

# NEWSLETTER MAY 2018

## DATA PROTECTION

ON MAY 25, 2018, THE EUROPEAN GENERAL DATA PROTECTION REGULATION (GDPR) WILL ENTER INTO FORCE. EVEN THOUGH IT WAS DESIGNED TO HARMONIZE DATA PROTECTION LAWS ACROSS THE EUROPEAN UNION, THE GDPR HAS EXTRATERRITORIAL EFFECTS AND WILL ALSO APPLY TO ENTITIES REGISTERED IN SWITZERLAND

*Yasmine Sözerman, Attorney-at-law,  
LL.M. Columbia Law School*

The GDPR was adopted by the European Parliament on April 14, 2016 and its provisions will become directly enforceable as of May 25, 2018.

Its scope of application exceeds the EU's border and will also affect entities registered in Switzerland.

This newsletter aims at providing an overview of the possible consequences of the GDPR on these entities.

### 1. Territorial scope

The extraterritorial scope of the GDPR will have an impact on Swiss entities in two main cases (i) where the Swiss entity is *established* within the EU and (ii) where it targets EU residents (Art. 3 GDPR).

#### *i. Entities established in the EU*

The GDPR will apply to entities, which are *established* within the EU regardless of whether the data processing takes place in the EU or not.

The notion of establishment is broad. It implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

In other terms, if an entity is registered in Switzerland, the existence for instance of active offices within the EU, even if they are not registered, might trigger the application of the GDPR.

This provision will also render the regulation applicable to Swiss entities, which outsource their data processing to an EU company.

### *ii. Entities targeting EU residents*

A Swiss entity might be subject to the GDPR if it processes personal data of residents of the EU in two cases:

- Where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment;

An entity will be considered offering goods or services in the EU if it can be ascertained that it intends to do so. The mere accessibility of the entity's website in the EU will not be sufficient. However, factors such as the use of a language, of a certain currency, the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the EU, may make it apparent that the entity intends to offer goods or services to EU residents.

- Where the processing of personal data is related to the monitoring of the behaviour of EU residents as long as their behaviour takes place within the EU.

The goal is to target the tracking of natural persons on the internet including potential subsequent use of personal data processing techniques, which consist in profiling a natural person, particularly in order to take decisions concerning her or him or to analyse or predict her or his personal preferences, behaviours and attitudes.

It will thus include all kinds of tracking and profiling on the internet, the use of cookies as well as behavioural advertisement.

Based on the foregoing, a Swiss entity shall notably analyse the possible application of the GDPR when it:

- has offices in the EU;
- has clients or employees in the EU;
- outsources data processing to EU entities;
- follows/analyses/processes the online behaviour of EU residents.

## **2. Main new principles and obligations**

The general principles of data protection remain the same under the GDPR. Some of the main changes are developed below.

### *i. The notion of consent*

Processing is notably lawful where a person has given consent to the processing of her or his personal data for one or more specific purposes (Art. 6 para. 1 lit. a GDPR).

Conditions to admit consent of the data subject have been strengthened.

According to Art. 4 para. 11 GDPR, "consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Consent should thus be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the person's agreement to the processing of personal data relating to her or him.

This could include ticking a box when visiting an internet website. However, silence, pre-ticked boxes or inactivity should not constitute consent.

## ii. *The information obligation*

Under Art. 13 and 14 GDPR, an entity will have the obligation to provide certain information when collecting the personal data, notably the identity of the person processing the data, the purposes of the processing, the legal basis, the recipients of the personal data and the period during which the personal data will be stored. Information must be provided in an intelligible and easily accessible form, using clear and plain language.

## iii. *The right to be forgotten*

A person has the right to request the erasure of her/his personal data under certain circumstances, notably if the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, if the consent is withdrawn or if the personal data have been unlawfully processed (Art. 17 GDPR).

## iv. *The obligation to hold a record of processing activities*

Under Art. 30 GDPR, entities subject to the GDPR shall maintain a record of processing activities. The record shall notably include the purposes of the processing, a description of the categories of data subjects and of personal data and the categories of recipients of the personal data.

Such obligation shall not apply to an entity employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences.

## v. *The obligation to designate a representative in the EU*

Where an entity outside the EU is submitted to the GDPR based on the “targeting criterion” (see 1.ii

above), it shall designate in writing a representative in the EU (Art. 27 GDPR).

This obligation however does not apply when data processing:

- is occasional,
- does not include, on a large scale, processing of special categories of data (such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation), and
- is unlikely to result in a risk to the rights and freedoms of natural persons.

## vi. *The obligation to designate a data protection officer*

According to Art. 37 GDPR, an entity submitted to the GDPR shall designate a data protection officer in the three following cases:

- the personal data processing is carried out by a public authority or body (except for courts acting in their judicial capacity);
- the core activities of the entity consist of processing operations; or
- the core activities of the entity consist of processing on a large scale of special categories of data in particular sensitive data.

## vii. *The penalties*

Infringements to the GDPR can lead to different penalties, the most severe being administrative fines of up to EUR 20’000’000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Art. 83 GDPR).

Financial penalties will however be an *ultima ratio*. The supervisory authorities will usually issue warnings or reprimands (Art. 58 para. 2 GDPR).

### 3. Conclusion

Many Swiss entities might be submitted to the GDPR and will have to comply with the obligations it entails as of May 25, 2018.

In parallel, Swiss data protection law is currently under review.

Consequently, and irrespective of whether they are submitted to the European regulation, it might be the occasion for Swiss entities to review and adapt their data protection policies.

*For further information :*

*Yasmine Sözerman* ([sozerman@jmrlegal.ch](mailto:sozerman@jmrlegal.ch))

*Jean-Marc Reymond* ([reymond@jmrlegal.ch](mailto:reymond@jmrlegal.ch))

*The content of this Newsletter cannot be comprehended as a legal opinion. Should you wish an opinion on your particular situation, your usual person of contact at Reymond & Partners or one of the above-mentioned attorneys-at-law are at your disposal.*