KPT, Postfach, CH-3001 Bern
kpt.ch

Bearbeitungsreglement KPT-Informationssystem

(Gemäss Art. 21 VDSG und Art 84b KVG)

Version 3.0 gültig ab 1. April 2021

Inhaltsverzeichnis

1 Ausgangslage ... 3

2 Inhalt ... 3

3 System Dokumentation ... 3

3.1 Betroffene Organisationseinheiten ... 3
3.2 Schnittstellenbeschreibung ... 3
3.3 Datenherkunft ... 4
3.4 Datenempfänger ... 4
3.5 Zwecke, für welche die Daten regelmässig bekannt gegeben werden ... 4
3.6 Umfang der Datenweitergabe ... 5

4 Organigramm des systembetreibenden Organs (SbO) ... 5

5 Verantwortlichkeiten ... 5

6 Dokumentation über die Planung, die Realisierung und den Betrieb der Datensammlung ... 5

7 Anmeldung der Datensammlung beim EDÖB (Art. 16 VDSG) ... 5

8 Prozessdokumentation KPT-Informationssystem ... 6

9 Kontrollverfahren sowie technische und organisatorische Massnahmen nach Art. 20 VDSG ... 6

9.1 Zugangs-/Zutrittskontrolle ... 6
9.2 Zugriffskontrolle ... 6
9.3 Eingabekontrolle (Protokollierung) ... 6
9.4 Datenträgerkontrolle / Speicherkontrolle ... 6
9.5 Transportkontrolle ... 7
9.6 Bekanntgabekontrolle ... 7
9.7 Benutzerkontrolle ... 7

10 Beschreibung der Datenfelder und der Organisationseinheiten, die darauf Zugriff haben (Art. 21, Abs. 2, Bst e VDSG) ... 7

11 Art und Umfang des Zugriffs der Benutzer der Datensammlung (Art. 21, Abs. 2, Bst f VDSG) ... 7

12 Ausbildung der Benutzer der Datensammlung ... 8

13 Die Datenbearbeitungsverfahren, insbesondere die Verfahren bei der Berichtigung, Sperrung, Anonymisierung (Pseudonymisierung), Speicherung, Aufbewahrung, Archivierung oder Vernichtung der Daten (Art. 21, Abs. 2, Bst g VDSG) ... 8

14 Die Konfiguration der Informatikmittel (Art. 21, Abs. 2, Bst h VDSG) ... 8

15 Das Verfahren zur Ausübung des Auskunftsrechts (Art. 21, Abs. 2, Bst i VDSG) ... 8

16 Publikation ... 8

1 Ausgangslage

Die KPT Krankenkasse AG ist Inhaberin der, dem eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldeten, automatisierten Datensammlung «**KPT- Informationssystem»**, welche besonders schützenswerte Daten und Persönlichkeitsprofile enthält. Die Datensammlung bezweckt die Durchführung und Abwicklung der Kranken- und Unfallversicherung im Bereich der obligatorischen Krankenpflegeversicherung und der Krankenzusatzversicherung nach VVG.

Gestützt auf Art. 11 sowie 21 der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) ist für die Datensammlung ein Bearbeitungsreglement zu erstellen. Gemäss Art. 84b des Bundesgesetzes über die Krankenversicherung (KVG) ist das Reglement dem EDÖB zur Beurteilung vorzulegen und muss öffentlich zugänglich sein.

2 Inhalt

Dieses Bearbeitungsreglement umschreibt insbesondere die Datenbearbeitungs- und Kontrollverfahren sowie den Betrieb des «KPT-Informationssystems». Weiter enthält das Reglement die für die Meldepflicht erforderlichen Angaben (Art. 16 VDSG) sowie Angaben über das für den Datenschutz und die Datensicherheit der Daten verantwortliche Organ, die Herkunft der Daten, die Zwecke, für welche die Daten regelmässig bekannt gegeben werden, die Kontrollverfahren und insbesondere die technischen und organisatorischen Massnahmen nach Art. 20 VDSG, die Beschreibung der Datenfelder und die Organisationseinheiten, die darauf Zugriff haben, Art und Umfang des Zugriffs der Benutzer der Datensammlung, die Datenbearbeitungsverfahren, insbesondere die Verfahren bei der Berichtigung, Sperrung, Anonymisierung, Speicherung, Aufbewahrung, Archivierung oder Vernichtung der Daten, die Konfiguration der Informatikmittel sowie das Verfahren zur Ausübung des Auskunftsrechts.

Dieses Bearbeitungsreglement gilt auch für die unabhängige Datenannahmestelle gemäss Art. 59a KVV, welche intern bei der KPT betrieben wird.

3 System Dokumentation

3.1 Betroffene Organisationseinheiten

Die KPT Krankenkasse AG ist das systembetreibende und als Inhaberin der automatisierten Datensammlung «KPT-Informationssystem» das dafür verantwortliche Organ.

3.2 Schnittstellenbeschreibung

Einige Dienstleistungen, welche teilweise auch die Bearbeitung von Personendaten umfassen, hat die KPT gestützt auf Art. 84 KVG an die Outsourcing Partner für den Betrieb IT, sowie die Partner Dokumentenbearbeitung und Postlösungen ausgelagert. Die datenschutzkonforme Bearbeitung der Daten wie auch die Datensicherheit wurde in den jeweiligen Verträgen und SLA's geregelt. Die IT-Partner sind zudem teilweise nach verschiedenen ISO-Normen (insbesondere ISO 9001: Qualitätsmanagementsystem sowie ISO/IEC 27001: Informationssicherheits-Managementsystem) zertifiziert.

Die KPT bleibt als Inhaberin der Datensammlung weiterhin verantwortlich für die Einhaltung des Datenschutzes für die ausgelagerten Bereiche (Art. 22 VDSG).

Im Rahmen der Durchführung und Abwicklung der Kranken- und Unfallversicherung im Bereich der obligatorischen Krankenpflegeversicherung gemäss KVG unterhält die KPT Schnittstellen zu Datenbezügern und -lieferanten, welche nachfolgend beschrieben werden.

Empfänger/Lieferant	Zweck	Besonders schützenswerte Personendaten	Auslöser
Banken / Finanzdienstleister	Zahlungsverkehr	Nein	Automatisch / Manuell
Behörden / Gerichte	Art. 82 KVG Art. 84a KVG	Ja	Manuell
Datendrehscheibe	Leistungsverarbeitung KVG	Ja	Automatisch
Externe Druckerei	Kundenmagazin	Nein	Automatisch
Gemeinsame Einrichtung KVG	Risikoausgleich	Nein	Manuell
HMO-Partner	Gatekeeping, Einhaltung Vertrag	Ja	Automatisch
Kantone	Individuelle Prämienverbilligung	Ja	Manuell
Leistungserbringer	Art. 84a KVG	Ja	Automatisch / Manuell
Partner telemedizinische Dienstleistung	Gesundheitsbetreuung	Ja	Automatisch
Partner Regress	Regress	Ja	Automatisch
Santésuisse	Auskünfte, ZSR, Datenpool	Nein	Automatisch
Sozialversicherer	Art. 84a KVG	Ja	Manuell
VEKA	Versichertenkarte (KVG Art. 42a, VVK)	Ja	Automatisch
Versicherte	Auskunft	Ja	Automatisch / Manuell
Zentrales Vertragsregister (ZVR)	Auskunft	Nein	Manuell

3.3 Datenherkunft

Die Daten stammen von Leistungserbringern, Versicherten, anderen Sozialversicherungen, Behörden und Finanzdienstleistern.

3.4 Datenempfänger

Datenempfänger ist die KPT Krankenkasse AG. Persönlich adressierte Dokumente (vor allem Direktions- und Vertrauensarztdokumente) gehen direkt an die betreffenden KPT Mitarbeitenden. Die anderen Dokumente (Briefe, Formulare sowie Rechnungen) werden vom Partner Dokumentenbearbeitung (Outsourcingpartner) digitalisiert, strukturiert und transcodiert und in das «KPT Informationssystem» bzw. in den Workflow eingespeist.

Bei der Rechnungsstellung im stationären Bereich, Typ DRG, leitet der Leistungserbringer die Datensätze systematisch mit den administrativen und den medizinischen Angaben nach Artikel 59 Absatz 1 KVV gekoppelt mit der Rechnung an die unabhängige Datenannahmestelle der KPT gemäss Art. 59a KVV.

Die Prozesse für die einzelnen Datenbearbeitungen sind in internen Prozessdokumenten festgehalten.

3.5 Zwecke, für welche die Daten regelmässig bekannt gegeben werden

Der Zweck der Datenweitergabe ist in jedem Fall die Durchführung der obligatorischen Krankenpflegeversicherung gemäss dem Bundesgesetz über die Krankenversicherung (KVG). Genauere Angaben sind der Schnittstellenbeschreibung (Ziffer 3.2) zu entnehmen.

3.6 Umfang der Datenweitergabe

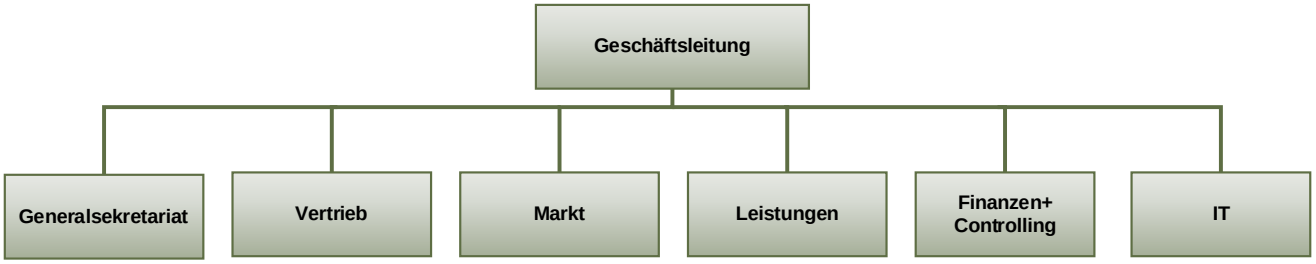
Aus der Schnittstellenbeschreibung (Ziffer 3.2) wird ersichtlich, welche Daten jeweils an welche Empfänger weitergegeben werden. Die Daten werden ausschliesslich zum Zweck

- der besonderen Amts- und Verwaltungshilfe gemäss Art. 32 Abs. 2 ATSG und Art. 82 KVG,
- der Aufklärung und Beratung gemäss Art. 27 ATSG,
- der Akteneinsicht gemäss Art. 47 ATSG
- sowie im Rahmen der Datenbekanntgabe im Sinne von Art. 84a KVG

weitergegeben.

Eine weitergehende Datenbekanntgabe erfolgt nur im Einzelfall bei Einwilligung durch die versicherte Person. Weiter erfolgt eine Datenweitergabe nur unter Einhaltung der Grundsätze gemäss Art. 4ff. des Bundesgesetzes über den Datenschutz (DSG), insbesondere nur im Rahmen des Zweckmässigkeits- und Verhältnismässigkeitsgebotes.

4 Organigramm des systembetreibenden Organs (SbO)



5 Verantwortlichkeiten

Die Geschäftsleitung der KPT Krankenkasse AG trägt als Inhaberin der Datensammlung die Verantwortung für den Datenschutz und die Datensicherheit. Die Belange des Datenschutzes und der Datensicherheit werden durch die Governance Funktionen (Datenschutz, Corporate Security, Compliance und IRKM) abgedeckt. Die Governance Funktionen beraten die Geschäftsleitung, erstellen Vorgaben und sind in die Kontrollprozesse eingebunden.

6 Dokumentation über die Planung, die Realisierung und den Betrieb der Datensammlung

Der Betrieb der Datensammlung ist in geeigneter Form dokumentiert.

Die technische Dokumentation der Systemkomponenten erfolgt in entsprechenden Betriebshandbüchern.

Die Planung und Realisierungen von Aktualisierungen (Lifecycle) und Weiterentwicklungen werden über das Projektmanagement nach HERMES geführt und dokumentiert.

7 Anmeldung der Datensammlung beim EDÖB (Art. 16 VDSG)

Die KPT Krankenkasse AG hat gemäss Art. 11a Abs. 5 lit. e DSG einen Datenschutzverantwortlichen bezeichnet, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis der Datensammlungen führt. Damit ist die KPT von der Anmeldungspflicht der Datensammlung beim EDÖB befreit.

8 Prozessdokumentation KPT-Informationssystem

Die Datenbearbeitungsprozesse des «KPT-Informationssystems» sind im zentralen Prozessmanagement-Tool dokumentiert und für alle KPT-Mitarbeitenden einsehbar.

9 Kontrollverfahren sowie technische und organisatorische Massnahmen nach Art. 20 VDSG

9.1 Zugangs-/Zutrittskontrolle

Um sicherzustellen, dass unbefugte Personen keinen Zugang zu den Gebäuden der KPT haben, ist der Zutritt nur den Mitarbeitenden der KPT, welche im Besitz eines Badge oder Schlüssels sind, möglich.

Die Büroräumlichkeiten dürfen nur zu dienstlichen Zwecken betreten werden. Unbekannten Personen wird kein Zutritt zum Gebäude gewährt. Im Zweifelsfall haben sich Personen auszuweisen.

Besucherinnen und Besucher müssen sich beim Empfang ausweisen und registrieren. Sie werden durch eine KPT-Kontaktperson am Empfang abgeholt und dürfen sich nur in Begleitung im Gebäude bewegen. Der Gebäudezutritt ist in internen Weisungen geregelt.

9.2 Zugriffskontrolle

Die KPT verfügt über eine mehrstufige Sicherheitsinfrastruktur für den Zugriff auf das «KPT-Informationssystem». Alle Mitarbeitenden verfügen über ein Login für die Benutzung des Systems.

Die Zugriffsrechte werden mittels eines Rollen-basierten Zugriffsberechtigungssystems geregelt und in Berechtigungskonzepten sowie Zugriffsmatrix festgehalten (Art. 21, Abs. 2, Bst e VDSG).

Durch die Definition und Umsetzung geeigneter Berechtigungskonzepte wird der Zugriff auf Datensammlungen gemäss «need to know» Prinzip eingeschränkt (Aufgabenerfüllung gemäss Art. 84 KVG). Damit wird sichergestellt, dass keine unbefugte Einsichtnahme, Veränderung oder Löschung erfolgen kann.

Die Mitarbeitenden, welche zur Aufgabenerfüllung über Zugriffsrechte verfügen, werden durch entsprechende Vorgabedokumente zur korrekten Datenbearbeitung angehalten.

9.3 Eingabekontrolle (Protokollierung)

Alle Zutritte und Zugriffe werden nachvollziehbar protokolliert.

Die KPT führt eine Protokollierung über die wichtigsten durchgeführten Aktivitäten durch. Zur Kontrolle der Einhaltung der Nutzungsregelung wertet die KPT die Protokollierungen in anonymer Form aus.

Wird ein Missbrauch festgestellt oder entsteht ein Missbrauchsverdacht, so werden die Auswertungen der Protokollierungen namentlich ausgewertet. Bei einem nachgewiesenen Missbrauch werden entsprechende Sanktionen eingeleitet. Die Mitarbeitenden der KPT sind über dieses Vorgehen informiert.

9.4 Datenträgerkontrolle / Speicherkontrolle

Weiter stellt die KPT durch geeignete Massnahmen sicher, dass keine unbefugten Personen Daten im «KPT-Informationssystem» lesen, kopieren, verändern oder entfernen können und keine unbefugte Eingabe in den Speicher sowie keine unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten erfolgen kann.

So wird zum einen wie vorangehend aufgeführt, durch die Zugangskontrolle sichergestellt, dass unbefugte externe Personen keinen Zutritt zu den Gebäuden der KPT haben, so dass eine Datenbearbeitung durch unbefugte Externe ausgeschlossen werden kann. Um eine unbefugte Datenbearbeitung durch Mitarbeitende der KPT zu verhindern, beschränkt oder verhindert die KPT durch technische Massnahmen

den Zugriff auf Daten, welche die Mitarbeitenden nicht benötigen, um die ihnen nach dem KVG übertragenen Aufgaben zu erfüllen (Art. 84 KVG). Weitere Ausführungen zur Zugriffsbeschränkung sind unter Ziffer 11 dieses Reglements festgehalten.

Weiter werden die Mitarbeitenden in verschiedenen Reglementen sowie Weisungen zur korrekten Datenbearbeitung angehalten. So wird den Mitarbeitenden mittels Datenschutzreglementen die korrekte Datenbearbeitung vermittelt.

Bestimmte von Mitarbeitenden durchgeführte Änderungen können in den Systemen zurückverfolgt werden (siehe Ziffer 9.3).

9.5 Transportkontrolle

Die KPT stellt mittels technischen und organisatorischen Massnahmen sicher, dass bei der Übermittlung von Personendaten (z.B. E-Mail) sowie beim Transport von Datenträgern keine unbefugten Dritten Einsicht in die Daten erhalten oder Daten manipulieren können (z.B. durch Verschlüsselung, HIN-Mail oder Weisungen zum Umgang mit E-Mails).

9.6 Bekanntgabekontrolle

Der Empfänger von Personendaten wird entweder manuell oder durch technische Hilfsmittel verifiziert.

9.7 Benutzerkontrolle

Siehe Ziffer 9.2

10 Beschreibung der Datenfelder und der Organisationseinheiten, die darauf Zugriff haben (Art. 21, Abs. 2, Bst e VDSG)

Die Zugriffsrechte im «KPT-Informationssystem» werden mittels eines Rollen-basierten Zugriffsberechtigungssystems geregelt. In einer Zugriffsmatrix ist festgehalten, welche Rollen über welche Arten von Zugriff im «KPT-Informationssystem» verfügen.

11 Art und Umfang des Zugriffs der Benutzer der Datensammlung (Art. 21, Abs. 2, Bst f VDSG)

Es erhalten nur diejenigen Mitarbeitenden Zugriff auf das «KPT-Informationssystem», die diesen tatsächlich benötigen. Die Mitarbeitenden werden einem Benutzerprofil zugeteilt (vgl. oben Ziff. 9.2) und erhalten sodann eine persönliche Zugriffsberechtigung, welche nicht an Drittpersonen weitergegeben werden darf. Insbesondere wird auch festgestellt, ob die Mitarbeitenden lediglich eine Anfrageberechtigung benötigen, oder darüber hinaus eine Mutationsberechtigung.

Auf MCD-Daten, welche bei der unabhängigen Datenannahmestelle der KPT eingehen und durch diese automatisiert verarbeitet werden, haben die Mitarbeitenden der KPT keinen Zugriff. Werden Rechnungen durch die Datenannahmestelle zur Überprüfung ausgelenkt, erhalten die mit der Fallüberprüfung beauftragten Mitarbeitenden bis zum Fallabschluss Zugriff auf die Rechnungen sowie die dazugehörigen MCD. Der Zugriff auf die MCD wird mit Fallabschluss gesperrt.

Die Berechtigungsanträge sind durch die jeweiligen Vorgesetzten und den Berechtigungseigentümer zu genehmigen. Die Berechtigungen sind den Mitarbeitenden wieder zu entziehen, wenn sie für die übertragenen Aufgaben nicht mehr notwendig sind.

12 Ausbildung der Benutzer der Datensammlung

Die Benutzer des «KPT-Informationssystems» werden auf verschiedene Wege im datenschutzrechtlichen Bereich wie auch anwendungstechnisch geschult. So haben sämtliche neueintretende Mitarbeitende der KPT eine Datenschutzschulung zu absolvieren. Ebenfalls ist eine Schulung betreffend die Anwendungen des «KPT-Informationssystems» zu durchlaufen. Weiter schult die KPT die Mitarbeitenden durch ein E-Learning Modul im Bereich Datenschutz.

Die Benutzer des «KPT-Informationssystems» werden im ganzen System feldbezogen von verschiedenen Anwendungshandbüchern, sowie im Bereich Datenschutz von Datenschutzreglementen unterstützt.

13 Die Datenbearbeitungsverfahren, insbesondere die Verfahren bei der Berichtigung, Sperrung, Anonymisierung (Pseudonymisierung), Speicherung, Aufbewahrung, Archivierung oder Vernichtung der Daten (Art. 21, Abs. 2, Bst g VDSG)

Jede von einem Mitarbeitenden der KPT durchgeführte Mutation wird technisch festgehalten (vgl. oben Ziff. 9.3). Es ist stets der alte sowie der neue Stand nach der Mutation ersichtlich um die Nachvollziehbarkeit der Datenbearbeitung sicherzustellen.

Die Datenbearbeitungsverfahren sind in spezifischen Weisungen, Reglementen und Handbüchern dokumentiert.

14 Die Konfiguration der Informatikmittel (Art. 21, Abs. 2, Bst h VDSG)

Die von der KPT nach Absprache mit den Outsourcing Partnern eingesetzte Hard- und Software entspricht internationalen Standards und diese werden regelmässig durch unabhängige Prüfer kontrolliert (ISAE-3402; ISO 27001).

Die Dokumentationen der Konfiguration der für das «KPT-Informationssystem» eingesetzten Informatikmittel werden im Bereich IT sowie bei den Outsourcing Partnern der KPT aufbewahrt und bei Bedarf nachgeführt.

15 Das Verfahren zur Ausübung des Auskunftsrechts (Art. 21, Abs. 2, Bst i VDSG)

Auskunftsbegehren gemäss Art. 8 DSG sind an den betrieblichen Datenschutzbeauftragten zu stellen:

KPT
Datenschutz
Wankdorfallee 3
3014 Bern
datenschutz@kpt.ch

16 Publikation

Gemäss Art. 84b KVG wird dieses Reglement im Internet unter kpt.ch publiziert.