Die Stuttgarter
Der Vorsorgeversicherer

Technische und organisatorische Maßnahmen Art. 32 DSGVO

01.01.2026

Dokumenteneigenschaften

Geltungsbereich	Alle Gesellschaften der Stuttgarter (Stuttgarter Lebensversicherung a.G., DIREKTE LEBEN Versicherung AG, Stuttgarter Versicherung AG, Stuttgarter Versicherung Holding AG, Direkte Service Management GmbH, Stuttgarter Vorsorge Management GmbH)
Status	Freigegeben / Veröffentlicht
Versionsdatum	01.01.2026
Vertraulichkeitsklausel	offen
Empfängerkreis	Alle Mitarbeiter, Auftraggeber und Auftragnehmer der Stuttgarter

Inhaltsverzeichnis

1 Rechenzentren

Das Rechenzentrum ist bei einem Dienstleister, der Kyndryl Deutschland GmbH, redundant auf zwei physische Standorte gespiegelt.
Die hierfür verwendeten Rechenzentren sind nach Standard

- SAE 3402
- ISO 27001
- ISO 9001
- PCI DSS
- TV-IT TSI Level 4
- German Federal Office for Information Security testation, EUCoC

zertifiziert. Mit dem Dienstleister wurden technische und organisatorische Maßnahmen vereinbart. Die Ausgliederung ist der BaFin angezeigt.

Das SAP-System wird durch den Dienstleister Collogia IT Services GmbH als SAP Managed Cloud Services in Netcologne-Rechenzentren betrieben.

Die hierfür geschlossenen Verträge regeln die Bereitstellung, den Betrieb und die Überwachung der Betriebsmittel. Das ISMS im Bereich SAP Managed Services ist nach ISO27001 zertifiziert.

Die Arbeitsplatz-Client-Systeme basieren auf Microsoft Windows und Microsoft Office365-Cloud-Internetdiensten in europäischen Microsoft-Rechenzentren. Datagroup Stuttgart GmbH stellt die Client-Arbeitsplätze und die damit verbundenen Microsoft Office365-Dienste zur Verfügung

Die folgenden technischen und organisatorischen Maßnahmen beziehen sich auf die Hauptverwaltung der Stuttgarter , Rotebühlstr. 120, 70197 Stuttgart.
Abweichende Regelungen für die Filialdirektionen werden explizit benannt.

2 Vertraulichkeit

2.1 Zutrittskontrolle

Maßnahmen, mit denen Unbefugten der Zutritt zu DV-Anlagen verwehrt wird, auf denen personenbezogene Daten verarbeitet werden.

- Der Einlass in das Gebäude wird durch den Empfang, Pförtner kontrolliert. Das Betreten und Verlassen des Gebäudes von Besuchern wird protokolliert.
- Der Einlass in den Geschäftsbereich ist durch Magnetkarte / Fingerprint abgesichert.

- Der Wachdienst verwaltet und protokolliert grundsätzlich Schlüsselübergaben. Die Schlüssel für die Verteilerräume werden durch die Systemadministration verwaltet.
- Die Gebäudesicherung erfolgt durch einen Wachdienst mit regelmäßigen Kontrollgängen 7 Tage, 24 Stunden die Woche.
- Das Gebäude, insbesondere sicherheitsrelevante Bereiche, sind alarmgesichert.
- Die Überwachung der Gebäudezugänge erfolgt durch Kameras.
- Eine Richtlinie regelt die Berechtigungsverfahren für den Zutritt von Mitarbeitern und betriebsfremden Personen.
- Schützenswerte Bereiche sind eingerichtet und werden physisch im Zutritt geschützt. (Arbeitsvorbereitung, Operating, Output, Datenschutzhaus, Systemprogrammierung, IDV, Telekommunikation)

Regelung für die Filialdirektionen:

- Die Büroräume sind abgeschlossen. Der Zutritt erfolgt nur über berechtigte Personen.

Regelung für das mobile Arbeiten:

- Der Zutritt beim mobilen Arbeiten (z.B. zu Heimarbeitsplätzen, Handy, Tablet) ist über Personalvereinbarungen geregelt.

2.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte DV-Anlagen benutzen.

- Über eine eindeutige Benutzerkennung und Authentifizierungsverfahren nach Stand der Technik ist ein Anwender identifizierbar.
- Die Vergabe/der Entzug von Berechtigungen ist in einem verbindlichen Verfahren geregelt.
- Das Unternehmensnetzwerk ist risikoorientiert segmentiert.
- Die Nutzung externer Speichermedien ist geregelt und wird restriktiv gehandhabt.
- Die Zugriffe und Zugriffsversuche werden protokolliert.
- Die Daten auf mobilen Geräten werden grundsätzlich verschlüsselt.
- Die Anzahl der fehlerhaften Anmeldeversuche ist begrenzt.
- Passwort-Rücksetzungen werden über ein verbindliches Verfahren geregelt.
- Der Arbeitsplatzrechner wird durch eine automatische Bildschirmsperre gesichert.

2.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass Befugte DV-Verfahren ausschließlich gemäß ihrer Zugriffsberechtigung benutzen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Ein Lösch- und Entsorgungskonzept für Datenträger ist implementiert.
- Ein Berechtigungskonzept zur Erteilung differenzierter Berechtigungen ist definiert und technisch umgesetzt.
- Zugriffsberechtigungen auf die Bestandssysteme, SAP und kritische Berechtigungen werden regelmäßig rezertifiziert.
- Ein Zugriff wird erst nach der Verpflichtung auf die Vertraulichkeit und den Datenschutz erteilt.

2.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

- Der Entwicklungs- und Produktionsbetrieb sind funktional über isolierte Systeme getrennt.
- Selektive Zugriffsverfahren für Gesellschaften und Bestände gewährleisten die interne Mandantenfähigkeit.

2.5 Pseudonymisierung

Maßnahmen, die gewährleisten, dass die Verarbeitung personenbezogener Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

- Testdaten für Entwicklertests werden pseudonymisiert zur Verfügung gestellt.

3 Integrität

3.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder bei Speicherung auf Datenträger nicht von Unbefugten entwendet oder manipuliert werden können.

- Der Versand personenbezogener und sonstiger vertraulicher Informationen wird über die Richtlinie zum Schutz von Informationen bei der Übermittlung geregelt.
- Für den Versand entsprechend qualifizierter Informationen ist ein Verschlüsselungsverfahren eingerichtet.
- Der externe Zugriff erfolgt über etablierte, abgesicherte Verbindungsstandards wie GSA (Global Secure Access) bzw. VPN (Virtual Private Network).

3.2 Eingabekontrolle

Maßnahmen, die gewährleisten, das nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systemen eingegeben, verändert oder entfernt worden sind.

- In den Bestandssystemen und SAP werden Bewegungen (Eingaben, Änderungen oder Löschungen) über Identifikationsmerkmale des Benutzers (z.B. aus der Authentifizierung) und Zeitstempel protokolliert.
- Die Archivierung und Aufbewahrung der Protokolldateien erfolgt nach festgelegten Fristen, abhängig von Geschäftsvorfällen.

4 Verfügbarkeit und Belastbarkeit

4.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Ein Notfallkonzept ist implementiert.
- Ein Perimeterschutz wird durch Firewall, IDS und Virenschutz gewährleistet. Das Update auf die Virensignaturen erfolgt mehrmals täglich.
- Zur Überprüfung der Wirksamkeit unserer Maßnahmen werden regelmäßig Penetration-Tests durchgeführt.
- Als hoch verfügbar klassifizierte Systeme werden redundant bereitgestellt.
- Eine unterbrechungsfreie Stromversorgung, sowie eine redundante Verkabelung sind installiert.
- Das gesamte DV-System wird in zwei physisch getrennten Rechenzentren gespiegelt.
- Ein vollständiges Backup- und Recovery-Konzept mit täglicher Sicherung und katastrophensicherer Aufbewahrung der Datenträger ist implementiert.

- Das Backup-Verfahren berücksichtigt Regelungen über Rhythmus, Medium, Aufbewahrungszeit und -ort.

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Datenschutzfreundliche Voreinstellungen

Der Datenschutz und die Datensicherheit werden schon bei der Planung und Entwicklung von IT-Systemen berücksichtigt (Privacy by Design)

- Datenschutzrechtliche Belange sind im Vorgehensmodell zur Anwendungsentwicklung in den entsprechenden Aktivitäten und Artefakten berücksichtigt.

5.2 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

- Auftragsvergabe oder Auftragsannahme werden nur über Verträge zur Auftragsverarbeitung bzw. Verträge mit Dienstleistern ohne Auftragsverarbeitung bzw. Verträge zur gemeinsamen Verantwortlichkeit abgeschlossen.
- Eine Kontrolle der Arbeitsergebnisse erfolgt durch den Fachbereich und den Datenschutzbeauftragten.