November 2020

Newsletter No. 146

The revised Data Protection Act – recommendations for implementation

The revised Swiss Federal Data Protection Act is expected to enter into force in early to mid-2022. It contains hardly any practically relevant transitional periods – obligations such as the duty to inform, the duty to perform a data protection impact assessment or to report data security breaches will largely apply from the date of entry into force. Timely compliance with these obligations requires preparation. The objectives and scope of implementation projects vary largely depending on, for example, the size and complexity of the company, the business model, the expectations towards the industry concerned and whether the General Data Protection Regulation (GDPR) is already implemented. A pragmatic and target-oriented approach is essential.

walderwyss attorneys at law

By Jürg Schneider
Dr. iur., Attorney at Law
Partner
Direct phone: +41 58 658 55 71
juerg.schneider@walderwyss.com

and David Vasella
Dr. iur., Attorney at Law
Partner
Direct phone: +41 58 658 52 87
david.vasella@walderwyss.com

and Lena Götzinger
Attorney at Law (Bar Association Frankfurt am Main)
Associate
Direct phone: +41 58 658 56 63
lena.goetzinger@walderwyss.com

The current Swiss Federal Data Protection Act (**DPA**) has been in force since 1993. Since then, digitisation has significantly changed business models, risks for data subjects and expectations for data protection and privacy. In the EEA, the General Data Protection Regulation (**GDPR**) entered into force in May 2018 and the Council of Europe Convention 108 was revised. The DPA is also being revised, in many respects along the lines of the GDPR. In turn, both obligations and risks for companies have been tightened, whilst the position of the Federal Data Protection and Information Commissioner (**FDPIC**) has been significantly strengthened.

In contrast to the GDPR, the revised Data Protection Act (**revDPA**) applies to all companies that have a registered office in Switzerland or whose processing has an impact here - including companies without international business. There are hardly any special provisions for SMEs. Therefore, preparatory or implementation measures are necessary for all companies (including companies outside the regulated sectors and that may not process particularly sensitive or extensive data or be in the public eye).

However, implementation is only successful and sustainable if the complexity and risks of the respective company's business environment are being considered. A one-size-fits-all approach is just as misguided as a detail-obsessed implementation. A pragmatic and target-oriented approach is essential.

Key amendments

The revDPA was passed by parliament on 25 September 2020. Consequently, the respective data protection ordinances, especially the Federal Data Protection Ordinance (**DPO**), need to be revised. The start of the consultation process on the revised DPO (**revDPO**) is expected in mid-2021. Both the revDPO and the revDPA are expected to enter into force in early to mid-2022.

Some amendments will have an impact in practice but will be of little importance for a company's compliance, e.g. its restriction to data processing concerning individuals. The following amendments, however, are of primary importance for implementation:

i. Controllers and processors are each obliged to keep an inventory of their processing activities ("inventory of processing activities"), equal to the corresponding obligation under the GDPR.

ii. Controllers can appoint a data protection advisor, which makes it easier to carry out data protection impact assessments.

iii. The revDPA stipulates a general duty to inform when collecting personal data, which no longer only applies to sensitive personal data. Yet, no new consent requirements are established, not even for profiling.

iv. Swiss data protection law requires an appropriate handling of risks for data subjects. This includes that the data controller assesses potential risks already at the planning stage of processing activities and consciously decides how to comply with data protection ("privacy by design"). In the case of processing with a greater risk for data subjects, the risk assessment must take the form of a data protection impact assessment and be documented.

v. Under certain circumstances, controllers established abroad are obliged to appoint a representative in Switzerland.

vi. When interacting with customers, suppliers and partners, the rights and obligations under data protection law need to be contractually allocated, e.g. by means of an agreement between controllers and processors.

vii. The rights of data subjects are strengthened, e.g. by the new right to receive a copy of certain data in machine-readable form.

viii. The timely deletion or anonymisation of personal data remains important.

ix. In the case of certain intentional violations, the individuals responsible may be fined up to CHF 250,000. A fine of up to CHF 50,000 may be imposed on the company instead where the individuals responsible for the breach cannot be or are not identified. In addition, there are liability, operational and reputational risks due to a possible intervention by the FDPIC.

Implementation

The implementation of the revDPA requires early planning. However, the crucial steps can be realised with relatively low effort. A step-by-step approach in which certain measures are given priority and further measures are tackled thereafter is usually possible and reasonable. Moreover, the work require for implementation also depends on whether, and to which degree, the GDPR has already been implemented.

Clarification of the need for implementation. Before starting an implementation project, the company - or group - should determine the relevant legal framework. Are the GDPR and national laws of EEA member states applicable? Do any additional sectoral provisions apply in Switzerland or abroad, e.g. secrecy protection regulations or insurance, financial market, health or human research law? Does the company act as a private or (also) as a federal body? In this context entities can also decide whether and to what extent a voluntary application of the GDPR is appropriate.

Inventories of processing activities. Both the GDPR and the revDPA require "inventories of processing activities", i.e. inventories in which the various processing activities are recorded (both by controllers and processors). Exceptions may apply to SMEs. Creating an inventory at least in certain areas - often supported by appropriate technical solutions - is usually a sensible first step. Inventories provide a certain clarity and guidance for the company (or the responsible persons in charge, respectively) with regard to further implementation measures. If companies have already created inventories on processing activities based on the GDPR, these should also satisfy the revDPA requirements. Equally important as the creation of inventories on processing activities is their maintenance. Therefore, it is necessary to develop strategies on how new or changed processing activities are recorded.

Internal responsibilities. Companies should implement an appropriate structure and the necessary expertise to comply with data protection obligations, provided such a structure does not already exist. If the GDPR applies, a data protection officer may need to be appointed where the GDPR or national laws require to do so. Whilst the revDPA does not foresee such an obligation, the voluntary appointment of a data protection advisor can be advantageous. Notably, such appointment exempts the company from the obligation to report certain riskier processing activities to the FDPIC (cf. Article 23 para. 4 revDPA).

Further documentation. Contrary to the GDPR, there is no general duty under the revDPA for the controller to comprehensively document compliance with data protection law. Nonetheless, documentation to a certain extent is necessary. Considering the general processing principles and special sectoral provisions, it is advisable to train employees in the relevant departments. Furthermore, it is prudent or even necessary to develop policies, guidelines and fact sheets. If such documents (implementing the GDPR) already exist, they need to be adapted to the revDPA – although with limited effort.

Transparency, consent and information. In addition to the principle of transparency, the revDPA introduces a new, general and active duty to provide information, whose infringement is subject to sanctions. It is therefore necessary to first check where and how personal data is collected, and which privacy notices are already in use (e.g. in general terms and conditions). In a few instances the revDPA sets stricter requirements than the GDPR. It needs to be clarified whether and where the consent of the data subjects is necessary or sensible and in what form it can be obtained. Consent may also be required by other laws, e.g. in the case of confidentiality obligations.

Collaboration with third parties. In collaboration with suppliers and customers, but also in the case of group-internal data flows, data protection competencies and accountabilities must be determined and agreed. Also, in accordance with the revDPA, controllers and processors are obliged to enter into a contract regarding the processing on behalf of the controller, which should be in writing. However, the required content does not go as far as under the GDPR, the requirements of which have become more or less a de-facto standard. Appropriate agreements may also be necessary in the case of joint responsibility and data transfers between independent controllers.

Data security and security breaches. Companies need to ensure that data processing is aligned with the principle of data protection by default in order to continuously guarantee data security and breaches can be detected, communicated internally, escalated if necessary and, under certain circumstances, notified to the FDPIC or the competent authorities or data subjects. This obligation applies simultaneously to any sectoral legal reporting obligations, for example of financial institutions.

Rights of data subjects. The rights of data subjects already existing today have been partly reworded and complemented by the new right to data portability. If data subject requests are frequent, suitable processes must be developed. Even companies that have already implemented the GDPR should review their practices, since the revDPA differs from the GDPR in a few - but important – aspects.

Data protection compliance requires planning

The implementation of the GDPR and the revDPA is not necessarily costly or time-consuming but requires planning. For reasons of budgeting and reporting alone, tangible planning is necessary. Only then can companies react appropriately to changes and delays. Walder Wyss AG can provide support to clients with a tried-and-tested toolbox of instructions, checklists and templates that reduce effort, time and costs. We are also happy to provide companies with guidelines for implementation – you are welcome to contact us.