WENGERPLATTNER

Corporate and Commercial Law / IP & IT - December 2017

EU General Data Protection Regulation: Implications for Swiss Businesses

Authors: Dr. Oliver Künzler and Dr. Martina Braun

Extensive efforts are currently underway to bring data protection law in line with rapid technological developments. These initiatives include the new General Data Protection Regulation (EU GDPR) which applies within the EU from 25 May 2018. Although the EU GDPR is not directly applicable in Switzerland, many Swiss businesses fall within its scope.

This newsletter outlines the impact of the EU GDPR on Swiss businesses and what action they need to take.

Application of the EU GDPR

The EU GDPR applies, if businesses in Switzerland:

- **supply goods or services to individuals in the EU and process their personal data;**
- **monitor the behaviour of individuals within the EU (web tracking);**
- **process personal data on behalf of an undertaking in the EU (i.e. contract data processing);**
- **outsource data processing activities to an undertaking in the EU;**
- **enter into agreements stipulating that the law of an EU member state is the governing law.**

EU General Data Protection Regulation: Implications for Swiss Businesses

The EU GDPR does not confine itself to harmonise national legislations and reaffirm current EU data protection principles, but rather enhances data protection rights in significant parts. This also impacts on Swiss data protection legislation, which will need to be revised and amended in line with EU standards.

Dr. Oliver Künzler
Partner in the businessgroup for Corporate and Commercial Law
oliver.kuenzler@wenger-plattner.ch

Dr. Martina Braun
Senior Associate in the IP & IT team
martina.braun@wenger-plattner.ch

Introduction

The EU GDPR was adopted on 27 April 2016. A two-year transition period for implementation was granted, ending on 25 May 2018. From this date, the EU GDPR will apply immediately and, in principle, uniformly across all EU member states. However, member states are allowed a degree of latitude in enacting the relevant national implementing regulations.

Applicability of the EU GDPR to Swiss businesses?

As regards its personal scope, the EU GDPR applies both to the parties responsible for making decisions as to the purposes and means of processing data ("controllers") and those responsible for processing data on behalf of a controller ("processors").

In terms of its material scope, the EU GDPR makes no distinction with regard to the volume of data or type of personal data processed. However, the protection afforded by the EU GDPR does not extend to the data of legal entities. Moreover, the EU GDPR does not apply to data processed in the course of a personal or household activity.

All natural persons within the EU shall be able to claim protection under the EU GDPR. Accordingly, the territorial scope of the EU GDPR also extends to controllers and processors that are not established in the EU, but supply goods and services to data subjects within the EU and process their personal data in this context. The same applies to undertakings that are not established in the EU but record and analyse the behaviour of data subjects (e.g. businesses engaged in web tracking).

Moreover, the EU GDPR applies to the processing of personal data in the context of the activities of an establishment in the EU, regardless of where the data processing takes place. This would be the case, for instance, if a Swiss data centre were to perform operations for clients based in the EU, or if a Swiss parent company were to process client data for a subsidiary with a registered office in the EU for the purpose of supporting its business activities.

In light of the above, many Swiss businesses will fall within the scope of the EU GDPR.

Overview of the EU GDPR

The processing of personal data is only lawful under the EU GDPR if the data subject has given valid consent or if any of the other prerequisites set out in the Regulation apply (e.g. performance of a contract, compliance with a legal obligation, pursuit of legitimate interests).

The EU GDPR imposes stringent requirements for obtaining valid consent from data subjects. Consent must be freely given, informed and requires for each individual case an unambiguous indication of the data subject´s wishes in the specific circumstances by way of a clear affirmative action. An implied consent is no longer sufficient (consent must be given through clear affirmative action, e.g. by clicking a button). Moreover, the data subjects have the right to withdraw their consent at any time.

Revision of the Swiss Data Protection Act

On 15 September 2017, the Federal Council submitted its message concerning the complete revision of the Swiss Data Protection Act (DPA) and the relevant draft bill.

The key objective is to update the DPA and align the Swiss legislation with the EU data protection law. More specifically, it is intended to facilitate ratification of the revised Council of Europe Convention ETS No. 108 and adoption of EU Directive 2016/680 on the protection of natural persons with regard to the processing of personal data in relation to criminal matters. Switzerland must implement this Directive to comply with its obligations under the Schengen Agreement. A further aim is to achieve convergence with the EU GDPR, thus ensuring that Switzerland continues to be recognised as a non-EU country providing an equivalent level of data protection on the basis of a so-called "adequacy decision" by the EU. Securing such an adequacy determination is crucial for the Swiss economy.

Pursuant to the draft bill, the rights of data subjects shall be reinforced (enhanced transparency obligations, more stringent requirements for obtaining valid consent, and requirements pertaining to data protection by default). It is also intended to promote self-regulatory measures, extend the powers of the Swiss Federal Data Protection and Information Commissioner (FDPIC), and tighten up the penalty provisions.

Although the draft bill must first be debated by Parliament, it is reasonably likely that the DPA will be aligned with the EU data protection law.

The EU GDPR attaches the utmost importance to the principle of transparency. It gives expression to this principle by setting out comprehensive obligations to provide information and to grant access rights. Controllers must provide information on their identity as well as contact details and, where applicable, the contact details of the controller's representative and/or its data protection officer. It must be indicated what data will be collected and processed, the purposes of the processing, and the period for which the personal data will be stored. Where applicable, information must be provided on the recipients of the data and on the transfer of data to a non-EU or non-EEA country. In addition, data subjects must be informed of their right to request access to and rectification or erasure of their personal data, their right to object to processing, and their right to lodge a complaint with a supervisory authority. This information must be concise, easily accessible and easy to understand, and written in clear and plain language. Additionally, visualisation may also be used.

In addition to the above rights, all data subjects have the right, subject to certain conditions, to request personal data concerning them to be transmitted in a structured, commonly used and machine-readable format (right to data portability).

Along with the data processing principles currently in effect, the EU GDPR establishes the notion of accountability of controllers. From now on, anyone processing personal data should not merely comply with data protection rules but also be able to demonstrate compliance. It follows from this principle of accountability that records of all data processing activities have to be kept. Only businesses employing fewer than 250 persons, which only process data on an occasional basis, are exempted from this requirement, unless the processing activities present serious risks or involve sensitive personal data.

Businesses not established in the EU, which supply goods or services within the EU or monitor the behaviour of persons within the EU, must appoint an EU representative unless the data processing (i) is only occasional, (ii) does not include sensitive personal data, and (iii) does not involve any special risk. The EU GDPR also introduces the requirement to designate an internal data protection officer in certain circumstances. This will apply, in particular, if the core activities of an enterprise consist in the regular and systematic monitoring of data subjects or the processing of sensitive data on a large scale.

Furthermore, the EU GDPR requires the implementation of appropriate technical measures that meet the principles of data protection by design and data protection by default (e.g. data minimisation, pseudonymisation).

Where the processing of data is likely to pose a high risk to data subjects, a data protection impact assessment must be carried out. Such an assessment must include, inter alia, a description of the data processing operations envisaged, an assessment of the risks involved, and a list of the measures in place to address such risks.

There is an obligation to report and communicate any personal data breaches. As a general rule, controllers must report any breaches to the supervisory authority without delay and not later than 72 hours after having become aware of the breach, unless the breach does not pose a risk to the rights and freedoms of data subjects. Any data breach that entails a high risk for data subjects must be communicated to the data subjects concerned. In any case, all instances of breach and the relevant measures taken must be documented.

The supervisory authorities to be designated by each member state have considerably broader powers than those

Provided that this has not been done yet, it is time for every business in Switzerland to evaluate whether actions need to be taken regarding the EU GDPR and if so, to implement the required measures.

conferred to the Federal Data Protection and Information Commissioner (FDPIC).

Among other things, supervisory authorities will have the power to impose fines as administrative sanctions (up to EUR 20,000,000 or 4% of the total worldwide annual turnover for the preceding financial year).

Measures to be taken

All Swiss-based businesses, regardless of size, need to establish whether they are affected by the EU GDPR. If this is the case, it will be necessary to identify which personal data is collected and processed and ascertain where, by whom and how the data is collected and processed and for what purposes. The data protection measures and procedures in place must also be documented.

Businesses will subsequently need to establish which data protection rules apply, whether they need to comply with these, and identify any gaps that need to be addressed. Following a risk-based approach, the necessary measures must then be implemented. These may include, for example:

- measures regarding the provision of information (e.g. privacy statement);
- entering into or amending agreements with processors;
- assessing the legal basis for data processing;
- obtaining the consent of data subjects where required;
- establishing internal procedures to safeguard the rights of data subjects (right to obtain and access information, right to have information rectified or erased, and right to object);
- technical and organisational protection measures;
- documenting data processing activities;
- implementing the necessary procedures regarding data breaches;
- conducting data protection impact assessments, where required;
- designating a data protection officer and/or EU representative, where required.

Finally, it will be necessary to ensure that any measures and procedures established are implemented and maintained on an ongoing basis. To this end, it is essential to (i) designate responsible officers within the organisation, (ii) ensure that such officers have adequate resources, and (iii) raise awareness of data protection issues in general.

Outlook and practical recommendations

The EU GDPR affects many Swiss businesses. Efforts are also underway to achieve convergence between the Swiss Data Protection Act and EU data protection law. It is therefore advisable for all Swiss businesses to review their procedures and measures in relation to data processing.

In order to ensure that the steps described above are implemented as effectively and efficiently as possible, it is beneficial to set up a task force. The task force should include personnel from IT, Legal & Compliance and HR as well as the parties responsible for processing data, and must be given all necessary resources. Finally, it is essential to integrate any key decision-makers into the process.

Basel: Aeschenvorstadt 55 | CH-4010 Basel | T +41 61 279 70 00 | basel@wenger-plattner.ch
Zürich: Seestrasse 39 | CH-8700 Küsnacht-Zürich | T +41 43 222 38 00 | zuerich@wenger-plattner.ch
Bern: Jungfraustrasse 1 | CH-3000 Bern 6 | T +41 31 357 00 00 | bern@wenger-plattner.ch

www.wenger-plattner.ch