Bearbeitungsreglement
Ausgabe 2023

Inhaltsverzeichnis

1 Allgemeine Bestimmungen

1.1 Rechtliche Grundlage

Gestützt auf Art. 6 Datenschutzverordnung (DSV) in Verbindung mit Art. 84b des Bundesgesetzes über die Krankenversicherung (KVG) hat Aquilana Versicherungen (Aquilana) für die automatisierten Datenbearbeitungen das vorliegende Bearbeitungsreglement (Reglement) erstellt. Die nachfolgenden Bestimmungen gelten sinngemäss auch für den Bereich der von Aquilana angebotenen Zusatzversicherungen.

1.2 Ziel des Bearbeitungsreglements

Das Bearbeitungsreglement umschreibt insbesondere die Datenbearbeitungs- und Kontrollverfahren sowie den Betrieb der elektronischen Datenbearbeitung. 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 die entsprechenden Informationssysteme und automatisierten Datenbearbeitungen.

1.3 Zweck der Datenbearbeitung

Der Zweck der Datenbearbeitung ist in Art. 84 KVG geregelt. Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung des Gesetzes beauftragten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten (Art. 5 lit. c Bundesgesetz über den Datenschutz [DSG]), zu bearbeiten, um die ihnen nach dem Gesetz übertragenen Aufgaben zu erfüllen.

1.4 Verantwortliche Stelle

Aquilana ist verantwortlich für die Abwicklung der Krankenversicherung und somit Inhaberin der Datensammlungen. Mit den im Reglement vorgesehenen Massnahmen sorgt Aquilana für die Einhaltung der gesetzlichen Vorschriften.

1.5 Definition automatisierte Datenbearbeitung

Bundesorgane und deren Auftragsbearbeiter – auch private – haben bei einer automatisierten Datenbearbeitung ein Bearbeitungsreglement zu erstellen, wenn sie

- besonders schützenswerte Personendaten bearbeiten (Art. 6 Abs. 1 lit. a DSV);
- ein Profiling durchführen (Art. 6 Abs. 1 lit. b DSV);
- bei möglichem schwerwiegendem Eingriff in die Grundrechte betroffener Personen (Art. 34 Abs. 2 lit. c DSG) (Art. 6 Abs. 1 lit. c DSV);
- beim Zugriff von anderen Behörden (Kantone, ausländische Behörden, internationalen Organisationen) oder privaten Personen (Art. 6 Abs. 1 lit. d DSV);
- bei der Verknüpfung verschiedener Datenbestände (Art. 6 Abs. 1 lit. e DSV);
- bei einem gemeinsamen Informationssystem oder gemeinsamer Bewirtschaftung von Datenbeständen mit anderen Bundesorganen (Art. 6 Abs. 1 lit. f DSV)

Die Datenbearbeitungen sind automatisiert, wenn sie computergestützt erfolgen.

1.6 Richtlinie Datenschutz und Datensicherheit

Die Richtlinie Datenschutz und Datensicherheit (Richtlinie) bzw. die entsprechende Datenschutz- und Datensicherheitserklärung wird bei Stellenantritt durch die Mitarbeitenden unterzeichnet. Die Richtlinie ergänzt Ziffer 1.7 Datenschutz der Allgemeinen Arbeitsvertrags-Bedingungen der Aquilana. Anlässlich von periodischen Schulungen werden die Mitarbeitenden über die Entwicklung im Datenschutzbereich informiert und sensibilisiert. Die Mitarbeitenden sind in ihrer Funktion für die Schaffung der notwendigen und angemessenen Rahmenbedingungen für den Datenschutz und die Datensicherheit verantwortlich.

1.7 Schweigepflicht nach Art. 33 ATSG und Art. 62 DSG

Sämtliche Mitarbeitenden unterstehen während und über das Arbeitsverhältnis hinaus der Schweigepflicht nach Art. 33 des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) und Art. 62 DSG. Die Schweigepflicht bildet Bestandteil der unter Ziffer 1.6 erwähnten Richtlinie.

2. EDV-Struktur

2.1 Übersicht

Aquilana arbeitet auf dem System Syrius ASE, welches vom externen IT-Partner, Centris AG, betreut wird. Auf Syrius ASE werden die versicherungsrelevanten Daten bearbeitet:

- Vertragsdaten (Vorname, Name, Geburtsdatum, Versicherten-Nr., Adresse, Versichertendeckung, Versichertenkarte usw.)
- Leistungsverarbeitung (für die Abrechnung nötige Leistungsdaten)
- Spezialfälle Leistungsverarbeitung (Taggeld, Auslandrechnungen, Regress)
- Inkasso, Mahnwesen
- Archiv

2.2 Schnittstellen

Verschiedene Schnittstellen ergeben sich aufgrund von Subsystemen, welche zum Teil durch gesetzliche Vorgaben bedingt sind. So wird der vertrauensärztliche Dienst (VAD), die DRG-Prüfstelle (Diagnosis Related Groups, dianosebezogene Fallgruppen) und das Case Management (Fallmanagement) vom externen Partner RVK (Verband der kleinen und mittleren Krankenkassen) betreut. Als zertifizierte Datenannahmestelle (DAS) nutzt Aquilana den zertifizierten DAS-IT-Service der Centris AG.

Die Zusammenarbeit mit der Sasis AG, einer Tochtergesellschaft von Santésuisse (Verband der schweizerischen Krankenversicherer im Bereich der sozialen Krankenversicherung) findet im Bereich der Kartenproduktion, von statistischen Auswertungen und künftig zur elektronischen Abwicklung des Ein- und Austrittverfahrens statt.

Das Inkassoverfahren ab Stufe Betreibung wird auf dem internen System debit4you weiter verarbeitet. Die dafür notwendigen Daten werden von Syrius ASE mittels Schnittstelle überspielt.

Externe Partner unterstützen Aquilana ausserdem bei der elektronischen Rechnungsverarbeitung, bei der Datenarchivierung und –vernichtung, bei Behandlungen im Ausland (Notrufzentrale), Aktuariat, Rechts-dienst, Bankgeschäften und Kommunikation.

Authentifizierung, Verschlüsselungs- und Übertragungstechnologien sowie ein periodischer externer IT-Security-Check sind Massnahmen, um die Einhaltung des Datenschutzes und der Datensicherheit in Bezug auf die Schnittstellen sicherzustellen.

2.3 Outsourcing

Voraussetzung für die Übertragung der Bearbeitung von Personendaten an externe Partner ist, dass die Daten so bearbeitet werden, wie Aquilana das selbst tun würde und die Übertragung durch keine Geheimhaltungspflicht verboten ist. Diese Partner bestätigen mit Vertragsunterzeichnung die Einhaltung der Datenschutzbestimmungen für sich und ihre Hilfspersonen.

2.4 IT-Infrastruktur

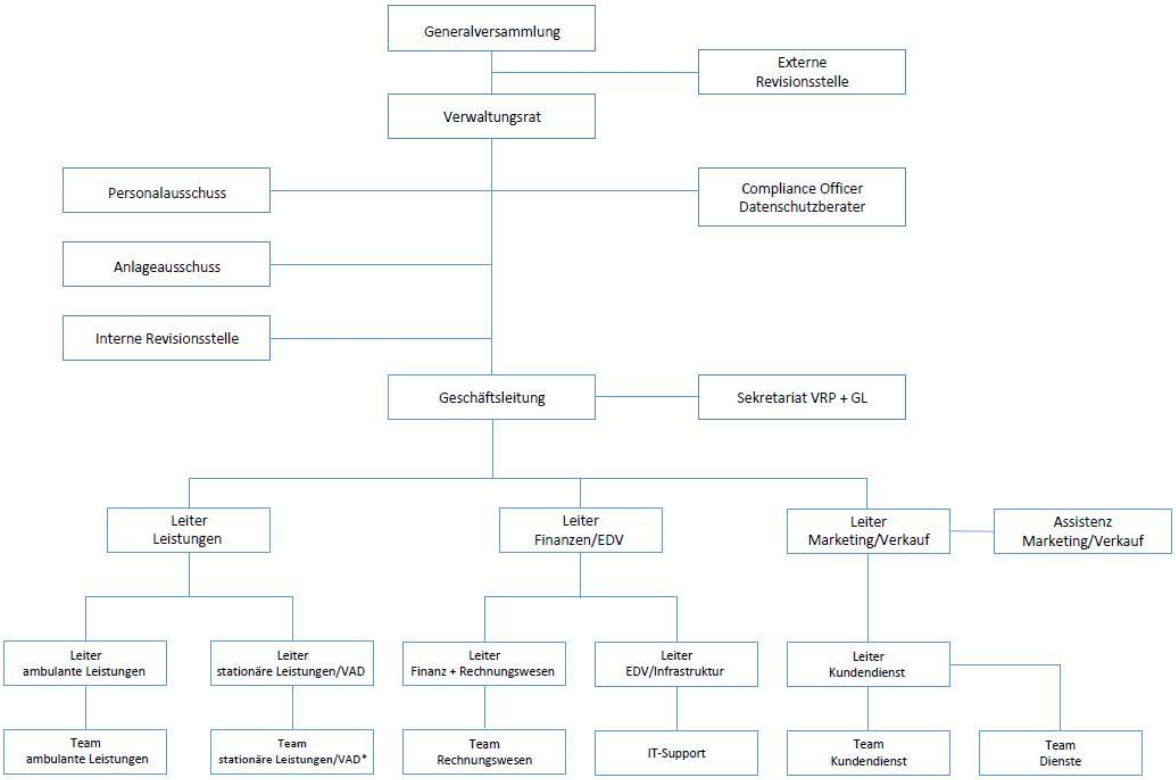
Sowohl die Firewall als auch das Antivirus-Programm werden regelmässig automatisch aktualisiert.

3. Organisation

3.1 Geschäftsstellen, Filialen

Aquilana bedient Ihre Kunden aus der ganzen Schweiz und acht EU-Staaten vom Geschäftssitz in Baden aus. Sie führt weder weitere Geschäftsstellen noch Filialen.

3.2 Organisationsstruktur



Aquilana ist in drei Bereiche aufgeteilt:

- Leistungen
- Finanzen / EDV
- Marketing / Verkauf

Die drei Bereichsleiter bilden zusammen mit dem Geschäftsführer die Geschäftsleitung.

* In Funktion als Hilfsperson des Vertrauensarztes dem VAD unterstellt. Leiter Leistungen ohne Weisungsbefugnis.

4. Benutzer und Datenzugriff

4.1 Benutzer

Abhängig von Funktion und Rolle, die ein Mitarbeitender wahrnimmt, wird die Zugriffsberechtigung (Einsichts- und/oder Mutationsrecht) erteilt und dokumentiert. Für Wartung und Problemlösung erhält der IT-Outsourcing-Partner Zugriff auf die betroffenen IT-Systeme.

4.2 Benutzerverwaltung

Die Benutzerverwaltung erfolgt zentral durch den internen IT-Koordinator. Die Geschäftsleitung ist für die Definition der IT-Zugriffsrechte der einzelnen Mitarbeitenden zuständig.

4.3 Aufhebung der Zugriffsberechtigung

Die Benutzer sind so lange und in dem Umfang zugriffsberechtigt, als sie die Daten für die Ausübung ihrer Arbeitsfunktion benötigen. Bei Austritt sowie bei Aufgabenwechsel innerhalb der Aquilana wird die Zugriffsberechtigung entzogen und die für den neuen Aufgabenbereich benötigten Zugriffsberechtigungen werden neu zugewiesen.

4.4 Ausbildung der Benutzer

Die Benutzer werden auf Syrius ASE und den übrigen, für den Betrieb notwendigen Applikationen intern und extern geschult.

4.5 Prozessabläufe, interne Richtlinien

Die Arbeitsprozesse werden im Management-Informations-System „Toolbox“ von Swiss GRC abgebildet und umschrieben. Ebenso sind die internen Richtlinien über dieses System abrufbar.
Die Beschreibung des Anwendungsbereiches und die technischen Abgrenzungen werden in den Richtlinien Bearbeitungsreglement SwissDRG (elektronische Daten) und im Bearbeitungsreglement SwissDRG (Papierprozess) dargestellt.

5. Bearbeiten von Daten

5.1 Datenbeschaffung

Die Daten stammen in erster Linie von den Versicherten selbst sowie von den von Versicherten ermächtigten Personen und Stellen (Leistungserbringer, Versicherungen, Amtsstellen usw.), aus der Leistungsabwicklung von Leistungserbringern sowie von Amtsstellen (z.B. Prämienverbilligungen, Asylwesen).

5.2 Datenkategorien

Es werden folgende wesentlichen Datenkategorien im System geführt:

- Name, Vorname
- Adresse
- Nationalität
- Sprache
- Sozialversicherungs-Nr.
- Versicherten Nr. (Partner Nr.)
- Zahladressen

- Vertragsdaten
- Leistungsdaten
- Prämiendaten
- Mahndaten

5.3 Bekanntgabe von Daten an Dritte

Eine Bekanntgabe von Daten an Dritte ist gemäss Art. 84a in Verbindung mit Art. 84 KVG nur erlaubt, wenn diese aus rechtlichen Gründen einen Anspruch auf diese Daten haben (z.B. Behörden, Gerichte) oder eine entsprechende schriftliche Einwilligung des Betroffenen vorliegt. Nach der Übertragung ist der Dritte als Datenempfänger für den Datenschutz und die Datensicherheit verantwortlich.

Daten können insbesondere bekannt gegeben werden für die Datenbearbeitung zur:

- Einhaltung der Versicherungspflicht
- Beurteilung der Leistungsansprüche
- Verhinderung ungerechtfertigter Bezüge
- Koordination mit Leistungen anderer Sozialversicherer
- Geltendmachung eines Rückgriffrechts gegenüber haftpflichtigen Dritten
- Führen von Statistiken
- Zuweisung oder Verifikation der Sozialversicherungsnummer.

5.4 Datenschutzberater

Aquilana verfügt über einen betrieblichen Datenschutzberater, der die Einhaltung des Datenschutzes prüft und Korrekturmassnahmen empfiehlt, den Verwaltungsrat, die Geschäftsleitung und Mitarbeitenden berät und sie bei der operativen Umsetzung des Datenschutzes im Betrieb unterstützt.

6. Archivierung und Vernichtung

6.1 Aufbewahrungspflicht und Wiederherstellung

Für die Aufbewahrung von Geschäftsunterlagen gilt grundsätzlich die gesetzliche Aufbewahrungsfrist von 10 Jahren (Art. 958f Abs. 1 Obligationenrecht [OR]). Werden die Geschäftsunterlagen in elektronischer oder vergleichbarer Weise aufbewahrt, so müssen sie jederzeit wieder lesbar gemacht werden können (Art. 958f Abs. 3 OR).

6.2 Vernichtung physisch vorhandener Daten

Bei der Vernichtung von vertraulichen oder besonders schützenswerten Daten in physischer Form muss der Datenschutz gewährleistet sein, d.h. die Unterlagen dürfen nicht in öffentlich zugänglichen Behältern der Vernichtung zugeführt werden.

6.3 Vernichtung elektronisch gespeicherter Daten

Elektronische Datenträger müssen vor der Vernichtung unlesbar gemacht werden oder die Vernichtung durch ein für die Entsorgung von elektronischen Datenträgern zertifiziertes Unternehmen erfolgen. Die elektronisch gespeicherten Daten werden nach Ablauf der Aufbewahrungspflicht mit Spezialprogrammen endgültig gelöscht.

7. Technische und organisatorische Massnahmen

7.1 Zutrittskontrolle

Der Zugang zu den Räumlichkeiten der Aquilana ist nur mit Schlüssel möglich. Damit ist der direkte Zutritt durch Dritte, mit Ausnahme des Schalterbereichs, nicht möglich. Zu Räumen mit erhöhten Datensicherheitsbedürfnissen (z.B. Serverraum) hat nur ein eingeschränkter Kreis von Mitarbeitenden Zugang. Ausserhalb der Arbeitszeiten werden die Büros abgeschlossen. Ergänzend gilt die Clear Desk Policy.

Das allgemeine Archiv ist nur eingeschränkt den Mitarbeitenden von Aquilana zugänglich. Vertrauliche Unterlagen, wie jene des Verwaltungsrates, der Geschäftsleitung und des Vertrauensärztlichen Dienstes, werden separat im GL-Archiv archiviert und der Zugang ist jeweils nur den verantwortlichen Mitarbeitenden möglich.

7.2 Authentifizierung der Benutzer

Um auf Daten und Programme zuzugreifen muss sich der Mitarbeitende mittels Passwort identifizieren. Der Zugriff auf die Daten durch einen eingeschränkten Kreis von Mitarbeitenden von ausserhalb der Organisation erfolgt mittels einer zweistufigen Authentifizierung über verschlüsselte Leitungen.

7.3 Zusammenarbeit mit Partnern

Der Austausch von besonders schützenswerten Daten mit unseren externen Partnern erfolgt in einem geschützten Bereich.

8. Rechte der Betroffenen

8.1 Informationspflicht beim Beschaffen von Personendaten

Art. 19 DSG und Art. 13 DSV verlangen die Information der betroffenen Person, wenn Personendaten beschafft werden. Aufgrund des gesetzlichen Auftrages nach KVG zur Bearbeitung von Gesundheitsdaten gilt die Ausnahmeregelung nach Art. 20 Abs. 1 lit. b DSG, wonach die Informationspflicht des Verantwortlichen entfällt, wenn die Bearbeitung gesetzlich vorgesehen ist.

8.2 Auskunftsrecht nach Art. 25 DSG

Jede Person kann von Aquilana schriftlich Auskunft darüber verlangen, ob Daten über sie bearbeitet werden. Das Auskunftsrecht richtet sich nach Art. 25 und 26 DSG sowie und Art. 16 ff. DSV. Die Auskunftsgesuche sind unter Beilage der Kopie eines amtlichen Ausweises an Aquilana Versicherungen, z.H. Datenschutzberater, Bruggerstrasse 46, 5400 Baden, zu richten.

8.3 Berichtigungs- und Löschungsrechte

Die betroffenen Personen können gemäss Art. 6 Abs. 5 DSG verlangen, dass ihre Daten berichtigt, vernichtet oder die Bekanntgabe an Dritte gesperrt werden. Die entsprechenden Gesuche sind an Aquilana Versicherungen, z.H. Datenschutzberater, Bruggerstrasse 46, 5400 Baden, zu richten.

8.4 Recht auf Datenherausgabe und -übertragung

Jede Person kann vom Verantwortlichen die Herausgabe ihrer Personendaten, die sie ihm bekanntgegeben hat, in einem gängigen elektronischen Format verlangen, wenn:

a. der Verantwortliche die Daten automatisiert bearbeitet; und

b. die Daten mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages zwischen dem Verantwortlichen und der betroffenen Person bearbeitet werden.

Die betroffene Person kann zudem vom Verantwortlichen verlangen, dass er ihre Personendaten einem anderen Verantwortlichen überträgt, wenn die gesetzlichen Voraussetzungen erfüllt sind und dies keinen unverhältnismässigen Aufwand erfordert.

Das Recht auf Datenherausgabe und -übertragung richtet sich nach Art. 28 und 29 DSG sowie und Art. 20 ff. DSV. Die Gesuche sind unter Beilage der Kopie eines amtlichen Ausweises an Aquilana Versicherungen, z.H. Datenschutzberater, Bruggerstrasse 46, 5400 Baden, zu richten.

9. Abschliessende Bestimmungen

9.1 Änderungen des Reglements

Das Bearbeitungsreglement wird in Ergänzung zur Richtlinie Datenschutz und Datensicherheit sowie dem Archivierungs-Reglement vom Verantwortlichen regelmässig aktualisiert. Dieses Reglement kann jederzeit geändert werden. Änderungen bedürfen der Schriftform und der Zustimmung der Geschäftsleitung. Die Verantwortung für die Aktualisierung trägt der Datenschutzberater der Aquilana. Die aktualisierte Version des Bearbeitungsreglements wird dem EDÖB zugestellt (Art. 84b KVG).

9.2 Inkrafttreten

Dieses Reglement wurde anlässlich der Geschäftsleitungssitzung vom 14. August 2023 genehmigt und tritt per 1. September 2023 in Kraft. Es ersetzt das Bearbeitungsreglement Ausgabe 2021.

Aquilana Versicherungen

Werner Stoller
Geschäftsführer

Marc Rothe
Datenschutzberater