Grant Thornton

New Data Protection Act as of 1 September 2023

The new Data Protection Act will come into force on 1 September 2023 – the deadline is approaching. What should financial service providers do in the next 3 months to drive the implementation forward? What are the biggest challenges?

Boris Hofer, Director, Regulatory & Compliance in conversation with Bettina Neresheimer, Head Marketing & Communication discuss these and other burning questions around the implementation of the new data protection law.

Bettina Neresheimer: On 1 September 2023, the new data protection legislation will come into force, what does this mean for financial service providers?
Boris Hofer: Practically all companies and thus also financial service providers process personal data (e.g. customer data, employee data). Accordingly, they will be affected by the new regulations. However, there are of course significant differences depending on the size, business model, etc. of the company.

Bettina Neresheimer: In what way?
Boris Hofer: To answer this question, one has to look at the new provisions in greater detail. One example: There are new regulations on how a relationship between two companies is to be regulated if one of these companies processes personal data on behalf of the other, e.g. by outsourcing IT services. In this context, one speaks of so-called processors. The number and complexity of such cooperations as well as a foreign connection can lead to a greater or lesser need for adaptation. If, on the other hand, a financial service provider processes all personal data exclusively "in-house", there is no need for action in this regard.

Bettina Neresheimer: How do you assess the implementation status of the individual financial service providers and what support are you currently being asked for?
Boris Hofer: We notice big differences. Most companies do not have to start from scratch. Asset managers that have outsourced the compliance function usually already have a framework that can be built upon. Finally, larger financial service providers have often driven implementation forward within the framework of extensive projects. Accordingly, we are currently requested for initial needs analyses, for implementation projects as well as for the assessment of already implemented data protection frameworks.

> "We recommend that companies initially get a broad overview of where and how they could be affected by the new regulations."

Bettina Neresheimer: Many financial service providers ask themselves: "Where should I start"?
Boris Hofer: A good question. We recommend that companies initially get a broad overview of where and how they could be affected by the new regulations. This requires knowledge about the type and scope of the personal data processed in the company. Our experience shows that with this "initial risk profile" it is already possible to estimate to a certain extent whether or where major adjustments will be necessary and how quickly this work should be carried out.

On the other hand, a responsible person should be identified within the company to deal with the issue and to coordinate and ensure the implementation of the new regulations. We see it relatively often with our clients that the competences of the compliance function are expanded accordingly. From a certain company size or complexity, however, a separate specialist unit is then common.

Bettina Neresheimer: What happens after that?
Boris Hofer: The "initial risk profile" that has been created provides a good overview. However, it is usually not yet sufficient to feel comfortable and to make the appropriate risk and implementation decisions. We therefore recommend that all financial service providers – regardless of their size and the initially estimated risk – systematically determine which "delta" exists to the new regulations. This is the only way to create a reliable basis for decision-making.

Bettina Neresheimer: This sounds rather complicated and especially for smaller financial service providers at best very burdensome...
Boris Hofer: ...the challenge is indeed that the outcome of the analysis should not be anticipated, even if this may be tempting from time to time. Thus, in our opinion, there is no way around a well-founded analysis. Without the corresponding experience and expertise, however, there is indeed the risk that too much or too little is clarified.

Bettina Neresheimer: Which adaptations are likely to require the most time and effort to implement?
Boris Hofer: This depends on the risk profile and the size of the company and, if applicable, on what already exists. For example, many financial service providers already have a data protection declaration that serves as a basis and can be adapted. Regardless of this, the review of the contracts with cooperation partners or the implementation of data security should certainly be tackled promptly, as adjustments in these areas cannot usually be made overnight.

Bettina Neresheimer: What do you have to pay particular attention to when implementing data security regulations?
Boris Hofer: This is actually a separate topic, especially since data security does not refer exclusively to the protection of personal data.

Today, a large part of personal data is available in digital form. Particular care must be taken when protecting electronic data, because once the need for protection has been determined, technical and organisational measures must be implemented to ensure the protection of personal data. It must be ensured that the data is only accessible to authorised persons (confidentiality), that the data is available when it is needed (availability), that the data cannot be changed (integrity) and that it can be traced when the data was processed and by whom (traceability).

The issue of traceability in particular could cause headaches for some manufacturers of applications that contain personal data.

Bettina Neresheimer: Can you explain this in more detail?
Boris Hofer: Applications are usually relatively good at logging the traceability of data changes. The situation is different when reading data. Read accesses are not always logged by default.

With Christopher Oehri and his team, Grant Thornton has proven specialists in this area who are happy to answer any questions.

Bettina Neresheimer: Your thoughts on the topic of "fines" in the new data protection legislation?
Boris Hofer: The catalogue of fines, which has been greatly expanded compared to the current legislation, should not be underestimated. It is true that not all violations of the new data protection legislation are included in this catalogue and negligent actions should generally not lead to a fine. With good preparation and a good framework, the risk can therefore already be limited. Since the maximum fines of CHF 250,000 are very high and these fines are basically of a personal nature, a company cannot afford to completely ignore this aspect of the new data protection legislation. Convictions of its own employees are certainly not in the interest of a financial services provider.

Bettina Neresheimer: There are still a good three months left for implementation. Is that enough or where do you see bottlenecks?
Boris Hofer: Financial service providers who have not yet started implementation are certainly well advised not to wait any longer. If they start promptly, timely implementation still seems possible even for companies with slightly more complex circumstances. For all companies, however, "the sooner the better" now applies.

Bettina Neresheimer: Finally, a personal question: What is the exciting thing about data protection for you?
Boris Hofer: Data protection affects a company in its entirety and cannot be viewed in isolation, e.g. as a purely legal issue or as the sole challenge of information security. I then assume that both the importance and complexity of data protection will continue to increase. If you look at the rapid developments in the field of machine learning (keyword: Artificial Intelligence), for example, it is already clear that there is a lot more to come.
The cross-functional implementation of data protection requirements, taking into account the various interests and with a view to the future, are thus and at least for me the most exciting thing about projects in this area.

Neresheimer: Thank you very much for the interview!

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

Further information about the topic "New Data Protection Act":

New Data Protection law as of 1 September 2023 – Most important updates at a glance (article in German)

The revision of the Federal Act on Data Protection

Grant Thornton