



Datenschutz-Weisung GS SRK adaptiert für SRK Kanton Zug

Version	Basis Version GS V3.0 / 13. 06. 2023 für Version SRK Kanton Zug V1.0/14.04.2025
Kurztitel	
Datenschutz-Erklärung SRK Kanton Zug	
Ziel und Zweck	Diese Weisung legt verbindliche Regeln für die Bearbeitung von Personendaten innerhalb des SRK Kanton Zug fest. Nebst den Datenschutz-Grundsätzen des SRK bildet die vorliegende Weisung die Grundlage und Garantie für den Schutz von Personendaten im Sinne von verbindlichen internen Datenschutzvorschriften.
Geltungsbereich	Diese Weisung gilt für alle Mitarbeitenden, Ehrenamtlichen und Freiwilligen des SRK Kanton Zug sowie die durch das SRK Kanton Zug beauftragten Personen.
Gültig ab 1.5.2025	



Inhalt

1. Einleitung	3
2. Verantwortlichkeiten	3
2.1. Verantwortlichkeiten im SRK Kanton Zug	3
2.2. Datenschutzberater/in	4
3. Allgemeine Grundsätze für die Bearbeitung von Personendaten	5
4. Rechtmässigkeit der Bearbeitung von Personendaten	6
4.1. Einwilligung der betroffenen Person	7
4.2. Erfüllung eines Vertrags	7
4.3. Überwiegendes privates und öffentliches Interesse	7
4.4. Gesetzliche Grundlage	8
4.5. Forschung, Planung oder Statistik	8
5. Rechte der betroffenen Person	8
5.1. Recht auf transparente und umfassende Information	8
5.2. Weitere Rechte	9
6. Weitergabe von Personendaten an Dritte	9
6.1. Weitergabe an interne Empfänger (innerhalb des SRK Kanton Zug)	10
6.2. Weitergabe an externe Empfänger	10
6.3. Weitergabe von Personendaten ins Ausland oder an internationale Organe	11
7. Verzeichnis und Dokumentation der Bearbeitungstätigkeiten	11
7.1. Verzeichnis der Bearbeitungstätigkeiten	12
7.2. Neue Bearbeitungstätigkeiten	12
7.3. Datenschutz-Folgenabschätzung	12
8. Datensicherheit	13
9. Aufbewahrung und Löschung von Personendaten	14
9.1. Aufbewahrungsfristen	14
9.2. Pseudonymisierung und Anonymisierung von Personendaten	14
9.3. Löschung von Personendaten	15
10. Meldung einer Datenschutzverletzung	15
10.1. Meldung innerhalb des SRK Kanton Zug	15
10.2. Meldung an den EDÖB	16
10.3. Meldung an die betroffene(n) Person(en)	16
11. Schlussbestimmungen	17
Anhang: Begriffe	18



1. Einleitung

Das SRK sammelt und bearbeitet aufgrund seiner Vielzahl an Tätigkeiten eine bedeutende Anzahl an Personendaten. Die sieben Rotkreuzgrundsätze leiten uns in unserer täglichen Arbeit und gebieten uns, dem Schutz von Personendaten, insbesondere besonders schützenswerten Personendaten, ein angemessenes Gewicht zu geben. 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.

Die vom Rotkreuzrat verabschiedeten **Datenschutz-Grundsätze des SRK** bilden den Rahmen und Stellenwert im Umgang mit Personendaten im SRK. Die vorliegende Weisung legt verbindliche Vorschriften für die Bearbeitung von Personendaten fest und kann durch weitere ausführende Weisungen zu einzelnen Bereichen ergänzt werden.

Ziel und Zweck dieser Weisung ist es, den Mitarbeitenden, Ehrenamtlichen und Freiwilligen des SRK Kanton Zug einen Leitfaden und ein Handbuch vorzugeben. Wo auf eine Weisung oder einen Prozess hingewiesen ist, sind diese zu beachten. Für Detailauskünfte steht der/die Datenschutzverantwortliche gerne zur Verfügung.

Alle Mitarbeitenden, Ehrenamtlichen und Freiwilligen des SRK Kanton Zug sind verpflichtet, sich an die Inhalte dieser Weisung und an die ausführenden Weisungen zu halten. Deren Einhaltung wird regelmässig überprüft. Im Falle von Missachtung oder Missbräuchen werden die erforderlichen Massnahmen ergriffen. Notwendige Abweichungen und Ausnahmen von dieser Weisung sind durch die Dateneigner:innen schriftlich zu begründen und dokumentieren.

Verhältnis zu den gesetzlichen Anforderungen: Für das SRK Kanton Zug gelten grundsätzlich die Bestimmungen des Bundesgesetzes über den Datenschutz und der dazugehörigen Verordnung. Im Rahmen von Angeboten an natürliche Personen in der EU oder im EWR oder bei der Beobachtung des Verhaltens solcher Personen gelten zudem die Bestimmungen der EU nach Massgabe der Datenschutzgrundverordnung (DSGVO). Diese Weisung führt die einschlägigen gesetzlichen Bestimmungen näher aus. Sollte eine Bestimmung dieser Weisung zu einem Verstoß gegen DSG oder die DSGVO führen, so ist dies dem/der Datenschutzverantwortliche zu melden.

2. Verantwortlichkeiten

2.1. Verantwortlichkeiten im SRK Kanton Zug

Für die Einhaltung und Umsetzung des Datenschutzes gelten die nachfolgenden Verantwortlichkeiten.

- Der **Rotkreuzrat** genehmigt die Datenschutz-Grundsätze des SRK, die in allen Rotkreuz-Organisationen und der GS SRK zusätzlich zu den gesetzlichen Bestimmungen gelten.
- **Die Geschäftsführung** trägt die Hauptverantwortung für den Schutz der Bearbeitung von Personendaten. Sie sorgt für deren Umsetzung, akzeptiert und trägt das operative Restrisiko.



- **Der/die Informationssicherheitsbeauftragte der GS Bern** ist für die Informations- und Datensicherheit sowie für die physische, technische und organisatorische Sicherheit zuständig, berät die Geschäftsführung des SRK Kanton Zug und leistet damit einen wichtigen Beitrag zur Einhaltung der Datenschutz-Bestimmungen.
- Der **Rechtsdienst SRK** ist ansprechbar für die Geschäftsführung für alle unklaren rechtlichen Fragen im Zusammenhang mit dem Schutz von Personendaten oder von Informationen. Ob Verträge mit den einschlägigen Datenschutzgesetzen übereinstimmen, soll vom Rechtsdienst SRK oder anderen Rechtsberatern vorgängig geprüft werden.
- Die **Dateneigner:innen** ist verantwortlich für eine Datensammlung bzw. Bearbeitungstätigkeit. Ihm/ihr obliegt der ordnungsgemässe Schutz und die Klassifizierung der Personendaten und Informationen. Er/sie bestimmt über Zugriff, Veränderung und Weitergabe der Daten und schützt diese mit entsprechenden Massnahmen vor unerlaubten Zugriffen.
- Sämtliche **Mitarbeitenden, Ehrenamtlichen, Freiwilligen** und durch das SRK Kanton Zug **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 diese Weisung durch organisatorische, personelle und technische Massnahmen eingehalten werden und dass die für die Datenbearbeitungen verantwortlichen Personen ihre Verpflichtungen wahrnehmen.

Verstösse gegen das revidierte Datenschutzgesetz der Schweiz können zu hohen Bussen für Mitarbeitende, Ehrenamtliche und Freiwillige führen, die Personendaten konkret bearbeiten. Das SRK als Arbeitgeber kann zudem Sanktionen bis hin zur fristlosen Auflösung des Arbeitsverhältnisses aussprechen.

2.2. Datenschutzberater/in

Der/die Datenschutzberater/in berät das SRK Kanton Zug in Fragen des Datenschutzes und steht in engem Austausch mit dem/der Datenschutzbeauftragte/n der GS Bern. Der Begriff «Datenschutzberaterin» des DSG wird im SRK Kanton Zug mit den Begriffen «Datenschutzverantwortliche/r» bzw. «Datenschutzbeauftragte/r» analog verwendet.

Der/die Datenschutzberater/in ist Anlaufstelle für die betroffenen Personen, den EDÖB und für die Behörden, die in der Schweiz für den Datenschutz zuständig sind. Das SRK veröffentlicht die Kontaktdaten des/der Datenschutzverantwortlichen im Internet und teilt diese dem EDÖB mit.

Im Rahmen von neuen Projekten und bei geplanter Zusammenarbeit mit externen Dienstleistern wird der/die Datenschutzverantwortliche vorgängig konsultiert. Im Falle von unterschiedlichen Einschätzungen entscheidet die Geschäftsführung gestützt auf eine Güterabwägung.

Der/die Datenschutzverantwortliche wirkt bei der Anwendung der Datenschutzvorschriften mit, indem sie insbesondere die Bearbeitung von Personendaten prüft und Korrekturmassnahmen empfiehlt, wenn eine Verletzung der Datenschutzvorschriften festgestellt wird. Das SRK Kanton Zug sorgt dafür, dass der/die Datenschutzverantwortliche über eine Verletzung der Datensicherheit informiert wird.

Der/die Datenschutzverantwortliche berät das SRK Kanton Zug bei der Erstellung von Datenschutz-Folgenabschätzungen. Sie informiert über die Umsetzung und Fragen des Datenschutzes in Merkblättern, auch mithilfe des Datenschutzportals im Intranet der GS SRK. Sie schult und berät die Mitarbeitenden des SRK Kanton Zug in Fragen des Datenschutzes.

Der/die Datenschutzverantwortliche übt ihre Funktion gegenüber dem SRK fachlich unabhängig und weisungsungebunden aus. Ihr steht das Recht zu, in wichtigen Fällen die Geschäftsführung, den Vorstand oder wenn notwendig, die Mitgliederversammlung in dieser Reihenfolge zu informieren.

Das SRK stellt dem/der Datenschutzverantwortlichen die notwendigen Ressourcen zur Verfügung und gewährt Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten, die der/die Datenschutzverantwortliche zur Erfüllung der Aufgaben benötigt.

3. Allgemeine Grundsätze für die Bearbeitung von Personendaten

Alle Mitarbeitenden, Ehrenamtlichen und Freiwilligen halten sich an die im Bundesgesetz über den Datenschutz festgelegten allgemeinen Grundsätze. Daneben gelten auch die vom Rotkreuzrat verabschiedeten [Datenschutz-Grundsätze des SRK](#).

Die Einhaltung dieser Grundsätze muss von dem/der verantwortlichen Mitarbeitenden (Dateneigner/in) bei jeder Bearbeitung von Personendaten nachgewiesen werden können.

Grundsatz	Beschreibung
Rechtmässigkeit	Personendaten müssen auf rechtmässige Weise bearbeitet werden. Falls eine Rechtsgrundlage erforderlich ist, darf die Datenbearbeitung nur dann und soweit erfolgen, wie diese für den jeweiligen Verarbeitungsvorgang vorhanden ist (vgl. Kapitel 4).
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 den Datenverantwortlichen, den Bearbeitungszweck, mögliche Datenempfänger(kategorien), Auslandsbezüge und bei indirekter Datenerhebung über die Datenart (vgl. Kapitel 5).
Zweckbindung	Jede Erhebung und Bearbeitung von Personendaten muss einen bestimmten und für die betroffene Person erkennbaren Zweck verfolgen und nur so, dass es mit diesem Zweck vereinbar 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 oder ein entsprechendes Aufbewahrungsinteresse bestehen.
Datenrichtigkeit	Die bearbeiteten Personendaten sollen 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 (vgl. Kapitel 8). 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

Bei der Bearbeitung von Personendaten darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzt werden. Die Bearbeitung oder Erhebung von Personendaten ist nicht widerrechtlich, wenn ein «Rechtfertigungsgrund» durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz vorliegt.

Es gibt grundsätzlich folgende 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 sich der/die Dateneigner/in (ggf. zusammen mit dem/der Datenschutzberater/in) vergewissern, dass wo erforderlich ein Rechtfertigungsgrund vorliegt. (vgl. Kapitel 7). Nachfolgend werden die verschiedenen Rechtfertigungsgründe sowie Spezialfälle anhand von Beispielen erklärt.



4.1. Einwilligung der betroffenen Person

Die Einwilligung der betroffenen Person ist ein sehr aktiver und transparenter Rechtfertigungsgrund.

Vor der Einwilligung muss die betroffene Person umfassend über den Datenverantwortlichen, den Bearbeitungszweck, mögliche Datenempfänger (Kategorien), Auslandbezüge und bei indirekter Datenerhebung über die Datenart informiert werden (vgl. Kapitel 5.1). Die Einwilligung ist an keine Formvorschrift gebunden, sie muss jedoch freiwillig und eindeutig erteilt werden. Aus Beweisgründen empfiehlt sich aber eine schriftliche oder elektronische Erklärung.

Eine ausdrückliche Einwilligung ist für die Bearbeitung von **besonders schützenswerten Personendaten und für das Profiling mit hohem Risiko** erforderlich (vgl. Kapitel 4.6 sowie Definitionen im Anhang). 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 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). Ist dieser Zusammenhang nicht gegeben, das heisst, man will die Daten für einen anderen Zweck bearbeiten (z.B. um einer/m Leistungsbeziehenden Spendenaufrufe zuzustellen), so ist ein Rechtfertigungsgrund – primär in Form einer Einwilligung samt transparenter Information der betroffenen Person – notwendig.

4.3. Überwiegendes privates und öffentliches Interesse

Für die Erfüllung seines Mandats muss das SRK Personendaten sammeln und bearbeiten können. In diesem Zusammenhang ist es dem SRK 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, um lebenswichtige Interessen einer Person zu schützen, 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.

Diese Interessensabwägung muss stets unter Einbezug der/des Datenschutzverantwortliche/n vorgenommen werden.

4.4. Gesetzliche Grundlage

Die Erhebung oder Bearbeitung von Personendaten ist zulässig, wenn ein Gesetz, eine Verordnung oder ein anderer gesetzlicher Erlass dies explizit so 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. Für die eindeutige Interpretation der gesetzlichen Grundlage ist die Datenschutzberater/in beizuziehen.

4.5. Forschung, Planung oder Statistik

Der letzte Rechtfertigungsgrund ist die Bearbeitung von Personendaten für nicht personenbezogene Zwecke im Rahmen von Forschung, Planung oder Statistik. Hierfür gelten jedoch die Voraussetzungen, dass die Personendaten anonymisiert werden sobald der Bearbeitungszweck dies zulässt. Ist eine Anonymisierung unmöglich oder erfordert sie einen unverhältnismässigen Aufwand, so sind angemessene Massnahmen zu treffen, um die Bestimmbarkeit der betroffenen Person zu verhindern. Handelt es sich um besonders schützenswerte Personendaten, so sind diese Dritten so bekannt zu geben, dass die betroffene Person nicht bestimmbar ist; ist dies nicht möglich, so muss gewährleistet sein, dass die Dritten die Daten nur zu nicht personenbezogenen Zwecken bearbeiten. Die Publikation der Resultate hat so zu erfolgen, dass kein Rückschluss auf die betroffenen Personen möglich ist.

5. Rechte der betroffenen Person

In den Datenschutz-Grundsätzen hat sich das SRK verpflichtet, die Rechte der betroffenen Personen auf umfassende Information, Auskunft, Korrektur, Löschung und Datenportabilität der über sie gespeicherten Personendaten zu wahren. Das SRK Kanton Zug verfügt deshalb über entsprechende Prozesse, um die Betroffenenrechte vollständig und fristgerecht zu garantieren.

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 Verantwortliche¹ (vgl. Glossar im Anhang zum Begriff «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 gesetzlich garantierten Rechte nicht wahrnehmen.

Die betroffene Person muss mindestens über die Identität des Verantwortlichen, den Bearbeitungszweck, Empfänger (Kategorien), denen Personendaten bekannt gegeben werden (vgl. Kapitel 6.2), sowie bei einer Weitergabe der Personendaten ins Ausland über den Staat oder

¹ Da es sich beim Begriff «der Verantwortliche», als auch bei den noch folgenden Begriffen «der Auftragsbearbeiter» und «der Empfänger», um offizielle rechtliche Konzepte handelt, die sich primär auf juristische und nicht natürliche Personen beziehen, wird hier nur die männliche Form verwendet.



das internationale Organ (vgl. Kapitel 6.3) informiert werden, im Fall einer indirekten Datenerhebung (nicht von der betroffenen Person selbst) auch über die Datenarten. Die Information kann individuell oder kollektiv erfolgen, beispielsweise die auf der Website veröffentlichte Datenschutzerklärung, auf die aber im Einzelnen immer hingewiesen werden sollte. Die betroffene Person soll bei der Beschaffung ihrer Personendaten die wichtigsten Informationen bereits auf der ersten Kommunikationsstufe erhalten.

5.2 Weitere Rechte

Daneben gelten für die betroffene Person, deren Personendaten im SRK Kanton Zug bearbeitet werden, die folgenden Rechte:

- das Recht auf **Auskunft**, unter anderem über die Herkunft, den Erhebungs- und Verwendungszweck, die geplante Dauer der Speicherung sowie die Art der Bearbeitung ihrer gespeicherten 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 **Widerruf einer Einwilligung**;
- das Recht auf **Löschung**, soweit nicht zwingende gesetzliche Gründe oder überwiegende (berechtigte) Interessen die Speicherung und weitere Bearbeitung erfordern. Je nachdem kann die Löschung auch 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.

Die genaue Umsetzung dieser Rechte sowie die damit verbundenen Prozesse sind im DSG geregelt.

6. Weitergabe von Personendaten an Dritte

Es gibt Fälle, wo Personendaten nicht nur innerhalb des SRK Kanton Zug bearbeitet, sondern an Dritte weitergeben werden. Dies ist zum Beispiel der Fall, wenn Personendaten an Vertragspartner, Rotkreuz-Organisationen oder Behörden aus bestimmten Gründen weitergegeben werden. Damit dies rechtmässig ist, braucht es jeweils einen Rechtfertigungsgrund, insbesondere wenn die Personendaten dabei zu einem anderen Zweck bearbeitet werden oder besonders schützenswerte Personendaten bekanntgegeben werden (vgl. Kapitel 4).



6.1 Weitergabe an interne Empfänger (innerhalb des SRK Kanton Zug)

Grundsätzlich dürfen Personendaten an interne Empfänger, das heisst an andere Bereiche oder Teams innerhalb des SRK Kanton Zug, weitergegeben werden, wenn dies zur Erfüllung des Auftrags notwendig ist.

6.2 Weitergabe an externe Empfänger

Personendaten können an Dritte ausserhalb des SRK Kanton Zug zur Bearbeitung und Aufbewahrung weitergegeben werden, wenn dem SRK Kanton Zug selbst die Ressourcen fehlen oder Dritte diese Aufgabe besser erfüllen können.

Wenn ein Dritter im Auftrag und auf Anweisung des SRK Kanton Zug Personendaten bearbeitet, ohne dass diesem die gesamte Verantwortung hierfür übertragen worden ist, liegt eine **Auftragsbearbeitung** vor. Eine Auftragsbearbeitung ist nur erlaubt, wenn dies gesetzlich oder vertraglich möglich ist (z.B. nicht durch das Arztgeheimnis oder eine Geheimhaltungsklausel in einem Vertrag verboten ist) und der Auftragsbearbeiter die Bearbeitung nur so erfüllt, wie sie der Verantwortliche erfüllen dürfte. Wenn es sich um eine Weitergabe innerhalb derselben juristischen Person gemäss Kapitel 6.1 handelt, liegt keine Auftragsbearbeitung vor.



Beispiele:

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

Der 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. Je höher ein mit der Bearbeitung verbundenes Risiko ist, umso aufmerksamer muss der Verantwortliche bei der Formulierung der Anweisungen sein.
- **Sorgfalt bei der Überwachung:** Der Verantwortliche muss die Einhaltung der datenschutzrechtlichen Pflichten und des vertraglich vereinbarten Auftrags überwachen um jegliche Verletzungen zu vermeiden.

Wenn sich der Auftragsbearbeiter im Ausland befindet, muss der Verantwortliche zudem die Bestimmungen aus Kapitel 6.3 berücksichtigen. Gemäss den Datenschutz-Grundsätzen des SRK werden Personendaten nach Möglichkeit nur in der Schweiz und der EU gespeichert.

Der Auftragsbearbeiter ist verpflichtet, die gesetzlichen und vertraglich vereinbarten Pflichten einzuhalten, insbesondere darf er Personendaten nur gemäss den Anweisungen des Verantwortlichen bearbeiten. Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche. Der Auftragsbearbeiter kann für die Bearbeitung wiederum einen Dritten (den sogenannten Unterauftragsbearbeiter) beauftragen, sofern er hierfür die Einwilligung des Verantwortlichen hat.

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

Das SRK Kanton Zug kann sowohl Verantwortlicher als auch Auftragsbearbeiter sein. Dies muss jeweils vertraglich in Form eines **Auftragsdatenbearbeitungsvertrags** geregelt werden. Jeder dieser Verträge muss sämtliche Aufgaben beinhalten, die der Verantwortliche dem Auftragsbearbeiter überträgt, als auch die Pflichten und Verantwortlichkeiten der beiden Parteien. Sämtliche Verträge werden auf Basis der Vorlage der GS Bern erstellt und werden gemäss Weisung Zeichnungsberechtigung unterschrieben.

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 gegeben 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 ist nicht möglich, 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.

Für die Weitergabe von Daten ins Ausland wird eine spezifische Weisung oder ein Merkblatt ausgearbeitet.

7. Verzeichnis und Dokumentation der Bearbeitungstätigkeiten

Die SRK Kanton Zug unterliegt nicht der gesetzlichen Pflicht ein Verzeichnis über alle Bearbeitungstätigkeiten zu führen und zu dokumentieren, dass ihre Bearbeitungstätigkeiten im

Einklang mit der Datenschutzgesetzgebung stehen. Experten raten jedoch ein solches Verzeichnis der Bearbeitungstätigkeiten zu führen da dies als Basis für Datenschutzmassnahmen dienen. Im SRK Kanton Zug werden alle neuen Bearbeitungstätigkeiten vor Einführung geprüft und anschliessend im Verzeichnis durch den/die Datenschutzverantwortliche/n in Zusammenarbeit mit der Geschäftsführung und den Bereichsleitungen, den Dateneignern, dokumentiert.

7.1 Verzeichnis der Bearbeitungstätigkeiten

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

Sowohl der für die Bearbeitung Verantwortliche als auch der Auftragsbearbeiter müssen ein Verzeichnis der Bearbeitungstätigkeiten führen. Die Dateneigner/innen (vgl. Kapitel 2) sind für die regelmässige Überprüfung und Dokumentation von neuen Datenbearbeitungen verantwortlich.

7.2 Neue Bearbeitungstätigkeiten

Dateneigner/innen haben die Pflicht, neue und veränderte Bearbeitungstätigkeiten dem/der Datenschutzverantwortlichen zu melden, damit diese im Verzeichnis der Bearbeitungstätigkeiten nachgeführt werden können. Bei der Planung neuer Vorhaben wie Projekten, Applikationen, Prozessen usw. müssen der/die Datenschutzverantwortliche sowie die IT, resp. Informationssicherheit und Geschäftsführung frühzeitig einbezogen werden, damit die notwendigen Massnahmen berücksichtigt werden können (Datenschutz by Design and by Default). Diese legen zusammen mit den Dateneigner/innen bei Bedarf geeignete Massnahmen fest. Zudem prüfen diese u.a. die Konformität mit der vorliegenden Weisung sowie den gesetzlichen Bestimmungen, die Notwendigkeit einer Datenschutzfolgeabschätzung sowie Massnahmen für die Gewährleistung der Sicherheit sowie allfällige vertragliche Vereinbarungen.

Beispiele für neue Bearbeitungstätigkeiten: Erfassung von Ausweisnummern für die Reiseorganisation, 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.

Wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann, ist eine Datenschutz-Folgenabschätzung zu erstellen.

Das hohe Risiko ergibt sich, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Es liegt namentlich vor:

- a. bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten;
- b. wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.

Die DSFA wird durch den/die Dateneigner/in durchgeführt und anschliessend von der Beauftragten für Datenschutz geprüft. In der DSFA wird eine dokumentierte Interessenabwägung zwischen den Interessen des Verantwortlichen und denen der betroffenen Person vorgenommen.

Ergibt sich aus der Datenschutz-Folgenabschätzung, dass die geplante Bearbeitung trotz der vom SRK vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat, so ist der/die Datenschutzverantwortlich oder die Geschäftsführung befugt, die Stellungnahme des EDÖB einzuholen.

8. Datensicherheit

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

Zur Gewährleistung einer angemessenen Datensicherheit ist der Schutzbedarf der Personendaten zu bestimmen und geeignete technische und organisatorische Massnahmen festzulegen. 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 die Vernichtung oder den Verlust von Daten oder Irrtümer, Fälschungen und unberechtigten Zugang.

Die wichtigsten technischen und organisatorischen Massnahmen sind:

- Pseudonymisierung und Verschlüsselung der Personendaten bei Aufbewahrung und Austausch
- Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der Applikationen
- Protokollierung Bearbeitungsvorgängen, in gewissen Fällen aufzubewahren getrennt vom System, in welchem die Personendaten bearbeitet werden
- Sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten gemäss Need-to-Know-Prinzip
- Privacy by Design und by Default
- 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.

Für die Anforderungen an die Datensicherheit gelten die einschlägigen Rechtsnormen sowie die Richtlinien zur Informationssicherheit des SRK Kanton Zug.

9. Aufbewahrung und Löschung von Personendaten

Personendaten müssen während ihres gesamten Lebenszyklus geschützt werden und bleiben. Dies umfasst den Moment der 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 folgenden Gründen jedoch 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)

Die Bestimmung der Aufbewahrungsdauer und -fristen ist nicht immer ganz einfach und muss von Fall zu Fall entschieden werden. Als Basis gelten das Merkblatt zur Aufbewahrung und Löschung von Personendaten des SRK Kanton Zug.

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 konkrete 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 die die Grundsätze des Datenschutzes gelten.

Bei der **Anonymisierung** hingegen werden die Daten selber und alle Möglichkeiten, die Originaldaten wieder zu erlangen, definitiv beseitigt. Die Person lässt sich nicht mehr identifizieren, und der Vorgang ist irreversibel. Vollkommen anonymisierte Daten gelten daher nicht mehr als Personendaten.



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

9.3 Löschung 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 entsprechend gelöscht werden. Personendaten auf Papier, v.a. besonders schützenswerte Personendaten, müssen geschreddert werden. Für Datenträger und Medien gelten das Merkblatt zur Aufbewahrung und Löschung von Personendaten des SRK Kanton Zug sowie die allgemeinen Richtlinien Informationssicherheit und Datenschutz.

10. 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 und dadurch schwerwiegende Beeinträchtigungen für die Interessen und Rechte der betroffenen Personen drohen.

10.1 Meldung innerhalb des SRK Kanton Zug

Jede/r Mitarbeitende, Ehrenamtliche und Freiwillige des SRK Kanton Zug muss unverzüglich einen tatsächlich eingetretenen oder drohenden Vorfall dem/der Datenschutzverantwortliche/n melden, welche/r die Geschäftsführung informiert und ggf. mit dem Informationssicherheitsbeauftragten der GS SRK Kontakt aufnimmt. Dasselbe gilt, wenn ein Auftragsbearbeiter eine Datenschutzverletzung an das SRK Kanton Zug meldet.

Der/die Datenschutzberater/in wird den Vorfall mit Unterstützung der relevanten Abteilungen auf Verletzung des Datenschutzes hin prüfen und Massnahmen empfehlen, um die Auswirkungen der Datenschutzverletzung für die betroffene Person und das SRK soweit möglich zu minimieren. Diese Massnahmen werden durch alle relevanten Abteilungen (betroffene Abteilung, Rechtsdienst, Kommunikation, IT, etc.) umgesetzt. Soweit erforderlich wird die Verletzung den zuständigen Aufsichtsbehörden (primär EDÖB) und den betroffenen Personen gemeldet.

10.2 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
- soweit möglich Zeitpunkt und Dauer
- soweit möglich Kategorien und ungefähre Anzahl der betroffenen Personendaten
- soweit möglich Kategorien und ungefähre Anzahl der betroffenen Personen
- die Folgen, einschliesslich Risiken für die betroffenen Personen
- die getroffenen oder geplanten Massnahmen zur Behebung der Situation oder zur Milderung ihrer Folgen

Die Meldung erfolgt durch den/die Datenschutzverantwortliche in Absprache mit der Geschäftsführung.

10.3 Meldung an die betroffene(n) Person(en)

Die betroffene Person muss über die Verletzung ihrer Personendaten informiert werden, wenn es zu ihrem Schutz erforderlich ist. Dies ist insbesondere der Fall, wenn die betroffene Person notwendige Schritte zu ihrem Schutz unternehmen kann (z.B. Änderung des Passworts). Dasselbe gilt, wenn der EDÖB dies verlangt.

Besonders 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 Datenschutzberater/in in Absprache mit dem/der Direktor/in.



11. Schlussbestimmungen

Diese Weisung wurde von der Geschäftsführung des SRK Kanton Zug am 13. Juli 2023 genehmigt. Sie tritt am 1. September 2023 in Kraft.

Diese Weisung wird regelmässig überprüft und bei Bedarf angepasst. Die Mitarbeitenden, Ehrenamtlichen und Freiwilligen werden in geeigneter Weise darüber informiert. Sämtliche Unterlagen wie Weisungen, Merkblätter, Vorlagen, Checklisten usw. stehen [auf der Informations-Plattform](#) zur Verfügung.

Gültig ab / Gültig bis:	Gültig ab 1. Mai 2025
Unterschrift:	Stefanie Holm, Geschäftsführung
Datum:	1. Mai 2025
Verteiler:	Alle Mitarbeitenden, Ehrenamtlichen und Freiwilligen des SRK Kanton Zug
Verantwortlich für Dokument:	Basis Version GS: Regina Zwahlen, Datenschutzberaterin, GS SRK Version SRK Kanton Zug: Stefanie Holm

Anhang: Begriffe

Definition	Beschreibung
Personendaten	<p>Alle Angaben, die sich auf eine <i>bestimmte oder bestimmbar</i>e natürliche Person (im Folgenden «betroffene Person») beziehen.</p> <p>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 (vgl. Kapitel 9.2).</p>
Besonders schützenswerte Personendaten	<p>Personendaten, welche aufgrund ihrer Eigenschaften einen erhöhten Schutzbedarf haben.</p> <p>Gemäss dem Gesetz sind die folgenden Personendaten als solche zu betrachten:</p> <ul style="list-style-type: none"> • 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
Betroffene Person	<p>Natürliche Person über die Personendaten bearbeitet werden. Juristische Personen, d.h. Unternehmen usw. sind im Gegensatz zu natürlichen Personen (private Personen, Individuen) nicht vom DSG betroffen.</p>
Bearbeiten	<p>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.</p>



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.
Auftragsbearbeiter	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. Abteilungs-, Fachbereichs- 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.