Richtig gut versichert.

sympany

Bearbeitungs-reglement

Bearbeitungsreglement Sympany

	Inhalt	Seite
1	**Allgemeines**	**3**
1.1	Ziel des Bearbeitungsreglements	3
1.2	Verantwortliche Stellen	3
1.3	Schnittstellen	3
1.4	Betrieb des Informationssystems	3
2	**Arten von Personendaten, Herkunft, Bearbeitungszweck und Datenweitergabe**	**4**
3	**Technische und organisatorische Massnahmen sowie Kontrollverfahren nach Art. 3 DSV**	**4**
3.1	Zugangskontrolle	4
3.2	Datenträgerkontrolle	4
3.3	Kontrolle bei der Nutzung von Endgeräten	4
3.4	Bekanntgabekontrolle	4
3.5	Speicherkontrolle	4
3.6	Zugriffskontrolle	4
3.7	Eingabekontrolle	5
3.8	Protokollierung	5
3.9	Ausbildung der Mitarbeitenden	5
4	**Version/Änderung**	**5**

Bearbeitungsreglement Sympany

1 Allgemeines

Aufgrund Art. 5 und 6 der Verordnung über den Datenschutz (Datenschutzverordnung, DSV) haben die Vivao Sympany AG als verantwortliches Bundesorgan und die Sympany Versicherungen AG als private Verantwortliche (nachfolgend mit «Sympany» bezeichnet) für die automatisierte Bearbeitung der personenbezogenen Daten ein Bearbeitungsreglement zu erstellen. Gemäss Art. 84b KVG muss das Reglement dem Eidgenössischen Öffentlichkeits- und Datenschutzbeauftragten (EDÖB) zur Beurteilung vorgelegt werden und öffentlich zugänglich sein.

Ausführliche Datenschutzbestimmungen finden sich in der Datenschutzerklärung auf www.sympany.ch.

1.1 Ziel des Bearbeitungsreglements

Das Bearbeitungsreglement umschreibt die Datenbearbeitungs- und Kontrollverfahren, den Betrieb der elektronischen Datenbearbeitung sowie Massnahmen zur Datensicherheit und macht zusätzlich Angaben zur internen Organisation.

Das Bearbeitungsreglement gilt auch für die Datenbearbeitung im Rahmen der unabhängigen Datenannahmestelle (DAS) gemäss Art. 59a KVV. Die Einzelheiten für die entsprechende Datenbearbeitung werden in separaten Handbüchern festgelegt.

1.2 Verantwortliche Stellen

Die Rechtsträger der Sympany Gruppe (Vivao Sympany AG und Sympany Versicherungen AG) betreiben gemeinsam als verantwortliches Organ die IT-Systeme. Die Geschäftsleitung von Sympany trägt die Verantwortung für den Datenschutz und für die Datensicherheit. Die Geschäftsleitung besteht aus den Bereichen Direktion, Markt, Human Resources/ Corporate Functions, Operations & IT und Finanzen & Unternehmenskunden.

Die Belange des Datenschutzes und der Datensicherheit werden durch die Governance-Funktionen (Datenschutz, IT Security, Risk und Compliance Management) abgedeckt. Die Governance-Funktionen beraten die Geschäftsleitung, erstellen Vorgaben und sind in die Kontrollprozesse eingebunden.

1.3 Schnittstellen

Verschiedene Schnittstellen ermöglichen den Kontakt zu externen Dienstleistern und Leistungserbringern, die unter anderem direkt mit Sympany abrechnen. Mittels Authentifizierung, Verschlüsselungs- und Übertragungstechnologie werden der Datenschutz und die entsprechende Datensicherheit gewährleistet.

Bei der Bearbeitung von Personendaten im Rahmen der DAS (Datenannahmestelle) arbeitet Sympany mit der Outsourcingpartnerin Centris AG, Solothurn, zusammen, die von der Schweizerischen Vereinigung für Qualitäts- und Management-Systeme SQS gemäss der Verordnung über die Datenschutzzertifizierungen (VDSZ) zertifiziert ist. Die Zusammenarbeit von Sympany mit Centris AG ist in einem Zusammenarbeitsvertrag sowie in weiteren Handbüchern geregelt und dokumentiert. Zudem empfängt der Schweizerische Verband für Gemeinschaftsaufgaben der Krankenversicherer (SVK) für Sympany Rechnungen von erbrachten SVK-Leistungen. Die Einzelheiten dieses Outsourcings mit dem SVK sind in einem Dienstleistungsvertrag geregelt.

Die Datenübermittlung aufgrund behördlicher Anordnung erfolgt gemäss den entsprechenden rechtlichen Vorgaben.

1.4 Betrieb des Informationssystems

Der Betrieb des Informationssystems ist in geeigneter Form dokumentiert und erfolgt durch interne und externe Dienstleister. Die datenschutzkonforme Bearbeitung der Daten wie auch die Datensicherheit bei der Bearbeitung durch die externen Dienstleister werden in den jeweiligen Verträgen und Service Level Agreements geregelt. Die IT-Partner sind teilweise nach verschiedenen ISO-Normen zertifiziert (ISO/IEC 27001: Informationssicherheitsmanagementsystem).

Änderungen beim Betrieb werden mittels definiertem Change-Prozess durch Sympany initialisiert und in Zusammenarbeit mit den Applikationsbetreibern durchgeführt. Dieser Prozess ist nachvollziehbar dokumentiert und im Rahmen des internen Kontrollsystems durch eine externe Prüfungsgesellschaft geprüft.

In Weisungen, Handbüchern und anderen Vorgaben werden die Datenbearbeitungen und der Betrieb des Informationssystems definiert und die Prozesse im zentralen Qualitätsmanagementtool dokumentiert. Die verantwortlichen Organisationseinheiten sind verpflichtet, diese Dokumentationen regelmässig zu aktualisieren.

Personendaten gelangen über das Sympany Webportal und die Vertriebs-Software in das Kernsystem, welches beim Inkasso, der Leistungsabrechnung und -rückerstattung durch Finanz- und Rechnungsprüfungs-Software unterstützt wird. Die Daten werden über eine gesonderte Software archiviert. Die Systeme werden zusätzlich durch ein Tool für Customer Relationship unterstützt.

2 Arten von Personendaten, Herkunft, Bearbeitungszweck und Datenweitergabe

Sympany informiert in der Datenschutzerklärung (www.sympany.ch) welche Daten beschafft und bearbeitet werden, zu welchen Zweck und aufgrund welcher Rechtsgrundlage sie bearbeitet werden und wem Daten bekannt gegeben werden. In der Datenschutzerklärung wird zudem auf die Betroffenenrechte wie z.B. das Recht auf Auskunft oder Datenlöschung hingewiesen.

3 Technische und organisatorische Massnahmen sowie Kontrollverfahren nach Art. 3 DSV

3.1 Zugangskontrolle

Der Zugang zu den Büroräumlichkeiten von Sympany wird mittels Gebäudeleitsystem und Badgeverwaltung sichergestellt und überwacht. Es gelten die Vorgaben aus der entsprechenden internen Weisung. Sämtliche Zutritte werden anhand definierter mitarbeiterbezogener Zutrittsprofile gesteuert. Zutritt zu weiteren Gebäuden von Sympany ist ebenfalls nur mittels entsprechendem Zutrittsmittel möglich. Die Arbeitsplätze sind vor dem Zutritt unbefugter Dritter geschützt.

Mittels Clear Desk Policy sind die Mitarbeitenden von Sympany verpflichtet, vertrauliche Daten durch entsprechende Massnahmen zu schützen. Diese Massnahmen zur Wahrung der Vertraulichkeit gelten auch für die Arbeit im Homeoffice.

Spezialräume und Räume, in denen hochsensible Daten verarbeitet werden, wie z.B. Räume der Personalabteilung oder des Vertrauensärztlichen Dienstes, sind separat geschützt.

3.2 Datenträgerkontrolle

Durch die informationstechnische Ausstattung ist es einem begrenzten berechtigten Personenkreis möglich, Daten auf lokalen Datenträgern zu bearbeiten, zu löschen oder zu kopieren. Die Erstellung von Datenträgern unterliegt einem Genehmigungsverfahren.

3.3 Kontrolle bei der Nutzung von Endgeräten

Zum individuellen Drucken von Dokumenten wird der Druckauftrag mit dem persönlichen Badge der Mitarbeitenden direkt am Drucker freigeschaltet. Das zentrale Drucken findet in einem geschützten Bereich statt.

Ausgedruckte Daten werden so aufbewahrt, dass Unbefugte diese nicht einsehen können. Die Entsorgung von physischen Dokumenten wird mittels speziell verschlossener Container (Aktenvernichter) durch autorisierte Firmen, die dem Datenschutz unterliegen, vorgenommen.

3.4 Bekanntgabekontrolle

Datenempfänger, denen Personendaten mittels Schnittstelle übermittelt werden, werden entweder manuell oder automatisch durch eingerichtete Programmierung identifiziert. Die Schnittstelle steuert die Identifizierung der Datenempfänger. Dies gilt insbesondere auch für die Datenbearbeitung im Rahmen der DAS bei der Zusammenarbeit mit der Centris AG.

3.5 Speicherkontrolle

Durch die Vergabe von Zugriffsberechtigungen auf Systeme und Applikationen von Sympany wird verhindert, dass Dritte Daten unberechtigt verändern und löschen können. Zudem werden benutzerspezifische Mutationsberechtigungen vergeben.

3.6 Zugriffskontrolle

Die Mitarbeitenden erhalten nur auf diejenigen Informationen Zugriff, die für die Ausübung ihrer Arbeitsfunktion erforderlich ist. Die Zugriffsberechtigungen werden auf der Basis eines detaillierten und dokumentierten Rollenkonzepts erteilt und zentral von der IT von Sympany verwaltet und von den Verantwortlichen halbjährlich geprüft. Für die Authentifizierung der Mitarbeitenden beim Zugriff auf das Sympany Netzwerk und die Applikationen ist die Angabe von Benutzername und Passwort erforderlich.

Die Berechtigungen werden den Mitarbeitenden aufgrund des Mitarbeiterprofils (Funktion, Organisation) erteilt oder entzogen. Im Rahmen der Datenannahmestelle werden die Zugriffsberechtigungen von Sympany Mitarbeitenden und von Mitarbeitenden der Outsorcingpartnerin Centris AG in einer gesonderten Dokumentation ausgewiesen.

Die Erteilung der Zugriffsberechtigungen bei Ein- und Austritt der Mitarbeitenden inkl. externen Mitarbeitenden unterliegt geregelten Verfahren. Berechtigungsanträge müssen vom Vorgesetzten gestellt werden. Zugriffsberechtigungen von Mitarbeitenden auf die Systeme werden nur nach Vorliegen eines Arbeitsvertrags und einer unterzeichne-

ten Vertraulichkeitserklärung erteilt. Mitarbeitende mit Sonderaufgaben müssen eine ergänzende Schweigepflichterklärung unterzeichnen.

Neue Mitarbeitende erhalten eine entsprechende Unterweisung. Bei einem Austritt werden die Zugriffsberechtigungen auf den Systemen unverzüglich gelöscht.

Sämtliche externen Mitarbeitenden unterschreiben vor ihrer Tätigkeit für Sympany eine persönliche Datenschutz- und Schweigepflichtvereinbarung.

Die Informationen werden mit geeigneten technischen Sicherheitsmassnahmen vor unberechtigtem Zugriff geschützt. Für allfällige Datensicherheitsvorfälle existiert ein Meldeprozess.

3.7 Eingabekontrolle

Durch Unterweisungen werden die Mitarbeitenden befähigt, Eingaben in den Systemen vorzunehmen. Die Fachführung ist für die Durchführungs- und Ergebniskontrolle verantwortlich. Aufgrund einer Protokollierung ist nachvollziehbar, welche Personendaten zu welcher Zeit von welcher Person eingegeben wurden.

3.8 Protokollierung

Einzelne Applikationen verfügen über eine Protokollierung der automatischen Bearbeitung, damit nachträglich festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben oder bekannt gegeben wurden. Die Protokollierungsdaten werden revisionsgerecht festgehalten.

Sie sind ausschliesslich denjenigen Organen zugänglich, denen die Überwachung der Datenschutz- und Sicherheitsvorschriften obliegt.

3.9 Ausbildung der Mitarbeitenden

Die Mitarbeitenden, welche die IT-Systeme nutzen, werden im Bereich Datenschutz durch Schulung sensibilisiert. Sämtliche neu eintretenden Mitarbeitenden müssen eine Datenschutzschulung absolvieren. Einmal jährlich werden alle Mitarbeitenden einer datenschutzrechtlichen Schulung unterzogen. Des Weiteren werden die Mitarbeiten im Bereich der Datensicherheit geschult.

Die Mitarbeitenden werden im System mit diversen Anwendungshandbüchern sowie mit Datenschutzvorgabedokumenten unterstützt.

4 Version/Änderung

Dieses Bearbeitungsreglement ist nicht Bestandteil eines Vertrags mit den Versicherten oder Dritten. Es kann jederzeit angepasst werden. Die auf der Sympany Website veröffentliche Version ist die aktuelle Fassung.