Briefing May 2020

The revised Data Protection Act – A Quest for Adequacy

While Swiss companies with customers in the EU have already had to move towards compliance with the EU General Data Protection Regulation (GDPR) including the new duties, such as the duty to inform, the duty to notify data breaches or the duty to implement a comprehensive register of all processing activities, companies only doing business in Switzerland have been spared from the same obligations. This is all about to change. The Swiss Parliament is debating the revision of the Federal Act on Data Protection (FADP), which will presumably enter into force in 2021. One of the main goals of the revised FADP is to be more in line with the GDPR.

The most important changes

The revised version of the FADP is still under discussion in the Swiss parliament. It is therefore not possible to make a final statement on what exactly the final provisions will include. However, there seems to be a consensus on the following new obligations:

– to actively inform people of all processing of their personal data upon its collection,

– to notify data breaches,

– to carry out data protection impact assessments,

– to keep a processing registry,

– to rely, where relevant, on unambiguous rather than implicit consent to process personal data.

Before we go into more detail regarding these changes, we will briefly discuss the context of the revision and its goals.

Why revise the FADP?

Under the GDPR, data transfers to countries outside the EU are allowed without restrictions when these countries are deemed to provide adequate protection for the transferred data. In the absence of such an "Adequacy Decision" delivered by the EU Commission, companies in the EU transferring data across borders have to comply with other safeguards which might prove cumbersome for companies in the EU and the importing countries alike.

As a result, companies outside of the EU have an economic interest in their country of "residence" being labelled as providing adequate protection for personal data, as it allows EU businesses to transfer data freely into their jurisdiction.

Switzerland, for now, is considered to provide such adequate protection. However, the EU Commission had evaluated Switzerland's adequacy under the predecessor of the GDPR, which was less comprehensive. The EU plans to review the Swiss Adequacy Decision

in June this year. This time, the GDPR is set to be the standard.

So that unrestricted data transfers can continue, Switzerland needs to be considered adequate under this new framework. In part, this interest in retaining adequacy with EU legislation is the reason for the revision of the FADP. Other reasons include the reinforcement of everybody's digital rights in the wake of the latest technologies and the granting of new responsibilities to the Federal Data Protection and Information Commissioner (FDPIC), Switzerland's supervisory authority regarding data protection.

The proposed changes

The revision of the FADP aims at moving Switzerland's data protection law closer to its European counterpart. One fundamental change is that, like in the GDPR, data concerning legal persons such as companies will no longer be protected under the revised FADP. In addition, the move towards the EU legislation results in the following proposed changes.

Obligations of Data Controllers

A data controller is a person (corporate or natural) that determines the purposes and means of processing personal data. Processing can be anything from collecting to analyzing, sharing, storing and deleting of personal data.

Under the revised FADP, the data controller will have the obligation to notify individuals of all processing of personal data. With the current FADP, only the processing of sensitive personal data (such as health data or data on religious beliefs) as well as the establishment of personality profiles have to be notified to the concerned person.

Furthermore, data breaches that result in a high risk to the person whose data has been breached will have to be notified to the FDPIC. A data breach occurs whenever there is an unauthorized disclosure of personal data, for instance when a USB-key is lost or when a company is hacked. The data controller will also have to notify such a breach to the affected person directly, if their protection requires it (*e.g.* to block a credit card after its details were compromised) or if the FDPIC instructs the data controller to do so.

If a new processing activity potentially presents a high risk to the rights of the persons whose data is processed, the data controller will have to conduct a so-called Data Protection Impact Assessment. This assessment evaluates the risks associated with the processing activities (*e.g.* based on the type or amount of data that is processed) and is to be shared with the FDPIC in case the risks turn out to be high. The FDPIC will then render a (non-binding) opinion on the planned processing activities. The purpose of this assessment is for data controllers to be more aware of the processing taking place within their operation.

To keep track of all the processing of personal data that takes place within a company, certain data controllers will have to maintain a processing registry that provides details on the processing purpose, type of processed data, recipients of data etc. There will likely be an exception to this obligation for businesses with fewer than 250 employees.

Under the current FADP, whenever the consent of the relevant person is required, it is enough that said consent is implied. Under the revised FADP, this will no longer be enough – consent will have to be unambiguous, *e.g.* by actively ticking a box.

Higher Fines

When an executive whose company is subject to GDPR asks why the company should care about the new duties under data protection law, their general counsel usually refers to the hefty fines for non-compliance (up to 20 Million Euros or 4% of worldwide annual turnover, whichever is higher).

Under the revised FADP, non-compliance will not be as costly as it is under the GDPR. The fine will be increased from CHF 10,000 to a maximum of CHF 250,000. However, and other than in the EU, the fine is and will remain of criminal nature rather than administrative. Also, it will generally be imposed on the individual responsible for non-compliance rather than the company itself.

More extensive powers for the FDPIC

Under the current FADP, the FDPIC has the authority to conduct investigations, to issue recommendations and to consult.

If the revised version of the FADP enters into force as it stands now, the FDPIC will move closer to its more powerful European counterparts. The revised FADP will give the FDPIC the authority to issue orders, up to and including the suspension of processing and the destruction of personal data.

However, the FDPIC will still not have the competence to issue fines directly. If the FDPIC becomes aware of conduct that is subject to sanctions, it will have to inform the relevant criminal authorities, which will then take over.

What to expect if Switzerland is not considered adequate

Should the EU Commission come to the conclusion that Switzerland's data protection law does not provide adequate protection according to GDPR, European businesses that transfer personal data to Switzerland will have to rely on alternative safeguards.

The most readily available of these alternative safeguards are standard contractual clauses regarding data protection. These clauses are established by the EU Commission and enable EU businesses to transfer personal data to their non-European counterparts who agree to apply an adequate level of data protection when processing the personal data they receive.

Swiss businesses with significant ties to the EU can, therefore, expect multiple requests from their EU business partners to sign such clauses in case the revised FADP is not considered adequate.

What are the next steps?

Parliament will further consult on the revised FADP during its summer session in June. Whether or not the results of this discussion are sufficiently clear for the EU Commission to reach a positive decision regarding Switzerland's adequacy in data protection remains to be seen.

Authors

Dr. Jan Kleiner
Partner
T: +41 58 261 53 84
jan.kleiner@baerkarrer.ch

Dr. Rehana Harasgama
Associate
T: +41 58 261 54 51
rehana.harasgama@baerkarrer.ch

Manuel Hofmann
Junior Associate
T: +41 58 261 53 26
manuel.hofmann@baerkarrer.ch

Further Contact

Dr. Corrado Rampini
Partner
T: +41 58 261 52 83
corrado.rampini@baerkarrer.ch

Bär & Karrer Ltd.
Brandschenkestrasse 90
CH-8002 Zürich
Telefon: +41 58 261 50 00
Fax: +41 58 261 50 01
zurich@baerkarrer.ch

Quai de la Poste 12
CH-1211 Genf
Telefon: +41 58 261 57 00
Fax: +41 58 261 57 01
geneva@baerkarrer.ch

baerkarrer.ch
Zürich, Genf, Lugano, Zug