Grant Thornton

New data protection legislation – experiences with implementation

The revised Swiss Data Protection Act has been in force since 1 September 2023. In recent months, we have assisted a large number of financial service providers with the implementation of the new regulations. Our conclusion to date is that implementation can generally be accomplished with reasonable effort for the majority of the changes. However, the topic should not be underestimated and in general we can state that some innovations are easier to implement than others. In the following, we explain which topics are particularly in focus based on our practical experience with the new data protection law so far.

Classification[1]

	Banks / Securities houses	**Asset Management Institutes** (fund management companies, managers of collective assets)	**Asset manager / trustees**	**Other financial intermediaries** (SRO Supervisor)
Applicability	Yes	Yes	Yes	Yes
Relevance	High	Normal	High	High

[1] This is a highly simplified presentation, which should enable a quick initial classification of the topic. Each institution should determine the relevance and the concrete need for action individually.

Obtain an overview

It is absolutely essential that the financial service provider obtains an overview of the data processing in his institution at the beginning and considers roles and responsibilities accordingly. Without such a general overview, a rule-compliant implementation of the regulations will inevitably fail. Whether a formal record of processing activities is mandatory or useful must be decided on a case-by-case basis. In the projects we carried out, it has proven useful to draw up a record even in the case of only slightly more complex relationships (e.g. if several types of services are offered). The record can then be used as a basis for further implementation work.

Qualifying relationships with cooperation partners

The qualification of the relationships between the financial service provider and its respective cooperation partners (e.g. banks, IT, research service providers, corporate services, consultants) has proven to be particularly challenging. The new role model introduced with the revised Data Protection Act, with the “controller” and, if applicable, a “ processor” processing data on behalf of the controller, is only easy to implement at first glance. Contrary to a general usage of the language, not every contractual relationship that involves the transfer of personal data to a third party qualifies as processing on behalf of the controller within the meaning of the Data Protection

In practical implementation, all processing of personal data that is not carried out exclusively by the financial service provider must be checked to determine who is the “controller and whether there is also a “processor”.

In our projects, we have had good experiences with directly discussing such matters with the cooperation partners in order to understand in detail what personal data is processed, how and to what extent.

At least in cases where there is a processing on behalf of a controller, the contract between the financial service provider and its cooperation partner must be reviewed and, if necessary, adapted. The latter can be challenging in individual cases, especially if there are different views on the necessity of adjustments or their design.

Data security

Financial service providers must take suitable technical and organisational measures to adequately protect personal data. The Ordinance to the Data Protection Act contains an extensive catalogue of such technical and organisational measures. Apart from the fact that breaches of data security can have serious consequences, one should think here of the loss of client or employee data, for example: Anyone who violates the minimum data security requirements may be liable to prosecution.

In the practical implementation, we clarified in a first step which data security measures were already in place and documented them. Where IT services were outsourced to third parties, which was at least partially the case at the majority of the institutions we accompanied, we took this step together with these service providers whenever possible.

When assessing the appropriateness of the measures, the complexity of the circumstances must again be taken into account. Here, too, IT service providers were usually able to provide valuable input. However, the involvement of specialists is sometimes indispensable.

Implementation of the duty to provide information

For financial service providers who have a good overview of the data processing that takes place, the involvement of third parties and the existing measures for data security, the implementation of the duty to provide information is then possible with reasonable effort. However, since a breach of this duty can lead to a fine, a careful approach is highly recommended.

As a rule, the duty to provide information is formalized in one or more (e.g. separate for customers, employees, visitors to the website, etc.) privacy policies. If a website is available, it makes sense to publish the policy there. In addition, it should be pointed out in contracts and/or in the institution's general terms and conditions that the privacy policy can be found on the website of the financial service provider.

If there is no website, the privacy policy must be brought to the attention of the data subjects in another way. The information that the policy is generally available at the company is not sufficient.

Conclusion

Financial service providers who have not yet come to terms with the provisions of the new data protection law should do so promptly. Waiting is not an option. Although the work required for this is associated with effort, it can be efficiently implemented through good planning, a clear allocation of roles and responsibilities and, if necessary, with the involvement of the necessary specialist expertise.

Do you have any questions about the new Data Protection Act and/or its concrete implementation? Our specialists from the Regulatory & Compliance FS Team will be happy to support you. We look forward to hearing from you.

Boris Hofer
Director, Regulatory & Compliance FS
Grant Thornton AG
T +41 43 960 72 63
E boris.hofer@ch.gt.com

Yasmine Schwager
Assistant, Regulatory & Compliance FS
Grant Thornton AG
T +41 43 960 72 46
E yasmine.schwager@ch.gt.com

Grant Thornton