General Data Protection Regulation - GDPR

White paper for our corporate clients

For many years, Groupe Mutuel has been aware of the sensitivity of the personal information you entrust us with and understands the importance of protecting this data. This is why it makes every effort to manage personal and sensitive data responsibly, ethically and in compliance with the legislation to which it is subject.

At Groupe Mutuel, we believe it is our duty to be totally transparent to our clients and partners with regard to the rules and security measures we are implementing. The compliance of our customers and partners with data protection regulations also depends on our own compliance. Therefore, we take pride in being a role model. Groupe Mutuel intends to establish and strengthen a relation of absolute trust with its clients and partners in order to ensure the confidentiality and security of the personal data entrusted to it.

Therefore, we, Groupe Mutuel, our member companies and the partners to whom we subcontract a number of tasks, declare that:

- We attach great importance to the protection of our customers' and partners' data.
- We are subject to special data protection regulations in the insurance sector, in particular with regard to organisational and technical measures. These rules are contained in particular in the Federal Law on Data Protection (LPD/DSG), the Federal Law on the General Part of Social Insurance Law (LPGA/ATSG), the Federal Law on Health Insurance (LAMal/KVG), the Federal Law on Occupational benefits (LPP/BVG) and the Federal Law on Accident Insurance (LAA/UVG), as well as in the General Data Protection Regulation (GDPR).
- We educate and train our employees to take data protection and information security into account at every stage of their projects.
- We take the appropriate measures to comply with the European Data Protection Regulation (EDPR).
- We are committed to the general principles of the Law on Data Protection: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, retention limitation, integrity, confidentiality and liability.

Today, we have already taken measures within the context of our activities related to the services provided to our corporate clients:

- We have appointed a Data Protection Officer (DPO) who can be contacted at dataprotection@groupemutuel.ch.
- We have defined the type of personal data that is processed, namely:
  - the administrative data needed to manage the insurance contract and claims, including salary information;
  - data relating to the health of the persons concerned, illnesses, pregnancies and accidents they have suffered, the treatments they receive, medicines, rehabilitation measures, etc.
- We take the following security measures:
  - Implementation and operation of an information security management system (ISMS), based on the international standard ISO 27001. This standard requires, among other things, a risk analysis and the implementation of organisational and technical security measures to mitigate risks.
  - Regular audit of the organisation and systems in place, both by the internal audit and by external auditors.
  - External intrusion tests by companies specialised in computer security.
  - Classification of information in order to take appropriate action. For example, some sensitive data is encrypted, strong authentication is required for access to systems from outside and many security tools are used to control the elements in place.
  - Implementation and operation of a business continuity management system (BCMS), based on the international standard ISO 22301.
  - Establishment of a business continuity plan to ensure the continuity of critical processes in the event of a major crisis.
  - Implementation and operation of a quality management system (QMS), ISO 9001 certified, which ensures continuous process improvement.
- We do not retain personal data longer than is necessary, required by law, or required for the administration of the insurance contract, claims, rights of recourse, debt recovery and/or any disputes between the insurer, the insured, the intermediary or third parties.
- We store and manage data in Switzerland. In certain specific cases, we can call upon one or more external service providers, possibly based abroad. However, they remain subject to the same obligations as Groupe Mutuel, particularly with regard to medical or professional secrecy. We undertake to conclude agreements imposing strict data protection obligations on these external providers.
- We specify the purpose of processing personal data, namely:
  - the purpose indicated at the time of data collection, in the contract or in the related general or special terms and conditions, or in the law;
  - risk assessment, claims handling, administrative, statistical and financial monitoring of contracts.
- We limit the communication of personal data to specific and selected partners or third parties. These may be insurance intermediaries, reinsurers, compensation funds, doctors, experts, employers, hospitals, other insurers and healthcare providers, legal protection, social services or auditors.
- We process personal and sensitive data confidentially and only disclose them to third parties (e.g. reinsurer, doctors, beneficiaries, AI/IV disability office, social security of the insured person's country of residence) on the basis of legal obligations, court decisions, general terms and conditions of insurance or with the consent of the person concerned.

Groupe Mutuel
Rue des Cèdres 5 – P.O. Box – CH-1919 Martigny

Avenir Assurance Maladie SA – Easy Sana Assurance Maladie SA – Mutuel Assurance Maladie SA – Philos Assurance Maladie SA – SUPRA-1846 SA – AMB Assurances SA
Groupe Mutuel Assurances GMA SA – Mutuel Assurances SA – Groupe Mutuel Vie GMV SA
Foundations managed by Groupe Mutuel: Groupe Mutuel Prévoyance-GMP – Mutuelle Valaisanne de Prévoyance – Mutuelle Neuchâteloise Assurance Maladie

Edition 7.18