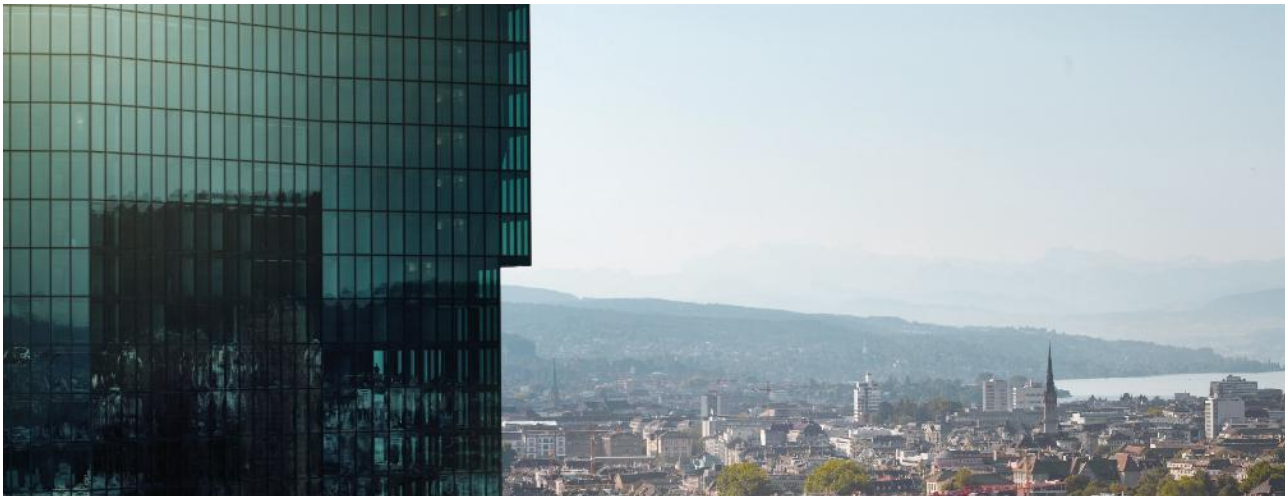
Revision of the Federal Act on Data Protection
Bulletin February 11, 2020



Revision of the Swiss Federal Act on Data Protection
How will it affect day-to-day business operations?

*The revision of the Swiss Federal Act on Data Protection (**DPA**) has entered the final phase. The parliamentary deliberations on the new DPA are almost complete, with only very few open points remaining. The new law is expected to enter into force in 2021. In this Bulletin, we answer the most important questions on the impact of the new DPA.*

What will not change?

Most importantly, the core **principles of Swiss data protection law will not change**. As already under the current DPA, the revised DPA will require compliance with a number of processing principles (such as transparency, purpose limitation, proportionality, data security, etc.), and the processing of personal data continues to be lawful if these processing principles are complied with.

In this respect, the revised DPA continues to differ from the EU General Data Protection Regulation (the **GDPR**). There will not be a need for a legal basis for each processing activity. Rather, a processing activity must only be justified based on consent, legal requirements or overriding private or public interests if any processing principle is not complied with, or if personal data is processed against the data subject's wish. Thus, the need for justification continues to be an exception rather than the default under the revised DPA.

In practice, we do not expect the revision of the DPA to have a major impact on how companies process personal data in Switzerland. Rather, the new DPA will have an impact on data protection governance and documentation needed to ensure compliance.

What will change?

Nevertheless, the revised DPA also brings a number of relevant changes. Largely, and not surprisingly, many of these changes are inspired by the GDPR and they will be familiar to data protection professionals working with the GDPR. The following changes are worth to be highlighted:

— Data relating to **legal entities will no longer be protected** by the DPA. As under the GDPR, only data relating to individuals will fall within the scope of the revised DPA.

— The data controller's **information duties** will be broadened. The controller will have to inform the data subjects at least about its identity and contact details, the purpose of processing and recipients or categories of recipients. The list provided in the DPA is however not comprehensive, and controllers will have to consider whether additional information needs to be provided to data subjects, so that they provide the "information needed for the data subjects to exercise their rights" under the DPA and to "ensure a transparent processing", as rather vaguely required by the revised DPA.

— There will be an increased need to **document processing activities** and to implement **governance processes**. Subject to certain exceptions applying to companies with less than 250 employees, data controllers and data processors will have to maintain **inventories of their processing activities**. For high risk processing activities, data controllers will have to perform a **data protection impact assessment**.

— The new DPA introduces a **data breach notification obligation** into Swiss law: The data controller will have to report any data breach that is expected to trigger a *high risk* for the personality rights of data subjects to the Swiss Federal Data Protection and Information Commissioner (the **FDPIC**); the notification is to be made **as soon as possible**. Thus, the threshold for a notification obligation to be triggered is slightly higher than under the GDPR. If needed to protect the data subjects, or if requested by the FDPIC, the data controller must also inform the affected data subjects.

— While the data subject rights will remain unchanged for most part, the revised DPA will introduce certain modifications regarding the **data subject access right**. In particular, it will likely be clarified that transfers among affiliates within the same group will not deprive the data controller from its right to refuse to provide information insofar as justified by its own overriding interests. Further, the revised DPA will introduce a right to **data portability** that is inspired by (but differs from) the GDPR.

— The revised DPA will regulate **automated individual decision making**. Subject to certain exceptions, an information duty applies to the extent that decisions are exclusively based on automated processing and have legal consequences for, or otherwise significantly impair the data subject. There will not be a prohibition of such decision making, but a right of the data subject to escalate to a human being for review.

— The new DPA will govern **profiling**, but the details are not yet resolved between the two parliamentary chambers. As it currently stands, the proposed regulation would be limited to certain restrictions with respect to performing credit checks and not have a relevant impact for most private companies.

— The revised DPA will distinguish between **controllers and processors**, essentially in the same way as the GDPR does. While the distinction already exists under the current DPA, it will now be expressly introduced into the new DPA. In substance, the new DPA does not provide for detailed requirements regarding **processor terms**, so that GDPR-compliant processor terms continue to be compliant also with the new DPA. Further, the new DPA expressly states that the appointment of subprocessors requires the approval of the data controller.

— The **obligation to register data files is abolished**.

— The **FDPIC is granted more extensive enforcement powers**. Under the new DPA, the FDPIC will be empowered to conduct investigations *ex officio* or upon complaint, to collect evidence and to issue orders. The FDPIC's orders will be binding, unless they are successfully appealed by the addressee. This deviates from the current law, that does not empower the FDPIC to issue binding orders to remedy non-compliance.

— The new DPA will significantly broaden the range of **sanctions** for non-compliance with the DPA. Under the new DPA, sanctions of up to CHF 250,000 can be triggered by a broad range of infringements of the DPA.

Will there be relevant changes regarding the export of personal data?

The core principles governing data exports will remain unchanged under the new DPA. Thus, data exports continue to be **permitted** to countries that have **adequate data protection laws** in place. Conversely, exports to third countries either require **justification** (such as the performance of an agreement with or in the interest of the data subject, overriding public interests, the enforcement of claims, etc.) or the **implementation of other remedies** to maintain an adequate level of data protection (e.g., by implementing standard contractual clauses, binding corporate rules, or other contractual arrangements, etc.).

However, there will be **a few amendments** with relevance for day-to-day business activities. *First,* the new DPA empowers the Federal Council to render **binding adequacy decisions** on the data protection level of foreign jurisdictions; the current non-binding FDPIC list of whitelisted countries will no longer be maintained. *Second,* the use of approved **standard contractual clauses will no longer have to be notified** to the FDPIC. *Third,* the possible justifications for exports to non-whitelisted countries are broadened in the context of foreign proceedings, given that the revised DPA will also **allow exports to exercise or enforce claims in proceedings at foreign authorities** (and not only courts, as under the current DPA). This will facilitate data exports for the purpose of foreign regulatory proceedings in front of administrative authorities rather than courts, which triggered a number of litigations under the current DPA. *Fourth,* the **information duties** of the data controller under the revised DPA will require the data controller to inform the data subject about the country to where the data will be exported, and the applicable justification or other remedy in case of exports to non-whitelisted countries.

Will the new DPA have extra-territorial reach?

Already the current DPA has a limited extra-territorial reach, which is the result of **Swiss international private law** that allows data subjects to choose Swiss law to apply in certain situations with respect to claims under data protection law. Going beyond that, the revised DPA will apply to **processing activities outside of Switzerland that take effect in Switzerland**. Further, data controllers domiciled outside of Switzerland will have to appoint a **representative in Switzerland** in case they process personal data of individuals in Switzerland and the processing (i) occurs in the context of the offering of products or services in Switzerland or to monitor the conduct of individuals in Switzerland, (ii) is extensive and regular and (iii) implies a high risk for the data subjects. The representative has to maintain an inventory of the relevant processing activities.

Will there be a Swiss Finish?

In general, the requirements under the revised DPA will not go beyond the level of protection of the GDPR. Most "Swiss finishes" that were included in the first draft of the DPA have been removed. As already mentioned, however, there are differences to be taken into account. For instance, the scope of the information duty of the data controller will not be delimited by a comprehensive list of information, but leave room for interpretation as to what specific information has to be provided.

Are there other differences to the GDPR?

There are a number of other differences compared to the GDPR. For instance, **consent** continues to be a viable means of justification for breach of privacy under the revised DPA as under the current DPA. In particular, and unlike under the GDPR, there will not be any unbundling requirements introduced into Swiss law. Differences also exist with respect to data subject rights.

What are the sanctions under the DPA?

While the sanctions for breaches of the new DPA will be **more severe** compared with the current law, they are still moderate when compared to the GDPR. It is important to note, however, that the revised DPA will not provide for administrative sanctions against companies, but continue to target responsible individuals based on criminal liability. Accordingly, an individual's non-compliance with the new DPA may be fined with up to CHF 250,000. If it would require a disproportionate effort to identify the individual offender acting within a company and the expected fine does not exceed CHF 50,000, the company can be fined instead.

What are the next steps?

A few differences remain to be resolved in parliament. In substance, these relate to the regulation of profiling activities and to details regarding the information duties, the data subject access right, and the justification of processing activities in the context of credit checks. Likely, the remaining differences will be resolved during Q1 of 2020. While a public referendum on the revised DPA is a possibility, no calls for a referendum have been made so far.

When will the DPA enter into force?

As it currently stands, the revised DPA will likely enter into force early 2021.

Will there be a general transitional period?

No, the revised DPA will not provide for a general transitional period. It will apply going forward as from its entry into force, with limited exceptions (e.g., in respect of ongoing proceedings, and the application of the principle of privacy-by-design).

How do companies prepare for the new DPA?

For businesses that have already implemented GDPR compliance, only limited changes are to be expected. For instance, they may have to review and update their documentation – such as privacy policies – to address the DPA requirements, extend their inventories to cover Swiss processing activities that were previously carved-out, and implement processes to comply with Swiss data breach notification obligations.

For businesses that have not yet complied with the GDPR, major implications are to be expected. In particular, they will have to review their data protection organization, governance and documentation, and their agreements with third parties.

In particular, the following steps and activities are to be considered in view of the new DPA:

- **Review the organization.** Consider establishing a data protection competence center for governance purposes and as internal and external point of contact for related questions.
- **Identify and document processing activities.** Understanding and documenting processing activities is key to enable an appropriate data protection governance. This applies even if there may not be a formal obligation to maintain an inventory, as may be the case for small and medium companies.
- **Assess compliance of the processing activities.** Check whether the requirements under the new DPA will be complied with. If not, implement necessary changes. Prioritize high risk processing activities and non-compliances that may have a high impact.

— **Implement appropriate processes.** Assess whether appropriate processes are in place to deal with data subject rights. There is no need to have a formal process in all circumstances, but processes should facilitate compliance. For instance, companies need to be in a position to adequately deal with data subject rights and data breach notification obligations.

— **Update relevant documentation.** For a large part, data protection compliance relies on up-to date and appropriate documentation. For instance, privacy policies need to be in place to inform employees, business partners and the public about processing activities, cross-border transfers may have to be secured by means of contractual arrangements with the data importer, and appropriate processor terms have to be implemented with third party processors. In view of the implementation of the revised DPA, this documentation needs to be reviewed and updated.

— **Review data security measures.** Companies will continue to have to make sure that personal data is appropriately secured to avoid data breaches. Thus, security measures need to be reviewed and updated from time to time.

— **Consider whether a representative in Switzerland needs to be appointed.** For certain foreign companies, the revised DPA will require the appointment of a representative in Switzerland.

— **Prepare for inquiries.** The obligation to demonstrate compliance with the DPA rests upon data controllers. Thus, be prepared to answer inquiries from authorities and to demonstrate compliance.

If you have any queries related to this Bulletin, please refer to your contact person at Homburger or to:

Gregor Bühler
Dr. iur., LL.M., Attorney-at-law, Partner
gregor.buehler@homburger.ch
T +41 43 222 16 44

Luca Dal Molin
lic. iur., LL.M., Attorney-at-law, Partner
luca.dalmolin@homburger.ch
T +41 43 222 12 97

Jeremy Reichlin
MLaw, Attorney-at-law
jeremy.reichlin@homburger.ch
T +41 43 222 16 03

Kirsten Schmidt
Dr. iur., LL.M., Attorney-at-law
kirsten.schmidt@homburger.ch
T +41 43 222 15 26

Homburger AG
Prime Tower
Hardstrasse 201
CH-8005 Zurich

T +41 43 222 10 00
F +41 43 222 15 00
www.homburger.ch