RL.23-007

(BRgl-VWe)

Bearbeitungsreglement Versicherungswesen (inkl. Datenannahmestelle / DAS)

Dokumenten-Nr.	RL.23-007 (BRgl-VWe)
Autor	eDSB (MB)
Dokumenten-Eigner	Leiterin Legal, Risk, Compliance & Datenschutz
Status Dokument	Genehmigt
Version	15.5
Inkraftsetzung	01.09.2023

Inhaltsverzeichnis

1. Grundlagen

Nach Art. 5 und 6 Verordnung über den Datenschutz (Datenschutzverordnung, DSV) i.V.m. Art. 84b des Bundesgesetzes über die Krankenversicherung (KVG) und Art. 59 Abs. 6 der Verordnung zum Bundesgesetz über die Krankenversicherung (KVV) hat die ÖKK Kranken- und Unfallversicherungen AG (hiernach „ÖKK“) für die automatisierte Datenbearbeitung von besonders schützenswerten Daten ein Bearbeitungsreglement zu erstellen.

Das vorliegende Bearbeitungsreglement enthält insbesondere Angaben zur internen Organisation, zum Datenbearbeitungs- und Kontrollverfahren sowie zu den Massnahmen zur Gewährleistung der Datensicherheit zur Durchführung und Abwicklung der Kranken- und Unfallversicherung sowie zur Datenannahmestelle (DAS).

Gemäss Art. 84b KVG ist das Reglement dem EDÖB zur Beurteilung vorzulegen und muss öffentlich zugänglich sein.

2. Herkunft, Zweck, Umfang der Datenbearbeitung

Die Daten für das Versicherungswesen stammen von den Versicherten, anderen Sozialversicherungen, Gerichten und Betreibungsämtern sowie von den in den Umsystemen verwalteten Versichertenstammdaten.

Zweck der Datenbearbeitung der ÖKK ist die Durchführung und Abwicklung der Kranken- und Unfallversicherung.

Die Daten für die DAS stammen von Leistungserbringern gemäss KVG und VVG.

Der Zweck der Datenbearbeitung der DAS besteht in der Abwicklung der Prüfung und Vergütung von stationären Rechnungen.

Zweck und Umfang der Datenbearbeitungen sind näher in der Datenschutzerklärung der ÖKK sowie im Verzeichnis der Bearbeitungstätigkeiten erläutert.

3. Datenbearbeitung durch und Bekanntgabe an Dritte

Die Datenbearbeitung erfolgt gestützt auf Art. 42 i.V.m. Art. 84 KVG. Die Bearbeitung der Diagnosedaten erfolgt ausschliesslich zur Überprüfung der Rechnungen auf die durch Art. 56 KVG vorgegebene Pflicht des Krankenversicherers, die Einhaltung der Wirtschaftlichkeit zu überprüfen.

Für die Abwicklung der stationären Leistungen sieht Art. 49 KVG diagnosebasierte Fallpauschalen (SwissDRG) vor. Dem Versicherer müssen Angaben über Haupt- und Nebendiagnosen sowie Behandlungen und Prozeduren auf der Rechnung mitgeteilt werden. Diese Informationen sind im «Minimal Clinical Dataset» (MCD) enthalten.

Für die Abwicklung von ambulanten Leistungen (Ärzte und Spitäler) wurde durch die FMH und santésuisse das TARMED-Tarifwerk entwickelt und vom Bundesrat als allgemeinverbindlich erklärt. Es gilt für alle ambulanten ärztlichen Behandlungen in Arztpraxen und Spitälern, jedoch nicht für Leistungen im zahnärztlichen Bereich, Laboranalysen, Physio- und Ergotherapie, Logopädie, Ernährungsberatung, Stoma- und Hebammenleistungen sowie Leistungen von Chiropraktikern.

Nach Art. 56 KVG sind die Krankenversicherer verpflichtet, zur Wirtschaftlichkeit der Leistungen beizutragen, indem sie in den Tarifverträgen mit den Leistungserbringern Massnahmen zur Sicherstellung der Wirtschaftlichkeit der Leistungen vorsehen und vertraglich eine Methode zur Kontrolle der Wirtschaftlichkeit festlegen

Die Datenbearbeitung durch Dritte sowie die Bekanntgabe an Dritte ist in der Datenschutzerklärung der ÖKK näher umschrieben.

4. Rechte der betroffenen Personen

Die Rechte der betroffenen Personen sind in der Datenschutzerklärung der ÖKK näher umschrieben.

5. Verantwortliche Stellen

Die Geschäftsleitung der ÖKK trägt die Gesamtverantwortung für die Durchführung der obligatorischen und privaten Krankenversicherung gemäss den Art. 25–31 KVG bzw. gemäss VVG.

Sie wird dabei durch Dateneigner (Informations-, Prozess- und Systemverantwortliche), Applikationseigner (technische Verantwortliche) und den Datenschutzberater unterstützt.

Die Mitarbeitenden sollen sich stets der Bedeutung der Informationssicherheit und des Datenschutzes bewusst sein und aktiv an der Abwehr und Bekämpfung von materiellen und ideellen Schäden mitwirken. Sie unterstehen für die obligatorische Krankenversicherung der Schweigepflicht nach Art. 33 des Bundesgesetzes über den allgemeinen Teil des Sozialversicherungsrechts (ATSG). Mitarbeitende der DAS unterstehen zudem dem ärztlichen Berufsgeheimnis nach Art. 321 Strafgesetzbuch (StGB).

6. Struktur des ÖKK-Informationssystems Versicherungswesen und Datenannahmestelle

6.1. Systeme zur Datenbearbeitung

Im ÖKK-Informationssystem Versicherungswesen und DAS und ihren Subsystemen (Durchführung der obligatorischen und privaten Krankenversicherung und Abwicklung der Prüfung und Vergütung von stationären Rechnungen nach KVG) werden die Daten erfasst. Diese sind modular aufgebaut. Verschiedene technische Schnittstellen ermöglichen den direkten Kontakt mit Leistungserbringern.

Die Informatikabteilung von ÖKK führt ein zentrales Inventar aller Informatiksysteme mit den entsprechenden Konfigurationen, welche durch die ÖKK Abteilungen Betrieb Informatik bzw. Applikationen betreut werden. Weisungen im Umgang mit Informatiksystemen und Endgeräten sind der Weisung Informationssicherheit [03.0011] zu entnehmen. Der Betrieb der IT-Systeme ist in geeigneter Form dokumentiert.

Unterlagen über die Planung und Realisierung des ÖKK-Informationssystems Versicherungswesen und DAS liegen bei der ÖKK Informatik vor.

Für den Betrieb führt die ÖKK eine IKS-Dokumentation.

Zu den verschiedenen Subsystemen gibt es intern erstellte Benutzerhandbücher. Weiteres wird in Weisungen, Reglementen und Leistungshandbüchern festgelegt. Diese werden von den zuständigen Organisationseinheiten regelmässig aktualisiert. Publiziert sind diese im ÖKK-Intranet „Piazza“.

Die Fachführungen der zuständigen Organisationseinheiten schaffen mittels spezifischen Anweisungen einen gleichbleibenden Level der Leistungsbeurteilung nach KVG.

7. Technische und organisatorische Massnahmen

7.1. Allgemeines

Die ÖKK trifft technische und organisatorische Massnahmen, damit die bearbeiteten Daten ihrem Schutzbedarf entsprechen, d.h.:

- nur Berechtigten zugänglich sind (Vertraulichkeit);
- verfügbar sind, wenn sie benötigt werden (Verfügbarkeit);
- nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität);
- nachvollziehbar bearbeitet werden (Nachvollziehbarkeit).

7.2. Zugriffskontrolle

Zugriffsberechtigt auf das ÖKK-Informationssystem Versicherungswesen und der Abwicklung der Prüfung und Vergütung von akut stationären Rechnungen sind die Mitarbeitenden der ÖKK, soweit sie dies zur Ausübung ihres Auftrags „Durchführung der obligatorischen und privaten Krankenversicherung“ benötigen. Durch die Vergabe von Zugriffsberechtigungen auf Systeme und Applikationen von ÖKK nach dem sog. „Need to know-Prinzip“ wird verhindert, dass Dritte Daten unberechtigt bearbeiten können.

Die Benutzerverwaltung wird durch die IT sichergestellt.

Jeder Benutzer erhält hierbei einen persönlichen Benutzer-Account. Passwortrichtlinien werden gemäss Weisung Informationssicherheit [03.0011] durchgesetzt. Für Subsysteme, welche eine eigene Benutzerverwaltung resp. ein eigenes Zugriffskontrollsystem besitzen, gelten dieselben Vorgaben gemäss Weisung Informationssicherheit [03.0011].

Die IKS-Anforderungen an die Benutzerverwaltung stellen sicher, dass:

- Nur berechtigte Personen auf Applikationen und Daten zugreifen können (inklusive Programme, Tabellen und entsprechende Ressourcen);
- Diese Personen nur die für sie vorgesehenen Funktionen ausführen können;
- Sämtliche Komponenten der Applikation berücksichtigt werden wie Programme, Datenbanken, Betriebssysteme, Netzwerke und Remote Zugriff;
- Die Gewaltentrennung eingehalten ist.

Auch die Anforderungen an den Prozess zur Vergabe von Berechtigungen sind im Rahmen des IKS festgelegt.

- Sämtliche Anträge an die Benutzerverwaltung wie Neuanlagen, Anpassungen in den Benutzerberechtigungen oder Löschungen müssen durch autorisierte Personen genehmigt werden. Im Falle der Berechtigungsvergabe ist zu spezifizieren, welche Berechtigungen der Benutzer erhalten soll. Im Falle einer Anpassung in den Benutzerberechtigungen ist zu spezifizieren, welche Berechtigungen gelöscht werden sollen bzw. welche Berechtigungen neu vergeben werden sollen.
- Bei der Benutzerverwaltung muss folgende Gewaltentrennung eingehalten werden:
    - Der Antragsteller darf nicht gleichzeitig den Antrag genehmigen;
    - Derjenige, der den Antrag genehmigt, muss dem Antragsteller hierarchisch übergeordnet sein. Ausnahmen bestehen auf Stufe Bereichsleiter;
    - Der Antragsteller und derjenige, der den Antrag genehmigt, dürfen den Antrag nicht ausführen;

- Derjenige, der Zugriffsverstösse überwacht, darf nicht Antragssteller sein. Er darf auch nicht derjenige sein, der die Anträge genehmigt oder ausführt;
- Diejenigen, die Administratoren-Aktionen durchführen können, dürfen nicht die Überwachung der Administratoren-Aktionen ausführen.

Die Vergabe der Zugriffsberechtigungen ist wie folgt geregelt:

1. User wird einer Rolle zugewiesen;
2. den Rollen werden entsprechende Zugriffsberechtigungen in Form von Tasks und Processes erteilt.

Die Zuordnung der einzelnen Rollen zu Task und Processes ist im Hauptsystem hinterlegt und kann eingefordert werden. Die Vergabeprozesse für Zugriffsberechtigungen weiterer Subsysteme (auf welche ÖKK zugriffsberechtigt ist) erfolgt analog dem Zugriffsberechtigungsprozess für das Hauptsystem.

Die Benutzer des ÖKK-Informationssystems Versicherungswesen und DAS sind nur so lange zugriffsberechtigt, als sie die Daten für die Ausübung ihrer Arbeitsfunktion benötigen. Bei Austritten sowie bei Aufgabenwechseln innerhalb von ÖKK wird die Zugriffsberechtigung entzogen und die für den neuen Aufgabenbereich benötigten Zugriffsberechtigungen müssen neu beantragt werden.

Die Test- und Produktionssysteme werden strikt getrennt. Die Zugriffsberechtigungen auf den Testsystemen sind analog den Produktionssystemen zu handhaben.

Administratoren des ÖKK-Informationssystems Versicherungswesen verfügen über persönliche und dedizierte Administratoren-Accounts.

Im Rahmen des IKS wird festgelegt, dass Log-Aufzeichnungen von Administratoren-Aktionen geführt werden müssen (siehe Infrastruktur Benutzerverwaltung, Realisierungskonzept [14.0023]).

7.3. Zugangskontrolle

Die Räumlichkeiten der Agenturen sind während den Öffnungszeiten frei zugänglich. Es befinden sich aber jederzeit Mitarbeitende der Agenturen in den Räumlichkeiten, welche externe Personen während ihres Aufenthalts in den Räumlichkeiten der Agenturen begleiten.

Am Hauptsitz sind sämtliche Räumlichkeiten der ÖKK, in welchen besonders schützenswerte Personendaten bearbeitet werden, elektronisch und/oder mechanisch vor dem Zutritt unbefugter Personen gesichert. Das elektronische Schliesssystem am Hauptsitz basiert auf einer eigenen Benutzerverwaltung. Die Logistik führt ein Protokoll über den Betrieb der Schliessvorrichtungen.

Besonders sensitive Räume, wie VAD-Räume, die Technikräume und die Rechenzentren, sind wie folgt gesichert:

- Die elektronischen Datenträger in den von der ÖKK betriebenen Rechenzentren und dezentrale Server sind mit einer erhöhten Sicherheitsanforderung (Badge und Code) ausschliesslich für den Zugang spezifisch berechtigter Personen gesichert;
- Die elektronischen Datenträger in dezentralen Servern und Computern, welche nicht durch die IT der ÖKK betrieben werden, sind denselben Sicherheitsvorkehrungen unterstellt, wie diejenigen, welche durch diese selbst betrieben werden.
- Die Zugangskontrolle der VAD-Räume ist im Bearbeitungsreglement VAD [03.0014] reglementiert.

In der Weisung Informationssicherheit [03.0011] werden Mitarbeitende verpflichtet, als vertraulich klassifizierte Unterlagen wegzuschliessen und den Computer vor Verlassen des Arbeitsplatzes zu sperren.

Die Entsorgung von Papierdokumenten ist in der Weisung Datenschutz [03.0009] geregelt. Elektronische Datenträger werden durch ein zertifiziertes Entsorgungsunternehmen im Auftrag und unter Begleitung der Abteilung Betrieb Informatik fachgerecht entsorgt.

7.4. Benutzerkontrolle/Zugriffskontrolle

Die Nutzung der Subsysteme, die schreibenden und lesenden Zugriffe sowie die Nutzung von Funktionen zur Datenübertragung werden durch Zugriffsberechtigungen gesteuert.

Weisungen und Umsetzung der Zugriffskontrolle sind dem Kap. 7.3 zu entnehmen.

7.5. Personendatenträgerkontrollen /Datenträgerkontrolle

Durch informationstechnische Vorkehrungen ist es ausschliesslich berechtigten Personen möglich, Daten auf den elektronischen Datenträgern zu bearbeiten. Nur berechtigte Personen erhalten Zugriff auf das ÖKK-Informationssystem Versicherungswesen sowie auf das DAS, auf die Subsysteme und insbesondere auch auf das System des VAD.

In der Weisung Informationssicherheit [03.0011] werden Weisungen für den Umgang mit klassifizierten Informationen/Daten der Stufe D3 („hohe Datenschutzrelevanz“) und V3 („ÖKK-VERTRAULICH“) erlassen.

7.6. Speicherkontrolle

Die Benutzer erhalten spezifische Berechtigungen für Mutationen in den entsprechenden Subsystemen, die sie für die Erfüllung der nach dem Krankenversicherungsgesetz übertragenen Aufgaben benötigen. Die Berechtigungen werden periodisch überprüft (siehe auch Kap. 7.10).

Daten dürfen nur auf Systemen von ÖKK oder den Outsourcern gespeichert werden. Eine Speicherung der D3- und V3-Daten auf privaten Geräten und in der „Cloud“ ist gemäss Weisung Informationssicherheit [03.0011] untersagt.

Anonymisierung und Pseudonymisierung von Daten ist in der Weisung Datenschutz [03.0009] definiert.

7.7. Transportkontrolle

Das Drucken von Dokumenten erfolgt auf dezentralen Druckern, welche alle in für die Öffentlichkeit unzugänglichen Bereichen untergebracht sind.

Grosse Druckaufträge für den Massenversand werden nicht durch ÖKK vorgenommen, sondern durch die Centris AG. Dort werden diese Daten miteinander verknüpft, gedruckt und maschinell verpackt. Wenn der Massenversand erfolgreich erledigt wurde, werden die Daten gelöscht.

Die Speicherung von D3-/V3-Daten auf physischen Datenträgern zum Transport erfolgt ausschliesslich verschlüsselt (siehe auch Weisung Informationssicherheit [03.0011]).

Für den Transport per Kurier oder Post sind die Vorgaben der Weisung Informationssicherheit [03.0011] zu befolgen.

Das interne ÖKK-Netzwerk wird generell als vertraulich eingestuft. Datentransfers ausserhalb des Netzwerks erfolgen verschlüsselt oder mittels definierter Punkt zu Punkt Verbindung.

ÖKK ist Teilnehmer des HIN-Netzwerkes, welches den verschlüsselten Mailversand zwischen allen Teilnehmenden ermöglicht (bspw. Ärzte, Spitäler).

Die Versandkisten an Unternehmen, welche Rechnungen zum Scanning enthalten, werden plombiert via nachverfolgbare A-Post verschickt.

7.8. Bekanntgabekontrolle

Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, werden über die Schnittstellen identifiziert.

7.9. Eingabekontrolle/Protokollierung

Die Nachvollziehbarkeit der Eingaben, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden, wird mittels Protokollierungen belegt.

Für die Protokollierung und dein sog. „Audit Trail“ werden die in den Applikationen standardmässig vorhandenen Funktionalitäten und Logfiles verwendet.

Die Protokollierung wird in Anwendung von Art. 4 DSV durchgeführt. Das heisst., die Protokolle werden während eines Jahres revisionsgerecht festgehalten. Sie sind ausschliesslich den Organen zugänglich, denen die Überwachung der Datenschutzvorschriften obliegt und dürfen nur für diesen Zweck verwendet werden.

Über die Protokollierung werden die Mitarbeitenden im Rahmen der ordentlichen Ausbildung und mittels Weisung Informationssicherheit [03.0011] informiert.

7.10. Periodische Kontrollen

Im Rahmen des IKS und dem Realisierungskonzept Syrius Benutzerverwaltung werden jährlich folgende Kontrollen durchgeführt und Nachweise gefordert:

- Ablage und Nachvollziehbarkeit des formalisierten Zugriffsberechtigungsprozesses;
- Erstellung einer Benutzerliste aus den Subsystemen mit entsprechenden Berechtigungen, die von den Fachbereichen zu prüfen und zu genehmigen ist;
- Nachweis, dass die Überwachung von Zugriffsverstössen periodisch erfolgt ist;
- Nachweis, dass die Log-Aufzeichnungen von Administratoren-Aktionen periodisch überprüft werden;
- Nachweis, dass die geforderten Passwort- und Sicherheitseinstellungen erfüllt wurden.

Zusätzlich werden folgende Kontrollen durchgeführt.

- Stichproben bezüglich der Einhaltung von Weisungen;
- Periodische Stichproben durch die Vorgesetzten.

7.11. Massnahmen im Bereich der Endgeräte

Es dürfen nur ÖKK-eigene Endgeräte oder speziell freigegebene Geräte am internen Netzwerk angeschlossen werden. Siehe Weisung Informationssicherheit [03.0011], die von sämtlichen Mitarbeitenden der ÖKK unterzeichnet wird.

Die Endgeräte sind in zutrittsgeschützten Zonen platziert. Für den Umgang mit und die Datenspeicherung auf mobilen Endgeräten sind Vorgaben in der Weisung Informationssicherheit [03.0011] erlassen worden.

Ausgedruckte Daten werden so aufbewahrt, dass Drittpersonen (z.B. Raumpflegepersonal) diese nicht einsehen und/oder kopieren können. Diese Daten werden in Anwendung der Weisung Informationssicherheit [03.0011] verschlossen aufbewahrt.

7.12. Benutzerunterstützung und Meldepflicht

Fachlich werden die Benutzer durch die Fachführungen der Organisationseinheit unterstützt.

Die technische Unterstützung bezüglich Informatikmittel wird durch die ÖKK Informatik sowie von den jeweiligen Applikationseignern erbracht.

Die Benutzer sind über die Klassifizierung der im ÖKK-Informationssystem Versicherungswesen bearbeitbaren Daten und die Vorschriften im Umgang mit dem System sowie den Daten orientiert. Die Bestimmungen sind in der Weisung Informationssicherheit [03.0011] beschrieben. Mögliche Sanktionen bei vorsätzlichen oder fahrlässigen Verletzungen der Informatiksicherheit sind den Benutzern bekannt.

Sämtliche Benutzer sind verpflichtet, folgende Feststellungen den Applikationseignern zu melden:

- Fehler in den erfassten Daten;
- Fehler bei der Identität der registrierten Person (beispielsweise ungleiche Angaben zur gleichen Person in den verschiedenen Subsystemen);
- Fehler in den Stammdaten oder deren Strukturen;
- Beobachtete oder vermutete Schwachstellen bzw. Sicherheitsmängel des Systems;
- Nicht umgesetzte oder nicht eingehaltene Sicherheitsmassnahmen;
- Unvorhergesehene Ereignisse, die eine Auswirkung auf die Informatiksicherheit haben können;
- Bezüglich Datensammlung besteht gemäss Weisung Datenschutz [03.0009] eine Meldepflicht zuhanden des Datenschutzberaters.

8. Inkrafttreten

Das vorliegende Bearbeitungsreglement trat am 16.04.2013 in Kraft und wurde letztmalig per 1. September 2023 überarbeitet.

9. Genehmigung

Das vorliegende Bearbeitungsreglement wurde von der Geschäftsleitung genehmigt.