BIANCHISCHWALD

NEWS

NEW FEDERAL DATA PROTECTION ACT FOR SWITZERLAND

On 25 September 2020, the Swiss Parliament passed the revised Federal Data Protection Act ("rDPA"). It is not yet clear when the new law will enter into force. At its earliest, it may be expected for the second half of 2021. As there are no transition periods in the rDPA, it is advisable to start preparations in a timely manner.

An important goal of the revision was to ensure an adequate level of protection of personal data in line with the EU's General Data Protection Regulation ("GDPR"). This is necessary so that Switzerland can continue to benefit from the advantages of the EU Commission's adequacy decision currently in place. Without an adequate level of protection, personal data from the European Economic Area ("EEA") could only be transferred to Switzerland with additional security measures. It is unclear when the EU Commission will adopt its decision on the adequacy of the rDPA.

WHAT CHANGES?

The revision does not lead to fundamentally different requirements for the handling of personal data. Data processing in Switzerland is generally permissible for private companies and a justification (such as the consent of the data subject) is only required if the data processing is an infringement of the data subject's personality rights. Nevertheless, numerous changes must be observed. The most important changes, which will be relevant for many companies, are outlined below. The rDPA also amends the rules for processing personal data by federal public authorities. These changes are beyond the scope of the following overview.

RECORDS OF PROCESSING ACTIVITIES

The processing of personal data now requires that the controller (i.e. the natural or legal person who decides on the purposes and means of data processing) keeps a record of its processing activities. The same obligation applies to processors who process personal data on behalf of the controller. The minimum content of these records is specified by law and includes, for example, the identity of the data controller, the purpose of processing, the categories of data subjects and the categories of personal data processed. The Swiss Federal Council may provide for exceptions for SMEs with fewer than 250 employees, whose processing of personal data entails with a low risk for infringements of personal rights. However, the draft ordinance regulating these exemptions is not yet available. The extent to which companies will be exempted from this administrative obligation, remains unclear for the time being. In any case, compliance with data protection rules will be difficult to achieve without an (at least rudimentary) overview of the processing activities.

EXTENDED INFORMATION OBLIGATIONS

The rDPA expressly provides for an obligation to inform the data subject in connection with the processing of personal data. Sufficient information must be made available to the data subjects so that the transparency of data processing and the realization of their rights under the rDPA are guaranteed. The necessary information includes at least the identity and contact details of the controller, as well as the processing purpose for which the personal data is being collected. If the personal data is disclosed to third parties or transferred abroad, further information is required. The intentional violation of this obligation may have criminal consequences.

OBLIGATION TO REPORT BREACHES IN DATA SECURITY

If a breach of data security leads to a high risk for the data subject (e.g. violation of personal rights or fundamental rights), the Federal Data Protection and Information Commissioner ("FDPIC") must be notified in future. A breach of data security occurs, in particular, if personal data is unintentionally lost, destroyed or altered or becomes accessible to unauthorized persons. The law does not set a fixed deadline for such a notification but does stipulate that the notification must be made as soon as possible. The minimum content of the notification is prescribed by law: In particular, the nature of the data security breach, its consequences and the measures (planned or adopted) must be reported.

DATA PROTECTION IMPACT ASSESSMENT

The controller must prepare a so-called Data Protection Impact Assessment ("DPIA") if a planned processing activity may entail a high risk of violations of personality rights. A high risk exists, in particular, when new technologies are used, when particularly sensitive personal data (such as health data) are processed extensively (e.g. in a medical research project) or when extensive public areas are systematically monitored (e.g. a public railroad station). In addition to the description of the planned processing, the DPIA must contain an assessment of the risks and the planned protective measures. If a high risk remains despite the protective measures, the planned processing must be submitted to the FDPIC. If the FDPIC raises objections to the planned processing, he proposes suitable protective measures to the controller. Since the FDPIC has two months (or even three months in the case of complex processing) for his feedback, it is recommended to start the DPIA early.

REPRESENTATIVE IN SWITZERLAND

The rDPA provides for additional rights for the data subjects. The rights to receive and data surrender and transmission (so-called data portability) as well as the obligation to inform in the case of automated individual decisions should be mentioned in particular. The right to data portability allows the data subject to request from the data controller, free of charge, the surrender of his/her personal data (which he/she has disclosed to the data controller) in a common (machine-readable) format. Likewise, the data subject may request that the personal data be transferred to another controller. This presupposes that the data controller processes the data in an automated (i.e. not analog) way and that the personal data are processed in direct connection with a contract with the data subject or based on the consent of the data subject. Possible areas of application for this provision are, for example, a change of bank or insurance provider. The data subject may request that the existing personal data be transferred directly to the new service provider. For the companies, this right means that the technical prerequisites for fulfilling this right must be implemented.

Furthermore, an information obligation is introduced for decisions based exclusively on automated processing of personal data. The data controller must inform the data subject if the decision may significantly affect the data subject or if the decision "entails a legal consequence". Such a legal consequence is, in particular, the conclusion or termination of a contract. It is to be expected that the FDPIC will publish guidelines or information sheets to specify these undefined legal terms in more detail. Until such guidance is available, it is advisable to inform the data subjects in case of doubt.

ENFORCEMENT AND SANCTIONS

To ensure compliance with data protection obligations, criminal sanctions have been significantly increased. Breaches of data protection regulations can in future be punished with fines of up to CHF 250'000 (compared to CHF 10'000 in the past). Criminal liability is, in principle, directed against the natural person who commits the violation. The executive bodies of companies that intentionally or negligently fail to stop the breach in violation of a legal obligation may also be liable to prosecution. Likewise, in certain cases, the legal entity may be exposed to criminal sanctions. The cantons are responsible for the prosecution of criminal violations of the rDPA.

At the same time, the FDPIC receives new competences. In future, his sphere of influence will no longer be limited to a few subject areas, but he will be able to take action in all cases of data protection breaches. In addition, the FDPIC will be able to issue binding decrees and order the controllers to adapt or stop data processing and to delete the personal data concerned. Deliberate disregard of such orders can be prosecuted under criminal law.

WHAT ACTIONS NEED TO BE TAKEN?

The implementation of the rDPA will in most likely be more straightforward if a company has already implemented the requirements of the GDPR. In such cases, the existing internal data protection framework can be adapted to the specifics of the rDPA, which only requires selective changes. Foreign entities have to assess whether they have to appoint a representative in Switzerland.

If no GDPR framework has been developed (or if a periodic review of the framework is in order), the first step is to check which personal data is processed in the company and in what ways (so-called "data mapping"). Personal data covers all information that refers to an identified or identifiable natural person. This term thus includes, for example, information about employees, customers and contact persons of suppliers as well as website visitors. In contrast to the current Data Protection Act, personal data of legal entities will no longer be covered by the rDPA.

The results of the data mapping should be outlined in an overview (the record of processing activities), checked periodically and amended if

necessary. Based on this overview, the company can assess whether all required documents have been drafted and all processes required by the rDPA are sufficiently documented. As a minimum, we recommend assessing the following:

- Relationship with data processors (are there written contracts and do the contracts meet the requirements of the rDPA?)

- Data transfers abroad (are transfers to countries without a sufficient level of protection only carried out with appropriate safeguards?)

- Privacy notice (does it cover all processing of personal data and does the information meet the minimum requirements of the rDPA?)

- Is there a process in place to fulfill the obligation to report breaches in data security?

- Is there a process for conducting Data Protection Impact Assessment?

- Is it ensured that inquiries from data subjects can be processed in time and completely?

CHRISTOPH GASSER
Attorney-at-law, Dr. iur., LL.M. University of Michigan
Part-time judge at the Federal Patent Court
Partner | Zurich

THIERRY BURNENS
Attorney-at-law, M.A. HSG, CIPP/E
Associate | Zurich

STEPHANIE VOLZ
Attorney-at-law, Dr. iur.
Associate | Zurich

BIANCHISCHWALD LLC
mail@bianchischwald.ch
bianchischwald.ch

GENEVA
5, rue Jacques-Balmat
P.O. Box 5839
CH-1211 Geneva 11
P +41 58 220 36 00
F +41 58 220 36 01

ZURICH
St. Annagasse 9
P.O. Box 1162
CH-8021 Zurich
P +41 58 220 37 00
F +41 58 220 37 01

LAUSANNE
12, avenue des Toises
P.O. Box 5410
CH-1002 Lausanne
P +41 58 220 36 70
F +41 58 220 36 71

BERN
Elfenstrasse 19
P.O. Box 1208
3000 Bern 16
P +41 58 220 37 70
F +41 58 220 37 71