

## Datenschutz-Grundverordnung (DSGVO)

# Whitepaper für unsere Kundenunternehmen

Die Groupe Mutuel ist sich der Sensibilität der persönlichen Informationen, die Sie ihr anvertrauen, bewusst und sorgt für eine hohe Datensicherheit. Deshalb verpflichtet sie sich, alle Personendaten und sensible Daten verantwortungsvoll, ethisch und unter Einhaltung der geltenden Gesetzgebung zu bearbeiten.

Bei der Groupe Mutuel sehen wir es als unsere Pflicht an, unseren Kunden und Partnern gegenüber vollständig transparent zu sein bezüglich Sicherheitsregeln und -massnahmen, die wir umsetzen. Die Einhaltung der Bestimmungen zum Datenschutz durch unsere Kunden setzt auch deren Einhaltung durch die Groupe Mutuel voraus. Unsere Vorbildrolle ist uns wichtig. Ziel der Groupe Mutuel ist, eine Vertrauensbeziehung zu ihren Kunden und Partnern aufzubauen und diese zu stärken, damit die Vertraulichkeit und Sicherheit der ihr anvertrauten Personendaten gewährleistet ist.

### Deshalb erklären wir, die Groupe Mutuel, und die uns angeschlossenen Gesellschaften sowie unsere Partner, an die wir bestimmte Aufgaben delegieren,:

- dass wir dem Schutz der Daten unserer Kunden und Partner grösste Wichtigkeit beimessen,
- dass wir uns besonderen Regeln bezüglich Datenschutz im Versicherungsbereich unterstellen, insbesondere betreffend organisatorische und technische Massnahmen; diese Regeln sind insbesondere im Datenschutzgesetz (DSG), dem allgemeinen Teil des Sozialversicherungsrechts (ATSG), dem Krankenversicherungsgesetz (KVG), dem Gesetz über die berufliche Vorsorge (BVG), dem Unfallversicherungsgesetz (UVG) und in der Datenschutz-Grundverordnung (DSGVO) festgehalten,
- dass wir unsere Mitarbeitenden sensibilisieren und ausbilden, damit sie den Datenschutz und die Informationssicherheit bei jedem Schritt ihrer Projekte berücksichtigen,
- dass wir angemessene Massnahmen zur Einhaltung der Europäischen Datenschutz-Grundverordnung (DSGVO) treffen,
- dass wir uns verpflichten, die allgemeinen Grundsätze des Datenschutzgesetzes einzuhalten, insbesondere: Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität, Vertraulichkeit und Rechenschaftspflicht.

## Wir haben bereits Massnahmen im Rahmen unserer Tätigkeiten im Zusammenhang mit Leistungen für unsere Unternehmenskunden, ergriffen:

- Wir haben einen Data Protection Officer (DPO) ernannt, den Sie unter [dataprotection@groupemutuel.ch](mailto:dataprotection@groupemutuel.ch) erreichen.
- Wir haben die Art der bearbeiteten Personendaten definiert:
  - administrative Daten, die zur Verwaltung des Versicherungsvertrags und von Schadenfällen nötig sind, inklusive Lohnangaben
  - Daten über die Gesundheit der betroffenen Personen, Krankheiten, Schwangerschaften und Unfälle, bezogene medizinische Leistungen, Medikamente und Rehabilitierungsmassnahmen u. a.
- Wir ergreifen folgende Sicherheitsmassnahmen:
  - Einführung und Betrieb eines Managementsystems für Informationssicherheit (ISMS), das auf der internationalen Norm ISO 27001 basiert. Diese Norm schreibt unter anderem die Umsetzung einer Risikoanalyse und das Ergreifen von organisatorischen und technischen Sicherheitsmassnahmen vor, womit die Risiken vermindert werden.
  - regelmässige Audits der Organisation und der vorhandenen Systeme durch das interne Audit und externe Auditoren
  - externe Penetrationstests durch auf Informationssicherheit spezialisierte Unternehmen
  - Klassifizierung der Informationen, um angemessene Massnahmen zu treffen. Beispielsweise werden bestimmte sensible Daten verschlüsselt, eine starke Authentifizierungsmethode ist nötig zum externen Zugang zu den Systemen und zahlreiche Sicherheitstools werden benutzt, um die bestehenden Elemente zu kontrollieren.
  - Einführung und Betrieb eines Business Continuity Management Systems (BCMS), das auf der Norm ISO 22301 basiert
  - Erstellung eines Plans für die Geschäftskontinuität, um bei einer erheblichen Störung eine Weiterführung kritischer Prozesse zu gewährleisten
  - Einführung und Nutzung eines Qualitätsmanagementsystems (QMS), das nach ISO 9001 zertifiziert ist und die ständige Verbesserung der Prozesse gewährleistet
- Wir bewahren die Personendaten nicht länger auf als es gesetzlich vorgeschrieben ist und für die Verwaltung des Versicherungsvertrags, der Schadenfälle, der Verfahrens- und Beschwerderechte, des Inkassos und/oder für eventuelle Streitigkeiten zwischen Versicherer, Versichertem, Vermittler oder Dritten nötig ist.
- Wir hosten und verwalten die Daten in der Schweiz. In bestimmten Sonderfällen können wir externe Leistungserbringer beauftragen, die im Ausland ansässig sein können. Diese unterstehen jedoch den gleichen Verpflichtungen wie die Groupe Mutuel, insbesondere bezüglich der ärztlichen Schweigepflicht oder des Berufsgeheimnisses. Wir verpflichten uns, mit externen Leistungserbringern Verträge mit strengen Vorgaben über den Datenschutz abzuschliessen.
- Wir definieren den Zweck der Bearbeitung von Personendaten:
  - der bei der Datenbeschaffung angegebene, im Vertrag, den entsprechenden allgemeinen oder besonderen Versicherungsbedingungen oder im Gesetz genannte Zweck
  - die Risikoeinschätzung, Bearbeitung von Schadenfällen, administrative, statistische und finanzielle Abwicklung der Verträge
- Wir begrenzen die Weitergabe von Personendaten auf spezifische und ausgewählte Partner oder Dritte. Dies können Versicherungsvermittler, Rückversicherer, Ausgleichskassen, Ärzte, Experten, Arbeitgeber, Spitäler, andere Versicherer, Leistungserbringer, Rechtsschutzversicherer, Sozialdienste oder Revisionsstellen sein.
- Wir behandeln die Personendaten und sensiblen Daten vertraulich. Sie werden nur auf der Grundlage von gesetzlichen Verpflichtungen, von Gerichtsentscheiden, der allgemeinen Versicherungsbedingungen oder der Zustimmung der betroffenen Person an Dritte (z. B. Rückversicherer, Ärzte, Begünstigte, IV-Stelle, Sozialversicherungsträger des Wohnlandes der versicherten Person) weitergegeben.

Groupe Mutuel

Gesundheit® Leben® Vermögen® Unternehmen®

**Groupe Mutuel**

Rue des Cèdres 5 – Postfach – CH-1919 Martigny

