

Datenbearbeitungsreglement der Sanitas Gruppe

1. Einführung

Die Sanitas Krankenversicherung (nachfolgend Sanitas) bearbeitet in den Bereichen des Krankenversicherungsgesetzes (KVG) und des Unfallversicherungsgesetzes (UVG) als Bundesorgan und als private juristische Person im Bereich des Versicherungsvertragsgesetzes (VVG) Personendaten im Sinne des Datenschutzgesetzes (DSG).

Gestützt auf Art. 12 des Bundesgesetzes über den Datenschutz (DSG) und Art. 5 und Art. 6 der Verordnung über den Datenschutz (DSV) ist Sanitas gehalten, u.a. ein Bearbeitungsreglement zu erstellen.

1.1. Zweck und Umfang

Das Bearbeitungsreglement sorgt für die notwendige Transparenz im Umfeld der Datenbearbeitung.

Die Datenbearbeitung durch Sanitas soll auch von "Nicht-Experten" verstanden und beurteilt werden können.

In diesem Bearbeitungsreglement werden die Grundsätze der Datenbearbeitung i.S. des DSG festgehalten. Sanitas beachtet insbesondere folgende Grundsätze:

- Die Datenbearbeitung durch Sanitas erfolgt gestützt auf gesetzliche Grundlagen oder aufgrund der ausdrücklichen Einwilligung der betroffenen. Eine ausdrückliche Einwilligung muss u.a. dann vorliegen, wenn ein Profiling mit hohem Risiko durch eine private Person erfolgt oder bei einem Profiling durch ein Bundesorgan.
- Personendaten werden nur zu dem Zweck bearbeitet, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Der Zweck der Bearbeitung von Personendaten und ihre Beschaffung müssen ausdrücklich angegeben, für den Betroffenen erkennbar oder aus den Umständen ersichtlich sein.
- Der Umfang der Bearbeitung steht in einem angemessenen Verhältnis zum Zweck und ist auf das zur Zielerreichung Notwendige beschränkt.
- Personendaten werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.
- Die Daten werden durch angemessene technische und organisatorische Massnahmen geschützt. Fehlerhafte Daten werden berichtigt.
- Die Rechte des Betroffenen werden gewahrt. Sie erhalten vollständige Auskunft über ihre gespeicherten Daten und können deren Löschung oder Berichtigung verlangen.

1.2. Aktualität

Der Inhaber der Datensammlung überprüft das Reglement und die Beschreibungen der Datensammlungen jährlich auf ihre Aktualität und teilt dem DSB allfällige Änderungen mit oder bestätigt die Aktualität.

1.3. Definitionen und Abkürzungen

Die folgenden Abkürzungen werden im Datenbearbeitungsreglement verwendet:

- DSB Datenschutzberater der Sanitas-Gruppe
- DSG Bundesgesetz vom 20. September 2020 über den Datenschutz, SR 235.1

- EDÖB Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
- DSV Datenschutzverordnung vom 31. August 2022, SR 235.11
- KVG Bundesgesetz vom 18. März 1994 über die Krankenversicherung, SR 832.10
- VA Vertrauensarzt
- VAD Vertrauensärztlicher Dienst

2. Anmeldung der Datensammlung beim EDÖB

Sanitas erfüllt die Vorlagepflicht an den EDÖB gemäss Art. 84b KVG.

3. Datenschutz und Datensicherheit

3.1. Datenschutz

Der Verwaltungsrat der Sanitas-Gruppe trägt die Gesamtverantwortung für die Einhaltung des Datenschutzes. Er delegiert die Umsetzung an die Geschäftsleitung der Gruppengesellschaften.

Die Geschäftsleitung ist für die Umsetzung, Kommunikation, Kontrolle und Überwachung der vorgegebenen Datenschutzpolitik in der gesamten Sanitas Gruppe verantwortlich. Sie stellt sicher, dass Sanitas über eine effiziente Organisation verfügt, welche die Einhaltung des Datenschutzes unterstützt. Sanitas hat einen Datenschutzberater, welcher seinerseits für die Umsetzung der Datenschutzvorgaben sorgt und mit den notwendigen personellen und finanziellen Ressourcen ausgestattet ist.

Der Datenschutzberater der Sanitas Gruppe (DSB) gibt die wichtigsten Verhaltensweisen bezüglich Datenschutz vor und sorgt für die Einhaltung der auf die Unternehmen der Sanitas Gruppe anwendbaren datenschutzrechtlichen Vorschriften.

Der DSB erlässt in Zusammenarbeit mit den massgebenden internen Stellen entsprechende Richtlinien für die Einhaltung der Gesetze und Standards. Diese bezwecken vor allem die Schaffung einer optimalen Transparenz bei der Bearbeitung von Personendaten, um eine fachgemässe Identifikation und Beurteilung allfälliger Datenschutzrisiken zu ermöglichen.

Die Mitarbeitenden sind in ihrem Zuständigkeitsbereich für die Einhaltung aller datenschutzrechtlichen Bestimmungen, insbesondere der Auskunfts- und Schweigepflicht, verantwortlich. Weder Vorgesetzte noch Mitarbeitende können diese Verantwortung delegieren. Jeder Mitarbeitende der Sanitas hat bei der Anstellung eine Datenschutzerklärung zu unterzeichnen. Mitarbeitende von Sanitas haben ausserdem während und nach Beendigung des Arbeitsverhältnisses gegenüber Dritten Verschwiegenheit über Informationen zu wahren, die ihnen im Rahmen ihrer beruflichen Tätigkeit bekannt werden, insbesondere über medizinische Daten. Die Vorgesetzten sorgen dafür, dass die Mitarbeitenden laufend über die geltenden gesetzlichen und internen Bestimmungen informiert werden.

Dieses Bearbeitungsreglement regelt ausserdem die Zugriffskriterien und den Erwerb der Zugriffsrechte sowie den Umgang mit den aus der Datensammlung gewonnenen Informationen. Der Zugriff der Berechtigten wird dabei auf diejenigen Personendaten beschränkt, die sie für die Erfüllung ihrer Aufgabe benötigen.

Zutritt zu Räumlichkeiten, in denen besonders schützenswerte Personendaten bearbeitet werden, sind durch Zutrittsbeschränkungen geschützt. Zutritt haben nur Sanitas-Mitarbeitende

oder Dritte, die in einem Beratungsverhältnis zu Sanitas stehen und eine Datenschutz- und Geheimhaltungserklärung unterzeichnet haben. Der Zutritt zum vertrauensärztlichen Dienst untersteht zusätzlichen Restriktionen.

Für die Nutzung von Hard- und Software, Internet und E-Mail sind zudem Weisungen zum sicheren Umgang mit Hard- und Software, Internet und E-Mail massgebend.

3.2. Datensicherheit

Zum Schutz der Systeme sind Zugriffe generell nur möglich, wenn sich die zugreifende Person mittels Benutzername und Kennwort legitimieren kann. Clients und IT-Anwendungen mit Zugriff auf besonders schützenswerte Personendaten sind ausserdem mit zusätzlichen Beschränkungen ausgerüstet.

3.2.1. Allgemeine Massnahmen

Die Betriebssysteme von Sanitas werden regelmässig geprüft und gegen Angriffe durch Malware geschützt. Zum Schutz der Datensammlungen gegen unbefugte oder zufällige Vernichtung, zufälligen Verlust, technische Fehler, Fälschungen, Diebstahl oder widerrechtliche Verwendung und unbefugte Bearbeitung bestehen folgende Massnahmen:

- Datensicherungen
- Protokollierung
- Zugriffsschutz
- gesicherte Netzwerke
- externe Kommunikation (E-Mail, Internet) besonders schützenswerter Personendaten nur mit ausreichender Verschlüsselung
- Zutrittsbeschränkung zu Rechenzentrum, Netzwerken und anderen technischen Einrichtungen der Datenhaltung und Datenverarbeitung

3.2.2. Besondere Massnahmen

Zutrittskontrolle

Der Zutritt zu Gebäuden von Sanitas ist mit einem Badgesystem gesichert. Besucher müssen sich beim Empfang anmelden. Die Räume / Gebäude mit technischen Einrichtungen der Datenübertragung und Datenhaltung wie z.B. Server, Router, Switchs usw. sind mit Schliess- und / oder Zutrittssystemen gesichert und nur einem eingeschränkten Personenkreis zugänglich. Räume und Gebäude mit Clients, die Zugriff zu Datensammlungen ermöglichen, sind mit Zutrittssystemen gesichert.

Personendatenträgerkontrolle

Die Massnahmen der Zutrittsbeschränkung sowie der Zugriffsbeschränkung dienen auch der Personendatenträgerkontrolle. Durch technische Vorkehrungen ist es ausschliesslich befugten Personen möglich, Daten auf elektronischen Datenträgern zu bearbeiten.

Transportkontrolle

Unbefugten Personen ist das Lesen, Kopieren (auf andere Laufwerke oder Datenträger), Drucken, Verändern oder Entfernen von Datenträgern zu verunmöglichen.

Sensitive Informationen dürfen nicht in unchiffrierter Form via elektronische Post (E-Mail) versendet werden. Wo immer möglich, wird der nötige Datentransport von sensitiven Informationen elektronisch und mit einem anerkannten Verfahren verschlüsselt durchgeführt.

Der physische Datentransport wird mittels eines gesicherten Transportsystems durchgeführt, die Daten werden für den Transport mit einem anerkannten Verfahren verschlüsselt und der Schlüssel wird separat transportiert.

Bekanntgabekontrolle und Schnittstellenbeschreibung

Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, werden identifiziert und die Einhaltung der gesetzlichen Anforderungen für eine Bekanntgabe (gesetzliche Grundlage, Einverständniserklärung) sichergestellt. Datenübertragungen werden protokolliert und die Identität der Daten wird vor deren Übertragung geprüft.

Speicherkontrolle

Unbefugte Eingaben, Veränderungen oder Löschungen in den Speicher werden durch Zugangs- und Berechtigungskontrollen (z.B. Benutzername / Kennwort) sowie durch die IT-Anwendungen unterbunden. Beim Auswechseln von Datenspeichern (Festplatten) oder beim Ersatz von Computern (PC und Server) wird dafür gesorgt, dass sämtliche Daten unwiderruflich gelöscht werden.

Benutzerkontrolle

Der Zugriff auf Datenverarbeitungssysteme ist grundsätzlich durch technische Massnahmen geschützt und muss für den einzelnen Mitarbeitenden genehmigt werden. Das Informationssystem gewährt den Mitarbeitenden differenzierte Zugangsrechte. Der Zugriff der berechtigten Personen wird dabei auf diejenigen Daten beschränkt, welche die berechtigten Personen zur Erfüllung ihrer Aufgabe tatsächlich benötigen.

Zugriffskontrolle / Berechtigungen

Der Zugriff auf Daten der automatisierten Verarbeitung ist den Mitarbeitenden nur mittels IT-Anwendungen möglich. Die hierfür notwendigen Berechtigungen sind zu beantragen. Die Mitarbeitenden besitzen nur Benutzungsrechte für IT-Anwendungen, die sie zur Aufgabenerfüllung benötigen und innerhalb der IT-Anwendungen nur für Funktionsbereiche, die ihren Aufgaben entsprechen. 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.

Die interne Organisation legt für jeden Mitarbeitenden die Zugangsrechte über ein Zugriffskonzept fest. Je sensibler die Daten, die bearbeitet werden, desto höher sind die Anforderungen an die Autorisierung der Zugriffsberechtigten. Über die erteilten Berechtigungen wird eine Liste (Audit-Logfile) geführt.

Der Fernzugriff auf die Datenverarbeitungssysteme ist nur speziell autorisierten Personen über verschlüsselte Zugänge möglich.

Eingabekontrolle

Eingaben und Mutationen werden protokolliert. Soweit Daten automatisiert eingegeben oder mutiert werden – was hauptsächlich beim elektronischen Datenaustausch oder bei automatisierten Folgeverarbeitungen wie Zahlungsläufen usw. geschieht – wird grundsätzlich der Datenursprung und die Verarbeitungszeit protokolliert.

4. Datenbearbeitungsverfahren

4.1. Auskunftsrecht

Für die Gewährung der Einsichtsrechte von Versicherten in ihre eigenen Daten ist der Datenschutzberater der Sanitas zuständig. Dieser beschafft sich die Daten, erteilt die Auskunft und sorgt allenfalls für die Datenberichtigung gemäss intern definiertem Prozess.

Anfragen können schriftlich an folgende Adresse gerichtet werden:

Sanitas Krankenversicherung

Datenschutzberater

Jägergasse 3

8021 Zürich

4.2. Berichtigungsverfahren

Erfasste Personen können nach erfolgter Identifizierung verlangen, dass über sie erfasste Daten, die unverhältnismässig oder nicht zur Vertragsabwicklung erforderlich sind, berichtigt oder vernichtet werden. Der Datenschutzberater der Sanitas entscheidet über derartige Anträge.

4.3. Sperrung von Daten

Alle in einer Datensammlung erfassten Personen, können nach erfolgter Identifizierung verlangen, dass die Datenbearbeitung und insbesondere die Bekanntgabe ihrer Daten an Dritte, gesperrt wird. Der Datenschutzberater der Sanitas entscheidet über derartige Anträge und entscheidet über die Folgen der Umsetzung.

4.4. Anonymisierung

Tests und Projekte werden mit anonymisierten Daten durchgeführt. Statistische Daten werden gemäss den gesetzlichen Vorgaben anonymisiert. Ein Rückschluss auf konkrete Personen ist nicht möglich.

4.5. Archivierung

Daten werden gemäss den gesetzlichen Anforderungen und den betriebsinternen Weisungen aufbewahrt.

4.6. Backup / Restore

Für alle relevanten und so in den Verträgen definierten Daten werden regelmässige Datensicherungen durchgeführt. Die Datenbanken regelmässig in ein separates Verzeichnis kopiert und davon ein Backup erstellt. Die Wiederbeschaffung der Daten ist durch das Backup Systems sichergestellt.

4.7. Protokollierung

Definierte Importe (siehe Punkt «Schnittstellen») und Benutzeranmeldungen in Systemen, die eine Protokollierung zulassen werden protokolliert. Zur Kontrolle der Einhaltung der Nutzungsregelung kann Sanitas die Protokollierungen in anonymer Form auswerten. Wird ein Missbrauch festgestellt oder besteht ein Missbrauchsverdacht, kann Sanitas eine umfassende Nutzungsauswertung vornehmen. Die Protokolldaten werden während eines Jahres revisionsgerecht aufbewahrt.

4.8. Definition der Datensammlungen

Die Datensammlungen von Sanitas orientieren sich an den Geschäftsprozessen. Daraus ergeben sich folgende Datensammlungen:

Stamm- / Vertragsdaten

- Leistungsdaten
- Finanzdaten
- Offert- und Antragsdaten
- Regressfälle
- Betreuungsdossier
- Telefoniedaten
- Kostengutsprachen
- Vermittlerdaten

4.8.1. Schnittstellen

Die geschäftsrelevanten, externen Schnittstellenbeschreibungen beinhalten die Herkunft der Daten, den Adressaten, den Zweck, die Datenart und die Information, in welcher Periodizität und mittels welcher Art die Daten übermittelt werden.

In der Schnittstellenbeschreibung sind folgende Angaben zur Datenweitergabe (Bekanntgabe) festgehalten:

- Woher stammen die Daten?
- Wer erhält die Daten?
- Zu welchem Zweck werden die Daten weitergegeben?
- Welche Daten werden weitergegeben?
- In welcher Periodizität werden die Daten weitergegeben?
- Von wem wurde die Weitergabe initiiert?
- In welcher Form werden die Daten weitergegeben?

4.8.2. Prozesse

Daten werden von Sanitas nach definierten Prozessen erhoben, bearbeitet und weitergeleitet. Die einzelnen Prozesse sind in Prozessbeschreibungen festgehalten, die für den internen Gebrauch bestimmt sind.

4.8.3. Verantwortlichkeiten

- Datenschutz allgemein und Anfragen für Einsicht: Datenschutzberater Sanitas
- Technische Datensicherheit: Geschäftsbereich IT
- Vernichtung elektronischer Daten: Geschäftsbereich IT
- Unterlagen für den Vertrauensarzt: Vertrauensarzt
- Zugangskontrollen: Sicherheitsbeauftragter Sanitas

5. Schlussbestimmungen

5.1. Inkrafttreten

Dieses Reglement ersetzt alle vorher publizierten Reglemente Dieses Dokument tritt per 1.9.2023 in Kraft*.

5.2. Ergänzende Dokumente

- Bearbeitungsreglemente
- Verzeichnis der Bearbeitungstätigkeiten
- Zugriffskonzepte Datensammlungen

* Beschluss der Geschäftsleitung