das gilt für die Beschaffung, Einspeisung in die Applikation(en) und über alle Bearbeitungsschritte hinweg bis zu ihrer Vernichtung, Anonymisierung oder Archivierung.

9.1. Aufbewahrungsfristen

Personendaten dürfen nur so lange bearbeitet und aufbewahrt werden, als diese für die Erreichung des Zwecks, für den sie erhoben wurden, notwendig sind. Eine längere Aufbewahrung ist aus den folgenden Gründen möglich:

- Erfüllung von gesetzlichen Pflichten (z.B. Aufbewahrungs- und Dokumentationspflichten aus dem Zivil- oder Steuerrecht)
- Erfüllung von vertraglichen Pflichten (z.B. Erstellung eines Arbeitszeugnisses)
- Erfüllung von berechtigten privaten Interessen (z.B. Geltendmachung oder Verteidigung von Rechtsansprüchen)

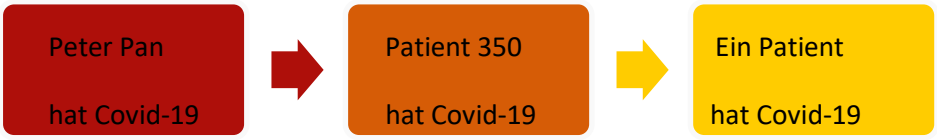
9.2. Pseudonymisierung und Anonymisierung von Personendaten

Damit die Personen, deren Daten in einem System bearbeitet werden, nicht mehr identifiziert werden können, können die Daten pseudonymisiert oder anonymisiert werden.

Bei der Pseudonymisierung werden alle Daten, die Rückschlüsse auf eine bestimmte Person zulassen, durch neutrale Angaben (Pseudonym) ersetzt. Eine Konkordanztabelle hält fest, welches Pseudonym welchen identifizierenden Daten entspricht. Solange diese Tabelle besteht und zugänglich ist, kann

die Pseudonymisierung rückgängig gemacht werden. Pseudonymisierte Personendaten bleiben Personendaten, für welche die Grundsätze des Datenschutzes gelten.

Bei der Anonymisierung hingegen werden die Daten und jede Möglichkeit, die Originaldaten wieder herzustellen, definitiv verunmöglicht. Die betroffene Person lässt sich nicht mehr identifizieren, und der Vorgang ist irreversibel. Vollkommen anonymisierte Daten gelten daher nicht mehr als Personendaten.



Personendaten **Pseudonymisierung** **Anonymisierung**

Während die Pseudonymisierung als sinnvolle Massnahme für die Erhöhung des Datenschutzes gilt, ist die Anonymisierung eine Alternative zur Löschung von Personendaten. Beide Massnahen sollten so oft wie möglich genutzt werden.

9.3. Löschen von Personendaten

Sobald die Personendaten zum Zweck der Bearbeitung nicht mehr notwendig sind, müssen diese vernichtet oder anonymisiert werden. Dasselbe gilt, wenn eine betroffene Person explizit die Löschung der Daten fordert. Bei elektronisch gespeicherten Daten reicht oft eine einfache Löschung nicht aus, sie dürfen nie mehr zugänglich sein und müssen entsprechend durch die IT gelöscht werden. Personendaten auf Papier, v.a. besonders schützenswerte Personendaten, müssen geschreddert werden. Das Vernichten kann nicht delegiert werden, zuständig ist die verantwortliche Person.

10. Website und E-Mail

10.1. Datenschutz

Das SRK SO weist darauf hin, dass die Datenübertragung im Internet (z.B. bei der Kommunikation per E-Mail) Sicherheitslücken aufweisen kann. Ein lückenloser Schutz der Daten vor dem Zugriff durch Dritte ist nicht möglich.

10.2. Datenerfassung

Daten werden erfasst, wenn die betroffene Person das SRK SO kontaktiert. Das kann durch Ausfüllen eines Kontaktformulars oder via E-Mail geschehen. Weitere Daten werden automatisch beim Besuch der Website durch unsere IT-Systeme erfasst. Das sind vor allem technische Daten (z.B. Internetbrowser, Betriebssystem oder Uhrzeit des Seitenaufrufs).

10.3. SSL- bzw TLS-Verschlüsselung

Die Websites nutzen aus Sicherheitsgründen und zum Schutz der Übertragung vertraulicher Inhalte eine SSL- bzw. TLS-Verschlüsselung. Eine verschlüsselte Verbindung erkennt man daran, dass die Adresszeile des Browsers von “http://” auf “https://” wechselt und an dem Schloss-Symbol in der Browserzeile. Wenn die SSL- bzw. TLS-Verschlüsselung aktiviert ist, können die Daten, welche die Person an das SRK SO übermitteln, nicht von Dritten mitgelesen werden.

10.4. Cookies

Wir verwenden Cookies. Diese richten auf dem Rechner der betroffenen Person keinen Schaden an und enthalten keine Viren. Cookies dienen dazu, das Angebot nutzerfreundlicher, effektiver und sicherer zu machen. Cookies sind kleine Textdateien, die auf dem Rechner abgelegt werden und die der Browser speichert.

Die meisten der vom SRK SO verwendeten Cookies sind so genannte “Session-Cookies”. Sie werden nach Ende des Besuchs automatisch gelöscht. Andere Cookies bleiben auf dem Endgerät gespeichert bis die Person diese löschen. Diese Cookies ermöglichen es advo5, den Browser beim nächsten Besuch wiederzuerkennen.

Cookies, die zur Durchführung des elektronischen Kommunikationsvorgangs oder zur Bereitstellung bestimmter, von der betroffenen Person erwünschter Funktionen, zum Beispiel zum Wegklicken eines geöffneten Fensters, erforderlich sind, werden gespeichert, weil das SRK SO ein berechtigtes Interesse an der Speicherung von Cookies zur technisch fehlerfreien und optimierten Bereitstellung der Dienste hat. Mit der Aktivierung der einzelnen Cookies können sich die Besucher der Website einverstanden erklären oder diese sperren lassen. Der Cookiebanner bietet die entsprechenden Einstellungen.

10.5. Kontaktformular

Füllt die betroffene Person das Kontaktformular aus, werden diese Angaben zwecks Bearbeitung der Anfrage gespeichert. Die im Kontaktformular eingegebenen Daten bleiben vorhanden, bis die betroffene Person uns zur Löschung auffordert, die Einwilligung zur Speicherung widerruft oder der Zweck für die Datenspeicherung entfällt.

11. Meldung einer Datenschutzverletzung

Unter einer Datenschutzverletzung («Data Breach») ist jede interne oder externe Verletzung der Sicherheit von Personendaten zu verstehen, die:

- zur Vernichtung,
- zum Verlust,
- zur Veränderung,

- zu unbefugtem Zugriff oder
- zur unerlaubten Verwendung

dieser Daten führt.

11.1. Meldung innerhalb des SRK SO

Jede/r Mitarbeitende, Ehrenamtliche und Freiwillige des SRK SO muss einen tatsächlich eingetretenen oder drohenden Vorfall an die Beauftragte für Datenschutz melden. Dasselbe gilt, wenn ein Beauftragter eine Datenschutzverletzung an das SRK SO meldet.

Die Beauftragte für Datenschutz wird mit Unterstützung der relevanten Stellen (Geschäftsleitung, IT, Bereichsleiter, Kommunikation) den Vorfall prüfen und alle notwendigen Massnahmen ergreifen, um die Auswirkungen der Datenschutzverletzung für die betroffene Person und das SRK SO soweit möglich zu minimieren. Soweit erforderlich wird die Verletzung den zuständigen Aufsichtsbehörden (primär EDÖB) und den betroffenen Personen gemeldet.

11.2. Meldung an den EDÖB

Jede Verletzung der Sicherheit von Personendaten, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte des Betroffenen darstellen kann, muss dem EDÖB gemeldet werden. Die Ankündigung erfolgt so rasch wie möglich ab dem Zeitpunkt, an dem die (wahrscheinlich) unberechtigte Bearbeitung bekannt wird.

Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhaltes zu umfassen, insbesondere:

- die Art der Datenschutzverletzung
- ungefähre Anzahl der betroffenen Personen
- die Folgen für die betroffenen Personen
- die getroffenen oder geplanten Massnahmen zur Behebung der Situation oder zur Milderung ihrer Folgen

Die Meldung erfolgt durch die Beauftragte für Datenschutz in Absprache mit der Geschäftsleitung.

11.3. Meldung an die betroffene(n) Person(en)

Die betroffene Person muss über die Verletzung ihrer Personendaten informiert werden, wenn dadurch die Risiken für ihre Persönlichkeitsverletzung oder die Verletzung ihrer Grundrechte verringert werden. Dies ist insbesondere der Fall, wenn die betroffene Person notwendige Schritte zu ihrem Schutz einleiten kann (z.B. Änderung des Passworts). Dasselbe gilt, wenn der EDÖB dies verlangt.

In den folgenden Fällen kann die Mitteilung an die betroffene Person eingeschränkt, aufgeschoben oder darauf verzichtet werden:

- überwiegende Interessen eines Dritten

- gesetzliche Geheimhaltungspflicht
- Informationspflicht kann nicht erfüllt werden oder erfordert einen unverhältnismässigen Aufwand
- Information einer grossen Zahl von Personen mittels öffentlicher Bekanntgabe

Die Meldung erfolgt durch die Beauftragte für Datenschutz in Absprache mit der Geschäftsleitung.

12. Schlussbestimmungen

Dieses Reglement wird regelmässig überprüft und bei Bedarf angepasst. Die Mitarbeitenden und Freiwilligen werden in geeigneter Weise darüber informiert.

Unterschriften

Dr. iur. A. Häfliger	Nancy Savoldelli
Präsident	Vizepräsidentin

13. Anhang

Dieses Reglement wird regelmässig überprüft und bei Bedarf angepasst. Die Mitarbeitenden, Ehrenamtlichen und Freiwilligen werden darüber informiert.

Definition	Beschreibung
Personendaten	Alle Angaben, die sich auf eine *bestimmte oder bestimmbare* natürliche Person (im Folgenden «betroffene Person») beziehen. Als bestimmt bzw. bestimmbar wird eine natürliche Person angesehen, die direkt oder indirekt bestimmt oder identifiziert werden kann. Die Identifizierung kann über eine einzige Information möglich sein (Telefonnummer, Hausnummer, AHV-Nummer, Fingerabdrücke) oder über den Abgleich verschiedener Informationen (Adresse, Geburtsdatum, Zivilstand). Sie kann sich auch über den Hinweis auf Informationen, die sich aus den Umständen oder dem Kontext ableiten lassen, ergeben (Identifikationsnummer, Standortdaten). Anonymisierte Personendaten sind keine Personendaten mehr, pseudonymisierte aber schon.
Besonders schützenswerte Personendaten	Personendaten, welche aufgrund ihrer Eigenschaften einen erhöhten Schutzbedarf haben. Darunter fallen: • Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten • Daten über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit • Genetische und biometrische Daten • Massnahmen der sozialen Hilfe • Administrative oder strafrechtliche Verfolgung und Sanktionen
Betroffene Person	Natürliche und juristische Person über die Personendaten bearbeitet werden.
Bearbeiten	Jeder Umgang mit Personendaten, unabhängig von der Art und Form ihrer Bearbeitung (digital, auf Papier, mündlich), insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.

Bearbeitungstätigkeit	Tätigkeiten oder Kategorien von Tätigkeiten bei denen Personendaten bearbeitet werden, normalerweise mit einem gemeinsamen Zweck.
Bekanntgeben	Das Übermitteln oder Zugänglichmachen von Personendaten.
Profiling	Jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser Person zu analysieren oder vorherzusagen.
Profiling mit hohem Risiko	Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.
Verantwortlicher	Person oder Bundesorgan, die oder das allein (oder zusammen mit anderen, d.h. gemeinsame Verantwortliche) über den Zweck und die Mittel der Bearbeitung der Personendaten entscheidet.
Beauftragter (Auftragsdatenbearbeiter)	Person oder Bundesorgan, die oder das im Auftrag des/der Verantwortlichen Personendaten bearbeitet.
Dateneigner/in	Person, die für die Bearbeitung der Personendaten verantwortlich ist, z.B. Bereichs- oder Projektleitende.
Dritte	Alle natürlichen oder juristischen Personen, Behörden oder andere Stellen, ausser der betroffenen Person, dem Verantwortlichen und dem Auftragsbearbeiter.
Empfänger	Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der Personendaten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

Bundesorgan	Behörde oder Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist.
Internationales Organ	Alle internationalen Institutionen, seien dies Organisationen oder Gerichte (z.B. IKRK).
Applikation	System, Hard- oder Software mit dem/der Personendaten bearbeitet werden.
Pseudonymisierung	Veränderung von Personendaten in einer Weise, dass die Personendaten nur bei Hinzuziehung zusätzlicher Informationen einer bestimmten Person zugeordnet werden können. Für die Gewährleistung eines effektiven Schutzes müssen diese zusätzlichen Informationen gesondert aufbewahrt werden.
Anonymisierung	Vorgang, bei dem Personendaten so verändert werden, dass nicht mehr auf die betroffene Person geschlossen werden kann. Diese Methode gilt als nützliche Alternative zur Löschung von Personendaten.