Reglement
über die Bearbeitung von Daten

Validierung und Änderungen

Name des Reglements	Genehmigt von:	Name und Funktion der für das Reglement zuständigen Person	Inkrafttreten	Version
Reglement über die Bearbeitung von Daten	Verwaltungsrat	Serge Husmann, Datenschutzverantwortlicher	1. Juli 2016	Dritte Fassung

Inhaltsverzeichnis

Mitteilung des Generaldirektors

Liebe Kollegin, lieber Kollege

Die Assura-Gruppe misst dem Aufbau und dem Erhalt einer auf gegenseitigem Vertrauen beruhenden Beziehung zu ihren Versicherten grösste Bedeutung zu. Wir erhalten deren schützenswerte Daten unmittelbar von ihnen oder von den Leistungserbringern zur Bearbeitung.

Unsere gesamte Organisation zielt darauf ab, diese Daten effizient zu bearbeiten und sie unter Wahrung ihres vertraulichen Charakters im Interesse der Versicherten angemessen zu schützen.

Die Einhaltung der gesetzlichen und reglementarischen Vorgaben, insbesondere des Bundesgesetzes über die Krankenversicherung und des Datenschutzgesetzes ist in diesem Zusammenhang von äusserster Wichtigkeit. Die Assura-Gruppe hat deshalb interne Vorschriften und Prozesse eingeführt, mit denen die vertrauliche Bearbeitung der Daten unserer Versicherten sichergestellt werden kann.

Ich bitte Sie, die Vorschriften und Grundsätze des vorliegenden Reglements sowie die sich daraus allenfalls ergebenden Weisungen und abteilungsspezifischen Instruktionen im Sinne eines wirksamen Schutzes der Daten unserer Versicherten zur Kenntnis zu nehmen und anzuwenden.

Freundliche Grüsse

Eric Bernheim, Generaldirektor

Einleitung

Auf Grundlage von Art. 21 VDSG und Art. 84*b* KVG erläutert das vorliegende Reglement die Bearbeitung von Daten, einschliesslich personenbezogener Daten, innerhalb der Organisation der im Organisationsreglement definierten Assura-Gruppe.

Des Weiteren legt es die Grundsätze fest, welche die Gesellschaften der Assura-Gruppe im Rahmen ihrer Tätigkeit bei der Sammlung, Bearbeitung, Weiterleitung und Vernichtung von Daten zu befolgen haben. In diesem Sinn steht das vorliegende Reglement gleichzeitig für die allgemeine Datenschutz- und Datensicherheitspolitik gemäss Kreisschreiben Nr. 7.1 des BAG vom 1. Juli 2013.

1. Rechtsgrundlage und Geltungsbereich

1.1 Rechtsgrundlage

Das vorliegende Reglement stützt sich namentlich auf das:

- Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG) und die dazu gehörende Verordnung (VDSG) vom 14. Juni 1993;
- Bundesgesetz vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) und die dazu gehörende Verordnung (ATSV) vom 11. September 2002;
- Bundesgesetz vom 18. März 1994 über die Krankenversicherung (KVG) und die dazu gehörende Verordnung (KVV) vom 27. Juni 1995;
- Bundesgesetz vom 2. April 1908 über den Versicherungsvertrag (VVG);

1.2 Zuständigkeit

Die Herausgabe des vorliegenden Reglements sowie allfällige nachträgliche Änderungen liegen in der Kompetenz des Verwaltungsrates.

1.3 Geltungsbereich

Das vorliegende Reglement ist auf alle Gesellschaften der Assura-Gruppe, deren Organisation im Organisationsreglement der Assura-Gruppe definiert ist, anwendbar und annulliert sämtliche früheren, dazu im Widerspruch stehenden Richtlinien und Bestimmungen.

Alle Mitarbeiterinnen und Mitarbeiter sind verpflichtet, das vorliegende Reglement zu befolgen.

2. Definitionen

Definition der im vorliegenden Reglement verwendeten Begriffe:

- **Daten**

Alle Informationen im weiteren Sinn über die Assura-Gruppe oder deren Gesellschaften, insbesondere über deren Organisation, Arbeitsabläufe und -prozesse, Entscheidungen sowie über deren Versicherte, Mitarbeitende und Bevollmächtigte.

- **Personendaten**

Jede Art von Information über eine bestimmte oder bestimmbare Person, im Allgemeinen über eine versicherte Person oder über Mitarbeitende der Assura-Gruppe.

- **Besonders schützenswerte Daten**

Alle personenbezogenen Daten über den gesundheitlichen Zustand, über religiöse, politische oder weltanschauliche Ansichten, über die finanzielle Lage sowie über administrative oder strafrechtliche Sanktionen und Verfolgungen.

- **Bearbeiten von Personendaten**

Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.

- **Datensammlung**

Sammlung von zumeist personenbezogenen Daten.

- **Inhaber der Daten oder einer Datensammlung**

Das Organ, die Abteilung oder die natürliche Person, die für die Führung der Datensammlung und den Zugang zu derselben verantwortlich ist.

- **Betroffene Personen**

Natürliche oder juristische Personen, über die personenbezogene Daten bearbeitet werden.

3. Allgemeine Grundsätze über das Bearbeiten von Personendaten

3.1 Rechtmässigkeit

Die Bearbeitung von Personendaten darf nur rechtmässig erfolgen, d.h. nicht im Widerspruch zum Gesetz stehen. Sie bedarf einer rechtlichen Grundlage oder der Zustimmung der betroffenen Personen.

3.2 Verhältnismässigkeit

Die Bearbeitung von Personendaten hat sich auf das Mass zu beschränken, das für den verfolgten Zweck objektiv erforderlich ist.

3.3 Treu und Glauben

Die Bearbeitung von Personendaten darf nur zu dem Zweck erfolgen, der den betroffenen Personen angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

3.4 Richtigkeit

Die bearbeiteten Personendaten müssen richtig sein und allenfalls berichtigt werden können. Die betroffene Person kann verlangen, dass falsche Daten berichtigt werden.

3.5 Zugang zu Personendaten

Mitarbeiterinnen und Mitarbeiter der Assura-Gruppe haben nur Zugang zu Personendaten, die zur Ausübung ihrer Arbeit erforderlich sind.

3.6 Übermittlung von Personendaten

Aufgrund der Organisation der Assura-Gruppe dürfen Personendaten bei Bedarf und auf vertraglicher oder gesetzlicher Grundlage von Dienstleistern der Gruppe, die denselben Regeln und Grundlagen unterstellt sind, bearbeitet werden.

Die Bearbeitung von Personendaten kann ferner unter denselben Bedingungen an Dritte übertragen werden, sofern keine gesetzliche oder vertragliche Geheimhaltungspflicht dies verbietet und die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun würde.

3.7 Sicherheit von Personendaten

Die Daten der Assura-Gruppe einschliesslich der Personendaten müssen gemäss deren Klassifizierung durch angemessene technische und organisatorische Massnahmen vor unbefugter Bearbeitung geschützt werden.

3.8 Strengere Vorschrift

Die Assura-Gruppe ist in mehreren Versicherungsbereichen aktiv. Bei widersprüchlichen Vorschriften im Zusammenhang mit dem Schutz der Personendaten wendet die Assura-Gruppe im Allgemeinen die strengere Vorschrift an. Im gegenteiligen Fall hat sie ihre Wahl schriftlich zu begründen.

3.9 Verschwiegenheitspflicht

Personen, die im Rahmen eines Arbeitsvertrages oder im Auftrag der Assura-Gruppe Personendaten bearbeiten, sind verpflichtet, Dritten gegenüber Verschwiegenheit zu bewahren. Die Verschwiegenheitspflicht gilt auch nach Beendigung der Vertragsbeziehung.

Ausnahmen werden bei entsprechender gesetzlicher Grundlage gewährt.

3.10 Ausbildung

Um zu gewährleisten, dass die Mitarbeitenden der Assura-Gruppe die Datenschutzbestimmungen befolgen, werden sie hinreichend zum Thema Datenschutz ausgebildet.

4. Bearbeitung von Personendaten (insb. gemäss Art. 84 KVG)

Die Gesellschaften der Assura-Gruppe bearbeiten Personendaten im Wesentlichen zu folgenden Zwecken:

- Überprüfung der Versicherungspflicht;
- Berechnung und Erhebung von Prämien und Ansprüchen auf Prämienverbilligungen;
- Erstellung, Berechnung, Koordinierung oder Gewährung von Versicherungsleistungen;
- Geltendmachung von Regressansprüchen gegenüber Dritten;
- Erstellen von Statistiken;
- Berechnung des Risikoausgleichs;
- Zuweisung oder Prüfung der AHV-Nummer;
- Umsetzung oder Beaufsichtigung der Einhaltung von Vorschriften;
- mit Zustimmung oder im Interesse der betroffenen Person zu weiteren Zwecken. Es kann sich dabei um ein finanzielles oder informationsbezogenes Interesse handeln. In solchen Situationen werden die spezifischen Anfragen der Versicherten soweit als möglich berücksichtigt.

5. Bekanntgabe von Personendaten (insb. gemäss Art. 84 *a* KVG)

Sofern kein überwiegendes Privatinteresse entgegensteht, dürfen Daten bekannt gegeben werden an:

- andere mit der Durchführung und der Kontrolle sowie der Beaufsichtigung des ATSG oder KVG betreuten Organe, wenn sie für die Erfüllung besagter Aufgaben erforderlich sind (Vermeidung von Versicherungslücken, Prüfung von Leistungsgesuchen, Ausübung des Beschwerderechts, Überprüfung der AHV-Nr., usw.);
- Kantonsbehörden, wenn sie zur Planung der Spitäler und Pflegeheime sowie zur Beurteilung der Tarife erforderlich sind;
- Organe für Bundesstatistik oder an andere Einrichtungen, die mit der Erhebung von anonymen Statistikdaten beauftrag werden;
- Behörden für Quellensteuer, gemäss Art. 88 und 100 des Bundesgesetzes vom 14. Dezember 1990 über die direkte Bundessteuer und der entsprechenden kantonalen Reglemente;
- Strafuntersuchungsbehörden, wenn die Anzeige oder Abwendung eines Verbrechens die Datenbekanntgabe erfordert;
- Sozialhilfebehörden, wenn sie zur Festsetzung, Änderung oder Rückerstattung von Leistungen beziehungsweise für die Verhinderung ungerechtfertigter Bezüge erforderlich sind;
- Zivilgerichte, wenn sie für die Beurteilung eines familien- oder erbrechtlichen Streitfalles erforderlich sind;
- Strafgerichte oder Strafuntersuchungsbehörden, wenn sie für die Abklärung eines Verbrechens oder eines Vergehens erforderlich sind;
- Betreibungsämter, gemäss Art. 91, 163 und 222 des Bundesgesetzes über Schuldbetreibung und Konkurs;
- Kinder- und Erwachsenenschutzbehörden nach Art. 448 ZGB;
- Sozialhilfebehörden oder an andere für Zahlungsausstände zuständige kantonale Stellen, wenn die versicherte Person fällige Prämien oder Kostenbeteiligungen nach erfolgloser Mahnung nicht bezahlen;
- andere Verwaltungs- oder Rechtsbehörden des Bundes, der Kantone, Bezirke oder Gemeinden im Rahmen der Amtshilfe;
- Drittpersonen, insbesondere an Vertragspartner, mit Zustimmung oder im Interesse der betroffenen Person oder zur Einhaltung von Vorschriften.

Die Daten werden grundsätzlich schriftlich und kostenlos mitgeteilt.

6. Allgemeine Massnahmen zur Gewährleistung des Datenschutzes

6.1 Physischer Datenzugang

Die Räumlichkeiten der Assura-Gruppe, in denen Daten einschliesslich Personendaten bearbeitet werden, werden mithilfe eines elektronischen Kontrollsystems (Badge) vor Eingriffen durch unbefugte Drittpersonen geschützt.

Die Zugangsrechte werden unter Berücksichtigung der Funktion der Mitarbeitenden mit Zugriffsprofilen verwaltet. Ausnahmen davon müssen begründet sein, beaufsichtigt und regelmässig kontrolliert werden.

Die Zugangsrechte zu den Räumlichkeiten der Assura-Gruppe werden durch den Dienst Sicherheit und Elektrizität (Informatikabteilung) erteilt und verwaltet und unterstehen der Verantwortung der jeweiligen Fachbereiche.

6.2 Zugang zu elektronischen Daten

Der Zugang zu den Informationssystemen der Assura-Gruppe ist nur mit einem Benutzernamen und einem Passwort mit beschränkter Geltungsdauer möglich.

Die Zugangsrechte zu den Informationssystemen werden gemäss Profilen, die von den Fachbereichen definiert werden, durch die Informatikabteilung zugewiesen und durch die Human Resources verwaltet. Ausnahmen davon müssen begründet sein, beaufsichtigt und regelmässig kontrolliert werden.

Der oder die Verantwortliche der Informatiksicherheit sorgt für die Umsetzung (s. Kap. 7.13 infra).

6.3 Clear Desk Policy

Vertrauliche Akten und Dokumente werden zugangssicher aufbewahrt (in geschlossenen Schreibtischen oder Schränken); auf den Schreibtischen dürfen sich nur Dokumente befinden, die zur Ausführung der pendenten Aufgaben erforderlich sind.

6.4 Datenträger

Einzig ordnungsgemäss berechtigte Personen dürfen Daten auf elektronischen Datenträgern bearbeiten.

6.5 Datentransport

Die Assura-Gruppe sorgt mit entsprechenden technischen Vorkehrungen dafür, dass es unbefugten Personen nicht möglich ist, Personendaten beim Übermitteln oder Transport zu lesen, zu kopieren, zu ändern oder zu löschen.

6.6 Datenklassifizierung

Die Daten der Assura-Gruppe einschliesslich der Personendaten werden in vier Stufen unterteilt und wie folgt geschützt:

6.6.1 Öffentliche Daten und Dokumente (Stufe 1)

Öffentliche Daten und Dokumente können unbegrenzt nach Aussen weitergeleitet werden.

Besondere Sicherheitsvorkehrungen, auch punkto Vernichtung, sind bei öffentlichen Daten und Dokumenten nicht notwendig.

6.6.2 Interne Daten und Dokumente (Stufe 2)

a. Definition

Die internen Daten und Dokumente sind nur für den Gebrauch innerhalb der Assura-Gruppe bestimmt. Mit Zustimmung des Verfassers des Dokuments oder des Inhabers der Daten können diese Daten in begrenztem und gezieltem Einsatz auch extern verwendet werden.

Die internen Daten und Dokumente enthalten keine besonders schützenswerten Personendaten.

b. Schutzmassnahmen

Die internen Daten und Dokumente müssen durch folgende Massnahmen vor unbefugten Zugriffen und unbefugter Bearbeitung geschützt werden:

- Allgemeine Massnahmen zur Gewährleistung des Datenschutzes (s. Kap. 6.1 bis 6.5 oben);
- Die Vernichtung von internen Daten und Dokumenten erfordert zudem ein besonderes, zentralisiertes Vorgehen (Deponieren der Dokumente in den zur Dokumentenvernichtung vorgesehenen Containern).

6.6.3 Vertrauliche Daten und Dokumente (Stufe 3)

a. Definition

Der Zugang zu vertraulichen Daten und deren Bearbeitung ist auch innerhalb der Assura-Gruppe begrenzt.

Personen, die Zugang zu diesen Daten und Dokumenten haben und diese bearbeiten, sind namentlich bekannt und befolgen die Grundsätze des vorliegenden Reglements.

Daten und Dokumente, deren Klassifizierung nicht feststeht, sind als vertraulich zu behandeln.

b. Schutzmassnahmen

Vertrauliche Daten und Dokumente müssen durch folgende Massnahmen vor unbefugten Zugriffen und unbefugter Bearbeitung geschützt werden:

- Massnahmen zum Schutz interner Daten und Dokumente (Stufe 2);
- Zugriffsschutz durch Benutzerprofil
- Im Allgemeinen Verschlüsselung der zu übertragenden elektronischen Daten;
- Verschlossene Umschläge mit Kennzeichnung "Vertraulich" bei interner Briefpost;
- Schutz der Dokumente in abschliessbaren Schränken;
- Vernichtung durch Aktenvernichter;
- Definitive Löschung obsoleter Datenträger;
- Überwachung und regelmässige Kontrolle der Zugangsrechte gemäss Benutzerprofil.

6.7 Streng vertrauliche oder geheime Daten und Dokumente (Stufe 4)

6.7.1 Definition

Daten und Dokumente dieser Art dürfen nur von bestimmten, namentlich bekannten Personen übermittelt werden. Sie werden an bestimmte, im Dokument namentlich erwähnte Personen übermittelt.

Der Versand von streng vertraulichen Daten per E-Mail ist streng zu begrenzen.

Die Liste der Personen, die im Besitz dieser Daten sind, ist beschränkt und namentlich bekannt und kann jederzeit ausgehändigt werden.

6.7.2 Schutzmassnahmen

Die streng vertraulichen oder geheimen Daten und Dokumente müssen durch folgende Massnahmen vor unbefugten Zugriffen und unbefugter Bearbeitung geschützt werden:

- Massnahmen zum Schutz von vertraulichen Daten und Dokumenten (Stufe 3)
- Zugriffsschutz ausschliesslich durch befugte Person;
- Je nach Fall Verwendung eines Passwortes zum Zugriffsschutz.

6.8 Aufbewahrung und Vernichtung von Daten

Die Aufbewahrungsdauer entspricht den spezifischen gesetzlichen Bestimmungen des schweizerischen Rechts.

Nach Ablauf der gesetzlichen Aufbewahrungspflicht hat jede Abteilung für die Vernichtung der Dokumente zu sorgen.

Eine Weisung legt die übliche Datenaufbewahrungsdauer fest.

7. Betroffene Abteilungen und Verantwortlichkeiten

7.1 Mitarbeitende

Alle Mitarbeitenden haben für die Umsetzung und Einhaltung des vorliegenden Reglements zu sorgen und sind verpflichtet, ihre gesetzliche (insb. Art. 32 ATSG, Art. 35 DSG) und arbeitsvertragliche Diskretions- und Verschwiegenheitspflicht jederzeit wahrzunehmen.

7.2 Geschäftsleitung

Die Geschäftsleitung der Assura-Gruppe ist für die Umsetzung einer datenschutzkonformen internen Organisation verantwortlich.

Sie wird dabei vom unternehmensinternen Datenschutzverantwortlichen unterstützt.

7.3 Kader

Alle Führungskräfte sind in ihrem Verantwortungs- und Zuständigkeitsbereich dafür verantwortlich, dass sie und ihre Mitarbeitenden die Anforderungen des Datenschutzes verstehen, umsetzen und einhalten.

Insbesondere stellen sie sicher, dass

- die Zugriffsberechtigungen ihrer Mitarbeitenden den Aufgaben entsprechend richtig definiert sind;
- ihre Mitarbeitenden den Inhalt und die Bedeutung des Datenschutzes kennen;
- die Einhaltung des Datenschutzes in ihrem Verantwortungsbereich regelmässig kontrolliert wird.

7.4 Inhaber der Daten

Die Bearbeitung von Daten einschliesslich Personendaten innerhalb der Assura-Gruppe ist inhabergebunden.

Nebst seiner Vertraulichkeitspflicht trägt der Inhaber einer Datensammlung die Verantwortung dafür, dass die Daten der richtigen Vertraulichkeitsstufe zugeordnet werden, dass die Klassifizierung

aktualisiert und den Betroffenen mitgeteilt wird. Er wendet die entsprechenden Schutzmassnahmen an und sorgt dafür, dass sie befolgt werden.

7.5 Datenschutzverantwortlicher

Die Assura-Gruppe ernennt einen unabhängigen Datenschutzverantwortlichen, der die interne Umsetzung der Datenschutzbestimmungen für Personendaten gewährleistet.

Der Datenschutzberater erfüllt insbesondere folgende Aufgaben:

- Er prüft, ob sämtliche Verträge und Projekte, die die Bearbeitung von Personendaten beinhalten, datenschutzkonform sind;
- Er führt ein Verzeichnis der Personendatensammlungen;
- Er sorgt dafür, dass das vorliegende Reglement regelmässig aktualisiert und innerhalb des Unternehmens befolgt wird;
- Er sorgt dafür, dass Gesuche um Akteneinsicht im Sinne von Art. 8 DSG fristgerecht und inhaltlich korrekt beantwortet werden;
- Er sorgt dafür, dass die Mitarbeitenden über die Einhaltung des Datenschutzes ausgebildet werden;
- Er amtet als Verbindungsstelle zum eidgenössischen Datenschutzbeauftragten;
- Er unterstützt die operativen Dienste bei der Planung und Umsetzung von Massnahmen im Bereich des Schutzes und der Sicherheit von Personendaten;
- Er informiert die Geschäftsleitung über seine Tätigkeit, empfiehlt erforderlichenfalls Korrekturmassnahmen und koordiniert deren Umsetzung.

7.6 Versicherungstechnik

Die Abteilung für Versicherungstechnik trägt die Verantwortung dafür, dass die Basisdaten der Versicherten geschützt sind, insbesondere beim Bei- oder Austritt und bei Änderungen (Anträge, Policen, Mutationen, Plattform « Kundenbereich », Gesundheitsfragebogen, usw.).

7.7 Leistungen

7.7.1 Allgemeine Verantwortlichkeit

Die Leistungsabteilung ist im Rahmen der Vergütung von Leistungen (Bearbeitung von Rechnungen, Leistungsabrechnungen, Austausch mit Leistungserbringern, Kostengutsprachen, usw.) für die Einhaltung des Datenschutzes verantwortlich.

7.7.2 Verantwortlichkeit im Rahmen von SwissDRG

Assura-Basis AG hat die Firma Centris AG in Solothurn mit der elektronischen Kontrolle der SwissDRG-Rechnungen beauftragt. Centris AG empfängt und prüft die von den Leistungserbringern übermittelten SwissDRG-Rechnungen. Rechnungen, die eine Besonderheit aufweisen, werden zur

gründlichen Überprüfung an die zertifizierte Datenannahmestelle der Assura-Basis AG weitergeleitet. Die Mitarbeitenden der Datenannahmestelle gehören einer unabhängigen Einheit, der DRG-Zelle, an und haben (als Hilfskräfte des Vertrauensarztes) punkto Vertraulichkeit besondere Pflichten. Die Leistungsabteilung sorgt dafür, dass einzig die zertifizierte Datenannahmestelle Zugang hat zu den medizinischen Auskünften, die von den Leistungserbringern übermittelt werden.

7.8 Vertrauensarzt

Der Vertrauensarzt ist gemeinsam mit dem Datenschutzberater dafür verantwortlich, dass innerhalb des vertrauensärztlichen Dienstes die medizinischen Versichertendaten geschützt sind (insb. Fragebögen, Berichte, Briefe an den Vertrauensarzt, MCD).

Der Vertrauensarzt trifft aufgrund der besonders schützenswerten Daten, die in seinem Dienst bearbeitet werden, zusätzliche Schutz- und Sicherheitsmassnahmen.

7.9 Finanzen

Die Finanzabteilung trägt die Verantwortung dafür, dass der Datenschutz bei der Erhebung der Prämien gewährleistet ist (Kundenkonten, Zahlungen, Korrespondenz und Auskünfte bei Betreibungsverfahren, Verlustscheine).

7.10 Marketing und Vertrieb

Die Abteilung Marketing und Vertrieb ist im Zusammenhang mit den Versicherungsagenten und den Daten, die die Versicherten den Agenten liefern, für die Einhaltung des Datenschutzes verantwortlich.

7.11 Human Resources

Die Abteilung Human Resources ist für den Schutz der Mitarbeitendendaten zuständig. Davon ausgeschlossen sind Daten, welche deren Status als Versicherte der Assura betreffen (z. B. Policen- und Leistungsbearbeitung).

Die Abteilung Human Resources sorgt bei Ein- oder Austritt eines Mitarbeitenden oder bei internem Stellenwechsel für eine gute Verwaltung der Datenzugriffsrechte.

Die Abteilung Human Resources sorgt gemeinsam mit dem Datenschutzverantwortlichen dafür, dass die Ausbildung der Mitarbeitenden zum Datenschutz richtig ausgeführt wird.

7.12 Informatik

Die Informatikabteilung trägt die Verantwortung für die Sicherheit der elektronischen Daten, die durch die verschiedenen Informationssysteme der Assura-Gruppe bearbeitet werden (Zugriff, Internet, E-Mail, usw.). Sie wird hierbei durch den Verantwortlichen für die Sicherheit der Informationssysteme unterstützt.

7.13 Verantwortlicher für die Sicherheit der Informationssysteme

Der Verantwortliche für die Sicherheit der Informationssysteme ist für die Direktion als auch für die Mitarbeitenden der Assura-Gruppe und für die Partner der wichtigste Ansprechpartner, namentlich bei der Definition der Regeln, Architektur, Prozesse und Produkte, die erforderlich sind, um die Sicherheit der Informationssysteme zu gewährleisten.

Seine Aufgaben sind in einer Weisung genauer definiert.

8. Rechte der betroffenen Person

Personen, über die Daten bearbeitet werden, können jederzeit anfragen, ob Daten über sie bearbeitet werden und diese gegebenenfalls einsehen und verlangen, dass allfällige falsche Daten berichtigt werden.

Die Einsicht von Daten darf nur verweigert werden, wenn ein öffentliches oder privates Interesse dagegen spricht.

Aus Vertraulichkeitsgründen dürfen die vom vertrauensärztlichen Dienst verwalteten Daten nur an den behandelnden Arzt bzw. an die behandelnde Ärztin der versicherten Person oder an eine/n andere/n vom Versicherten bezeichneten Arzt bzw. Ärztin weitergeleitet werden.

Die Auskünfte werden im Allgemeinen schriftlich und kostenlos erteilt, ausser wenn die Gewährung der Akteneinsicht mit einem besonders grossen Arbeitsaufwand verbunden ist.

Diese Art von Auskünften müssen an den Datenschutzverantwortlichen der Assura-Gruppe gerichtet werden.

9. Inkrafttreten

Das vorliegende Reglement tritt am 1. Dezember 2014 in Kraft.

Die Änderungen vom 27. Mai 2016 treten per 1. Juli 2016 in Kraft.

Unterschriften Verwaltungsrat:

Name	**Unterschrift**
Jean-Luc Chenaux, Präsident	Sig.
Vincent Hort, Generalsekretär	Sig.

Pully, 27. Mai 2016