SKJV
CSCSP

Schweizerisches Kompetenzzentrum für den Justizvollzug
Centre suisse de compétences en matière d'exécution des sanctions pénales
Centro svizzero di competenze in materia d'esecuzione di sanzioni penali

# Internes Reglement für den Datenschutz und die Datensicherheit

**Version 1.0 / Januar 2026**

Route de l'Ancienne-Papeterie 210 | 1723 Marly, Suisse
+41 26 425 44 00 | info@skjv.ch

www.skjv.ch

# Inhaltsverzeichnis

**1 Präambel ..... 4**

**2 Allgemeine Bestimmungen ..... 4**

Art. 1 - Ziel und Rechtsgrundlagen ..... 4

Art. 2 – Sachlicher und persönlicher Geltungsbereich ..... 4

Art. 3 – Begriffe ..... 4

Art. 4 – Kategorien von durch das SKJV bearbeiteten Personendaten ..... 5

**3 Grundsätze für die Datenbearbeitung ..... 6**

Art. 5 – Allgemeine Datenschutzgrundsätze ..... 6

Art. 6 – Verhältnismässigkeit, Treu und Glauben und Transparenz ..... 7

**4 Organisation, interne Verantwortlichkeiten und verantwortungsvolle Verwaltung der Daten im Alltag und Grundsätze ..... 7**

4.1 Organisation und interne Verantwortlichkeiten ..... 7

Art. 7 – Allgemeine Verantwortlichkeit der Direktion ..... 7

Art. 8 – Datenschutzberaterin oder -berater ..... 7

Art. 9 – Individuelle Verantwortung der Mitarbeiterinnen und Mitarbeiter ..... 7

Art. 9a – Vorsichtsgrundsatz ..... 8

Art. 10 – Verantwortung der Kursleitenden, Referentinnen und Referenten und Leistungserbringenden ..... 8

Art. 11 – Auftragsbearbeiter und externe Leistungserbringende ..... 8

4.2 Verantwortungsvolle Verwaltung der Daten im Alltag ..... 9

Art. 12 – Verantwortungsvolle Verwaltung der Daten im Alltag ..... 9

Art. 13 – Zugriff und Bearbeitung der Daten auf SharePoint ..... 9

Art. 14 – Informationspflicht bei der Erhebung von Personendaten ..... 11

**5 Rechte der betroffenen Personen ..... 11**

Art. 15 – Die verschiedenen Rechte der betroffenen Personen ..... 11

Art. 16 – Einschränkung der Rechte der betroffenen Personen ..... 11

**6 Sicherheit und Verwaltung der Daten ..... 12**

Art. 17 – Allgemeine Sicherheitsgrundsätze ..... 12

Art. 18 – Technische und organisatorische Sicherheitsmassnahmen ..... 12

Art. 19 – Schulung und Sensibilisierung ..... 12

Art. 20 – Datenschutz-Folgenabschätzung ..... 12

Art. 21 – Umgang mit Vorfällen und Sicherheitsverletzungen ..... 12

Art. 22 – Nutzung der digitalen Instrumente und der künstlichen Intelligenz ..... 13

Art. 23 – Auslagerung der Datenbearbeitung ..... 13

**7 Bekanntgabe, Transparenz und Übertragung von Daten ..... 13**

Art. 24 – Interne Empfängerinnen und Empfänger ..... 13

Art. 25 – Externe Empfängerinnen und Empfänger ..... 13

Art. 26 – Bekanntgabe ins Ausland ..... 13

Art. 27 – Bekanntgabe an die Medien ..... 13

**8 Kontrolle, Überwachung und Schlussbestimmungen ..... 14**
Art. 28 – Aufsichtsbehörde ..... 14
Art. 29 – Interne Kontrolle und Audit ..... 14
Art. 30 – Unterbreitung und Genehmigung des Reglements ..... 14
Art. 31 – Verstösse und interne Sanktionen ..... 14
Art. 32 – Schadenersatz und Genugtuung ..... 14
Art. 33 – Überprüfung und Aktualisierung ..... 14
Art. 34 – Inkrafttreten ..... 15

# 1 Präambel

Der Stiftungsrat genehmigt und verabschiedet dieses Reglement, um die Konformität der Bearbeitung von Daten mit den gesetzlichen und reglementarischen Vorschriften, insbesondere dem Bundesgesetz über den Datenschutz (DSG), seinen Ausführungsverordnungen sowie gegebenenfalls und wenn sinnvoll der EU-Datenschutz-Grundverordnung (DSGVO) oder eventuell dem kantonalen Recht sicherzustellen.

# 2 Allgemeine Bestimmungen

## Art. 1 - Ziel und Rechtsgrundlagen

1 Dieses Reglement legt die grundlegenden Prinzipien und Verfahren sowie die Art und Weise fest, wie die Mitarbeiterinnen und Mitarbeiter des SKJV Personendaten bei der Erfüllung ihrer Aufgaben zu bearbeiten haben.

2 Das Ziel besteht darin, die Persönlichkeit und die Grundrechte aller Personen, deren Daten durch das SKJV bearbeitet werden, zu schützen. Dies betrifft insbesondere die Teilnehmenden an Aus- und Weiterbildungen, die Teilnehmenden an der Bildung im Strafvollzug (BiSt), die Partnerorganisationen, die Teilnehmenden an Forschungsprojekten, die Auftraggebenden sowie die Mitarbeitenden.

3 Die Bearbeitung von Personendaten durch das SKJV beruht auf Artikel 13 der Bundesverfassung (BV), dem Bundesgesetz über den Datenschutz (DSG) und seinen Ausführungsverordnungen, den Statuten der Stiftung, der Leistungsvereinbarung sowie den kantonalen Bestimmungen. Dieses Reglement wird durch ein ausführlicheres allgemeines Dokument mit dem Titel «Grundlagendokument zum Datenschutz»[1] ergänzt, das zusätzliche Erläuterungen und Präzisierungen enthält.

## Art. 2 – Sachlicher und persönlicher Geltungsbereich

1 Dieses Reglement gilt für jegliche Bearbeitung von Personendaten durch das SKJV im Rahmen seiner Aufgaben, unabhängig vom verwendeten Datenträger (Papier, elektronisch, audiovisuell oder andere), vom angewandten Verfahren oder von den bearbeiteten Daten.

2 Es gilt für das gesamte Personal des SKJV, einschliesslich Kursleitende, Referentinnen und Referenten, temporäre Angestellte, Lernende, Praktikantinnen und Praktikanten sowie Leihpersonal und für die externen Partnerinnen und Partner, einschliesslich Leistungserbringende sowie andere Vertragspartnerinnen und -partner.

3 Externe Mitarbeitende des SKJV, die ihre Aufgaben im Auftrag des SKJV bei den Justizvollzugsanstalten und Institutionen in den Kantonen wahrnehmen, unterliegen diesem Reglement und gleichzeitig dem kantonalen Recht des betreffenden Kantons, wenn dieser für die Datenbearbeitung verantwortlich ist.

## Art. 3 – Begriffe

Im Sinne dieses Reglements bedeuten:

a. **Personendaten**: alle Angaben, die sich auf eine bestimmte oder direkt oder indirekt bestimmbare natürliche Person beziehen;

b. **betroffene Person**: natürliche Person, über die Personendaten durch das SKJV bearbeitet werden;

c. **besonders schützenswerte Personendaten**: diese bilden eine besondere Kategorie von Personendaten, die aufgrund des erhöhten Risikos einer Verletzung der Persönlichkeitsrechte einen verstärkten Schutz geniessen:

[1] Siehe Anhang 1: Grundlagendokument

Dies betrifft die in Artikel 5 Buchstabe c DSG aufgeführten besonders schützenswerten Personendaten im engeren Sinn:

- 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;

sowie Daten, die in den Tätigkeitslisten des SKJV als solche betrachtet werden und die in der Praxis aufgrund ihrer besonders schützenswerten Natur als besonders schützenswerte Personendaten behandelt werden;

d. **Bearbeiten**: jeder Vorgang oder jede Vorgangsreihe im Zusammenhang mit Personendaten – unabhängig von den angewandten Mitteln oder Datenträgern (elektronisch, manuell oder kombiniert) - insbesondere das Beschaffen, Speichern, Aufbewahren, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten;

e. **Bekanntgeben**: das Übermitteln oder Zugänglichmachen von Personendaten, unabhängig vom Mittel, von der Dauer und vom Zweck;

f. **Auslagerung**: eine qualifizierte Form der Bearbeitung durch Auftragsbearbeiter, bei der IT-Ressourcen genutzt werden, auf die über ein Kommunikationsnetz aus der Ferne zugegriffen wird, um Daten zu speichern, zu bearbeiten und auszutauschen (Cloud Computing);

g. **Verantwortlicher**: die Stiftung SKJV, vertreten durch ihre Direktion, die über den Zweck und die Mittel der Bearbeitung von Personendaten entscheidet und die Konformität mit dem DSG sicherstellt;

h. **Einwilligung**: jede freiwillig, für den bestimmten Fall, in informierter Weise abgegebene Willensbekundung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Bearbeitung der sie betreffenden Personendaten einverstanden ist;

i. **Auftragsbearbeiter**: natürliche oder juristische Person, die im Auftrag des SKJV-Daten bearbeitet;

j. **Verletzung der Sicherheit der Personendaten**: jeder Vorfall, der dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden;

k. **Anonymisierung**: durch die Anonymisierung von Daten kann die Bestimmung der betroffenen natürlichen Person verhindert werden;

l. **Pseudonymisierung**: Bearbeitung der Personendaten in einer Weise, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können;

m. **Liste der Bearbeitungstätigkeiten**: bezeichnet sämtliche Vorgänge des SKJV, welche die Bearbeitung von Personendaten beinhalten, erstellt nach Bereich oder Abteilung[2].

## Art. 4 – Kategorien von durch das SKJV bearbeiteten Personendaten

1 Das SKJV bearbeitet gemäss seinen Tätigkeiten die folgenden Arten von Personendaten:

a. **Grundausbildung, Führungsausbildung und Weiterbildung**: Daten zu den Kursteilnehmenden, den Kursleitenden, den Prüfungen sowie zu den Kursunterlagen;

b. **Forschung und Entwicklung**: anonymisierte oder pseudonymisierte Projektdaten, Koordinaten der Projektpartnerinnen und -partner;

c. **Human Resources**: grundlegende Personendaten, Daten zu den Arbeitsverhältnissen;

d. **Kommunikation und Administration**: Korrespondenz, Adresslisten, Sitzungsprotokolle, Informationsbriefe (Newsletter);

[2] Siehe Anhang 2: Tätigkeitslisten des SKJV

e. **IT- und Nutzungsdaten**: Informationen zu den Zugriffsprotokollen und technischen Logdateien (Logfiles);

f. **Bildung im Strafvollzug**: Daten zu den inhaftierten Personen, zu den Prüfungen und Kursunterlagen sowie zu den Unterrichtenden.

2 Besonders schützenswerte Personendaten (zum Beispiel: Gesundheitsdaten, Strafregisterauszug) können nur bearbeitet werden, wenn das Gesetz dies ausdrücklich erlaubt oder wenn die betroffene Person ihre Einwilligung dazu gegeben hat.

# 3 Grundsätze für die Datenbearbeitung

## Art. 5 – Allgemeine Datenschutzgrundsätze

Bei der Ausführung ihrer Aufgaben haben die Personen, welche Daten bearbeiten, stets die folgenden Grundsätze zu beachten:

1 **Rechtsgrundlage**: Bei der Ausführung eines Prozesses, der die Bearbeitung von Personendaten beinhaltet, muss die mit dem Vorgang beauftragte Person sicherstellen, dass diese Bearbeitung auf einer Rechtsgrundlage beruht, direkt mit den Aufgaben des SKJV verbunden ist oder sich auf die ausdrückliche Einwilligung der betroffenen Person stützt;

2 **Zweckbindung**: Die Datenerhebung erfolgt ausschliesslich für festgelegte, eindeutige und legitime Zwecke, die mit den Tätigkeiten des SKJV verbunden sind;

3 **Grundsatz der Minimierung**: nur die für den Zweck der Bearbeitung zwingend notwendigen Daten werden erhoben und aufbewahrt;

4 **Richtigkeit und Aktualisierung**: Bei einem Vorgang der Bearbeitung von Personendaten stellt die mit dem Vorgang beauftragte Person sicher, dass diese Daten im Hinblick auf den Zweck ihrer Bearbeitung richtig, vollständig und aktuell sind. Jede festgestellte Unrichtigkeit muss unverzüglich korrigiert werden;

5 **Aufbewahrungsdauer und Löschung**:

a. die Daten werden nur für die Dauer aufbewahrt, die für die Erfüllung des Zwecks der Bearbeitung erforderlich ist;

b. nach Ablauf dieses Zeitraums werden sie vernichtet, anonymisiert oder auf gesicherte Weise gelöscht, oder je nach rechtlichen Bestimmungen archiviert, es sei denn, die betroffene Person erteile eine gegenteilige Einwilligung;

c. die für die verschiedenen Datenkategorien geltenden Fristen werden in der Liste der Bearbeitungstätigkeiten des SKJV[3] festgelegt und in einem spezifischen Anhang mit dem Titel Tabelle der Aufbewahrungsfristen der Daten[4] zusammengefasst;

d. Die Löschung oder die Vernichtung der Daten muss unter der Kontrolle der Datenschutzberaterin oder des Datenschutzberaters erfolgen und muss dokumentiert werden.

6 **Datensicherheit**
Alle mit Datenbearbeitungsvorgängen beauftragten Personen müssen:

a. die IT-Sicherheitsrichtlinien strikt einhalten;

b. jede verdächtige Tätigkeit oder jeden Sicherheitsvorfall unverzüglich it-support@skjv.ch melden;

c. die Daten ausschliesslich auf den durch das SKJV bereitgestellten Systemen speichern;

d. bei der Übertragung vertraulicher Dokumente gesicherte Kommunikationsmittel verwenden;

e. Personendaten mit der gebotenen Sorgfalt bearbeiten.

[3] Siehe Anhang 2: Liste der Bearbeitungstätigkeiten
[4] Siehe Anhang 3: Tabelle der Aufbewahrungsfristen

### Art. 6 – Verhältnismässigkeit, Treu und Glauben und Transparenz

1 Jede Erhebung und Bearbeitung von Daten muss, auf das für die Erfüllung des verfolgten Zwecks notwendige Mass beschränkt sein.

2 Bei der Erhebung informieren die mit dem Vorgang beauftragten Personen die betroffenen Personen klar und vollständig mit dem entsprechenden Formular[5] über die Art der erhobenen Daten und deren Verwendung.

3 Keine Personendaten dürfen zu Zwecken genutzt werden, die mit dem ursprünglichen Zweck der Bearbeitung unvereinbar sind, es sei denn, die betroffene Person gibt ihre Einwilligung oder es besteht eine ausdrückliche Rechtsgrundlage.

# 4 Organisation, interne Verantwortlichkeiten und verantwortungsvolle Verwaltung der Daten im Alltag und Grundsätze

## 4.1 Organisation und interne Verantwortlichkeiten

### Art. 7 – Allgemeine Verantwortlichkeit der Direktion

1 Die Direktion des SKJV trägt die allgemeine Verantwortung und erlässt die Leitlinien für die konkrete Anwendung in Form einer Richtlinie[6], von der jede mit der Bearbeitung von Daten beauftragte Person Kenntnis nehmen und sie unterzeichnen muss. Mit der Unterzeichnung dieser Richtlinie bekräftigt die betreffende Person ihr Verständnis und ihre Verpflichtung, die darin aufgeführten Bestimmungen einzuhalten.

2 Sie sorgt dafür, dass die Personen angemessen über ihre Pflichten im Bereich der Bearbeitung und der Sicherheit der Daten informiert werden und diese in alle internen Prozesse integrieren.

3 Die Teamverantwortlichen und die Personen, welche die Interventionen externer Partner überwachen, achten ebenfalls darauf, dass die mit der Bearbeitung von Daten beauftragten Personen nur über die notwendigen Zugriffsrechte verfügen.

### Art. 8 – Datenschutzberaterin oder -berater

1 Die Datenschutzberaterin oder der Datenschutzberater (im Folgenden: DSB) und die IT-Abteilung (ICT) unterstützen und überwachen die Umsetzung und Aktualisierung des Reglements.

2 Die Datenschutzberaterin oder der Datenschutzberater übt ihre bzw. seine Funktion unabhängig aus und berichtet direkt an die Direktion.

### Art. 9 – Individuelle Verantwortung der Mitarbeiterinnen und Mitarbeiter

1 **Allgemeine Verpflichtung**
Jede mit der Bearbeitung von Daten beauftragte Person hat bei der Ausübung ihrer Funktionen die Grundsätze des Datenschutzes einzuhalten, die Vertraulichkeit der bearbeiteten Informationen sicherzustellen und dafür zu sorgen, dass jede Bearbeitung in Übereinstimmung mit den internen Richtlinien des SKJV erfolgt.

2 **Sorgfaltspflicht**
Die mit der Bearbeitung von Daten beauftragten Personen müssen die Personendaten sorgfältig behandeln

[5] Siehe Anhang 4: Formular zur Informationspflicht
[6] Siehe Anhang 5: Richtlinie zur Anwendung des Datenschutzreglements

und jedem Risiko eines unbefugten Zugriffs, eines Verlusts, einer Änderung oder einer Vernichtung vorbeugen. Sie melden unverzüglich jede Situation, die ein Risiko aufweist oder jeden Sicherheitsvorfall ihrer oder ihrem Vorgesetzten, der IT-Abteilung sowie der Datenschutzberaterin oder dem Datenschutzberater.

3 **Vertraulichkeit**
Den mit der Bearbeitung von Daten beauftragten Personen ist es streng verboten, Informationen oder Personendaten, auf die sie im Rahmen ihrer Funktionen Zugriff haben, ohne Genehmigung gegenüber Dritten offenzulegen.

4 **Konforme Verwendung der digitalen Instrumente**
Die IT-Tools und die Technologien der künstlichen Intelligenz müssen hauptsächlich zu beruflichen Zwecken verwendet werden. Unter strikter Einhaltung der internen Richtlinien zur IT-Sicherheit und zum Datenschutz können sie auch privat genutzt werden.

5 **Grundsatz des berechtigten Informationsbedarfs (Need-to-know-Prinzip)**
Die Personendaten dürfen nur im für die Erfüllung der beruflichen Aufgaben strikt notwendigen Mass und ausschliesslich im Rahmen der Zwecke, für die sie erhoben wurden, konsultiert, genutzt oder geteilt werden.

6 **Individuelle Verantwortung**
Jede mit der Bearbeitung von Daten beauftragte Person bleibt verantwortlich für ihre Nutzung der Personendaten. Sie hat für die Vollständigkeit, die Verfügbarkeit und die Nachverfolgbarkeit der bearbeiteten Informationen zu sorgen.

## Art. 9a – Vorsichtsgrundsatz

Wenn eine mit der Bearbeitung von Daten beauftragte Person Zweifel hinsichtlich der Legitimität eines Zugriffs, einer Freigabe oder eines Ersuchens um die Übermittlung von Daten hat, muss sie auf die Öffnung oder Freigabe von Daten verzichten und unverzüglich Rat bei der oder dem Vorgesetzten, bei der IT-Abteilung oder bei der Datenschutzberaterin oder dem Datenschutzberater einholen.

## Art. 10 – Verantwortung der Kursleitenden, Referentinnen und Referenten und Leistungserbringenden

1 Die Kursleitenden, Referentinnen und Referenten sowie Leistungserbringenden unterstehen den gleichen Vertraulichkeits- und Datenschutzverpflichtungen wie das interne Personal und verpflichten sich schriftlich, diese einzuhalten.

2 Jeder Verstoss gegen diese Verpflichtungen kann zum Entzug des Auftrags oder zu andere Massnahmen führen.

## Art. 11 – Auftragsbearbeiter und externe Leistungserbringende

1 Wenn die Bearbeitung von Daten einem externen Leistungserbringenden anvertraut wird, handelt dieser oder diese ausschliesslich auf schriftlichen Auftrag des SKJV. Er oder sie kann ohne vorgängige Genehmigung durch das SKJV keine Weitervergabe vornehmen.

2 Der Vertrag über die Auftragsbearbeitung legt den Zweck, die Art und die Dauer der Bearbeitung fest, präzisiert die Vertraulichkeits- und Sicherheitsverpflichtungen, die jenen des SKJV entsprechen müssen, und gewährleistet, dass die Daten zu anderen Zwecken weder übermittelt noch genutzt werden.

3 Das SKJV bleibt der Verantwortliche, auch wenn die Bearbeitung durch Dritte erfolgt.

## 4.2 Verantwortungsvolle Verwaltung der Daten im Alltag

### Art. 12 – Verantwortungsvolle Verwaltung der Daten im Alltag

1 Jede mit der Bearbeitung von Daten beauftragte Person muss dieses Reglement bei der Ausführung ihrer beruflichen Tätigkeiten im Alltag aktiv anwenden:

2 **Elektronische Daten**

a. Ausschliesslich die durch das SKJV bereitgestellten oder ausdrücklich genehmigten Instrumente, Programme, Applikationen und Plattformen dürfen für die Erfüllung der beruflichen Aufgaben verwendet werden;

b. vertrauliche Daten dürfen ausschliesslich auf SharePoint oder anderen durch das SKJV genehmigten Systemen gespeichert werden;

c. die Verwendung privater Cloud-Dienste oder persönlicher USB-Sticks für berufliche Aufgaben ist nicht erlaubt;

d. Passwörter müssen sicher und vertraulich sein und regelmässig geändert werden, gemäss den Bestimmungen der ICT-Richtlinie zur Nutzung der IT-Instrumente;

e. E-Mails, die vertrauliche Daten enthalten, müssen gesichert übermittelt werden;

f. Jede Übertragung von Personendaten muss durch die Datenschutzberaterin oder den Datenschutzberater genehmigt werden.

3 **Daten auf materiellen Trägern (Papier)**

a. Dokumente, die Personendaten enthalten, müssen an einem sicheren Ort, unter Verschluss oder in einem Raum mit eingeschränktem Zugang aufbewahrt werden.

b. Nicht benötigte Ausdrucke oder Kopien müssen gesichert vernichtet werden.

4 **Daten von Sitzungen und Gesprächen**

a. Vertrauliche Informationen dürfen auf keinen Fall in den öffentlichen Räumen diskutiert oder ausgetauscht oder unbefugten Personen mitgeteilt werden;

b. Es ist streng verboten, besonders schützenswerte Daten oder persönliche Informationen über ungesicherte E-Mail, Chat- oder Sharing-Dienste zu übertragen

5 **Arbeit ausserhalb des Büros**

a. Bei der Arbeit im Homeoffice oder bei beruflichen Reisen müssen die mit der Bearbeitung von Daten beauftragten Personen den Sichtschutz der Bildschirme sicherstellen, die Sicherheit der bearbeiteten Daten gewährleisten und den Zugriff auf die befugten Personen beschränken;

b. die im beruflichen Rahmen genutzten mobilen Geräte (Notebooks, Tablets, Telefone usw.) müssen durch einen PIN-Code, ein sicheres Passwort oder eine biometrische Authentifizierung geschützt sein.

### Art. 13 – Zugriff und Bearbeitung der Daten auf SharePoint

1 **Zentrales System zur elektronischen Verwaltung und Archivierung - Grundsatz**

a. **SharePoint des SKJV** ist das zentrale System für die Bearbeitung, Verwaltung und Archivierung von elektronischen Dokumenten. Es wird für die Speicherung, den Austausch und die Aufbewahrung der Informationen im Rahmen der institutionellen Tätigkeiten verwendet;

b. Der Zugriff auf rein informative Daten und Dokumente, die keine Personendaten enthalten und deren Bearbeitungszeck nicht mit bestimmten oder bestimmbaren Personen verbunden ist, steht dem gesamten Personal des SKJV offen.

2 **Zugriffsbeschränkungen**

a. Jeder Bereich, jede Fachabteilung oder jeder Dienst verfügt auf SharePoint über einen Ordner für Daten und Dokumente, die persönliche, vertrauliche oder besonders schützenswerte Daten enthalten, mit klar festgelegten und regelmässig aktualisierten Zugriffsrechten;

b. der Zugriff auf diese Daten und Dokumente wird strikt auf die aufgrund ihrer Kompetenzen, Verantwortlichkeiten und operativen Bedürfnisse dafür ordnungsgemäss befugten Personen beschränkt. Dieser Zugriff wird von bestimmten Rechten begleitet, die regelmässig durch den Verantwortlichen oder die Verantwortliche des betroffenen Bereichs in Zusammenarbeit mit der IT-Abteilung überprüft und angepasst werden;

c. die Zugriffsrechte werden differenziert nach dem Need-to-Know-Prinzip erteilt und nur Personen, deren Funktionen dies erfordern, haben Zugriff auf die für die Erfüllung ihrer Aufgaben notwendigen Daten;

d. alle Bereiche, die Personendaten oder vertrauliche Informationen enthalten, sind strikt auf eine eingeschränkte Gruppe von befugten Personen beschränkt;

e. externe Personen wie Projektpartner oder Kursleitende können nur auf die spezifisch erlaubten und durch das SKJV für diesen Zweck bestimmten Bereiche zugreifen.

3 **Verwaltung und Kontrolle der Zugriffsrechte - Rollen und Verantwortlichkeiten**

a. Die Zugriffsrechte auf die verschiedenen anderen Systeme, Dokumente und digitalen Bereiche des SKJV werden aufgrund der Aufgaben, Verantwortlichkeiten und Funktionen der einzelnen Mitarbeiterinnen und Mitarbeiter erteilt;

b. der oder die Teamverantwortliche oder Bereichsleiter/in erteilt die Zugriffsrechte und sorgt für deren regelmässige Überprüfung, insbesondere bei Änderungen von Funktion oder Aufgaben sowie beim Austritt einer mit der Bearbeitung von Daten beauftragten Person;

c. die IT-Abteilung setzt die technischen Massnahmen und die Zugriffsrechte um, führt die Zugriffsprotokolle und sorgt für die Sicherheit der betroffenen Systeme. In Absprache mit der Direktion passt sie die Zugriffsrechte gemäss den operativen Bedürfnissen an;

d. die mit der Bearbeitung der Daten beauftragten Personen sind nicht berechtigt, selbst die Freigaben, Berechtigungen oder Freigabelinks zu ändern, und dürfen diese auch nicht an Dritte weitergeben, es sei denn, die Direktion oder die IT-Abteilung habe dies ausdrücklich genehmigt.

4 **Bearbeitung, Versionsverwaltung und Nachverfolgbarkeit der Dokumente**

a. Die Dokumente dürfen nur in den durch das SKJV spezifisch für diesen Zweck vorgesehenen Ordnern bearbeitet, gespeichert oder archiviert werden;

b. jede Änderung muss nachverfolgbar sein und den Erhalt des Versionsverlaufs ermöglichen, um die Integrität und Transparenz der Bearbeitung zu gewährleisten;

c. die Originaldokumente dürfen nur mit ausdrücklicher Genehmigung einer zuständigen Person gelöscht, geändert oder ersetzt werden.

5 **Vertraulicher Bereich – Bearbeitung von besonders schützenswerten Daten**

Die besonders schützenswerten Daten, namentlich die Personaldossiers, Bewerbungen oder Forschungsdaten, die persönliche Informationen enthalten, sind Gegenstand der folgenden verstärkten Einschränkungen:

a. Der Zugriff auf diese Daten ist strikt den durch die Direktion oder die für die Bearbeitung der Daten verantwortliche Person namentlich autorisierten Personen vorbehalten;

b. diese Daten dürfen ausschliesslich in den gesicherten und eingeschränkten Bereichen von SharePoint gespeichert werden, in Übereinstimmung mit den Richtlinien der IT-Abteilung;

c. ohne ausdrückliche Genehmigung durch den oder die für den jeweiligen Fall zuständigen Datenverantwortlichen oder Datenverantwortliche ist keine lokale Speicherung oder Übertragung dieser Daten ausserhalb von SharePoint erlaubt.

6 **Datenübertragung**

a. Personendaten dürfen nur übertragen oder zugänglich gemacht werden, wenn dies eine Gesetzesbestimmung vorsieht, die betroffene Person ihre Einwilligung dazu gegeben hat oder dies für die Erfüllung der Aufgaben des SKJV notwendig ist;

b. Gesuche um Datenübertragung müssen an die Datenschutzberaterin oder den Datenschutzberater gerichtet werden;

c. alle Freigabeberechtigungen auf SharePoint erfolgen gesichert, werden dokumentiert und regelmässig überprüft.

## Art. 14 – Informationspflicht bei der Erhebung von Personendaten

1 Die mit der Bearbeitung von Daten beauftragten Personen haben die betroffenen Personen klar und angemessen über die Erhebung der Personendaten zu informieren, egal ob diese direkt bei ihnen erfolgt oder nicht.

2 Bei der Erhebung kommunizieren sie der betroffenen Person zumindest die Identität und die Kontaktdaten der für die Bearbeitung verantwortlichen Person, den Zweck der Bearbeitung und gegebenenfalls die Empfänger oder die Kategorien von Empfängern, an welche die Personendaten weitergegeben werden.

# 5 Rechte der betroffenen Personen

## Art. 15 – Die verschiedenen Rechte der betroffenen Personen

1 **Auskunftsrecht**: Jede betroffene Person hat das Recht, Auskunft zu verlangen und zu erfahren, ob Daten über sie durch das SKJV bearbeitet werden, sowie diesbezügliche Informationen zu erhalten.

2 **Recht auf Berichtigung, Löschung oder Einschränkung**: sie kann die Berichtigung von unrichtigen oder unvollständigen Daten, die sie betreffen, deren Löschung oder die Einschränkung der Bearbeitung in den gesetzlich vorgesehenen Fällen verlangen.

3 **Recht auf Widerspruch und Einschränkung der Bekanntgabe**: sie kann sich auch jederzeit der Bearbeitung ihrer Personendaten widersetzen.

4 **Recht auf Einsicht vor Ort**: die betroffene Person kann mit Zustimmung des SKJV ihr Zugriffsrecht ausüben, indem sie vor Ort in den Räumlichkeiten des SKJV die sie betreffenden Daten in nicht elektronischer Form konsultiert.

5 **Modalitäten für die Ausübung der Rechte**: jede betroffene Person, die eines oder mehrere der obengenannten Rechte ausüben möchte, muss mit dem dafür vorgesehenen Formular[7] ein entsprechendes Gesuch an datenschutz@skjv.ch richten. Das SKJV prüft das Gesuch und entscheidet innert einer Frist von 30 Tagen.

## Art. 16 – Einschränkung der Rechte der betroffenen Personen

1 Das SKJV kann die Rechte der betroffenen Personen gemäss Artikel 15 Absatz 1 bis 4 dieses Reglements vorübergehend einschränken, wenn dies nötig ist für:

a. die Durchführung eines gesetzlichen Auftrags oder eines Verwaltungs- oder Strafverfahrens;

b. die Wahrung wesentlicher öffentlicher Interessen oder den Schutz der Rechte und Freiheiten von Dritten.

2 Diese Einschränkungen müssen verhältnismässig, begründet und dokumentiert sein. Die betroffenen Personen werden über die Einschränkung und deren Begründung informiert, es sei denn, diese Information gefährde den verfolgten Zweck.

[7] Siehe Anhang 6: Gesuchsformular zur Ausübung der Rechte

# 6 Sicherheit und Verwaltung der Daten

## Art. 17 – Allgemeine Sicherheitsgrundsätze

1 Das SKJV ergreift alle geeigneten technischen und organisatorischen Massnahmen, um die Daten zu sichern und jeglichen unberechtigten Zugriff, Verlust jegliche Veränderung oder unerwünschte Bekanntgabe der Daten zu vermeiden.

2 Diese Massnahmen berücksichtigen die Natur der Daten, den Bearbeitungszweck, die identifizierten Risiken, den Stand der Technik sowie die verfügbaren finanziellen Ressourcen.

## Art. 18 – Technische und organisatorische Sicherheitsmassnahmen

1 Die IT-Abteilung verwaltet die Logins und die Zugriffsrechte gemäss dem Need-to-Know-Prinzip und schützt das System vor jeglichen schadensverursachenden Vorfällen.

2 In organisatorischer Hinsicht sieht die Direktion klare interne Verfahren im Bereich der Datenverwaltung vor; sie organisiert die regelmässige Schulung und Sensibilisierung des Personals und dokumentiert die Vorfälle und die durchgeführten Korrekturmassnahmen.

## Art. 19 – Schulung und Sensibilisierung

1 Die Schulungen im Bereich Datenschutz und Datensicherheit sind für das gesamte Personal des SKJV und seine Leistungserbringenden obligatorisch.

Die Datenschutzberaterin bzw. der Datenschutzberater organisiert regelmässig Sensibilisierungsmassnahmen (Sitzungen, interne Kommunikation, Online-Hilfen, Best-Practice-Leitfaden) und sorgt für die regelmässige Aktualisierung des Inhalts der Schulungen und die Führung eines Teilnehmerverzeichnisses.

## Art. 19a – Integration und Schulung neu für die Bearbeitung von Daten verantwortlicher Personen

**Empfang, Information und obligatorische Grundschulung**
Bei ihrem Stellenantritt erhalten die neu mit der Bearbeitung von Daten beauftragten Personen schriftlich eine vollständige Information zu den geltenden Regeln im Bereich Datenschutz und Informationssicherheit. Sie haben auch eine obligatorische Grundschulung zu absolvieren.

## Art. 20 – Datenschutz-Folgenabschätzung

Wenn das SKJV eine Datenbearbeitung vorsieht, die ein hohes Risiko für die Rechte und Freiheiten der Personen mit sich bringt, wird vor der Umsetzung eine Folgenabschätzung (FA) durchgeführt. Die FA wird unter der Verantwortung der Datenschutzberaterin oder des Datenschutzberaters durchgeführt, die oder der die entsprechende Dokumentation aufbewahrt und der Direktion Bericht erstattet.

## Art. 21 – Umgang mit Vorfällen und Sicherheitsverletzungen

1 Die IT-Abteilung und die Datenschutzberaterin bzw. der Datenschutzberater untersuchen jede Sicherheitsverletzung von Personendaten und schlagen die erforderlichen Massnahmen zur Behebung vor.

2 Das SKJV informiert den EDÖB innert kürzester Frist und gegebenenfalls auch die betroffenen Personen, falls die Verletzung ein hohes Risiko für deren Rechte mit sich bringt.

### Art. 22 – Nutzung der digitalen Instrumente und der künstlichen Intelligenz

Die Nutzung der IT-Instrumente und der künstlichen Intelligenz im SKJV ist Gegenstand spezifischer Richtlinien, auf die hier ausdrücklich verwiesen wird[8].

### Art. 23 – Auslagerung der Datenbearbeitung

Das SKJV kann gewisse Bearbeitungsaktivitäten externen Dienstleistungserbringern anvertrauen (Hosting, Ausbildung, statistische Analyse usw.), wenn dies durch seine Organisation oder seinen Auftrag gerechtfertigt ist. Ein schriftlicher Vertrag präzisiert die Pflichten des Dienstleistungserbringers in Übereinstimmung mit Artikel 11 dieses Reglements.

## 7 Bekanntgabe, Transparenz und Übertragung von Daten

### Art. 24 – Interne Empfängerinnen und Empfänger

Personendaten dürfen nur den ordentlich befugten Personen gemäss dem Need-to-Know-Prinzip bekanntgegeben werden.

### Art. 25 – Externe Empfängerinnen und Empfänger

1 Das SKJV gibt Personendaten externen Empfängerinnern und Empfängern nur bekannt, wenn dies vom Gesetz vorgesehen ist, für die Erfüllung eines durch das SKJV erteilten Vertrags oder Auftrags nötig ist oder wenn die betroffene Person ihre ausdrückliche Einwilligung dazu gegeben hat.

2 Die Daten können namentlich den Bundesbehörden (SBFI, BJ, BFS, BAG usw.) oder Kantonsbehörden (zum Beispiel den Justizvollzugseinrichtungen), den Partnerinstitutionen in den Bereichen Bildung, Forschung oder Vollzugspolitik von strafrechtlichen Massnahmen und Sanktionen oder Bewährung sowie technischen und anderen Leistungserbringenden bekannt gegeben werden. Die Empfänger müssen ausreichende Sicherheitsgarantien liefern.

### Art. 26 – Bekanntgabe ins Ausland

Grundsätzlich gibt das SKJV keine Personendaten ins Ausland bekannt. Gegebenenfalls gelten die Bestimmungen des DSG.

### Art. 27 – Bekanntgabe an die Medien

Die mit der Bearbeitung von Daten beauftragte Person, die Daten an Behörden, Medien oder Dritte bekannt gibt, muss das Amtsgeheimnis, die Vertraulichkeit und den Schutz der Interessen des SKJV strikt einhalten. Solche Bekanntgaben müssen durch die Direktion, die Kommunikationsverantwortliche bzw. den Kommunikationsverantwortlichen oder die Datenschutzberaterin bzw. den Datenschutzberater abgesegnet und dokumentiert werden, so dass die Nachverfolgbarkeit und die Konformität mit dem DSG gewährleistet ist.

[8] Siehe: Richtlinien zur Nutzung der KI-Technologien

# 8 Kontrolle, Überwachung und Schlussbestimmungen

## Art. 28 – Aufsichtsbehörde

1 Das SKJV ist dem Bundesgesetz über den Datenschutz und der Aufsicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) unterstellt.

2 Das SKJV arbeitet uneingeschränkt mit dem EDÖB zusammen und liefert ihm alle für die Ausübung seiner Zuständigkeiten nötigen Informationen.

## Art. 29 – Interne Kontrolle und Audit

Im Auftrag der Direktion führt die Datenschutzberaterin oder der Datenschutzberater regelmässige Überprüfungen der Konformität der Bearbeitung durch, formuliert Empfehlungen oder Korrekturmassnahmen und hält alles im internen Verzeichnis der Verarbeitungstätigkeiten fest.

## Art. 30 – Unterbreitung und Genehmigung des Reglements

1 Das SKJV unterbreitet dieses Reglement dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten zur Information.

2 Bei substanziellen Änderungen oder neuen Bearbeitungen, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, konsultiert das SKJV den EDÖB vor ihrer Annahme.

3 Das Reglement tritt nach der Bestätigung durch den Stiftungsrat des SKJV, am 4. Dezember 2025, in Kraft.

## Art. 31 – Verstösse und interne Sanktionen

1 Bei Nicht-Einhaltung dieses Reglements kann die Direktion in Übereinstimmung mit den geltenden internen Regeln Disziplinarmassnahmen gegen die betroffene Mitarbeiterin oder den betroffenen Mitarbeiter verhängen.

2 Bei gravierenden Verletzungen, die unter das Strafrecht fallen, behält sich das SKJV das Recht vor, die zuständigen Justizbehörden zu informieren.

3 Bei Verstössen gegen das Reglement durch Leistungserbringende und externe Partner kann das SKJV den Vertrag auflösen und auf Letztere zurückgreifen.

## Art. 32 – Schadenersatz und Genugtuung

1 Jede Person, die infolge einer unrechtmässigen Bearbeitung ihrer Daten einen Schaden oder eine Persönlichkeitsverletzung erlitten hat, hat Anspruch auf Schadenersatz.

2 Die Direktion prüft zusammen mit der Datenschutzberaterin bzw. dem Datenschutzberater jeden Antrag auf Schadenersatz sorgfältig.

3 Gegebenenfalls bleiben die durch die Bundesgesetzgebung vorgesehenen Rechtsmittel vorbehalten.

## Art. 33 – Überprüfung und Aktualisierung

1 Das Reglement wird periodisch einer Überprüfung unterzogen. Diese erfolgt mindestens alle drei Jahre oder bei bedeutenden gesetzlichen oder organisatorischen Änderungen.

2 Die Anpassungsvorschläge werden durch die Datenschutzberaterin oder den Datenschutzberater formuliert und der Direktion zur Genehmigung unterbreitet.

3 Jede aktualisierte Version wird allen Mitarbeiterinnen und Mitarbeitern bekannt gegeben.

## Art. 34 – Inkrafttreten

1 Dieses Reglement tritt am durch den Stiftungsrat des SKJV bestimmten Datum in Kraft und ist verbindlich für das gesamte Personal des SKJV.

2 Es hebt alle früheren gegenteiligen Bestimmungen im Bereich des Datenschutzes auf und ersetzt diese.

Der Referenztext wird in den offiziellen Archiven des SKJV aufbewahrt.

Freiburg, 01. Januar 2026

Präsident des Stiftungsrates des SKJV,

Andreas Michel