1. Corporate Governance

Datenschutzreglement der Assura-Gruppe

Inhaltsverzeichnis

1. Zweck und Anwendungsbereich

1.1 Ziel

1.1.1 Ziel dieses Reglements ist die Festlegung der allgemeinen Politik der Assura-Gruppe für Datenschutz und Datensicherheit.

1.1.2 Es legt die Grundsätze und geltenden Regeln fest, die von den im Organisationsreglement der Assura-Gruppe definierten Gesellschaften der Assura-Gruppe und deren Mitarbeitenden zu befolgen sind, wenn diese Daten von potentiellen Kunden, versicherten Personen, sich Bewerbenden und Mitarbeitenden der Assura-Gruppe, von Dritten (wie Leistungserbringern und Versicherungsvermittlern) und Auftragsbearbeitern bearbeiten.

1.1.3 Die nachstehend aufgeführten Grundsätze und Regeln müssen insbesondere dazu dienen, die gesetzlichen Vorgaben zu erfüllen (insbesondere die des Bundesgesetzes über den Datenschutz (DSG) über die Bearbeitung personenbezogener Daten, seine Ausführungsbestimmungen (DSV und VDSZ)) sowie die regulatorischen Anforderungen der Aufsichtsbehörden.

1.2 Geltungsbereich

1.2.1 Das vorliegende Reglement ist auf alle im Organisationsreglement der Assura-Gruppe definierten Gesellschaften der Assura-Gruppe anwendbar.

1.2.2 Gemäss DSG ist zu unterscheiden zwischen (natürlichen und juristischen) privaten Personen wie der Figeas AG, der Assura AG und Versicherungsvermittlern einerseits sowie andererseits Bundesorganen wie der Assura-Basis AG, soweit gewisse spezifische Regeln auf diese anwendbar sind.

1.2.3 Davon betroffen sind sämtliche Daten, die Mitarbeitende, die Geschäftsleitung oder der Verwaltungsrat in Ausübung ihrer Funktion bearbeiten.

1.2.4 Das Reglement ist auch auf im Ausland bearbeitete Daten anwendbar, sobald diese Wirkung in der Schweiz entfalten.

1.2.5 Die Herausgabe des vorliegenden Reglements und aller nachfolgenden Änderungen obliegt der Zuständigkeit des Verwaltungsrates der Assura-Gruppe.

1.2.6 Wird im vorliegenden Reglement eine geschlechtsspezifische Form verwendet, schliesst dies die Personen aller Geschlechter mit ein, und eine Pluralform schliesst die Singularform mit ein und umgekehrt, ausser wenn sich aus dem Kontext zwingend etwas anderes ergibt.

2. Begriffe

Definition der im vorliegenden Reglement verwendeten Begriffe:

2.1 Bekanntgeben

Weitergeben oder Zugänglichmachen von Personendaten, einschliesslich im Ausland (Staaten oder internationale Organisationen)

2.2 Zustimmung

2.2.1 Jede freie, spezifische, klare und eindeutige Willensbekundung, mit der die betroffene Person in einer Erklärung oder durch eine schlüssige Handlung akzeptiert, dass sie betreffende personenbezogene Daten bearbeitet werden.

2.2.2 Für die Bearbeitung besonders schützenswerter Personendaten oder das Profiling durch ein Bundesorgan hat die Zustimmung ausdrücklich zu erfolgen, also durch eine ausdrückliche

und klare Zustimmungsbekundung durch die Person.

2.3 Automatisierte Einzelentscheidung

Entscheidung, die ausschliesslich auf der Grundlage einer automatisierten Bearbeitung von Personendaten ohne menschliches Eingreifen basiert und die rechtliche Auswirkungen für die Person hat oder sie erheblich beeinträchtigt.

2.4 Daten

2.4.1 Sämtliche Informationen betreffend die Assura-Gruppe oder deren Gesellschaften, potentielle Kunden, Mitarbeitenden, Leistungserbringer oder externe Partner (insbesondere die Versicherungsvermittler).

2.4.2 Als Daten betreffend die Assura-Gruppe oder deren Gesellschaften gelten Informationen über deren Organisation, Arbeitsabläufe und -prozesse sowie Entscheide.

2.5 Personendaten

Alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, namentlich Versicherte, potentielle Kunden, Mitarbeitende der Assura-Gruppe, Leistungserbringer oder externe Partner (insbesondere Versicherungsvermittler).

2.6 Besonders schützenswerte Daten

Sämtliche Daten über die Gesundheit, die Intimsphäre oder die ethnische oder Rassenzugehörigkeit, die religiösen, weltanschaulichen, politischen oder philosophischen Ansichten, gewerkschaftlichen Tätigkeiten, Massnahmen der sozialen Hilfe, Betreibungen, strafrechtliche oder administrative Sanktionen sowie genetische oder biometrische Daten.

2.7 Bundesorgan

Behörden oder Dienststellen des Bundes sowie Personen, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind. Die Assura-Basis AG ist ein Bundesorgan im Sinne des DSG.

2.8 Betroffene Personen

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

2.8.2 Im Sinne des DSG handelt es sich lediglich um natürliche Personen.

2.9 Private Person

Natürliche oder juristische private Person, die im Rahmen eines privatrechtlichen Verhältnisses Daten bearbeitet. Die Assura AG und ebenfalls die Figeas AG sind private Personen im Sinne des DSG.

2.10 Eidgenössische(r) Datenschutz- und Öffentlichkeitsbeauftragte(r) (EDÖB)

Die natürliche Person, die mit der Aufsicht über die ordentliche Anwendung der eidgenössischen Datenschutzbestimmungen betraut ist. Es handelt sich um die Aufsichtsbehörde in Sachen Datenschutz.

2.11 Profiling

2.11.1 Jede Art automatisierter Bearbeitung von Personendaten zur Bewertung bestimmter persönlicher Aspekte einer natürlichen Person, insbesondere zur Analyse oder Voraussage über die Arbeitsleistung, die wirtschaftliche oder gesundheitliche Situation, die persönlichen Vorlieben und Interessen, die Vertrauenswürdigkeit, das Verhalten, den Aufenthalt oder die Bewegungen dieser natürlichen Person.

2.11.2 Wenn das Profiling zu einer Datenzusammenstellung führt, die es erlaubt, wesentliche Persönlichkeitsmerkmale einer natürlichen Person zu bewerten, handelt es sich um ein Profiling mit hohem Risiko.

2.12 Für die Datenbearbeitung verantwortliche Person

(Natürliche oder juristische) private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen den Zweck und die Mittel zur Datenbearbeitung bestimmt, das heisst das Ziel und die Art und Weise der Bearbeitung.

2.13 Auftragsbearbeiter

Dienstleister, der auf Rechnung und gemäss den Anweisungen der für die Datenbearbeitung verantwortlichen Person Daten bearbeitet.

2.14 Datenbearbeitung

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

2.15 Verletzung der Datensicherheit

Jede Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verloren gehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

3. Rollen und Verantwortlichkeiten in Sachen Datenschutz

3.1 Geschäftsleitung

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

3.1.2 Sie wird dabei von der Datenschutzberaterin oder dem Datenschutzberater beraten.

3.2 Datenschutzberater/in

Aufgaben:

a) Bestimmt die Minimalanforderungen an den Datenschutz aufgrund der Art und des Zwecks der Bearbeitung.

b) Unterstützt die operativen Dienste bei der Planung und Umsetzung von Massnahmen im Bereich des Schutzes und der Sicherheit von Personendaten.

c) Überprüft, dass die Datenbearbeitung die gesetzlichen und reglementarischen Datenschutzanforderungen erfüllt, einschliesslich bei Verträgen und Unternehmensprojekten.

d) Wirkt beim Management und der Behebung von Sicherheitsvorfällen mit Personendaten mit.

e) Führt für die Assura AG, die Assura-Basis AG und die Figeas AG ein Register über die Bearbeitung von Personendaten gemäss dem Datenschutzgesetz. Für die Assura-Basis AG teilt er dieses dem Eidgenössischen Datenschutzbeauftragten mit.

f) Stellt sicher, dass Anfragen im Zusammenhang mit der Personendatenbearbeitung (Einsichtsrecht, Recht auf Vergessen, Recht auf Übertragbarkeit usw.) korrekt behandelt und innert der gesetzlichen Frist beantwortet werden.
g) Wirkt bei der Datenschutzausbildung der Mitarbeitenden mit.
h) Ist Hauptansprechperson der oder des Eidgenössischen Datenschutzbeauftragten und der von der Datenbearbeitung betroffenen Personen.
i) Berichtet regelmässig der Geschäftsleitung über die Konformität der Gesellschaften der Assura-Gruppe und legt bei festgestellter Nicht-Konformität einen Bericht über die getroffenen Massnahmen vor.
j) Sorgt dafür, dass das vorliegende Reglement regelmässig aktualisiert und durch die Assura-Gruppe eingehalten wird.

3.3 Chief Information Security Officer (CISO)

3.3.1 Die/Der CISO ist die Hauptansprechperson für die Geschäftsleitung und die Mitarbeitenden der Assura-Gruppe sowie die Partner, wenn es um die Bestimmung der Richtlinien und Standards zur Einhaltung der Sicherheit der Informationen und Informationssysteme geht.

3.3.2 Die Aufgaben der/des CISO sind in einer Weisung genauer definiert.

3.4 Mitarbeitende

Alle Mitarbeitenden sind dafür verantwortlich, Daten gemäss den Regeln und Grundlagen dieses Reglements zu bearbeiten.

3.5 Inhaber der Daten

Innerhalb der Assura-Gruppe müssen sämtliche Personendaten einen Inhaber haben. Der Inhaber der Daten ist die für ihre Bearbeitung verantwortliche Person. Diese Person ist für die richtige Klassifizierung der Daten gemäss Kapitel 7 dieses Reglements und ihre allenfalls erforderliche Aktualisierung verantwortlich.

3.6 Geschäftsbereich Kunden und Markt

Der Geschäftsbereich Kunden und Markt ist Inhaber der Daten, die im Rahmen der Neukundenwerbung für Versicherungsabschlüsse anfallen, sowie der Daten im Zusammenhang mit den Versicherungsvermittlern.

3.7 Geschäftsbereich Leistungen

3.7.1 Allgemeine Verantwortlichkeit

3.7.1.1 Der Geschäftsbereich Leistungen ist Inhaber der Daten, die im Rahmen des Abschlusses von Versicherungsverträgen, der Beziehung mit den versicherten Personen und der Erstattung von Leistungen (Austausch mit den Leistungserbringern, Garantien, Bearbeitung von Rechnungen, Leistungsabrechnungen usw.) bearbeitet werden.

3.7.1.2 Es gelten besondere Bestimmungen für die Bearbeitung der Daten von Mitarbeitenden, die bei den Gesellschaften der Assura-Gruppe versichert sind.

3.7.2 Kundendienst

Der Kundendienst ist verantwortlich für den Schutz der Versichertendaten, die er beim Eintritt, der Betreuung der Vertragsbeziehung und beim Austritt der Versicherten bearbeitet.

3.7.3 Vertrauensärztlicher Dienst und Vertrauensarztpersonen

3.7.3.1 Der vertrauensärztliche Dienst ist verantwortlich für den Schutz der medizinischen Versichertendaten, die er bearbeitet (insbesondere Gesundheitsfragebogen, Gutachten und Arztberichte).

3.7.3.2 Die Vertrauensarztperson sorgt für die Einhaltung der zusätzlichen Schutz- und Sicherheitsmassnahmen, die in Anbetracht für besonders schützenswerte Daten eingeführt wurden.

3.7.4 Verantwortlichkeit im Rahmen von SwissDRG

Die Mitarbeitenden der DRG-Zellen gehören einer besonderen Einheit an, die der Datenschutzzertifizierung untersteht. Sie sind für die «Minimal Clinical Datasets» (MCD, Haupt- und Nebendiagnosen sowie Behandlungen) verantwortlich. Deren Bearbeitung ist in einer besonderen Instruktion geregelt.

3.8 Geschäftsbereich Finanzen

Der Geschäftsbereich Finanzen ist Inhaber aller Finanzdaten der Gesellschaften der Assura-Gruppe sowie sämtlicher Finanzdaten der Versicherten, die insbesondere für die Prämienzahlungen, die Rückerstattung von Leistungen (Kundenkonten, Zahlungen, Korrespondenz und Auskünfte insbesondere zu Betreibungen und Verlustscheinen) und Daten betreffend Prämienverbilligungen bearbeitet werden.

3.9 Geschäftsbereich Entwicklung und Marketing

Der Geschäftsbereich Entwicklung und Marketing ist Inhaber der Daten, die er zu statistischen Zwecken, für das Reporting, Marketing-Kampagnen oder Kundenumfragen für die gesamte Assura-Gruppe bearbeitet.

3.10 Bereich Human Resources

Der Bereich Human Resources ist Inhaber der Personendaten der Mitarbeitenden mit Ausnahme der Daten, die ihren Versichertenstatus bei den Gesellschaften der Assura-Gruppe betreffen (z. B. Bearbeitung der Policen und Leistungen), die durch hierfür bestimmte Mitarbeitende des Geschäftsbereichs Leistungen bearbeitet werden.

3.11 Geschäftsbereich Informatik

Der Geschäftsbereich Informatik ist Inhaber der Konfigurationsdaten, Quellencodes und Geheiminformationen für den Zugriff auf die IT-Infrastrukturen. Er ist ausserdem dafür verantwortlich, technische und organisatorische Massnahmen für die Sicherheit der elektronischen Daten zu treffen, die in den verschiedenen von der Assura-Gruppe, ihren Mitarbeitenden und Partnern genutzten Informationssystemen bearbeitet werden (Zugriff, Internet, E-Mail usw.).

3.12 Eidgenössische(r) Datenschutz- und Öffentlichkeitsbeauftragte(r) (EDÖB)

3.12.1 <u>Kompetenzen der oder des EDÖB</u>

3.12.1.1 Die/Der EDÖB muss von Amtes wegen oder auf Anzeige eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnen, sobald Anzeichen den Eindruck erwecken, dass Datenbearbeitungen gegen gesetzliche oder Datenschutzbestimmungen verstossen könnten. Die/Der EDÖB kann auf eine Untersuchung verzichten, wenn die Verletzung

geringfügig ist oder wenn die für die Datenbearbeitung verantwortliche Person angemessene Massnahmen ergriffen hat, um den rechtmässigen Zustand wiederherzustellen.

3.12.1.2 Wird eine Untersuchung eröffnet, ist die für die Datenbearbeitung verantwortliche Person verpflichtet, mit der/dem EDÖB zusammenzuarbeiten und ihr/ihm die für ihre/seine Untersuchung erforderlichen Informationen zu liefern.

3.12.1.3 Wenn die für die Datenbearbeitung verantwortliche Person ihrer Pflicht zur Zusammenarbeit nicht nachkommt und die/der EDÖB eine Verletzung des Datenschutzes feststellt, kann sie/er verschiedene administrative Massnahmen gegen die für die Datenbearbeitung verantwortliche Person verfügen, wie etwa die Änderung, Beendigung oder Suspendierung eines Teils oder der gesamten Datenbearbeitung oder die Vernichtung oder Löschung aller oder eines Teils der Daten. Sie/Er kann ausserdem anordnen, dass Sicherheitsmassnahmen getroffen oder die betroffenen Personen informiert werden.

3.12.1.4 Die/Der EDÖB hat hingegen nicht die Befugnis, Bussen auszusprechen oder die für die Datenbearbeitung verantwortliche Person strafrechtlich zu belangen.

3.12.2 Sanktionen

3.12.2.1 Für private Personen

Gegen eine natürliche Person, die sich durch Unterlassen oder vorsätzlich der Verletzung der Informations-, Auskunfts- oder Mitwirkungs-, Sorgfalts- oder Schweigepflicht oder der Nichtbefolgung einer einstweiligen Verfügung des EDÖB schuldig gemacht hat, können die Strafverfolgungsbehörden auf Antrag eine Busse von höchstens CHF 250’000 verhängen.

3.12.2.2 Für Bundesorgane

Die unter Artikel 3.12.2.1 genannte Busse kann gegen die natürliche Person innerhalb eines Bundesorgans verhängt werden, die vorsätzlich und unter Verletzung ihrer Schweigepflicht Personendaten bekannt gibt, von denen sie im Rahmen ihrer Tätigkeit Kenntnis erhält. Die Schweigepflicht ist über die Beendigung des Arbeitsverhältnisses hinaus gültig.

3.12.2.3 Erfordert die Identifizierung der strafbaren Person innerhalb des Unternehmens unverhältnismässige Untersuchungsmassnahmen, wird das Unternehmen mit einer Busse von höchstens CHF 50’000 bestraft.

4. Pflichten der für die Datenbearbeitung verantwortlichen Person

4.1 Allgemeine Grundsätze

4.1.1 Rechtmässigkeit/Gesetzlichkeit

4.1.1.1 Für private Personen

Jede Bearbeitung von Personendaten muss rechtmässig sein, das heisst, sie darf nicht gegen eine zwingende Gesetzesbestimmung betreffend den Schutz der Persönlichkeit der natürlichen Person verstossen. Andernfalls muss ein Rechtfertigungsgrund (z. B. die Einwilligung) vorliegen, um die Bearbeitung durchzuführen.

4.1.1.2 Für Bundesorgane

Jede Art von Personendatenbearbeitung muss auf einer gesetzlichen Grundlage beruhen. Beim Fehlen eines Gesetzes, das eine solche Bearbeitung erlaubt, muss ein Rechtfertigungsgrund (z. B. die Einwilligung) vorliegen.

4.1.2 Verhältnismässigkeit

4.1.2.1 Es dürfen nur Personendaten bearbeitet werden, die zur Erreichung des Bearbeitungszwecks geeignet und objektiv erforderlich sind.

4.1.2.2 Die Bearbeitung muss in einem vernünftigen Verhältnis zum angestrebten Zweck und den verwendeten Mitteln stehen, und es müssen dabei die Rechte der betroffenen Personen so weit wie möglich gewahrt werden. Es ist systematisch zu prüfen, ob der Zweck mit einem weniger einschneidenden Mittel erfüllt werden kann.

4.1.3 Aufbewahrung von Personendaten

Personendaten müssen vernichtet oder anonymisiert werden, sobald sie für den Zweck der Bearbeitung nicht mehr erforderlich sind, sofern ihre Aufbewahrung nicht gesetzlich vorgeschrieben ist.

4.1.4 Guter Glauben und Transparenz

4.1.4.1 Jede Bearbeitung von Personendaten hat nur in gutem Glauben zu erfolgen, das heisst zu dem Zweck, der den betroffenen Personen beim Sammeln der Daten mitgeteilt wurde oder der sich aus dem Gesetz oder den Umständen ergibt. Ohne Wissen und gegen den Willen der betroffenen Person darf keine Datenbearbeitung stattfinden.

4.1.4.2 Sowohl das Sammeln als auch der Zweck der Bearbeitung müssen für die betroffene Person erkennbar sein.

4.1.5 Zweckbindung

4.1.5.1 Jede Bearbeitung von Personendaten muss den bei ihrem Sammeln mitgeteilten Zweck einhalten.

4.1.5.2 Jede weitere Bearbeitung muss mit den Zwecken vereinbar bleiben, die der betroffenen Person ursprünglich mitgeteilt wurden.

4.1.6 Richtigkeit

Die bearbeiteten Personendaten müssen korrekt und so aktuell sein, wie es die Umstände erlauben. Unter Vorbehalt anderslautender gesetzlichen Bestimmungen trifft die für die Datenbearbeitung verantwortliche Person geeignete Massnahmen, die es gestatten, unrichtige oder unvollständige Daten zu korrigieren, löschen oder vernichten. Zu diesem Zweck zeigen alle Mitarbeitenden die bei ihrer Tätigkeit festgestellten Unstimmigkeiten an.

4.1.7 Sicherheit von Personendaten

Die von der Assura-Gruppe bearbeiteten Personendaten müssen im Verhältnis zum damit verbundenen Risiko (Klassifikationsgrad) durch geeignete organisatorische und technische Massnahmen gegen interne und externe Verletzungen der Datensicherheit geschützt werden.

Diese Massnahmen müssen die Vertraulichkeit, die Verfügbarkeit, die Integrität und die Rückverfolgbarkeit der bearbeiteten Daten garantieren.

4.2 Informationspflicht

4.2.1 Wenn die für die Datenbearbeitung verantwortliche Person bei der betroffenen Person oder Dritten Personendaten sammelt, gibt sie der betroffenen Person die erforderlichen Informationen, damit diese ihre in Kapitel 6 genannten Rechte wahrnehmen kann und die Transparenz der Bearbeitungen gewährleistet wird. Sie teilt ihr mindestens Folgendes mit:

a) Identität und die Kontaktdaten der für die Datenbearbeitung verantwortlichen Person
b) Bearbeitungszweck
c) gegebenenfalls die Empfänger/innen oder die Kategorien von Empfänger/innen, denen Personendaten bekannt gegeben werden
d) gegebenenfalls der Name des Drittstaates, indem die Personendaten mitgeteilt wurden und die entsprechenden Garantien

4.2.2 Wenn Personendaten bei Dritten gesammelt werden, wird die betroffene Person innerhalb eines Monats nach Erhalt dieser Daten informiert, es sei denn, die Person hat zuvor ihre Einwilligung zum Sammeln der Daten gegeben oder es besteht eine gesetzliche Grundlage, die dieses rechtfertigt. Erfolgt vor Ablauf dieser Frist eine Mitteilung an Dritte, so hat die betroffene Person spätestens zum Zeitpunkt dieser Mitteilung informiert zu werden.

4.2.3 Die für die Datenbearbeitung verantwortliche Person ist in bestimmten im DSG vorgesehenen Situationen davon entbunden oder kann die Mitteilung von Informationen einschränken oder aufschieben, zum Beispiel, wenn die Person bereits informiert ist, die Bearbeitung gesetzlich vorgeschrieben ist oder überwiegende Interessen eines Dritten dies erfordern.

4.2.4 Die Auskunftspflicht wird insbesondere erfüllt durch die Publikation der Mitteilung zur Datenbearbeitung auf der Website der Assura-Gruppe sowie durch die Publikation des Bearbeitungsregisters durch das Bundesorgan.

4.3 Automatisierte Einzelentscheidung

4.3.1 Eine automatisierte Einzelentscheidung ist eine Entscheidung betreffend eine Person, die getroffen wird, indem Algorithmen ohne menschliches Zutun auf ihre persönlichen Daten angewendet werden.

4.3.2 Die durch eine solche Entscheidung betroffene Person, muss zuvor darüber informiert werden, um ihren Standpunkt darlegen zu können. Sie kann gegebenenfalls verlangen, dass die automatisierte Einzelentscheidung durch eine natürliche Person überprüft wird.

4.3.3 Diese Verpflichtung gilt nicht, wenn die Entscheidung in Zusammenhang mit dem Abschluss oder der Erfüllung eines Vertrags getroffen wird und dem Antrag der Person vollständig stattgegeben wurde oder wenn die Person dieser Art von Entscheidung ausdrücklich zugestimmt hat.

4.4 Mitteilung von Daten ins Ausland

4.4.1 Grundsatz

Personendaten können ins Ausland in ein Land mitgeteilt werden, dessen Gesetzgebung ein angemessenes Niveau gemäss der vom Bundesrat erstellten Liste aufweist, z. B. in ein Land der Europäischen Union.

4.4.2 Zusätzliche Garantien

Wenn die Gesetzgebung des Landes kein angemessenes Niveau aufweist, muss die für die Datenbearbeitung verantwortliche Person zusätzliche Massnahmen ergreifen, um ein geeignetes

Datenschutzniveau sicherzustellen, z. B. durch die Annahme von Vertragsklauseln, die von der oder vom EDÖB genehmigt wurden, oder die betroffene Person muss ausdrücklich ihre Einwilligung erteilen. In diesem Fall muss der/die Datenschutzberater/in vorab konsultiert und sein oder ihr Einverständnis eingeholt werden, bevor irgendeine Mitteilung in ein Land erfolgt, dessen Datenschutzniveau nicht ausreichend ist.

4.5 Verzeichnis der Bearbeitungstätigkeiten

4.5.1 Die Assura-Basis AG, die Assura AG oder die Figeas AG, sowie ihre Auftragsbearbeiter (für die auf ihre Rechnung bearbeiteten Daten) müssen je ein Register über alle Datenbearbeitungsaktivitäten führen. Das Register muss mindestens folgende Angaben enthalten:

a) die Identität der für die Datenbearbeitung verantwortlichen Person
b) den Bearbeitungszweck
c) eine Beschreibung der betroffenen Personenkategorien und der bearbeiteten Daten
d) die Kategorien der Empfänger
e) die Aufbewahrungsfrist der Daten und die Kriterien zu deren Bestimmung
f) eine allgemeine Beschreibung der Datensicherheitsmassnahmen
g) im Fall der Mitteilung von Daten ins Ausland: den Namen des betroffenen Staates und gegebenenfalls die vorgesehenen Garantien

4.5.2 Das Bearbeitungsregister muss bei jeder neuen Bearbeitung oder falls eine Änderung erforderlich sein sollte, jedoch mindestens einmal jährlich, aktualisiert werden.

4.5.3 Die Assura-Basis AG muss es in ihrer Eigenschaft als Bundesorgan bei der / beim EDÖB einreichen, die/der es auf ihrer/seiner Plattform publiziert. Die Assura AG und die Figeas AG müssen es auf Anfrage der/dem EDÖB zur Verfügung stellen.

4.6 Auswirkungsanalyse

4.6.1 Grundsatz

4.6.1.1 Die für die Datenbearbeitung verantwortliche Person muss für jede neue Personendatenbearbeitung, die insbesondere aufgrund der Natur der bearbeiteten Daten, des Umfangs und des Zwecks der Bearbeitung oder der Nutzung neuer Technologien ein erhöhtes Risiko für die betroffenen Personen birgt, eine Auswirkungsanalyse durchführen. Diese Auswirkungsanalyse hat unter der Berücksichtigung der Frist gemäss Artikel 4.6.1.4 spätestens vier Monate vor der vorgesehenen Datenbearbeitung zu erfolgen.

4.6.1.2 Für jede Bearbeitung muss vorab der/die Datenschutzberater/in konsultiert werden, um zu bestimmen, ob eine Auswirkungsanalyse erforderlich ist.

4.6.1.3 Die Auswirkungsanalyse muss mindestens zwei Jahre nach Beendigung der Bearbeitung aufbewahrt werden.

4.6.1.4 <u>Für Bundesorgane</u>

Sobald ein Bundesorgan eine neue Datenbearbeitung plant, muss zwingend eine Auswirkungsanalyse durchgeführt werden, wenn die Bedingungen gemäss Artikel 4.6.1.1 erfüllt sind.

Wenn die Analyse ergibt, dass trotz der getroffenen Massnahmen ein erhöhtes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person besteht, muss innert einer Frist von drei Monaten die oder der EDÖB konsultiert werden, um dieses zu bestimmen.

4.6.1.5 <u>Für private Personen</u>

Erfolgt die vorgesehene Bearbeitung aufgrund einer gesetzlichen Pflicht, besteht für die privatrechtliche Datenbearbeitung keine Pflicht zur Durchführung einer Auswirkungsanalyse.

In gewissen Fällen kann auch auf eine Analyse verzichtet werden, z. B. wenn ein zertifiziertes System oder Produkt oder ein zertifizierter Dienst benutzt wird.
Wird eine Auswirkungsanalyse der Datenschutzberaterin oder dem Datenschutzberater vorgelegt, kann darauf verzichtet werden, diese dem EDÖB zu unterbreiten.

4.6.2 Mindestinhalt

Die Auswirkungsanalyse muss mindestens folgende Angaben enthalten:
a) Beschreibung der geplanten Bearbeitung
b) Analyse des Risikos für die Persönlichkeit und die Grundrechte der betroffenen Person
c) die zum Schutz ihrer Persönlichkeit und Grundrechte vorgesehenen Massnahmen

4.7 «Privacy by Design» und «Privacy by Default»

4.7.1 Datenschutz durch Technikgestaltung (Privacy by Design)

Die für die Datenbearbeitung verantwortliche Person ist gehalten, für jedes neue Projekt, das eine Bearbeitung von Personendaten erfordert, bereits beim Erstellen des Projektkonzepts geeignete technische und organisatorische Massnahmen zu treffen, damit die Datenbearbeitung die Grundsätze gemäss Artikel 4.1 erfüllt.

4.7.2 Datenschutzfreundliche Voreinstellungen (Privacy by Default)

Stehen für die Personendatenbearbeitung bei einer Dienstleistung, einer Software oder einem Gerät verschiedene Möglichkeiten zur Auswahl und kann die betroffene Person diese Möglichkeiten selbst wählen, sorgt die für die Datenbearbeitung verantwortliche Person dafür, dass die Bearbeitung sich auf das unbedingt Notwendige beschränkt, um den Zweck der Datenbearbeitung zu erfüllen, es sei denn, die betroffene Person habe in eine erweiterte Datenbearbeitung eingewilligt. Zu diesem Zweck muss die für die Datenbearbeitung verantwortliche Person insbesondere geeignete Voreinstellungen vorsehen.

4.8 Ausbildung

Die für die Datenbearbeitung verantwortliche Person muss sich vergewissern, dass die Mitarbeitenden der Assura-Gruppe im Bereich Datenschutz regelmässig weitergebildet werden.

5. Auslagerung an Dritte (Auftragsbearbeitung)

5.1 Grundsatz

5.1.1 Die für die Datenbearbeitung verantwortliche Person kann die Datenbearbeitung an Dritte auslagern (an eine andere Gesellschaft der Assura-Gruppe oder einen externen Dienstleister), sofern folgende Bedingungen erfüllt sind:
a) Die Auslagerung an Dritte (Auftragsbearbeitung) ist vertraglich oder gesetzlich vorgesehen.
b) Es können nur Bearbeitungen ausgelagert werden, zu deren Bearbeitung die für die Datenbearbeitung verantwortliche Person selbst berechtigt ist.
c) Keine gesetzliche, vertragliche oder Geheimhaltungsverpflichtung verbietet die Auslagerung.

5.1.2 Die für die Datenbearbeitung verantwortliche Person bleibt in jedem Fall für den Schutz und die Sicherheit der Daten verantwortlich, deren Bearbeitung einem Dritten übertragen wurde.

5.2 Modalitäten

5.2.1 Pflichten der für die Datenbearbeitung verantwortlichen Person

5.2.1.1 Die für die Datenbearbeitung verantwortliche Person wählt den Auftragsbearbeiter, der ausreichende Sicherheiten betreffend den Schutz der Rechte der betroffenen Personen bietet (zum Beispiel aufgrund einer Zertifizierung).

5.2.1.2 Die für die Datenbearbeitung verantwortliche Person erteilt dem Auftragsbearbeiter Ad-hoc-Anweisungen, um den Schutz und die Sicherheit der Daten gewährleisten, die von diesem im Rahmen seines Auftrags bearbeitet wurden.

5.2.1.3 Die für die Datenbearbeitung verantwortliche Person muss durch regelmässige Kontrollen mindestens einmal jährlich sicherstellen, dass der Auftragsbearbeiter die Daten gemäss seinen Anweisungen und dem Vertrag bearbeitet.

5.2.1.4 Bei der Auftragsbearbeitung einer wesentlichen bzw. wichtigen Funktion sind zusätzliche Anforderungen in einer entsprechenden Weisung vorgesehen.

5.2.2 Pflichten der Auftragsbearbeiter

5.2.2.1 Der von der für die Datenbearbeitung verantwortlichen Person gewählte Auftragsbearbeiter muss jederzeit gewährleisten, dass die ihm anvertraute Datenbearbeitung die Anforderungen in Sachen Datensicherheit und -schutz erfüllt.

5.2.2.2 Der Auftragsbearbeiter darf die Daten nur gemäss den Anweisungen der für die Datenbearbeitung verantwortlichen Person und auf Rechnung derselben bearbeiten.

5.2.2.3 Der Auftragsbearbeiter ist verpflichtet, ein Bearbeitungsregister der von ihm bearbeiteten Personendaten gemäss Artikel 4.5.1. zu führen.

5.2.2.4 Der Auftragsbearbeiter darf die Datenbearbeitung seinerseits nur mit der vorgängigen Genehmigung der für die Datenbearbeitung verantwortlichen Person an Dritte auslagern.

6. Rechte der von einer Datenbearbeitung durch die Assura-Gruppe betroffenen Personen

6.1 Zugriffsrecht

6.1.1 Jede Person kann schriftlich oder auf elektronischem Weg von der für die Datenbearbeitung verantwortlichen Person verlangen, sämtliche durch die Assura-Gruppe bearbeiteten Daten einzusehen, die sie betreffen. Die Auskünfte werden grundsätzlich schriftlich erteilt, eine Einsichtnahme vor Ort ist indessen nach Absprache mit der für die Datenbearbeitung verantwortlichen Person möglich.

6.1.2 Die Ausübung dieses Rechts ist jederzeit ohne besondere Begründung möglich und kostenlos, sofern die Mitteilung der Auskünfte nicht unverhältnismässigen Aufwand erfordert, für den eine angemessene Kostenbeteiligung verlangt werden kann.

6.1.3 Die für die Datenbearbeitung verantwortliche Person kann in gewissen gesetzlich vorgesehenen Fällen Auskünfte verweigern, einschränken oder aufschieben, insbesondere wenn überwiegende Interessen von Dritten dies erfordern oder wenn der Antrag auf Einsicht offensichtlich unbegründet oder verfahrensbedingt ist.

6.1.4 Die Auskünfte müssen innerhalb von 30 Tagen ab Eingang des Gesuchs erteilt werden. Wenn diese Frist nicht eingehalten werden kann, informiert die für die Datenbearbeitung verantwortliche Person die betroffene Person innert dieser Frist und teilt ihr mit, bis wann die Informationen geliefert werden. Wenn die Auskunft verweigert, eingeschränkt oder aufgeschoben wird, teilt sie dies unter Angabe der Gründe ebenfalls innert dieser Frist mit.

6.2 Recht bei automatisierter Einzelentscheidung

Die von einer automatisierten Entscheidung gemäss Artikel 4.3.1 betroffene Person kann ihr Recht auf Überprüfung der Entscheidung durch eine natürliche Person ausüben.

6.3 Recht auf Datenübertragung

6.3.1 Jede von einer Datenbearbeitung betroffene Person kann verlangen, dass ihr die Personendaten, die sie selbst der für die Datenbearbeitung verantwortlichen Person mitgeteilt hat, in einer gängigen elektronischen Form übermittelt werden.

6.3.2 Dieses Recht ist lediglich anwendbar, wenn:
a) die Daten automatisiert bearbeitet werden,
b) dadurch keine Drittperson beeinträchtigt wird
c) und die Daten aufgrund einer Einwilligung bearbeitet wurden.

6.3.3 Nach Überprüfung der Rechtmässigkeit des Antrags durch den/die Datenschutzberater/in werden die Daten der betroffenen Person, soweit technisch möglich, in einem gängigen strukturierten und von einem Computer lesbaren Format übermittelt.

6.3.4 Die Ausübung des Rechts auf Datenübertragung kann aufgrund der in Artikel 6.1.3 genannten Gründen verweigert werden.

6.4 Einspruchsrecht

6.4.1 Jede von einer Datenbearbeitung betroffene Person kann aufgrund eines glaubhaft gemachten, schutzwürdigen Interessens ausdrücklich Einspruch dagegen einlegen, dass bestimmte Personendaten durch die für die Datenbearbeitung verantwortliche Person bearbeitet werden.

6.4.2 Dieses Einspruchsrecht kann verweigert werden, wenn:
a) die Datenbearbeitung auf einer gesetzlichen Grundlage beruht,
b) private oder öffentliche Interessen, die die Interessen der betroffenen Person überwiegen, dies erfordern.

6.5 Recht auf Vergessen

Jede von einer Datenbearbeitung betroffene Person kann von der für die Datenbearbeitung verantwortlichen Person verlangen, dass ihre Personendaten gelöscht oder anonymisiert werden, sobald die Verwendung ihrer Daten für den verfolgten Zweck nicht mehr erforderlich ist, wenn sie unrichtig sind oder die Bearbeitung auf der Einwilligung der Person beruht und sie diese widerrufen möchte.
Die Einschränkungen gemäss Artikel 6.4.2 gelten auch für die Ausübung dieses Rechts.

6.6 Recht auf Berichtigung

Wenn ihre Daten unrichtig oder unvollständig sind, kann jede von einer Datenbearbeitung betroffene Person von der für die Datenbearbeitung verantwortlichen Person verlangen, dass ihre Daten zur Aktualisierung berichtigt werden, sofern dies nicht durch ein Gesetz verboten ist.
Wenn die Unrichtigkeit von Personendaten nicht festgestellt werden kann, kann die betroffene Person von der für die Datenbearbeitung verantwortlichen Person verlangen, dass bei den betreffenden Daten ein Bestreitungsvermerk angebracht wird.

7. Grundsätze der Datensicherheit

Für die Datensicherheit erstellt die Assura-Gruppe eine Klassifikation mit folgenden vier Dimensionen: Vertraulichkeit, Integrität, Verfügbarkeit und Rückverfolgbarkeit. Für jede dieser vier Dimensionen wurden vier Kritikalitätsstufen definiert. Für jede dieser Stufen wurden spezifische Sicherheitsmassnahmen festgelegt.

7.1 Vertraulichkeit

Der Inhaber von Daten muss die von ihm bearbeiteten Daten gemäss den vier Vertraulichkeitsstufen der Assura-Gruppe klassifizieren. Diese sind: «Öffentlich», «Intern», «Vertraulich» und «Geheim».

7.1.1 Öffentliche Daten (Stufe 1)

Als «Öffentlich» klassifizierte Daten und Dokumente enthalten keinerlei Personendaten und sind zur freien Verbreitung und Einsicht ausserhalb der Assura-Gruppe bestimmt, ohne dass der Assura-Gruppe dadurch ein Schaden entsteht (Beispiele: Geschäftsbericht der Gruppe, Werbebroschüren). Auf dieser Stufe sind keinerlei Schutzmassnahmen erforderlich.

7.1.2 Interne Daten (Stufe 2)

7.1.2.1 Die als «Intern» klassifizierten Daten und Dokumente sind nur für den Gebrauch innerhalb der Assura-Gruppe bestimmt. Mit Zustimmung des Inhabers der Daten können diese in begrenztem und gezieltem Einsatz auch extern verwendet werden. (Beispiele: Organigramme, Reglemente, Weisungen) Ihre Weitergabe ausserhalb der Gruppe kann einen begrenzten Schaden für die Assura-Gruppe oder die Personen, deren Daten bearbeitet werden, haben. Es sind organisatorische und technische Massnahmen erforderlich, um den Zugang zu solchen Daten und Dokumenten zu begrenzen.

7.1.2.2 Als «Intern» klassifizierte Daten und Dokumente dürfen keine besonders schützenswerten Personendaten enthalten.

7.1.3 Vertrauliche Daten (Stufe 3)

7.1.3.1 Als «Vertraulich» klassifizierte Daten dürfen nur kontrolliert innerhalb der Assura-Gruppe weitergegeben werden (Beispiele: Personendaten von Versicherten oder Mitarbeitenden, Finanzdaten, Unternehmensprojekte). Ihre Weitergabe ausserhalb der Gruppe kann einen spürbaren Schaden für die Assura-Gruppe oder die betroffenen Personen bewirken. Die Personen, die Zugang zu diesen Arten von Daten haben, sind namentlich bekannt und befolgen die Grundsätze des vorliegenden Reglements.

7.1.3.2 Daten und Dokumente ohne Angabe ihrer Klassifizierung sind als vertraulich zu behandeln.

7.1.4 Geheime Daten (Stufe 4):

Als «Geheim» klassifizierte Daten dürfen nur in sehr begrenztem Umfang innerhalb der Assura-Gruppe weitergegeben werden (Beispiele: medizinische Daten von Versicherten oder Mitarbeitenden, Rentabilität von Produkten, Projekte zu Partnerschaften oder strategischen Verträgen). Ihre Weitergabe ausserhalb der Gruppe kann einen erheblichen Schaden für das Unternehmen bewirken. Sie dürfen nicht ohne die Einwilligung des Inhabers weitergegeben werden. Der Kreis der Personen, die Zugang zu dieser Art von Daten haben, ist sehr beschränkt und namentlich bekannt und kann jederzeit angegeben werden.

7.2 Integrität

Die Integrität ermöglicht die Genauigkeit der Daten zu gewährleisten, das heisst, dass Daten oder Dokumente nicht unbefugt verändert oder vernichtet wurden. Der Inhaber jeglicher Daten muss die Daten, die er bearbeitet, nach den vier von der Assura-Gruppe festgelegten Integritätsstufen klassifizieren:

7.2.1 Keine Vorgaben zur Integrität (Stufe 1)

Die Daten und Dokumente können verändert oder gelöscht werden, ohne dass der Assura-Gruppe oder den Personen, deren Daten bearbeitet werden, daraus ein Schaden entsteht. Auf dieser Stufe sind keine Massnahmen erforderlich.

7.2.2 Standard-Integrität (Stufe 2)

Werden Daten oder Dokumente auf dieser Stufe verändert oder gelöscht, so führt dies für die Assura-Gruppe oder die Personen, deren Daten bearbeitet werden, zu einem begrenzten Schaden (Zeitverlust bei der Bearbeitung; Notwendigkeit, bereits geleistete Arbeit erneut zu machen). Es sind organisatorische und technische Massnahmen erforderlich, um solche Auswirkungen von Änderungen oder Löschungen zu begrenzen.

7.2.3 Erhöhte Integrität (Stufe 3)

Werden Daten oder Dokumente auf dieser Stufe verändert oder gelöscht, so führt dies für die Assura-Gruppe oder die Personen, deren Daten bearbeitet werden, zu einem spürbaren Schaden (erheblicher Aufwand zur Korrektur der Fehler, Imageschaden, Beeinträchtigung der Beziehung mit der Kundschaft und den Partnern). Es sind organisatorische und technische Massnahmen erforderlich, um solche Auswirkungen von Änderungen oder Löschungen zu begrenzen.

7.2.4 Unabänderliche Integrität (Stufe 4)

Werden Daten oder Dokumente auf dieser Stufe verändert oder gelöscht, so führt dies für die Assura-Gruppe oder die Personen, deren Daten bearbeitet werden, zu einem schwerwiegenden Schaden (erheblicher Aufwand zur Korrektur der Fehler, grosser Imageschaden, dauerhafte Beeinträchtigung der Beziehung mit der Kundschaft und den Partnern, Verletzung gesetzlicher Pflichten). Es sind organisatorische und technische Massnahmen erforderlich, um solche Änderungen oder Löschungen zu verhindern. Für jede Änderung ist ein ausführliches Audit erforderlich.

7.3 Verfügbarkeit

Unter Verfügbarkeit versteht man einen jederzeit möglichen Zugriff auf die zur Ausführung der Tätigkeiten nötigen Daten mittels der entsprechenden Anwendungen. Die Business-Continuity-Strategie beschreibt insbesondere die Schlüsselprozesse und die Anwendungen, die diese unterstützen. Eine Ad-hoc-Instruktion über das Risikomanagement beschreibt hierzu fünf Kritikalitätsstufen für die Auswirkungen, das heisst schwerwiegend, gross, mittel, geringfügig und unbedeutend. Für jede dieser Stufen werden eine maximal zulässige Dauer von Ausfällen sowie Massnahmen zur Behebung beschrieben.

7.4 Rückverfolgbarkeit

Die Rückverfolgbarkeit gestattet es, jeden nicht befugten Zugriff zu identifizieren und den Ursprung eines Vorfalls aufgrund einer Registrierung zu bestimmen. Dies erlaubt insbesondere festzustellen, wer auf die Daten zugegriffen hat, ob eine Bearbeitung vorgenommen wurde und wann eine allfällige Änderung stattgefunden hat. Der Inhaber jeglicher Daten muss die Daten, die er bearbeitet, nach den vier von der Assura-Gruppe festgelegten Rückverfolgbarkeitskriterien klassifizieren.

7.4.1 Keine Rückverfolgbarkeit (Stufe 1)

Die Nichtrückverfolgbarkeit der Daten oder der Bearbeitung hat keinerlei Auswirkung für das Unternehmen oder die Personen, deren Daten bearbeitet werden. Auf dieser Ebene sind keine Massnahmen erforderlich.

7.4.2 Standard-Rückverfolgbarkeit (Stufe 2)

Die Nichtrückverfolgbarkeit auf dieser Stufe führt zu einem begrenzten Schaden für die Tätigkeit oder die Konformität des Unternehmens. Die internen Unternehmensprozesse und reglementarischen Vorgaben verlangen eine minimale Rückverfolgung des Zugriffs auf die Daten oder der Bearbeitung (wer hat auf die Daten wann und auf welchem Informationssystem zugegriffen).

7.4.3 Ausführliche Rückverfolgbarkeit (Stufe 3)

Die Nichtrückverfolgbarkeit auf dieser Stufe führt zu einem spürbaren Schaden für die Tätigkeit oder die Konformität des Unternehmens. Die internen Unternehmensprozesse und reglementarischen Vorgaben verlangen eine ausführliche Rückverfolgung des Zugriffs auf die Daten oder der Bearbeitung (wer hat auf welche Daten, zu welcher Zeit, auf welchem Informationssystem zugegriffen und welcher Art war die Bearbeitung).

7.4.4 Vollständige Rückverfolgbarkeit (Stufe 4)

Die Nichtrückverfolgbarkeit auf dieser Stufe führt zu einem schwerwiegenden Schaden für die Tätigkeit oder die Konformität des Unternehmens. Die internen Unternehmensprozesse und reglementarischen Vorgaben verlangen eine vollständige Rückverfolgung des Zugriffs auf die Daten oder der Bearbeitung (wer hat auf welche Daten, zu welcher Zeit, auf welchem Informationssystem zugegriffen, welcher Art war die Bearbeitung und was war der Zustand der Daten vor und nach der Bearbeitung).

8. Allgemeine Massnahmen zur Gewährleistung des Datenschutzes

8.1 Massnahmen zu physischen Daten

Zur Gewährleistung der Sicherheit und des Schutzes der physischen Daten innerhalb der Assura-Gruppe, müssen die Mitarbeitenden folgende Grundsätze einhalten:

a) *Zugang zu den Gebäuden:* Nur die Mitarbeitenden mit einem Badge sind befugt, die Räumlichkeiten der Assura-Gruppe zu betreten. Es ist verboten, einen Badge einem Dritten zu überlassen.
b) *Clear Desk Policy*: Physische Datenträger mit vertraulichen Daten sind an mit Schlüssel verschlossenen Orten (Schreibtischen oder Schränken) aufzubewahren.
c) *Interne Post:* Umschläge mit vertraulichen oder geheimen Daten müssen verschlossen und mit der Aufschrift «vertraulich» beschriftet werden.
d) *Vernichtung von Dokumenten:* Papierunterlagen mit vertraulichen oder geheimen Daten sowie interne Dokumente mit Personendaten müssen geschreddert werden.
e) *Weitergabe von Dokumenten:* Die Weitergabe von Papierdokumenten innerhalb und ausserhalb der Assura-Gruppe hat gezielt und begrenzt zu erfolgen und hat verhältnismässig zu sein.
f) *Aufbewahrung von Dokumenten:* Papierdokumente sind innerhalb der Assura-Gruppe aufzubewahren und müssen gemäss der entsprechenden internen Weisung aufbewahrt und vernichtet werden.

8.2 Massnahmen zu Daten in elektronischer Form

Der Schutz von Daten in elektronischer Form innerhalb der Assura-Gruppe erfolgt gemäss folgenden Grundsätzen:

a) Der Zugang zu den Informationssystemen der Assura-Gruppe erfordert eine systematische Authentifizierung und Berechtigung jeder Benutzerin und jedes Benutzers (Benutzernamen und Passwort erforderlich). Diese werden regelmässig im Laufe der Zeit gemäss der Ad-hoc-Anweisung erneuert.
b) Die Zugriffsrechte auf die Informationssysteme werden gemäss den durch die verschiedenen Fachbereiche definierten Berufsrollen vergeben. Ausnahmen werden begründet und regelmässig durch die Vorgesetzten und Anwendungsverantwortlichen der Fachbereiche überprüft. Die Zugriffsrechte werden jährlich überprüft.
c) Im Ruhezustand und bei ihrer Übertragung werden die Daten verschlüsselt.
d) Für die sensibelsten Informatikzugriffe kann eine starke Authentifizierung erforderlich sein.
e) Elektronische Daten müssen gemäss der diesbezüglichen internen Weisung archiviert und gelöscht werden.
f) Daten und Informationen werden vor dem Recycling von Computerhardware vernichtet.
g) Es werden technische Massnahmen und Lösungen eingesetzt, um den Verlust, den Diebstahl und den Abfluss von Daten und Cyberbedrohungen zu bekämpfen.

9 Schlussbestimmungen

Das vorliegende Reglement wurde am 5. Juli 2023 vom Verwaltungsrat genehmigt und tritt am 1. September 2023 in Kraft. Es ersetzt und annulliert das Reglement über die Bearbeitung von Daten vom 1. Juli 2016.