Briefing November 2020

Update: The Revised Federal Act on Data Protection – Get Ready Now

Since the adoption of the EU General Data Protection Regulation ("**GDPR**"), Swiss companies with activities in the EU have had to move towards compliance with stricter data protection rules, such as the duty to inform, to notify data breaches and to implement a comprehensive register of all processing activities. On 25 September 2020, the Swiss Parliament adopted the revised Federal Act on Data Protection ("**revFADP**"), which aims to be more in line with the GDPR and is expected to enter into force earliest 2022. As a result, even companies that may not be within the scope of application of the GDPR will now face additional compliance requirements.

Final Approval by the Parliament

On 25 September 2020, the Swiss Parliament adopted the revFADP.

The conciliation committee reached the following compromise with regard to the last remaining and disputed topics:

– The notion of high-risk profiling was introduced;

– Consent for high-risk profiling has to be explicit;

– Companies can only justify the processing of personal data to verify the creditworthiness of an individual with their overriding private interests if no sensitive personal data is processed and the creditworthiness test does not involve high-risk profiling.

Key Points of the Revision

The revFADP will provide the following main changes:

– The revFADP will no longer apply to personal data of legal entities

– The definition of sensitive personal data will explicitly include biometric and genetic data

– New governance obligations will be introduced, such as maintaining data processing registries, the obligation to report data breaches and the requirement to carry out data protection impact assessments

– A duty to actively inform if personal data is processed will apply

– Foreign companies with substantial activities in Switzerland may have to comply with the revFADP

and will have to appoint a Swiss representative (similar to companies conducting business in the EU under the GDPR)

– Individuals will have a right to data portability (similar to the GDPR)

– Under the revFADP, the maximum fine for non-compliance with specific duties will be increased from CHF 10,000 to CHF 250,000 and will still be imposed against the individual responsible for the breach

– The Federal Data Protection and Information Commissioner ("**FDPIC**") will have the competence to issue orders, but not to issue fines directly (unlike under the GDPR)

– The general data protection principles will remain largely unchanged; consent for the processing of personal data will still only be necessary if required by the revFADP (unlike under the GDPR)

– Companies will still not have a duty to appoint a data protection officer

Practical Impact for Companies

Obligations of Companies

Under 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 individual. The revFADP will require companies to inform individuals of any processing of personal data in the future.

Such a duty to inform will also apply in the case of automated decision-making: A company will have to inform individuals of decisions which are taken exclusively on the basis of automated processing – without the intervention or influence of a natural person – and which have legal consequences for individuals or impair them significantly. The decision has particular legal consequences for individuals when a contract is concluded or terminated based on that decision. In such cases, the individual has the right to be given the opportunity to state their position and to request the company to have an individual review the automated decision.

A company will be able to restrict, defer or waive the provision of information if it is necessary to protect the company's overriding interests and if the company does not disclose personal data to third parties. Companies controlled by the same legal entity are not deemed to be third parties. Among others, companies will also be exempted from their information duty if the affected individuals already have the required information, if the company is required to process personal data by law, if statutory confidentiality duties apply or if the notification would defeat the processing purpose (*e.g.* during an ongoing internal investigation). If a company does not comply with this duty, it can be fined under the revFADP.

Furthermore, companies will have to report those data breaches that result in a high risk to the person whose data has been breached to the FDPIC. A data breach occurs whenever there is an unauthorised disclosure of personal data, for instance when a USB stick is lost or when a company's IT infrastructure is hacked. A company 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 company to do so. Non-compliance will not lead to a fine under the revFADP.

If a new processing activity potentially presents a high risk to the rights of the persons whose data is processed (*e.g.* if sensitive personal data is processed extensively, if public spaces are monitored systematically and extensively or when new technologies are used for the processing), the company may 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 discussed with the FDPIC in case the risks remain high even with any planned measures to eliminate those risks. Companies which have appointed a data protection officer will be exempted from consulting the FDPIC. Non-compliance will not be fined under the revFADP.

To keep track of the processing of personal data that takes place within a company, companies will have to maintain a comprehensive processing register that provides details on the processing purpose, type of processed data, recipients of data etc., unless they employ fewer than 250 employees and the processing activities only pose a low risk to the personality and fundamental rights of the affected individuals. Non-compliance will be subject to fines under the revFADP.

Consent Requirements and Profiling

Processing personal data will only require consent where required under the revFADP. Such consent will have to be given unambiguously. In addition, consent will have to be explicit if it concerns the processing of sensitive personal data, high risk profiling by a private person or any profiling by a federal body.

The revFADP defines profiling similar to the GDPR. Essentially, profiling describes the automated processing of personal data, to analyse certain aspects of an individual's personality (*e.g.* to send them personalised ads). To give an example: If a retailer uses a computer to automatically select a list of all the customers who ordered a specific product to send them an email informing them about a new type of product that could also interest them, this can be considered profiling.

High-risk profiling will mean profiling that leads to a high risk to the personality or fundamental rights of an individual, as it enables an assessment of essential aspects of their personality by linking data to each other.

Other Important Changes in Detail

– Privacy-by-design and -default: Companies will have to plan and set up their processing activities so that they are compliant with data protection law. They will also be required to ensure that the data processing settings of their products and services are privacy-friendly by default.

– Right to data portability: In certain cases, individuals will have the right to receive their data in a commonly and machine-readable format so that they can transmit such data to a different company (*i.e.* if an individual wishes to switch to a different company). In certain cases, individuals may also request the company to transmit their personal data directly to that other company itself.

– More extensive powers for the FDPIC: The FDPIC's powers will no longer be limited to conducting investigations and issuing recommendations. Under the revFADP, the FDPIC will have the authority to issue orders such as the suspension of processing or the irreversible erasure of personal data under the threat of a fine. However, if the FDPIC becomes aware of conduct that should be fined, it will have to inform the criminal authorities and will not be able to issue a fine itself.

– Additional fines: Companies will also risk a fine for the violation of individuals' access rights, for the disclosure of personal data abroad or assigning data processing activities to third parties without appropriate safeguards, and for the failure to comply with the minimum data security standards issued by the Federal Council.

Key Steps for Companies to Get Ready

The revFADP does not provide for a transitional period. However, as it is not expected to enter into force before 2022, we recommend companies to use the time until then to immediately assess the impact of the revFADP on their business activities and start implementing processes necessary to comply with the new rules by 2022.

Initial steps will notably include:

– Review all processing activities and implement a comprehensive register of all processing activities, incl. profiling

– Review and adapt privacy policies to the new requirements (*e.g.* extended information duty, automated decision-making, etc.)

- Review contracts with data processors and third parties, especially those involving cross-border data transfers
- Review whether you act as a data processor and need to adapt or amend existing contracts
- Introduce a process and clear responsibilities for reporting and handling data breaches
- Implement a process and clear responsibilities for deciding on when a data protection impact assessment is required and for conducting such an assessment
- Review and possibly update internal processes to obtain consent
- Possibly appoint a data protection officer
- For companies outside of Switzerland: assess whether the revFADP applies to you and if yes, appoint a representative in Switzerland and communicate details of the representative to the FDPIC

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

Jessica Messerli
Junior Associate

T: +41 58 261 53 58
jessica.messerli@baerkarrer.ch

Further contact

Dr. Corrado Rampini
Partner

T: +41 58 261 52 83
corrado.rampini@baerkarrer.ch