CSS
Versicherung
Assurance
Assicurazione

Bearbeitungsreglement

für die Datensammlungen nach KVG

CSS Versicherung

Version 1.1 (aktualisiert am 30.11.2015)

Inhaltsverzeichnis

1. Einführung
1.1. Zweck und Umfang

Das Bearbeitungsreglement sorgt für die notwendige Transparenz im Umfeld sowohl der Systementwicklung als auch der Datenbearbeitung. Es ist in möglichst kurzer und verständlicher Form zu führen, so dass das Systementwicklung und Datenbearbeitung auch von "Nicht-Experten" verstanden bzw. beurteilt werden können. Es gilt dabei den Grundsatz "soviel wie nötig, und so wenig wie möglich", reglementarisch zu erfassen.

In diesem Bearbeitungsreglement werden die Grundsätze der Datenbearbeitung für alle Datensammlungen festgehalten.

1.2. Aktualität des Bearbeitungsreglements

Das Bearbeitungsreglement bzw. die Beschreibungen der Datensammlungen werden vom Datenowner laufend nachgeführt, um insbesondere Systemänderungen sowie die Durchführung von Kontrollen in der Betriebsphase zu dokumentieren. In jedem Fall überprüft der Inhaber das Reglement bzw. die Beschreibungen der Datensammlungen jährlich auf ihre Aktualität hin und teilt dem DSB allfällige Änderungen mit oder bestätigt die Aktualität.

1.3. Definitionen und Abkürzungen

Die folgenden Abkürzungen werden im Dokument verwendet:

Abkürzung	Beschreibung
DSB	Datenschutzbeauftragter der CSS Gruppe
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz, SR 235.1
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
KB	Konzernbereich
VDSG	Verordnung zum Bundesgesetz über den Datenschutz vom 23. Juni 1993, SR 235.11
KVG	Bundesgesetz vom 18. März 1994 über die Krankenversicherung, SR 832.10
IPV	Individuelle Prämienverbilligung
VA	Vertrauensarzt
VAD	Vertrauensärztlicher Dienst

2. Anmeldung der Datensammlung beim EDÖB

Die CSS verfügt über einen internen Datenschutzbeauftragten, was sie von der Pflicht zur Anmeldung der Datensammlungen beim EDÖB befreit (Art. 12a VDSG).

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

3. Datenschutz und die Datensicherheit
3.1. Datenschutz

Der Verwaltungsrat der CSS Gruppe trägt die Gesamtverantwortung für die Einhaltung des Datenschutzes. Er delegiert die Umsetzung einer geeigneten Organisation der Konzernleitung.

Die Konzernleitung ist für die Umsetzung, Kommunikation, Kontrolle und Überwachung der vorgegebenen Datenschutzpolitik, bzw. des Datenschutzreglements im gesamten CSS-Konzern verantwortlich. Sie stellt sicher, dass die CSS über eine effiziente Organisation verfügt, welche die Einhaltung des Datenschutzes unterstützt. Dazu schafft sie insbesondere die Stelle eines Datenschutzbeauftragten, welcher seinerseits für die Umsetzung der Datenschutzvorgaben sorgt und stattet diesen mit den notwendigen personellen und finanziellen Ressourcen aus.

Der Datenschutzbeauftragte des CSS Konzerns (DSB) gibt die wichtigsten Verhaltensweisen bezüglich Datenschutz vor und sorgt für die Einhaltung der auf die Unternehmen des CSS Konzerns 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 der automatisierten Bearbeitung von Personendaten, um eine fachgemässe Identifikation und Beurteilung allfälliger Datenschutzrisiken zu ermöglichen.

Für Datenschutzfragen ist ausserdem in jedem Konzernbereich eine Datenschutz-Ansprechperson bestimmt.

Alle Mitarbeitende sind in ihrem Zuständigkeitsbereich für die Einhaltung aller datenschutzrechtlichen Bestimmungen, insbesondere der Auskunfts- sowie der Schweigepflicht, verantwortlich. Weder Vorgesetzte noch Mitarbeitende können diese Verantwortung delegieren. Jeder Mitarbeiter der CSS hat bei der Anstellung eine Datenschutzverpflichtung zu unterzeichnen. Die jeweiligen Vorgesetzten überprüfen dies periodisch und sorgen dafür, dass die Mitarbeitenden laufend über die geltenden gesetzlichen und internen Bestimmungen informiert werden.

Dieses Bearbeitungsreglement regelt 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 die 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 sind zudem die Weisungen zum sicheren Umgang mit Hard- und Software und Internet und E-Mail massgebend.

3.2. Datensicherheit

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.

3.2.1. Allgemeine Massnahmen

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

Zugangskontrolle

Der Zutritt zu Gebäuden der CSS ist mit einem Badgesystem gesichert. Besucher haben sich jeweils beim Empfang anzumelden, bevor sie das Gebäude betreten können. Die Räume/Gebäude mit technischen Einrichtungen der Datenübertragung und Datenhaltung wie z.B. Server, Router, Switchs usw. sind mit Schliesssystemen oder Zutrittssystemen gesichert und nur einem eingeschränkten Personenkreis zugänglich.
Die Räume / Gebäude mit Clients, welche Zugriff zu Datensammlungen ermöglichen, sind mit Zutrittssystemen gesichert.

Personendatenträgerkontrolle

Die Massnahmen der Zutrittsbeschränkung sowie der Zugriffsbeschränkung dienen auch der Personendatenträgerkontrolle.

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) 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.

Bekanntgabekontrolle und Schnittstellenbeschreibung

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

Speicherkontrolle

Unbefugte Eingabe, Veränderungen oder Löschungen in den Speicher werden durch Zugangs- und Berechtigungskontrolle (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 insbesondere die nicht chiffrierten Daten sowie der freie Speicherplatz vollständig physisch gelöscht werden. Das regelmässige Update von Betriebssystemen und Anwendungen minimiert Angriffe durch Malware.

Benutzerkontrolle

Der Zugriff auf Datenverarbeitungssysteme ist grundsätzlich 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 Mitarbeiter für die einzelne Mitarbeiterin genehmigt werden. Das Informationssystem gewährt den Mitarbeiterinnen und Mitarbeiter differenzierte Zugangsrechte. Der Zugriff der berechtigten Personen wird dabei auf diejenigen Daten beschränkt, welche die berechtigten Personen zur Erfüllung ihrer Aufgabe tatsächlich benötigen.

Zugriffskontrolle

Der Zugriff auf Daten der automatisierten Verarbeitung ist den Mitarbeitern 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 und den Berechtigungseigentümer zu genehmigen. Die Berechtigungen sind den Mitarbeitern 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 verschlüsselte Zugänge mit Mehrfaktor-Authentisierung möglich.

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 grundsätzlich der Datenursprung und die Verarbeitungszeit protokolliert.

4. Datenbearbeitungsverfahren (Art. 21 Abs. 2 Bst g VDSG)

4.1. Auskunftsrecht

Für die Gewährung der Einsichtsrechte von Versicherten in ihre eigenen Daten ist der Datenschutzbeauftragte der CSS zuständig.
Dieser beschafft sich die Daten und erteilt die Auskunft und sorgt allenfalls für die Datenberichtigung gemäss intern definiertem Prozess.
Anfragen können mit Beilage einer Kopie eines amtlichen Ausweises an folgende Adresse gerichtet werden:

CSS Versicherung
Datenschutzbeauftragter
Tribschenstrasse 21
CH-6002 Luzern
Schweiz

4.2. Berichtigungsverfahren

Erfasste Personen können nach erfolgter Identifizierung verlangen, dass über sie erfasste Daten berichtigt oder vernichtet werden. Der Datenschutzbeauftragte der CSS 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 Datenschutzbeauftragte der CSS entscheidet über derartige Anträge.

4.4. Anonymisierung

Tests und Projekte erfolgen aufgrund generischer, nicht kundenbezogener Daten. Statistische Daten werden gemäss den gesetzlichen Vorgaben anonymisiert. Ein Rückschluss auf bestimmte Personen ist nicht möglich.

4.5. Archivierung

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

4.6. Backup/Restore

Die Datenbanken werden jede Nacht automatisiert in ein separates Verzeichnis kopiert und davon ein Backup erstellt.
Die Wiederbeschaffung der Daten ist dank des Backup Systems innert zwei Tagen möglich.

4.7. Protokollierung

Sämtliche Importe (siehe Punkt Schnittstellen) und Benutzeranmeldungen werden protokolliert. Zur Kontrolle der Einhaltung der Nutzungsregelung wertet die CSS die Protokollierungen in anonymer Form aus. Wird ein Missbrauch festgestellt oder besteht ein Missbrauchsverdacht, kann die CSS eine umfassende Nutzungsauswertung vornehmen.
Die Protokolldaten werden während eines Jahres revisionsgerecht aufbewahrt.

5. Definition der CSS Datensammlungen

Die Datensammlungen der CSS orientieren sich an den Geschäftsprozessen. Daraus ergeben sich folgende Datensammlungen:

- Antrag
- Besondere Bedingungen
- Betreibung
- Einzahlung
- Finanzabrechnung_Prämienabrechnung
- Finanzabrechnung_Provisionsabrechnung
- Kostengutsprachegesuch
- Kunde
- Kundendaten in der Finanzbuchhaltung
- Leisungsbeleg
- Leistungsbrechnung
- Leistungsformular
- Mahnung

- Medizinische Berichte
- Offerte
- Personenkonto
- Police
- Prämienverbilligung
- SAP HR
- VA-Daten
- Datenannahmestelle

Jede Datensammlung ist ausführlich beschrieben und dokumentiert.
Diese Beschreibungung enthalten insbesondere konkretisierende und ausführliche Aussagen zu folgenden Punkten:

- **Schnittstellen**

  Die Schnittstellenbeschreibung beinhaltet 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?

- **Berechtigungen**

  Jeder Mitarbeiter der CSS hat nur Zugriff auf diejenigen Daten, die er für seine Aufgabenerfüllung benötigt. Welche Organisationseinheiten dies im Falle jeder Datensammlung sind, wird detailliert beschrieben.

  In einem Berechtigungskonzept wird festgehalten, wie der Zugriff erfolgt, welche Berechtigungsprofile (Rollen) welche Funktionen ausüben können und auf welche Datenfelder zugegriffen werden kann.

- **Prozesse**

  Diese Dokumentation enthält eine ausführliche Beschreibung des Datenbearbeitungsprozesses.

6. Publikation

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

7. Wahrung berechtigter Interessen

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

8. Version

Dieses Reglement wurde am 30.11.2015 letztmals überarbeitet.