

EU General Data Protection Regulation (GDPR):

Effective since end of May, but realization still in early stages

Starting Point

The new European data protection regulation (GDPR) became effective on May 25, 2018, replacing the former Directive 95/46/EG on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Through its territorial extension, GDPR also impacts companies outside the European Economic Area (EEA) processing data related to natural persons resident in the EEA. Therefore, most Swiss banks are impacted by GDPR as they – e.g., serve European clients, employ EU-resident cross-border commuters, or mandate service providers from the EU and other EEA countries.

At the same time, Switzerland started the revision of the Swiss data protection law (Bundesgesetz über den Datenschutz, DSG) in order to strengthen data protection in Switzerland, ensure continuous equivalence with the European data protection, and avoid restrictions with regard to the European market access. Due to delays in the revision, the new DSG is not expected to become effective before 2019.

Against this backdrop, many Swiss banks started rather late with the implementation of GDPR. Per end of May, most institutions were able to implement the vast majority of GDPR requirements. However, many practical challenges remain.

Every bank should therefore ask itself, how well it is prepared for GDPR on the one hand and which gaps it needs to close with regard to the soon to be revised DSG on the other hand.

GDPR Health Check

Based on our advisory experience from GDPR projects at different banks, we have developed a GDPR Health Check, that permits an assessment of your bank's GDPR and DSG (current status) compliance without lead time. The assessment will be performed during a couple of workshops together with representatives from impacted areas of your institution.

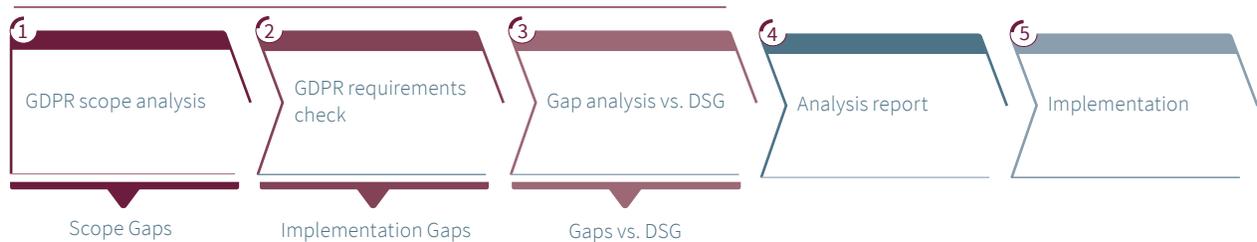
In a first step, we analyze the regional implementation scope together with you and identify possible scope gaps. In a second step, we jointly review how your bank has implemented GDPR based on a checklist summarizing the different requirements from an implementation perspective. Finally, we compare the GDPR implementation of your bank with DSG requirements (current status).

The results of the workshops are summarized in an analysis report. Of course, we will be pleased to support you in the implementation of findings, if desired.

Practical Challenges (examples):

- Definition and realization of a **compliance framework** helping to monitor, document, and evidence compliance with GDPR vis-a-vis supervisory authorities
- Laying down further **foundations for the data protection officer to perform his or her duties** such as the maintenance of the data processing register, the provision of regular trainings, the internal escalation, and reporting of data protection incidents
- Development and implementation of an **effective and efficient deletion concept**, that ensures an automated erasure of personal data in all systems (master-, sub-, and archiving systems) after lapse of legal processing grounds
- Definition and application of a systematic and consistent **risk assessment** – e.g., for data protection impact and data breach assessment (e.g., risk matrix)

Workshops:



Source: Synpulse

Our Experience – Your Benefit

The Synpulse GDPR Health Check offers the following advantages:

- Sustainability:** Based on our experience on GDPR (and other regulatory) projects, we have an excellent understanding of an audit-proof and sustainable implementation of regulatory requirements
- Speed:** By means of bundling our GDPR experience in a checklist, together with you, we are able to perform a Health Check without lead time
- Efficiency:** We understand where key implementation challenges lie and focus on those areas during our analysis (no «boil-the-ocean»)
- Outside-in view:** We have advised different banks with different implementation approaches and can provide you with examples of best practice of GDPR implementation
- Comprehensive approach:** Our banking know-how and interdisciplinary approach permits a detailed analysis of the GDPR implementation from a holistic viewpoint – which is particularly useful as regulatory requirements, organizational and process-wise implementation, as well as IT systems and architecture play an important role

Contact



Tina Freund
Associate Partner
tina.freund@synpulse.com



Eric Stehli
Associate Partner
eric.stehli@synpulse.com