

# Datenschutzreglement der PK KVO (Pensionskasse von Krankenversicherungsorganisationen)

## Inhaltsverzeichnis

1. Ziele des Datenschutzreglements .....	2
2. Geltungsbereich .....	2
3. Räumlicher Geltungsbereich .....	2
4. Begriffe.....	2
5. Allgemeine Grundsätze der Datenbearbeitung (Art. 6 DSGVO).....	3
5.1 <i>Rechtmässigkeit</i> .....	3
5.2 <i>Treu und Glauben</i> .....	3
5.3 <i>Transparenz</i> .....	3
5.4 <i>Zweckbindung</i> .....	3
5.5 <i>Datenaktualisierung / Datenrichtigkeit</i> .....	4
6. Privacy by design (Datenschutz durch Technik) und Privacy by default (Datenschutz durch datenschutzfreundliche Voreinstellungen) – Art. 7 DSGVO .....	4
7. Datensicherheit – Art. 8 DSGVO .....	4
8. Datenschutz-Folgenabschätzung .....	4
9. Verzeichnis der Bearbeitungstätigkeiten – Art. 12 DSGVO .....	4
10. Informationspflicht der PK KVO bei der Beschaffung von Personendaten – Art. 19 DSGVO	5
11. Auskunftsrecht der betroffenen Person – Art. 25 DSGVO .....	5
12. Bekanntgabe von Personendaten ins Ausland .....	5
13. Datenschutzberater/in – Art. 10 DSGVO .....	5
14. Einsatz von Auftragsbearbeitern .....	5
15. Informationspflichten der PK KVO als Verantwortlicher Informationspflicht .....	5
16. Interne Verantwortlichkeiten und Kontrollen .....	6
17. Kontroll- und Verbesserungsprozess sowie Checklisten .....	6
18. Audits .....	6
19. Meldung bei Verletzung der Datensicherheit.....	7
20. Sensibilisierung / Schulung der Mitarbeitenden.....	7
21. Löschkonzept .....	7
22. Lücken im Datenschutzreglement der PK KVO.....	7

## **1. Ziele des Datenschutzreglements**

Das Datenschutzreglement soll als zentrales Datenschutzdokument die Umsetzung der gesetzlichen und vertraglichen Anforderungen des revidierten Datenschutzes im Rahmen der Geschäftsführung und Verwaltung der Pensionskasse von Krankenversicherungs-Organisationen (PK KVO) unterstützen. Es regelt die Handhabung und dem Umgang der PK KVO mit dem revidierten Datenschutzgesetz (im Folgenden «DSG»). Neben den Bestimmungen des DSG, sind zudem die datenschutzrechtlichen Bestimmungen des Art. 85 a ff. BVG zu beachten. Diese finden als *lex specialis* Anwendung. Das Datenschutzreglement soll den Verantwortlichen der PK KVO als Vorlage dienen bei der Einhaltung und Umsetzung der gesetzlichen Vorgaben im Datenschutz.

## **2. Geltungsbereich**

Dieses Datenschutzreglement gilt für alle Personen, die sich mit der Führung, Geschäftsführung und Verwaltung der PK KVO befassen und ist anwendbar auf Versicherte, pensionierte Personen, angeschlossene Arbeitgeber und externe Dienstleister sofern das Bundesgesetz über die berufliche Vorsorge (BVG) nicht vorgeht.

## **3. Räumlicher Geltungsbereich**

Dieses Reglement gilt für Sachverhalte, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden.

Für privatrechtliche Ansprüche gilt das Bundesgesetz vom 18. Dezember 1987 über das Internationale Privatrecht. Vorbehalten bleiben zudem die Bestimmungen zum räumlichen Geltungsbereich des Strafgesetzbuchs.

## **4. Begriffe**

Das Datenschutzreglement der PK KVO orientiert sich an den Begriffen des neuen Datenschutzgesetzes des Bundes:

### *4.1 Personendaten:*

Alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

### *4.2 betroffene Person:*

Natürliche Person, über die Personendaten bearbeitet werden.

### *4.3 besonders schützenswerte Personendaten:*

1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten;
2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie;
3. genetische Daten;
4. biometrische Daten, die eine natürliche Person eindeutig identifizieren;
5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen;
6. Daten über Massnahmen der sozialen Hilfe.

### *4.4 Bearbeiten:*

Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.

### *4.5 Bekanntgeben:*

Das Übermitteln oder Zugänglichmachen von Personendaten.

#### *4.6 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 natürlichen Person zu analysieren oder vorherzusagen.

#### *4.7 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.

#### *4.8 Verletzung der Datensicherheit:*

Eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

#### *4.9 Verantwortlicher:*

Private Person, die allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet.

#### *4.10 Auftragsbearbeiter:*

Private Person, die im Auftrag des Verantwortlichen Personendaten bearbeitet.

### **5. Allgemeine Grundsätze der Datenbearbeitung (Art. 6 DSGVO<sup>1</sup>)**

Die PK KVO bearbeitet Personendaten gemäss den nachfolgenden Grundsätzen. Diese werden regelmässig überprüft.

#### *5.1 Rechtmässigkeit*

Die PK KVO bearbeitet die Personendaten der Versicherten und Rentnerinnen und Rentner rechtmässig. Dabei werden die Vorgaben des DSGVO und auch die Datenschutzbestimmungen gemäss BVG beachtet. Die PK KVO bearbeitet diese Personendaten mit Einwilligung der Versicherten und Rentnerinnen und Rentner auf der Basis von Formularen oder entsprechenden schriftlichen Informationen.

#### *5.2 Treu und Glauben*

Die Bearbeitung erfolgt nach Treu und Glauben verhältnismässig.

#### *5.3 Transparenz*

Die Verarbeitung der Daten der Versicherten und Rentnerinnen und Rentner erfolgen jederzeit für die entsprechende Person in einer transparenten Weise. Die PK KVO informiert die entsprechende Person über die Verarbeitung ihrer Daten und gibt im gleichen Rahmen jederzeit Auskunft über die für sie verarbeiteten Daten.

#### *5.4 Zweckbindung*

Die Bearbeitung der Personendaten durch die PK KVO erfolgt ausschliesslich zum Zweck der rechtmässigen Führung des individuellen Kontos der versicherten Personen oder der Rentnerinnen und Rentner.

---

<sup>1</sup> Verweisungen auf das «DSG» beziehen sich auf seine jeweils geltende Fassung. Die Nummerierung folgt dem revidierten DSGVO (in Kraft ab dem 1. September 2023).

### *5.5 Datenaktualisierung / Datenrichtigkeit*

Die PK KVO vergewissert sich bei der Datenbearbeitung regelmässig über deren Richtigkeit einschliesslich deren Aktualität und trifft die notwendigen Vorkehrungen dazu. Sollte die PK KVO Kenntnis davon erhalten, dass Daten im Hinblick auf den Zweck und die Verwaltung der Bearbeitung nicht richtig sind, werden diese nach Rücksprache mit den Versicherten und Rentnerinnen / Rentnern korrigiert.

### **6. Privacy by design (Datenschutz durch Technik) und Privacy by default (Datenschutz durch datenschutzfreundliche Voreinstellungen) – Art. 7 DSGVO**

Die technische Verwaltung und damit die Datenverarbeitung der PK KVO erfolgt mit einer Software der Firma Swiss Pension in der IT-Umgebung von santésuisse. Diese gestaltet sich technisch und organisatorisch so, dass die Datenschutzvorschriften eingehalten werden. Dies ist schon bei der Planung zu berücksichtigen (Privacy by design).

### **7. Datensicherheit – Art. 8 DSGVO**

Zum Schutz der bearbeiteten Personendaten ergreift die PK KVO zusammen mit santésuisse und Swiss Pension unter Berücksichtigung der Implementierungskosten geeignete und dem Stand der Technik entsprechende technische und organisatorische Massnahmen, um eine dem Risiko angemessene Datensicherheit zu gewährleisten. Insbesondere sorgt die PK KVO zusammen mit santésuisse und Swiss Pension für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten und die Nachvollziehbarkeit der Bearbeitung und schützt die Systeme gegen das Risiko, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Diese technischen und organisatorischen Massnahmen überprüft die PK KVO zusammen mit santésuisse und Swiss Pension periodisch über die gesamte Bearbeitungsdauer hinweg.

Vorgaben betreffend Datensicherheit werden vom Bereich IT der santésuisse in Zusammenarbeit mit dem/ der Datenschutzberater /-in (DB) erstellt, periodisch überprüft und ggf. angepasst. Dies betrifft insbesondere technische Massnahmen wie ein IT-Service-Level-Agreement, ein IT-Sicherheitskonzept, eine Berechtigungsmatrix sowie organisatorische Massnahmen wie Sorgfaltspflicht-, Vertraulichkeits- und Geheimhaltungsvereinbarungen.

### **8. Datenschutz-Folgenabschätzung**

Wenn eine Bearbeitung der personenbezogenen Daten ein erhöhtes Risiko darstellt, muss eine Datenschutz-Folgenabschätzung erfolgen. Hierbei muss eine Beschreibung der geplanten Bearbeitung, sowie eine Bewertung der Risiken erfolgen. Weiter müssen Massnahmen zum Schutz der Persönlichkeit getroffen werden. Die Vorprüfung, ob eine Datenschutz-Folgenabschätzung notwendig ist, hat erstmals initial innerhalb von 6 Monaten nach Inkrafttreten dieses Datenschutzreglements zu erfolgen. Danach ist die Anwendung der Datenschutz-Folgenabschätzung in regelmässigen Abständen durchzuführen.

### **9. Verzeichnis der Bearbeitungstätigkeiten – Art. 12 DSGVO**

Die Verantwortlichen der PK KVO müssen ein Verzeichnis der Bearbeitungstätigkeiten führen.

Das Verzeichnis des Verantwortlichen enthält mindestens:

1. die Identität des Verantwortlichen
2. den Bearbeitungszweck
3. eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten
4. die Kategorien der Empfängerinnen und Empfänger
5. wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer

6. wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit
7. falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien nach Artikel 16 Absatz 2. des Datenschutzgesetzes
8. Das Verzeichnis des Auftragsbearbeiters enthält Angaben zur Identität des Auftragsbearbeiters und des Verantwortlichen, zu den Kategorien von Bearbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden, sowie die Angaben gemäss Punkt 6 und 7.
9. Die PK KVO stellt sicher, dass das Verzeichnis stets aktuell ist.

#### **10. Informationspflicht der PK KVO bei der Beschaffung von Personendaten – Art. 19 DSG**

Die PK KVO informiert die betroffene Person über die Beschaffung von Personendaten im Rahmen der gesetzlichen Anforderungen.

#### **11. Auskunftsrecht der betroffenen Person – Art. 25 DSG**

Die PK KVO erteilt gemäss den gesetzlichen Anforderungen jeder Person auf deren Verlangen hin, in der Regel innerhalb von 30 Tagen grundsätzlich kostenlos, Auskunft darüber, ob Personendaten über sie bearbeitet werden, und stellt ihr gegebenenfalls die weiteren Angaben über die Datenbearbeitung zur Verfügung.

#### **12. Bekanntgabe von Personendaten ins Ausland**

Personendaten dürfen ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet. Dies liegt in der Regel vor, wenn zwischen der Schweiz und dem ausländischen Staat ein Sozialversicherungsabkommen abgeschlossen wurde.

Personendaten dürfen auch bekanntgegeben werden, wenn die betroffene Person ausdrücklich ihre Einwilligung dazu gibt.

#### **13. Datenschutzberater/in – Art. 10 DSG**

Der Stiftungsrat der PK KVO hat als Datenschutzberaterin die Infosec AG mit Sitz in Sursee gewählt. Sie dient als Anlaufstelle für betroffene Personen und Behörden sowie für die Beratung und Mitwirkung für die Umsetzung und Schulung der relevanten datenschutzrechtlichen Vorgaben. Die Datenschutzberaterin ist unabhängig und hat mindestens die Rechte und Aufgaben gemäss den gesetzlichen Anforderungen.

Die Datenschutzberaterin übt ihre Funktion gegenüber dem Verantwortlichen fachlich unabhängig und weisungsungebunden aus.

#### **14. Einsatz von Auftragsbearbeitern**

Es wird vertraglich sichergestellt, dass der jeweilige Auftragsbearbeiter sich an die aktuell gültigen datenschutzrechtlichen Bestimmungen hält. Zudem muss die Datensicherheit gewährleistet werden.

#### **15. Informationspflichten der PK KVO als Verantwortlicher Informationspflicht**

1. Der Verantwortliche informiert die betroffene Person angemessen über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden.
2. Er teilt der betroffenen Person bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist; er teilt ihr mindestens mit:

- a. die Identität und die Kontaktdaten des Verantwortlichen;
  - b. den Bearbeitungszweck;
  - c. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden.
3. Werden die Daten nicht bei der betroffenen Person beschafft, so teilt er ihr zudem die Kategorien der bearbeiteten Personendaten mit.
  4. Werden die Personendaten ins Ausland bekanntgegeben, so teilt er der betroffenen Person auch den Staat oder das internationale Organ und gegebenenfalls die Garantien nach Artikel 16 Absatz 2 oder die Anwendung einer Ausnahme nach Artikel 17 des Datenschutzgesetzes mit.

Die Ausnahmen zur Informationspflicht sind in Art. 20 des Datenschutzgesetzes geregelt.

### **16. Interne Verantwortlichkeiten und Kontrollen**

Die Verantwortung für die Umsetzung sowie die Kontrolle der Einhaltung der datenschutzrechtlichen Vorgaben und Massnahmen liegt zuoberst beim Stiftungsrat der PK KVO und obliegt dem Geschäftsführer der PK KVO.

Die Verantwortung für die Einhaltung der datenschutzrechtlichen Vorgaben und Massnahmen liegt in erster Linie bei den datenbearbeitenden Mitarbeitenden und dem Geschäftsführer der PK KVO.

### **17. Kontroll- und Verbesserungsprozess sowie Checklisten**

Ein Kontroll- und Verbesserungsprozess mit allfälligen daraus resultierenden Massnahmen wird 1x jährlich sowie bei Bedarf durchgeführt. Dieser wird mit Einzelinterviews durchgeführt.

Dazu gehört die Überprüfung von Zugriffsberechtigungen sowie getroffener Datenschutzmassnahmen. Die Datenbearbeitungsprozesse und ihre Überprüfungen werden schriftlich dokumentiert und können jederzeit ausgewiesen werden. Technische und organisatorische Massnahmen werden mindestens in Form von einem jährlich zu überprüfenden und bei Bedarf anzupassenden Kontrollformular überprüft.

### **18. Audits**

Gesetzlich erforderliche oder vertraglich vereinbarte Audits betreffend Bearbeitung von Personendaten werden durch die Datenschutzberaterin nach Möglichkeit in Anwesenheit von mindestens folgenden Personen durchgeführt:

- Geschäftsführer der PK KVO
- Pensionskassenverwalter
- Verantwortliche Personen von Auftragsbearbeitenden

Die PK KVO ermöglicht für die Prüfung – unter Vorbehalt besonderer Dringlichkeit nach angemessener Vorankündigung und während der Geschäftszeiten – im erforderlichen und jeweils zulässigen Masse den Zugang zu Systemen, in denen Personendaten bearbeitet werden.

Audits werden schriftlich dokumentiert sowie von verantwortlichen Personen von Auftragsbearbeitenden unterzeichnet.

Die PK KVO ist berechtigt, Audit- und Prüfberichte auch anderen Betroffenen zur Verfügung zu stellen.

### **19. Meldung bei Verletzung der Datensicherheit**

Die Meldung bei einer Datenschutzverletzung ist gemäss DSG obligatorisch. Wird ein Datenschutzvorfall identifiziert, so ergreift die Pensionskasse unverzüglich angemessene Massnahmen zu dessen Behebung oder zur Eindämmung der Folgen.

Zentrale Ansprechperson hierfür ist der Geschäftsführer der PK KVO. Er entscheidet in einem ersten Schritt über ein unmittelbares Vorgehen. Datenschutzvorfälle und die getroffenen Massnahmen werden dokumentiert.

Betroffene Personen werden ebenfalls im Einklang mit den gesetzlichen Vorgaben informiert. Soweit rechtlich erforderlich, ist auch der EDÖB zu informieren.

### **20. Sensibilisierung / Schulung der Mitarbeitenden**

Besonders wichtig ist die Sensibilisierung derjenigen Mitarbeitenden, die mit Personendaten arbeiten. Alle mit Personendaten befassten Mitarbeitenden der Pensionskasse oder im Auftrag von der Pensionskasse tätigen Dritten, haben eine Sorgfaltspflichterklärung zu unterzeichnen und die entsprechenden Datenbearbeitungsreglemente zu beachten. Inhaltlich für die Schulungen zuständig ist die/der Datenschutzberater/in der PK KVO. Diese/r orientiert sich an der aktuellen Gesetzgebung und Praxis und bildet sich regelmässig weiter.

### **21. Löschkonzept**

Das Löschkonzept richtet sich nach Art. 27i – 27k BVV2 und Art. 47 BVV2 bzw. Art. 958f OR.

### **22. Lücken im Datenschutzreglement der PK KVO**

In Fällen, für welche das Datenschutzreglement keine Bestimmungen enthält, gelten die Vorschriften des Datenschutzgesetzes des Bundes.

## Inkrafttreten des Datenschutzreglements

Dieses Datenschutzreglement tritt auf den 1. September 2023 in Kraft.


Solothurn, 30. Oktober 2023

Pensionskasse von Krankenversicherungs-  
Organisationen

Der Stiftungsrat



Jean-Pierre Dubois  
Präsident



Dr. Reto Flury  
Vize-Präsident