CyberWehr
RISK MANAGEMENT SOLUTIONS GMBH
Monika Wehr ▪ +41 79 348 55 63 ▪ 8803 Rüschlikon, Alte Landstrasse 109

Roadmap – Implementing Privacy in daily business:
The Swiss Data Protection Law and the EU Data Protection Regulation (GDPR) anchored therein require companies to comply with data protection requirements on a selective and structural basis. In particular, it means for export-oriented SMEs that in the event of a data protection breach, a company must not only be able to withstand the scrutiny of the supervisory authority but must also be able to prove to the supervisory authority that it was working in compliance with data protection regulations at a given point in time. There must be documented proof ("accountability") that the company complies with the data protection requirements on an ongoing basis, even for a case that occurred in the past.

Therefore my recommendation is that companies (depending on their size) shall create a data protection policy and/or a data protection manual in order to address the data protection requirements in their company.

Protecting a company's digital future starts with knowing the current inventory of personal data, where it is stored, and what measures are needed to prevent unauthorized access or even data theft.

Necessary steps to implement the requirements according to Swiss data act (DSG)/GDPR:

- ⇨ Optional: **Risk analysis ISO 27001/2** and determination of the hazard potential. The best method for the targeted determination of priorities for risk-mitigation measures.
- ⇨ **Information security and data protection management.** Internal data protection policy. Contingency planning for a prepared response to a data breach.
- ⇨ Comprehensive orientation on the legal requirements to avoid **fines** according to clause 83 GDPR due to insufficient compliance with information, storage or deletion obligations.
- ⇨ **The rights of data subjects:** access, information, to be forgotten, data portability, etc. according to clause 25, 28, 29 revDSG/Art. 12 – 14, 15 – 19 – 21, 30 GDPR**.** The introduction of a complaint management system with a deadline management (deletion concept). Are business processes and systems suitable, for example, to comply with the duty to information and the deletion of personal data immediately?
- ⇨ **Directory of Processing Activities (VVT),** clause 5 term f+g revDSG/ Art. 30 GDPR: documentation & proof of the individual processes, process description for each individual processing activity with details of legality, processing purpose, accuracy and timeliness of the data. Proof of appropriate technical and organizational measures.

- ⇨ **Data protection by technology design Data protection "by design" and "by default"** clause 7 revDSG para. 1+2/Art. 25 para. 2 + 32 GDPR. Appropriate technical and organizational measures to systematically protect the processing of personal data: data protection against breaches of integrity, confidentiality and availability, etc.

- ⇨ **Commissioned data processing,** clause 9 term 3 revDSG/Art. 28 GDPR. When must a contract be signed when involving external third parties, e.g., tax consultants, payroll accounting in data processing?

- ⇨ **ECJ ruling Schrems II of 12.7.2020** – legal framework of the **cloud** - do they meet the data protection security standard? Does limited access or "public access" make sense? Attention: if your cloud provider is located in the USA or a third country, there is an acute need for action where appropriate.

- ⇨ Are your **employees trained** in accordance with clause 39 GDPR to respond appropriately in the event of a data breach, to a complaint from a data subject, or to an email containing **malware**?

- ⇨ Notification of a data protection violation (**data breach**) pursuant to revDSG clause 24 new/GDPR clause 32-34 to supervisory authority/MELANI. Is there an **emergency concept** in the event of a crisis?

- ⇨ **"Accountability"** according to clause 30 GDPR: You are obliged to comply with the basic values of data protection: transparency, data minimization, confidentiality, integrity and availability. There is a legal obligation to provide proof to the supervisory authorities.

- ⇨ Updating the website **privacy policy**

- ⇨ **Automated software solution:** By means of a software solution, any company can implement data protection without its own know-how and without much effort, provided that the data protection coordinator has good IT skills. The creation of any data protection documentation can be fully automated with our software, a web-based solution.