The Swiss Data Protection Act has been revised and was passed by the Swiss Parliament in autumn 2020. It is based on the EU's General Data Protection Regulation (GDPR), but it does differ in one or two respects. The statutory adjustments are expected to enter into force during 2022.

The revised Data Protection Act (nDSG) is intended to create greater transparency concerning the use of personal data and strengthen the co-determination rights of the people whose data is being processed. Among other things, the act provides for the deletion of personal data in the event of termination of the processing activity, namely if a business relationship is ended.

The revisions are described in detail in various places, including here (Netzwoche article), which is why this article only briefly outlines the most important changes:

- strengthening of the rights of the persons concerned, namely by increasing transparency (information about data processing)
- promoting prevention and the individual responsibility of data processors
- strengthening data protection supervision (by the Federal Data Protection and Information Commissioner)
- extending legal sanctions

The consequences for data-processing companies in Switzerland should not be underestimated. The revised Data Protection Act affects banks as the parties responsible for their (personal) customer data, as well as outsourcing companies as the operators of applications that contain personal data. Companies will have to categorize and classify personal data (more) precisely and compile an inventory of systems to ensure that relevant measures can be realized within the context of data processing.

Consequently, the implementation of the nDSG requires detailed analytical and conceptual work before technical adjustments to the affected applications and any organizational changes can be commenced. Moreover, the nDSG affects the entire company: from the front to the back office, compliance and legal departments, any outsourcing partners and, as the responsible bodies, even the management team and the Board of Directors.

So how exactly can the implementation of the new requirements be tackled?

Processing directory

In the first step, the key element is the processing directory, which must be created and which brings together different processing purposes and applications. It is essential to develop a common understanding of personal data at the start. After all, not all personal data has to be granted the same level of attention within the context of the nDSG.

Among other things, the processing directory provides information about:

- the responsible party/order processor
- the processing purpose(s)
- justifications for processing
- the duty to supply information to the customer
- the origin of the data
- categories of affected persons and processed personal data

August 2021 | Silvan Lohri, Head Consulting Swisscom Banking | Swisscom Business Customers

- processing of personal data worthy of particular protection
- retention time
- measures to guarantee data security
- applications in which processing takes place

Experience has shown that a pragmatic level of detail should be reached in the processing directory: for instance, processing can be recorded along the bank's main processes (basic, payment transactions, investment, financing and pensions with specific additions (for example, processing in the context of marketing activities).

A list of applications, the data processed within them (categorized as CID, mass CID and not critical) and statements on persistent data retention subsequently help to establish the prioritization of the application to be addressed.

The projects that we have implemented with banks have shown that a pragmatic approach is sensible: not all personal data can be deleted from complex applications at the push of a button from day one. The amount of work required for "perfect" implementation in all applications is simply too large.

For this reason, a risk-based approach is sensible. The following principles can be used as assessment criteria: if, in an application,

- a large volume of personal data is processed,
- more sensitive data is processed (personal data worthy of particular protection) and/or
- various and high-risk forms of data processing are carried out,

the requirements for organizational and technical measures to guarantee data security are, accordingly, higher. This means that these applications should be granted high priority.

Technical solution concept

It is now a question of calculating and conceiving the technical feasibility of data deletion for the applications identified. Experience has shown that there is a lot to catch up on in this regard. Systems are designed to create, display and process data. However, they are missing a "button" to ultimately remove data in a controlled manner.

Application producers are thus (also) required to act: in an ideal scenario, deletions are carried out via proven processes with corresponding "checks and balances" and not on an ad hoc basis through the execution of a script directly on a database. In each case, it is important to consider dependencies between data sets, so no data omissions arise as a result of data deletion.

Important: even if banks generally focus on customer closures as an initial application case within the context of a pragmatic approach, the deletion of certain customer data at the customer's request should be considered, including within the framework of an ongoing customer relationship. However, it remains to be seen how many deletion requests of this type banks will be confronted with in the coming years. In our experience, banks have so far been conservative in the development of technical and organizational measures for these cases.

Implementation

Alongside the technical implementation of deletion functions and organizational adjustments, two further aspects should be considered:

1. analyses often show that the correction of personal data in systems is necessary prior to deletion. For example, contracts without an "expiration date" cannot be automatically deleted. In this case, it is important to enter the deletion date so that the document can be removed after the retention period. Experience has shown that such data correction can generate a great deal of work. For this reason as well, project activities relating to the nDSG must be started now if the time of entry into force in mid-2022 is to be realistic.
2. Data protection and security are not a matter (only) for the IT department but for company management (as well). Awareness of these topics must be strong in the management team. But not only in the management team. Constant sensitization and training of employees is required in order to minimize the risk of privacy policies being violated. The nDSG therefore constitutes another (necessary) opportunity to raise employee's awareness of this important topic.

Conclusion

The consequences of the revised Data Protection Act for banks should not be underestimated: alongside documentation obligations (keyword: processing directory), alterations to bank applications and organization should be expected. Accordingly, the topic should be addressed now.

At Swisscom we have been engaging with the topic of data protection and its legal provisions for years: whether in the context of our Swisscom end customers, as the number one outsourcing partner in the Swiss banking market or when providing consulting to banks concerning data protection.

Our Consulting and Compliance Team has supported various banks in this context with everything from

interpreting the nDSG to concepts and implementation. We would be delighted to support you, too. Please do not hesitate to contact us.

About the author:

Silvan Lohri
Head Consulting Swisscom Banking
Silvan.Lohri@swisscom.com
+41 79 700 47 49
LinkedIn
Website

August 2021 | Silvan Lohri, Head Consulting Swisscom Banking | Swisscom Business Customers