Bearbeitungsreglement

Für die Datensammlungen nach KVG

Sanagate AG

Version 2.0

Inhaltsverzeichnis

Abkürzungsverzeichnis

Die folgenden Abkürzungen werden im Dokument verwendet:

Abkürzung	Beschreibung
Abs.	Absatz
Art.	Artikel
ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts vom 6. Oktober 2000, SR 830.1
BAG	Bundesamt für Gesundheit
bzw.	beziehungsweise
ca.	circa
DSB	Datenschutzbeauftragter der Sanagate/CSS
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992, SR 235.1
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
etc.	et cetera
inkl.	inklusive
IT	Informationstechnologie
IV	Invalidenversicherung
IV	Bundesgesetz über die Invalidenversicherung vom 19. Juni 1959, SR 831.20
KVG	Bundesgesetz über die Krankenversicherung vom 18. März 1994, SR 832.10
lit.	litera
SR	Systematische Sammlung des Bundesrechts
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0
usw.	und so weiter
UV	Unfallversicherung
UVG	Bundesgesetz über die Unfallversicherung vom 20. März 1981, SR 832.20
VA	Vertrauensarzt
VAD	Vertrauensärztlicher Dienst
VDSG	Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993, SR 235.11
VVG	Bundesgesetz über den Versicherungsvertrag vom 2. April 1908, SR 221.229.1
z.B.	zum Beispiel

1 Allgemeiner Teil

1.1 Einführung

1.1.1 Zusammenarbeit mit der CSS und Ausschlüsse

Die Sanagate AG verfügt nicht über eine eigene Informatik Abteilung. Diese Dienstleitung wird von der CSS bezogen. Alle nachfolgend in diesem Dokument beschriebenen Punkte zur IT (Logfiles, Systemauswertungen, etc.) werden von der CSS zur Verfügung gestellt und von der Sanagate AG übernommen resp. angewendet.

Die Sanagate AG verfügt nicht über ein eigenes Sicherheitsmanagement. Diese Dienstleistung wird von der CSS bezogen. Erstellte Weisungen, Richtlinien und Massnahmen werden der Sanagate AG zur Verfügung gestellt und - sofern notwendig - von der Sanagate übernommen.

Alle Weisungen und Richtlinien zu diesen Themen stehen konzernweit zur Verfügung und können im Intranet (Datenschutz/Recht/Sicherheit) eingesehen werden.

1.1.2 Ziel des Bearbeitungsreglements

Das Bearbeitungsreglement umschreibt die Datenverarbeitungs- und Kontrollverfahren und den Betrieb der elektronischen Datenverarbeitung.

Es enthält Angaben über das für den Datenschutz und die Datensicherheit verantwortliche Organ, über die Herkunft der Daten und die Zwecke, für welche sie regelmässig bekannt gegeben werden und beschreibt das Verfahren für die Erteilung der Zugriffsberechtigungen auf Daten.

1.1.3 Zweck und Umfang

Das Bearbeitungsreglement sorgt für die notwendige Transparenz im Umfeld sowohl der Systementwicklung als auch der Datenbearbeitung.

Art. 84 KVG bestimmt, dass die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung des Gesetzes betrauten Organe befugt sind, Personendaten, einschliesslich besonders schützenswerter Daten und Persönlichkeitsprofilen, zu bearbeiten, welche sie benötigen, um die ihnen nach dem Gesetz übertragenen Aufgaben zu erfüllen.

Im allgemeinen Teil des Bearbeitungsreglements werden die Grundsätze der Datenbearbeitung für alle Datensammlungen festgehalten. Für detailliertere Informationen zu den einzelnen Datensammlungen wird auf die einzelnen Bearbeitungsreglemente verwiesen.

1.1.4 Rechtliche Grundlagen

Gestützt auf Art. 11 und Art. 21 VDSG in Verbindung mit Art. 84 KVG und Art. 96 UVG hat die Sanagate AG für die automatisierten Datensammlungen, die besonders schützenswerte Daten oder Persönlichkeitsprofile beinhalten, das vorliegende Bearbeitungsreglement erstellt.

1.1.5 Aktualität der Bearbeitungsreglemente

Der allgemeine Teil des Bearbeitungsreglements sowie die einzelnen Bearbeitungsreglemente werden vom Inhaber der Datensammlung laufend nachgeführt, um insbesondere Systemänderungen sowie die Durchführung von Kontrollen in der Betriebsphase zu dokumentieren. In jedem Fall überprüft der Inhaber das Reglement jährlich auf seine Aktualität hin und teilt dem DSB allfällige Änderungen mit oder bestätigt die Aktualität. Der Inhaber der Datensammlung ist in der jeweiligen Datensammlung aufgeführt.

1.2 Anmeldung der Datensammlung beim EDÖB

Die Sanagate AG verfügt über einen internen Datenschutzbeauftragten, was sie von der Pflicht zur Anmeldung der Datensammlungen beim EDÖB befreit (Art. 11a Abs. 5 lit. e DSG und Art. 12a VDSG).

Die Sanagate AG erfüllt die Vorlage- und Zugangspflicht an den EDÖB gemäss Art. 84b KVG.

1.3 Schweigepflicht nach Art. 33 ATSG

Sämtliche Mitarbeitende der Sanagate AG unterstehen der Schweigepflicht nach Art. 33 ATSG.

Bei einer Verletzung der Schweigepflicht unterstehen die Mitarbeitenden den Strafbestimmungen nach Art. 92 KVG und Art. 97 UVG.

Die Mitarbeitenden sind über allfällige Sanktionen informiert und unterzeichnen mit Eintritt in das Unternehmen eine Geheimhaltungs- und Schweigepflichterklärung.

2 Benutzer und Datenzugriff

2.1 Benutzer

Zugriffsberechtigt auf das Informationssystem der Sanagate AG sind:

- Die Mitarbeitenden der Sanagate AG, soweit sie dies zur Ausübung ihrer Aufgaben benötigen
- Systemadministratoren der Sanagate AG

2.2 Benutzerverwaltung

Die Benutzerverwaltung wird zentral von der IT der Sanagate AG geführt.
Interne Mitarbeitende werden via HR-Schnittstelle und externe Mitarbeitende über das jeweilige Sourcing gemeldet. Neue Identitäten inkl. Accounts werden nur erfasst, wenn ein gültiger Arbeitsvertrag oder ein Dienstleistungsvertrag existiert.

2.3 Persönliche Zugriffsberechtigung

Mit dem Eintritt in die Sanagate AG erhält jeder Benutzer gemäss Rollenmodell, ableitend an seiner Funktion, seine Zugangsberechtigungen zu Informationen. Alle weiteren benötigten Rechte müssen individuell beantragt werden. Dabei gilt, dass jeder Antrag durch den direkten Vorgesetzten sowie, je nach Berechtigungsrolle, zusätzlich durch den Rollengenehmiger bestätigt werden muss.

2.4 Aufhebung der Zugriffsberechtigung

Die Mitarbeitenden sind nur so lange auf das Informationssystem zugriffsberechtigt, als sie die Daten für die Ausübung ihrer Arbeitsfunktion benötigen. Bei Austritt sowie bei Aufgabenwechseln innerhalb der Sanagate AG wird die Zugriffsberechtigung entzogen und die für den neuen Aufgabenbereich benötigten Zugriffsberechtigungen werden über das Rollenmodell neu zugewiesen.

2.5 Ausbildung der Benutzer

Die Benutzer des Informationssystems werden in verschiedenen Kursen auf die korrekte Benutzung der jeweiligen Applikationen geschult.

2.6 Benutzerhandbücher und Bearbeitungsrichtlinien

Zu jeder Applikation bestehen entsprechende Benutzerhandbücher. In Weisungen, Reglementen und Richtlinien wird die Datenbearbeitung festgelegt. Diese werden von der jeweils zuständigen Stelle regelmässig aktualisiert.

2.7 IT-Dienstleister

Soweit der Betrieb des Informationssystems der Sanagate AG an externe IT-Dienstleister ausgelagert ist, folgen diese in ihrem Bereich analogen Regelungen.

3 Datenschutz und die Datensicherheit

3.1 Datenschutz

Der Verwaltungsrat der CSS Gruppe trägt die Gesamtverantwortung für die Einhaltung des Datenschutzes. Er delegiert deren Umsetzung dem Geschäftsführer der Sanagate AG.

Der Geschäftsführer ist für die Umsetzung, Kommunikation, Kontrolle und Überwachung der vorgegebenen Datenschutzpolitik, bzw. des Datenschutzreglements in der Sanagate AG verantwortlich. Er stellt sicher, dass die Sanagate AG über eine effiziente Organisation verfügt, welche die Einhaltung des Datenschutzes unterstützt. Dazu schafft er insbesondere die Stelle eines Datenschutzbeauftragten, welcher seinerseits für die Umsetzung der Datenschutzvorgaben sorgt und stattet diesen mit den notwendigen personellen und finanziellen Ressourcen aus.

Die Sanagate AG hat einen Datenschutzbeauftragten bezeichnet. Dieser übernimmt und kommuniziert die in Zusammenarbeit zwischen dem DSB und der CSS, mit dem Sicherheitsmanagement und dem für die physische Sicherheit Beauftragten entsprechenden Richtlinien über die Einhaltung der Gesetze und Standards. Diese Richtlinien bezwecken vor allem die Schaffung einer optimalen Transparenz der automatisierten Bearbeitung von Personendaten, um eine fachgemässe Auswertung und Beurteilung allfälliger Datenschutzrisiken zu ermöglichen.

Alle Mitarbeitende sind in ihrem Zuständigkeitsbereich für die Einhaltung der Bearbeitungsreglemente, insbesondere der Auskunfts- sowie der Schweigepflicht verantwortlich. Die jeweiligen Vorgesetzten überprüfen dies periodisch und sorgen dafür, dass die Mitarbeitenden laufend über die geltenden gesetzlichen und internen Bestimmungen informiert werden. Dazu werden regelmässig Schulungen durchgeführt.

Zutritt zu Räumlichkeiten, in denen Daten bearbeitet werden, haben Mitarbeitende, welche in einem Anstellungsverhältnis zur CSS stehen. Dritte haben nur Zutritt, sofern sie eine Datenschutz- und Geheimhaltungserklärung unterzeichnet haben. Dieser Zutritt von Mitarbeitenden oder Dritten wird sowohl in räumlicher als auch in zeitlicher Hinsicht auf das notwendige Minimum beschränkt. Der Zutritt zum vertrauensärztlichen Dienst und zum Rechenzentrum untersteht zusätzlichen Restriktionen.

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

3.2 Datensicherheit

Die Sanagate AG übernimmt die zu diesem Thema erstellten Richtlinien und Weisungen der CSS. Darin wird für alle Arten von Daten (Personendaten, besonders schützenswerte Personendaten, gefährliche Daten) eine Sicherheitsstufe (gering, mittel, hoch, sehr hoch) definiert. Verantwortlich für die Einhaltung dieser Richtlinien über die Datensicherheit liegt beim jeweiligen Fachbereich.

Zum Schutz der Systeme sind generell Zugriffe nur möglich, indem die Autorisierung der zugreifenden Person mittels Benutzername/Kennwort überprüft wird. Clients und IT-Anwendungen mit Zugriff auf besonders schützenswerte Daten sind mit einer zeitlichen Beschränkung ausgerüstet, d.h. wenn ein Client oder eine IT-Anwendung eine gewisse Zeit lang nicht benutzt wird, so ist eine erneute Eingabe des Kennworts nötig.

4 Bearbeitung der Daten und Datenkategorien

4.1 Zweck der Datensammlungen

Die Datensammlungen bezwecken die ordentliche Durchführung der Kranken- und Unfallversicherung im Rahmen der gesetzlich zulässigen Datenbearbeitung (Art. 84 KVG und Art. 96 UVG).

4.2 Datenbeschaffung

Die Daten stammen hauptsächlich von den Versicherten selbst, von den von Versicherten ermächtigten Personen und Stellen (Leistungserbringer nach KVG/UVG, Versicherungen, Amtsstellen, etc.) sowie aus der Leistungsabwicklung, bearbeitet von Leistungserbringern oder Amtsstellen (z.B. Prämienverbilligungen).

Die Daten können aber auch im Rahmen der Amts- und Verwaltungshilfe erhoben werden (Art. 32 ATSG).

4.3 Datensammlungen

Folgende personenbezogene Datensammlungen bestehen:

- SHARK: Durchführen von Leistungsabrechnungen
- AVIS: Bestandesverwaltung
- VAD Anfragen: Ablage medizinischer Unterlagen für den VAD
- MedCase Pool: Bearbeitung von Leistungsanfragen VAD

4.4 Datenkategorien

In einem internen Tool sind die Datenkategorien der Datensammlungen der Sanagate AG aufgeführt.

4.5 Datenbekanntgabe

Daten werden für folgende Zwecke bekanntgegeben:

- Auskunfts- und Meldepflichten (Gerichte, Ämter, Behörden, etc.)
- Abklärung und Beurteilung eines Leistungsanspruchs des Versicherten
- Koordination mit Leistungen anderer Sozialversicherungen
- Regress
- IT-Dienstleister

Unter Datenempfänger fallen:

- Versicherte und von ihnen bevollmächtigte Dritte
- Leistungserbringer (Versicherten Online-Verfahren)
- Behörden (Kanton, BAG, IV-Stellen, etc.)
- Verband der Krankenversicherer santésuisse, Partnerversicherungen
- Rechtsdienst, Sozialdienste, Vertrauensärzte
- Dienstleistungserbringer im Bereich Datenverarbeitung (z.B. Wirtschaftsprüfer, Regress)

4.6 Weitere Datenbekanntgabe

Die weitere Datenbekanntgabe ist abschliessend in Art. 84a KVG und Art. 97 UVG geregelt.

4.7 Datenbearbeitung im Auftrag

Die Sanagate AG kann Teile des Informationssystems-Betriebes und die damit verbundene Datenbearbeitung an Dienstleister im In- und Ausland auslagern. Sie beachtet hierbei die geltenden datenschutzrechtlichen Voraussetzungen. Erfolgt ein Zugriff aus einem Land ohne angemessenen Datenschutz, wird ein angemessener Datenschutz vertraglich sichergestellt und der Zugriff soweit wie möglich auf Ausnahmefälle beschränkt.

5 Technische und organisatorische Massnahmen

5.1 Allgemeines

Zum Schutz der Datensammlungen gegen unbefugte oder zufällige Vernichtung, zufälligen Verlust, technische Fehler, Fälschungen, Diebstahl oder widerrechtliche Verwendung und unbefugte Bearbeitung bestehen verschiedene Massnahmen. Im Folgenden werden die einzelnen Massnahmen der Sanagate AG beschrieben.

5.2 Zugangskontrolle

Unbefugte Dritte dürfen ohne Berechtigung und Begleitung keinen Zugang zu Räumlichkeiten erhalten, in denen Personendaten bearbeitet werden.

Der Zutritt zu Gebäuden der Sanagate AG ist mit einem Badge-System gesichert. Besucher haben sich jeweils beim Empfang anzumelden, bevor sie das Gebäude betreten können.

Sämtliche Räumlichkeiten der Sanagate AG in denen besonders schützenswerte Personendaten bearbeitet werden, sind entweder elektronisch oder manuell vor dem Zugang unbefugter Personen gesichert. Die Arbeitsplätze sind vor dem Zutritt unbefugter Dritter geschützt. Über die Schlüsselverwaltung und die elektronische Zutrittskontrolle wird durch die Verantwortlichen Protokoll geführt. Der Beauftragte für die physische Sicherheit kann jederzeit Einblick oder Auswertungen verlangen.

Die Spezialräume und sensible Räume mit technischen Einrichtungen der Datenübertragung und Datenhaltung wie z.B. Server, Router, Switchs usw. sind mit erhöhten physischen Sicherheitsanforderungen (Schliesssystemen oder Zutrittssystemen) gesichert und ausschliesslich nur einem eingeschränkten berechtigten Personenkreis zugänglich.

Die elektronischen Datenträger in dezentralen Servern und Computern, welche nicht durch die IT der Sanagate AG betrieben werden, sind vergleichbaren Sicherheitsvorkehrungen unterstellt, wie diejenigen, welche durch diese selbst betrieben werden.

Die Räume und Gebäude mit Clients, welche Zugriff zu der Datensammlung erlauben, sind mit Zutrittssystemen gesichert.

5.3 Personendatenträgerkontrolle

Es ist sichergestellt, dass Datenträger, die Personendaten enthalten, von unbefugten Personen weder gelesen, kopiert, verändert noch gelöscht werden können.

Durch informationstechnische Vorkehrungen ist es ausschliesslich berechtigten Personen möglich, Daten auf den elektronischen Datenträgern zu bearbeiten. Nur berechtigte Personen erhalten Zugriff auf das Informationssystem der Sanagate AG.

Die Massnahmen der Zugangskontrolle und Benutzerkontrolle dienen auch der Personendatenträgerkontrolle.

5.4 Transportkontrolle

Unbefugten Personen ist das Lesen, Kopieren (auf andere Laufwerke oder Datenträger), Drucken, Verändern oder Entfernen von Datenträgern zu verunmöglichen. Die Vertraulichkeit ist mit einem Verschlüsselungsverfahren und gleichwertigen Massnahmen gewährleistet.

Sensitive Informationen dürfen nicht in unchiffrierter Form via elektronischer Post (E-Mail) oder Telefax 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.

5.5 Authentifizierung der Benutzer

Der Zugriff auf Applikationen des Informationssystems der Sanagate AG wird durch die User-ID kombiniert mit einem zeitlich befristeten individuellen Passwort geschützt.

5.6 Bekanntgabekontrolle und Schnittstellenbeschreibung

Es wird gewährleistet, dass sensible Daten ausschliesslich an den berechtigten Empfänger gelangen. Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, werden identifiziert und die gesetzlichen Anforderungen für eine Bekanntgabe (gesetzliche Grundlage, Einverständniserklärung) müssen erfüllt sein.

Datenübertragungen werden protokolliert und die Identität der Daten wird vor deren Übertragung geprüft.

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

- Von wem 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?
- Mit Hilfe welchen Mediums werden die Daten weitergegeben?

5.7 Übermittlung von Daten

Die Übermittlung von Daten zwischen den Datenendstationen und den Hostcomputern ist durch das Übertragungsprotokoll geschützt.

5.8 Speicherkontrolle

Unbefugte Eingabe, Veränderungen oder Löschungen in den Speicher werden durch Zugangs- und Berechtigungskontrolle (z.B. Benutzername und Kennwort) sowie durch die IT-Anwendungen unterbunden.

Zum Schutz der Personendaten vor Verlust werden regelmässig Sicherungskopien erstellt. Da die Sicherungs-Datenträger alle im System gespeicherten Daten enthalten, werden sie besonders gesichert.

Beim Auswechseln von Datenspeichern (Festplatten) oder beim Ersatz von Computern (PC und Server) wird dafür gesorgt, dass insbesondere die nicht chiffrierten Daten sowie der freie Speicherplatz vollständig physisch gelöscht werden. Das regelmässige Update von Betriebssystemen und Anwendungen minimiert Angriffe durch Malware.

5.9 Technische Anforderungen an Endgeräte

Der Zugang zum internen Netzwerk der Sanagate AG ist eingeschränkt, durch spezifische Kontrollmassnahmen geschützt und überwacht. Bei externen IT-Dienstleistern bestehen für deren Netzwerke analoge Vorkehrungen.

5.10 Benutzerkontrolle

Der Zugriff auf Datenverarbeitungssysteme ist durch technische Massnahmen (Firewall) unterbunden, sofern der Zugriff nicht für die Bearbeitung von Daten notwendig ist. Jeder einzelne Zugriff ist 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.

Datenverarbeitungssysteme, auf denen Gesundheitsdaten bearbeitet werden, werden ohne Verbindungen nach aussen betrieben.

5.11 Zugriffskontrolle

Der Zugriff auf Daten der automatisierten Verarbeitung ist den Mitarbeitenden nur mittels IT-Anwendungen möglich. Die hierfür notwendigen Berechtigungen sind von den Mitarbeitenden 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 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 jede Mitarbeiterin und jeden Mitarbeiter die Zugangsrechte fest. Dazu erarbeitet sie eine Zugangsrechtematrix.

Je sensibler die Daten, die bearbeitet werden, desto höher sind die Anforderungen an die Authentifizierung des oder der Zugriffsberechtigten. Über die erteilten Berechtigungen wird eine Liste (Audit-Logfile) geführt. Der

Fernzugriff auf die Datenverarbeitungssysteme ist nur speziell autorisierten Personen über stark verschlüsselte Zugänge mit Mehrfaktor-Authentisierung möglich.

Um zu verhindern, dass Unbefugte auf ein System mit Personendaten zugreifen, ist für die Benutzer ein Passwortschutz geboten. Das Passwort muss zwingend regelmässig geändert werden. Bildschirme sind so aufgestellt, dass sie nur von der berechtigten Person eingesehen werden können. Bei Abwesenheit der berechtigten Person wird der Computer gesperrt, so dass dieser nur mittels Passworteingabe wieder gestartet werden kann.

Physische Dokumente mit Personendaten werden in abschliessbaren Behältnissen verschlossen aufbewahrt, wobei nur die berechtigte Person Zugriff auf diese Dokumente hat (z.B. abschliessbare Schubladen) oder via Aktenvernichter entsorgt.

5.12 Eingabekontrolle

Alle 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 der Datenursprung und die Verarbeitungszeit protokolliert. Die Nachvollziehbarkeit kann dadurch gewährleistet werden.

Aufgrund dieser präventiven Protokollmassnahme erübrigt sich eine weitere umfassende Protokollierung im EDV-System.

5.13 Benutzerunterstützung und Meldepflicht

Die Benutzer werden fachlich durch die Vorgesetzten der jeweiligen Bereiche unterstützt.

Die technische Unterstützung für die Datenendgeräte und das Netzwerk wird durch die IT der Sanagate AG erbracht oder in Auftrag gegeben.

Die Benutzer sind über die Sicherheitseinstufung des Informationssystems der Sanagate AG und die Vorschriften im Umgang mit dem System und dessen Daten orientiert. Die Bestimmungen sind in Handbüchern und Weisungen beschrieben. Mögliche Sanktionen bei vorsätzlichen oder fahrlässigen Verletzungen der Informationssicherheit sind den Benutzern bekannt.

Sämtliche Benutzer sind verpflichtet, folgende Feststellungen dem Vorgesetzten zu melden:

- Fehler in den erfassten Daten. Fehler bei der Identität der registrierten Person.
- 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 Informationssicherheit haben können.

5.14 Aufsicht und Verantwortlichkeit

Die Vorgesetzten haben die Aufsicht und Verantwortung darüber, dass sich ihre Mitarbeitenden an die Weisungen, das Bearbeitungsreglement und seine Anhänge und die externen IT-Dienstleister an ihre vertraglichen Vorgaben halten.

6 Datenbearbeitungsverfahren (Art. 21 Abs. 2 lit. g VDSG)

6.1 Auskunftsrecht

Jede Person kann von der Sanagate AG Auskunft darüber verlangen, ob und welche Daten über sie bearbeitet werden. Das Auskunftsrecht richtet sich nach Art. 8 und 9 DSG sowie Art. 1 und 2 VDSG. Die Auskunftsgesuche sind schriftlich unter Beilage einer Kopie eines amtlichen Ausweises an die unten genannte Adresse einzureichen.

Für die Gewährung der Einsichtsrechte von Versicherten in ihre eigenen Daten ist der Datenschutzbeauftragten der Sanagate AG zuständig.

Dieser beschafft sich die Daten und erteilt die Auskunft und sorgt allenfalls für die Datenberichtigung.

Anfragen können an folgende Adresse gerichtet werden:

Sanagate AG
Datenschutzbeauftragter
Postfach 3866
CH-6002 Luzern
Schweiz

6.2 Berichtigungsverfahren

Die Berichtigungs- und Löschungsgesuche betroffener Personen richten sich nach Art. 5 Abs. 2 DSG und Art. 25 DSG.

Erfasste Personen können nach erfolgter Identifizierung verlangen, dass über sie erfasste Daten berichtigt oder vernichtet werden. Der Datenschutzbeauftragte der Sanagate AG entscheidet über derartige Anträge. Die Gesuche sind schriftlich an die obengenannte Adresse zu richten.

6.3 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 Datenschutzbeauftragte der Sanagate AG entscheidet über derartige Anträge. Die Gesuche sind schriftlich an die obengenannte Adresse zu richten.

6.4 Anonymisierung

Tests und Projekte erfolgen aufgrund generischer, nicht kundenbezogener Daten. Dies erlaubt es, auf eine eigene Testumgebung bzw. ein Testsystem, welches eine separate Anwendung als auch eine logisch getrennte Datenbank bzw. Datenbasis beinhaltet, zu verzichten. Statistische Daten werden den gesetzlichen Vorgaben entsprechend pseudonymisiert oder anonymisiert. Ein Rückschluss auf bestimmte Personen ist nicht möglich.

6.5 Archivierung

Archivierungspflichtige Dokumente werden während der gesetzlich verlangten Dauer archiviert und vor Veränderungen und unbefugten Zugriffen geschützt. Nach Ablauf der gesetzlichen Archivierungsfrist sind die Daten zu löschen.

Zu beachten sind die betriebsinternen Weisungen.

6.6 Backup/Restore

Die Datenbanken werden jede Nacht automatisiert in ein separates Verzeichnis kopiert und davon ein Backup erstellt.

Die Wiederbeschaffung der Daten ist innert zwei Tagen möglich. Dies entspricht der Stufe 1 in der Wiederbeschaffungsfrist.

6.7 Protokollierung

Sämtliche Importe und Benutzeranmeldungen werden protokolliert. Die Protokolldaten werden während eines Jahres revisionsgerecht aufbewahrt. Nach einem Jahr werden die Protokolle vernichtet.

7 Publikation

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

8 Wahrung berechtigter Interessen

Aus Gründen der Sicherheit von Systemen, Prozessen und Daten, der Wahrung der Vertraulichkeit der Versicherten sowie des Schutzes von Geschäftsgeheimnissen der Sanagate AG und ihren Geschäftspartnern, werden die in diesem Reglement erwähnten Beschreibungen der Datensammlungen nicht öffentlich zugänglich gemacht.

9 Version

Dieses Reglement wurde am 20.01.2017 letztmals überarbeitet.