KPT, Postfach, CH-3001 Bern
kpt.ch

Bearbeitungsreglement KPT

(Gemäss Art. 5 und 6 DSV und Art 84b KVG)

Inhaltsverzeichnis

1 Ausgangslage

Die KPT Krankenkasse AG und die KPT Versicherungen AG bearbeiten (besonders schützenswerte) Personendaten. Die Datenbearbeitung bezweckt die Durchführung und Abwicklung der Kranken- und Unfallversicherung im Bereich der obligatorischen Krankenpflegeversicherung und der Krankenzusatzversicherung nach VVG.

Gestützt auf Art. 5 sowie 6 der Verordnung über den Datenschutz (Datenschutzverordnung, DSV) haben die KPT Krankenkasse AG als verantwortliches Bundesorgan sowie die KPT Versicherungen AG als private Verantwortliche für die automatisierte Bearbeitung ihrer Personendaten 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

Das Bearbeitungsreglement enthält insbesondere Angaben zur internen Organisation, zum Datenbearbeitungs- und Kontrollverfahren sowie zu den Massnahmen zur Gewährleistung der Datensicherheit.

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 und die KPT Versicherungen AG (nachfolgend KPT) betreiben gemeinsam als verantwortliches Organ die IT-Systeme.

3.2 Datenherkunft, Bearbeitungszwecke, Datenweitergabe

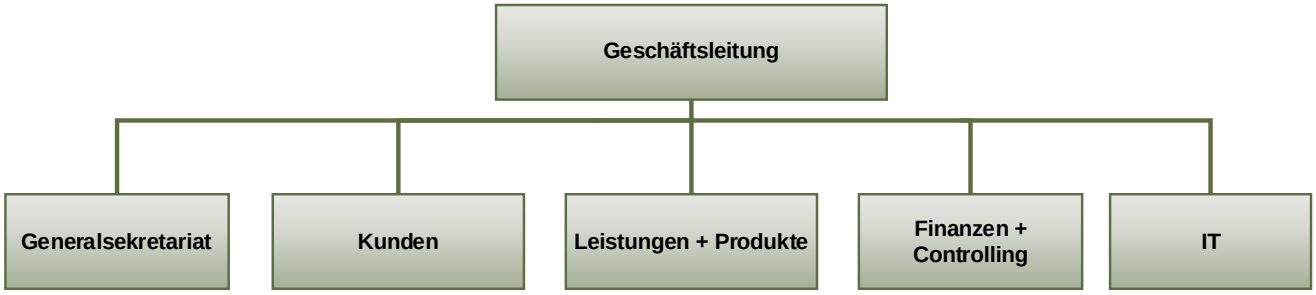
In der Datenschutzerklärung informiert die KPT transparent wie, zu welchen Zwecken und auf welcher Rechtsgrundlage sie Personendaten erhebt und bearbeitet und wem sie Personendaten bekannt gibt. Zudem werden die Betroffenen über ihre Rechte (Recht auf Auskunft, Berichtigung und Datenherausgabe) aufgeklärt.

3.3 Externe Dienstleister / Schnittstellen

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

Im Rahmen der Durchführung und Abwicklung der Kranken- und Unfallversicherung im Bereich der obligatorischen Krankenpflegeversicherung gemäss KVG sowie der Krankenzusatzversicherung gemäss VVG ermöglichen verschiedene Schnittstellen den direkten Kontakt mit Versicherten, externen Dienstleistern (z.B. Banken, Partner Regress, Behörden) und Leistungserbringern (z.B. HMO-Partner, Partner telemedizinische Dienstleistung). Der Datenschutz und die entsprechende Datensicherheit werden mittels starker Authentifizierung und moderner Verschlüsselungs- und Übertragungstechnologie gewährleistet.

4 Organigramm des systembetreibenden Organs (SbO)



5 Verantwortlichkeiten

Die Geschäftsleitung der KPT trägt 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 Betrieb der IT-Systeme ist in geeigneter Form dokumentiert.

Die Datenbearbeitungen werden in Reglementen, Weisungen und Handbüchern festgelegt und im zentralen Prozessmanagement-Tool sowie im Verzeichnis der Bearbeitungstätigkeiten dokumentiert. Die Unterlagen werden von den zuständigen Organisationseinheiten regelmässig aktualisiert.

Die technische Dokumentation der Systemkomponenten erfolgt in entsprechenden Betriebshandbüchern.

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

7 Kontrollverfahren sowie technische und organisatorische Massnahmen nach Art. 3 DSV

7.1 Allgemein

Die KPT orientiert sich bei technischen und organisatorischen Massnahmen der Datensicherheit an international etablierten Standards wie ISO/IEC 27001 und NIST (National Institute of Standards and Technology). Nebst diversen ISO-Zertifizierungen verfügen die IT Outsourcing Partner über einen ISAE-3402-Bericht, in dem das interne Kontrollsystem durch unabhängige Prüfer kontrolliert und dokumentiert wird.

7.2 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. Badges und Besucherausweise sind innerhalb der Gebäude gut sichtbar zu tragen. Im Zweifelsfall haben sich Personen auszuweisen.

Besucherinnen und Besucher müssen sich beim Empfang 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.

7.3 Zugriffskontrolle

Die KPT verfügt über eine mehrstufige Sicherheitsinfrastruktur für den Zugriff auf die IT-Systeme. Alle Mitarbeitenden verfügen über ein Login für deren Benutzung.

Die Zugriffsrechte werden mittels eines Rollen-basierten Zugriffsberechtigungssystems geregelt und in Berechtigungskonzepten sowie Zugriffsmatrix festgehalten.

Durch die Definition und Umsetzung geeigneter Berechtigungskonzepte wird der Zugriff auf Personendaten gemäss «need to know» Prinzip eingeschränkt. Insbesondere wird auch festgestellt, ob die Mitarbeitenden lediglich eine Anfrageberechtigung benötigen, oder darüber hinaus eine Mutationsberechtigung. Damit wird sichergestellt, dass keine unbefugte Einsichtnahme, Veränderung oder Löschung erfolgen kann.

Die Berechtigungen werden den Mitarbeitenden aufgrund des Mitarbeiterprofils (Organisation, Funktion, Kaderstufe) automatisiert erteilt oder entzogen.

Zusätzliche, manuelle Berechtigungsanträge durchlaufen ein 2- oder 3-stufiges Bewilligungsverfahren. Der Entzug von nicht mehr benötigten Berechtigungen erfolgt via definiertem Prozess.

Zusätzlich werden regelmässig Attestierungen für alle Berechtigungen durchgeführt. Berechtigungsanträge sind durch die jeweiligen Vorgesetzten und den Berechtigungseigentümer zu genehmigen. Die Berechtigungen werden den Mitarbeitenden entzogen, wenn sie für die übertragenen Aufgaben nicht mehr notwendig sind.

Auf MCD (Minimal Clinical Dataset)-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.

7.4 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.

7.5 Datenträgerkontrolle / Speicherkontrolle

Weiter stellt die KPT durch geeignete Massnahmen sicher, dass keine unbefugten Personen Daten in den IT-Systemen 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 übertragenen Aufgaben zu erfüllen. Weitere Ausführungen zur Zugriffsbeschränkung sind unter Ziffer 7.3 dieses Reglements festgehalten.

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

Bestimmte von Mitarbeitenden durchgeführte Änderungen können in den Systemen zurückverfolgt werden (siehe Ziffer 7.4).

7.6 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).

7.7 Bekanntgabekontrolle

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

7.8 Benutzerkontrolle

Siehe Ziffer 7.3

8 Protokollierung nach Art. 4 DSV

Zusätzlich zur Kontrolle der Zugriffe auf die IT-Systeme erfolgt eine Protokollierung der automatisierten Bearbeitung, damit nachträglich festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben oder bekannt gegeben wurden. Die Protokollierung wird in Anwendung von Art. 4 DSV durchgeführt. Die Protokolle werden während mindestens 12 Monaten revisionssicher aufbewahrt. Sie sind ausschliesslich den Organen und Personen zugänglich, denen die Überprüfung der Anwendung der Datenschutzvorschriften oder die Wahrung oder Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegt, und dürfen nur für diesen Zweck verwendet werden. Bei externen IT-Dienstleistern bestehen eigene Regelungen zur Protokollierung.

9 Ausbildung der Benutzer

Die Benutzer der IT-Systeme 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 IT-Anwendungen zu durchlaufen. Weiter schult die KPT die Mitarbeitenden durch ein E-Learning Modul im Bereich Datenschutz.

Die Benutzer werden im ganzen System feldbezogen mit verschiedenen Anwendungshandbüchern, sowie im Bereich Datenschutz mit Datenschutzvorgabedokumenten unterstützt.

10 Version / Änderung

Dieses Bearbeitungsreglement ist nicht Bestandteil eines Vertrags mit den Versicherten oder anderen Dritten. Es kann jederzeit angepasst werden. Die auf dieser Website veröffentliche Version ist die jeweils aktuelle Fassung.