CyberWehr
RISK MANAGEMENT SOLUTIONS GMBH
Monika Wehr ▪ +41 79 348 55 63 ▪ info@cyberwehr-rms.ch ▪ 8803 Rüschlikon, Alte Landstrasse 109

The goal of data protection compliance is data protection consulting

Which laws apply?
At the heart of the General Data Protection Regulation (GDPR) is protection for citizens: they should fundamentally retain sovereignty over their own data. The GDPR protects uniform and strong data protection in the EU; existing national laws in the individual EU countries have been adapted to the GDPR and guarantee a uniform level of data protection. Switzerland and the UK, as so-called third countries, have also adapted their data protection laws (DSG, Switzerland), also to facilitate trade relations with the EU. The DPA will enter into force in mid-2022 without transition periods. The GDPR applies regardless of whether the processing takes place in the EU or not. It also applies to all processing operations of personal data carried out by controllers and processors based in the EU.

What do DSGVO and DSG regulate? Legal requirements that must be considered in the company's business processes during implementation:
The DSGVO places the processing of personal data under a ban with a "permission proviso". For processing to be lawful, it may only take place in the EU if there is consent from the data subject or a legal obligation. This requirement has not been implemented 1:1 in Switzerland, so that companies that offer their goods and services in the EU must also consider the consent of the reader on their website when storing or tracking personal data with cookies. The legal conformity of the website must therefore also be checked. In the privacy policy, the responsible party must fulfill its duty to inform and explain how the data is processed by an organization, i.e., how this data is collected, used and whether it is passed on to third parties.

Stricter information and disclosure obligations when obtaining personal data and a reporting obligation in the event of loss of personal data (data protection breach/data mishap) should lead to greater transparency. Violation of these obligations will be punished with painful fines. Data protection will be adapted to new technological developments: various provisions on profiling and automated individual decisions as well as on data protection through technology are intended to further increase the protection of personal data.

Citizens (data subjects) can demand their rights, the right to access, information, objection, deletion of data and data portability. Performance objectives such as integrity, confidentiality, and availability of data lead to special requirements in data protection. Data protection by technical design (Privacy by Default) and data protection specifications in the construction and design (Privacy by Design) of devices, machines, applications and software require a risk-based approach, a mandatory exercise, not only for risk identification, but also for determining appropriate technical and organizational protection measures to meet the assurance objectives. In the case of processing particularly sensitive data, e.g., health data, a data protection impact assessment is a mandatory requirement. A particular risk is posed by data transfers to non-European countries, especially in the case of service providers based in a cloud. The legal obligation of "accountability" to maintain a documented list of processing activities serves as proof for the supervisory authorities.

We provide you with a roadmap for the pragmatic implementation of the legal requirements for your company.