Data protection for insurers: Everything under control?

The public is paying closer attention to data protection than ever before. Legal requirements have become much more extensive and complex since the partial revision of the Federal Act on Data Protection (FADP) entered into force on 1 September 2023. While insurers have introduced the revised Federal Act on Data Protection within the scope of elaborate projects, measures taken to address many aspects of it were only short-term in nature to save time and conserve resources. Since this comes with risks, insurers are well advised to actively manage those risks by having the maturity of their own implementation checked by a third party.

Entry into force

The partial revision of the FADP entered into force on 1 September 2023 without any transition period. Despite many amendments that align it with the EU General Data Protection Regulation (GDPR), the FADP still adheres to its own basic concept and, as a result, deviates from the European model in several different regards.

Impact on insurers

For insurers, processing personal data is an everyday part of doing business. That makes data protection indispensable, particularly when it comes to insurers that process particularly sensitive health-related data.

Sanctions

Unlike under the GDPR, data protection sanctions in Switzerland can be levied personally against responsible individuals – meaning the employees involved. Data protection violations can result in hefty fines of up to CHF 250,000.

Usually even more costly, however, is the reputational damage caused by data protection violations. It can take years for a company to regain the market's trust.

Implementation patchy

Most insurers have carried out internal FADP implementation projects. Many of them ran into difficulties, however, that they were unable to fully overcome before the FADP entered into force. This holds particularly true when it comes to incorporating the new FADP requirements into the internal control system.

Another weak spot at many companies is the automatic deletion of data. Because this is typically difficult to accomplish from a technical perspective and enormously expensive due to the complex interdependencies that exist between databases and data flows. IT systems are also being redesigned and modernized all the time, which is why some companies deliberately decide against making legacy systems "fit for purpose".

Our recommendations

Our "post-implementation check" examines whether all FADP-relevant aspects of the implementation project have been identified, weighted correctly and implemented. This offers valuable insights and can point out ways to close any gaps found as part of an ongoing improvement process.

We generally recommend that insurers continue to develop their data protection framework on an ongoing basis. They should define and document any binding responsibilities and processes this involves and incorporate those into their internal control system (ICS).

The effectiveness of data protection concepts should also be regularly measured using specific key performance indicators (KPIs) and reported to the board of directors.

Ultimately – and this is always pivotal – this framework must always be put into practice.

Data protection as a never-ending process

That means insurers cannot view data protection as a fixed list of requirements that simply need to be implemented. On the contrary: data protection is a never-ending process. Because once FADP implementation is done, it's then time for FADP optimization.

Our services

KPMG helps you with all aspects of data protection and offers a variety of different services such as:

- Audit of data protection compliance (gap analysis)
- Audit and improvement of the data protection control framework
- Measurement and reduction of residual compliance risks
- Development of company-specific concepts and programs, such as data deletion concepts
- Documentation of technical and organizational measures related to data protection
- Support from our DPO Support Service (on-call specialists) at any time on all matters related to data protection law

Our team of highly qualified specialists with a wealth of experience in the areas of data protection, IT security, legal and compliance, risk and project management, audit and certification, will be glad to help you on all data protection-related matters.

Contacts

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch

Dr. Thomas Bolliger
Client Partner Privacy

+41 79 354 52 67
tbolliger@kpmg.com

Alexander Lacher
Partner, Insurance Regulation & Compliance

+41 58 249 33 66
alacher@kpmg.com