

NEWS

NEW DATA PROTECTION REGIME IN SWITZERLAND AND IN EUROPE - WHAT SWISS COMPANIES NEED TO KNOW

REVISION OF THE DPA AND OF THE GDPR

The rapid processing technological change led to view the hitherto existing legal provisions are no longer adequate. Therefore, the European Council and the European Union («EU») have decided to adapt their existing legislation. The EU General Data Protection Regulation («GDPR») was adopted in 2016 and will enter into force on 25 May 2018. Accordingly, Switzerland also has to adapt to the European legal developments. On 15 September 2017, the Federal Council published the message on the total revision of the Data Protection Act («E-DPA»), which may enter into force at the earliest by the end of 2018.

WHO MUST COMPLY WITH THE GDPR

For Swiss companies, action might already be required in order to comply with the GDPR, since this regulation has a wide scope and will also apply to the processing of personal data outside the EU.

Also companies, which do not have establishments in the EU, may still be subject to the GDPR where the processing activities are related to offering goods or services in the EU and, thus, personal data (such as names and addresses) are processed, or where the data processing activities are related to the monitoring of persons of the EU, for example by means of online tracking or analysis tools. Moreover, anyone who processes data outside the EU on behalf of a company in the EU has to comply with the GDPR.

WHAT THE GDPR AND THE E-DPA BRING

The GDPR and the E-DPA provide for a number of changes in the field of data protection. The main changes are briefly outlined below:

With regard to the E-DPA, the first important change relates to the material scope of the revised law, which now applies only to the processing of data of individuals. In fact, the DPA in its actual state seems very rarely used by legal

In Switzerland as in neighboring countries, varied efforts are being made in order to strengthen the protection of personal data. This entails, in particular, the adaptation of the existing rules to new technologies and the Internet era.

In some instances, Swiss companies need to comply not only with Swiss data protection laws and regulations, but also with the new European regulation, which brings a number of novelties for the processing of personal data. A quick overview of the main changes is provided below.

entities which rather use legal instruments fitted to their needs such as unfair competition law. Moreover, the E-DPA further introduces the «profiling» notion. This wording aims to take into account the possibility of anonymous data matching, which are not taken into account by the existing legislation but which in practice allow the identification of the concerned individuals. An additional change is the new requirements in case of subcontracting or «sub-subcontracting» of a data process, the E-DPA provides, amongst other requirements, a preliminary approval by the data controller in case of a «sub-subcontract».

Both the GDPR and the E-DPA enhance the individuals' right to be informed. The GDPR requires that any concerned person shall be informed comprehensively and in a clear and plain language about the processing of his/her data. In Switzerland, under the E-DPA, the information may, depending on the circumstances, be communicated in a standardized form, for instance in the General terms and conditions. The right to be informed is, however, subject to certain exceptions.

In the EU, the conditions for obtaining consent have been restricted. The GDPR requires a clear affirmative act establishing the unambiguous indication of the individuals' wishes. Silence or inactivity should not constitute consent. Pursuant to European law, a pre-ticked box in which the user declares that it allows for a particular data process is nowadays not enough to consider that consent has been given. The situation under Swiss law seems to be different since such form of consent might still be valid under the E-DPA.

Both the EU and Switzerland provide for new obligations before personal data is processed. Before starting processing data, the controller has to carry out a Privacy Impact Assessment («PIA»), if the processing is likely to result in a high risk for the rights and freedom of the individuals concerned

by the process. The E-DPA considers the risk to be particularly high for example if data that is especially protected such as health data is processed at scale. Such is also the case when public grounds are being surveilled. Moreover, the data processing systems must be designed from the start in a way that protects the data («Privacy by Design»), and the default settings must imperatively be set in a way to best protect the data being processed («Privacy by Default»). For example, e-commerce sites should in general allow purchases without the client having to set up an account.

The duty to report a personal data breach is newly introduced by both the E-DPA and the GDPR. According to the GDPR, a personal data breach must be notified to the supervisory authority within 72 hours after becoming aware of the breach. The E-DPA provides for the obligation to notify a breach of personal data as soon as possible if it is likely to cause a high risk for the personality or the fundamental rights of the individual concerned. A high risk is given, for example, when sensitive and secret information on the individual is disclosed.

CONSEQUENCES OF A VIOLATION

Much attention has been focused on the heavy fines of the GDPR. In fact, the GDPR provides for

fines ranging up EUR 20 million or up to 4% of the company's worldwide turnover, whichever is higher. In this regard Swiss law is more moderate and limits fines to an amount of CHF 250'000 for an intentional violation of certain provisions. The legislator has also abandoned the idea to allow the Federal Data Protection and Information Commissioner to issue binding rules or to impose administrative fines, unlike analogue powers given to its European counterparts.

WHAT SHOULD BE DONE?

The task now for all companies is, by now at the latest, to seriously deal with data protection issues. As a first step, the impact of the new E-DPA and GDPR to one's own company shall be assessed. In this regard, an in-depth analysis of processing of personal data within the company is recommended.

On the basis of these results, the appropriate adaptations of the data processing system should be made in order to be compliant with the data protection regulation. For example, documents such as terms and conditions, contracts with third parties or internal and external rules on data processing (Data Policies) should be reviewed. Also companies, which do not process data in relation to the EU, will do well to make sure that they comply at least with the Swiss regulation which is largely identical to the EU solution.



CHRISTOPH GASSER
Attorney-at-Law, Dr. iur., LL.M.
Partner



STÉPHANIE CHUFFART
Attorney-at-Law, Dr. iur., LL.M.
Managing Associate



STEPHANIE VOLZ
Attorney-at-Law, Dr. iur., LL.M.
Associate

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
Genferstrasse 24
P.O. Box 1534
CH-8027 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 133
CH-3000 Bern 15
P +41 58 220 37 70
F +41 58 220 37 71