LENZ & STAEHELIN

The world's Swiss law firm

Update

Newsflash September 2017

EU Data Protection law: Required measures for Swiss companies

The EU General Data Protection Regulation ("GDPR") will apply directly throughout the EU as of 25 May 2018, but may also apply to Swiss companies. The following provides an overview as regards applicability of the GDPR to Swiss companies and required measures for compliance.

1. Extra-territorial scope

The GDPR applies to all companies in the EU and companies outside of the EU (including Switzerland) which (i) process personal data for EU companies, or (ii) process data of natural persons resident in the EU when offering goods or services or monitoring their behavior.

2. Risk based approach

The concept of accountability of data controllers ("**Controllers**") and processors ("**Processors**") based on the potential risk for the rights and freedoms of natural persons is one of the key concepts of the GDPR.

3. Key GDPR requirements

a) Records of data processing

Controllers and Processors must maintain records of data processing activities under their respective responsibility. This requirement does not, however, apply to companies with less than 250 employees in case of (i) low risk data processing, (ii) only occasional data processing, (iii) no sensitive data processing, and (iv) no processing of data relating to criminal records.

b) Demonstrating consent

Data processing requires the "consent" of the data subject or another justification (such as performance of a contract, compliance with EU law, legitimate interests, etc.). The prerequisites for lawful "consent" by the data subject (such as customers, employees, website visitors, suppliers and client representatives) are enhanced by the GDPR, as such consent must be freely given, specific, informed and unambiguous.

c) Extensive rights of data subjects

Mandatory rights of data subjects under the GDPR include the following:

› **Access to processed data**;

› **Return of data** in electronic form (data portability);

› **Rectification** and **completion** of data;

- **Erasure of data** (e.g. after withdrawal of consent) and information of certain third parties on such erasure;

- **Objection against/restriction as regards certain processing activities** (e.g. direct marketing);

- **Human intervention** (in cases where an automated decision can have legal or similar significant effects on the rights and freedoms of the data subject).

d) Data transfers to other countries

Cross-border transfers of personal data to countries which do not provide for adequate data protection (i.e. without the EU Commission's adequacy decision) require (in addition to the consent of the data subject) alternative measures under the GDPR. Except in cases of "approved certification" or "approved code of conduct" (industry self-regulation), the respective guarantees are customarily arranged for either (i) by binding corporate rules ("**BCR**"), or (ii) by data transfer agreements (controller-to-controller, or controller-to-processor) which within groups of companies are often entered into by way of accession to a framework multi-party data transfer agreement.

e) Data breach notifications

Records of all personal data breaches (including effects and remedial actions taken) must be maintained. Data breaches must be notified to the supervisory authority within 72 hours unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Any delay must be justified. In cases where a data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller must further notify the data breach to the data subjects without undue delay.

4. Selected additional GDPR requirements

a) Designation of a representative in the EU

Unless the data processing is limited to the occasional, small scale processing of non-sensitive personal data, Swiss companies need to designate a representative in the EU. Such representative may be an EU branch office of a Swiss company. It is expected that the responsibility of said representative will be limited to representation (not including liability).

b) Designation of a data protection officer

Controllers and Processor are required to designate a data protection officer ("**DPO**") in cases where (i) the core activities of the Controller or Processor consist of data processing requiring regular and systematic monitoring of data subjects on a large scale; or (ii) particularly sensitive data (special categories of data) is processed. Such DPOs, whether or not employed by the Controller or Processor, should be in a position to perform their duties and tasks in an independent manner.

c) Conducting privacy impact assessments

The GDPR formalizes the requirement to carry out privacy impact assessments ("**PIA**") in cases where a contemplated type of processing is likely to result in a high risk to the rights and freedoms of individuals (e.g. in the event of systematic monitoring of a publicly accessible area or in the context of profiling resulting in decisions having legal effects). The Controller must consult the supervisory authority prior to the processing if the PIA indicates that contemplated processing may indeed be of high risk.

5. Liability, administrative measures and sanctions

Data subjects can sue Controllers and Processors for any damage allegedly caused by them. In case of non-compliance, supervisory authorities can impose administrative measures against companies and impose monetary sanctions which are "effective, proportionate and dissuasive".

The monetary sanctions may amount up to 2% of total worldwide annual turnover or EUR 10 million (whichever is higher) for non-compliance regarding, e.g., records of data processing, data breach notifications, or PIA. For more fundamental non-compliance (e.g., as regards the principles for data processing, consent by data subjects, or the data subjects' rights), the sanctions increase to up to 4% and EUR 20 million, respectively.

6. Key implementation steps

Main steps for Controllers and Processors in Switzerland, which process personal data of EU residents or for EU companies (see 1. above), to implement any required measures should at least include the following:

- Identify and review (and document, as required) all data processing activities (complete and dynamic data mapping), including a determination of role played (Controller, Joint Controller, Processor) with respect to each type of personal data;
- Check consent declarations of data subjects for compliance with enhanced prerequisites for lawful consent (or collect new consents);
- Implement data governance, rules and responsibilities (including technical capability) to respond to requests of data subjects based on extended rights;
- Review agreements with contractors for data processing and other contractual arrangements (e.g. with group companies) as regards cross-border data transfers;
- Assess applicability of additional GDPR requirements (such as, e.g., appointment of a representative in the EU and/or a DPO, conducting of PIA, etc.).

As the GDPR follows a risk-based approach (see 2. above), not all of the above GDPR requirements will apply to every company. It will thus be crucial for Swiss companies to thoroughly identify and review their specific data processing activities and evaluate respective risks for the data subjects' rights and freedoms in order to take targeted measures for each applicable GDPR requirement to ensure and maintain compliance in an effective and cost-efficient way.

Please do not hesitate to contact us in case of any queries. Thank you.

Your contacts

Geneva / Lausanne

Guy Vermeil
guy.vermeil@lenzstaehelin.com
Tel: +41 58 450 70 00

Daniel Tunik
daniel.tunik@lenzstaehelin.com
Tel: +41 58 450 70 00

Yaniv Benhamou
yaniv.benhamou@lenzstaehelin.com
Tel: +41 58 450 70 00

Zurich

Lukas Morscher
lukas.morscher@lenzstaehelin.com
Tel: +41 58 450 80 00

Stefan Bürge
stefan.buerge@lenzstaehelin.com
Tel: +41 58 450 80 00

Leo Rusterholz
leo.rusterholz@lenzstaehelin.com
Tel: +41 58 450 80 00

Our offices

Geneva
Lenz & Staehelin
Route de Chêne 30
CH-1211 Genève 6
Tel: +41 58 450 70 00
Fax: +41 58 450 70 01

Zurich
Lenz & Staehelin
Brandschenkestrasse 24
CH-8027 Zürich
Tel: +41 58 450 80 00
Fax: +41 58 450 80 01

Lausanne
Lenz & Staehelin
Avenue du Tribunal-Fédéral 34
CH-1005 Lausanne
Tel: +41 58 450 70 00
Fax: +41 58 450 70 01

www.lenzstaehelin.com