Kellerhals Carrard

In a nutshell

2/2017

The European Union's General Data Protection Regulation – What Swiss companies need to know

In precisely one year's time, on **25 May 2018**, the European Union's General Data Protection Regulation ("GDPR") becomes directly applicable law in all its member states.

What, however, does that mean for Swiss companies? Is the GDPR binding on them too? And what are the obligations imposed on companies in the field of data protection?

Scope of the GDPR
The GDPR has a very far-reaching territorial scope, stretching beyond the borders of the EU. There are therefore certain constellations in which the GDPR also applies to companies domiciled in Switzerland.

That is the case according to Article 3 GDPR when a Swiss company processes personal data pertaining to individuals situated in the EU, if the Swiss company:

1. offers goods or services to the persons concerned in the EU (whether for payment or not); or
2. monitors the behaviour of the persons concerned in the EU.

What is relevant for establishing whether or not **goods and services are offered** is whether the (Swiss) company apparently intends to offer goods or services to the persons concerned in the EU. According to the regulation's recitals, indications for the existence of such an intention are to be taken from factors such as the use of a language or currency that is generally used in the particular EU member state but not in Switzerland, in combination with the possibility of ordering goods or services in that other language, or mentions of other customers or users situated within the EU. The mere fact of a Swiss company's website being accessible in the EU, on the other hand, is not of itself an indication that the company intends to offer goods and services there as well.

The intention to use the data processed to **monitor the behaviour of the persons concerned in the EU** is established, for instance, if the data is used to track the internet activities of such affected persons (with Google Analytics, for instance) and/or through the use of techniques for the creation of profiles of individuals for analysing or predicting the personal preferences, behaviour patterns or habits of the persons subjected to analysis or prediction.

That shows clearly that the scope of the GDPR is very broad and that Swiss companies must check whether they are going to have to abide by these new provisions. The selected examples set out below of obligations on companies arising out of the GDPR will provide an initial impression, but they are by no means to be understood as an exhaustive checklist.

Obligations on companies

A. Information for and consent from the person concerned
The European Union's data protection law differs from Swiss law in that it includes the concept of "prohibited unless authorised". What that means is that there is a general prohibition on the processing of data unless it is expressly permitted by a law or unless the person concerned consents to it.

For the consent of the person concerned to be valid, there are certain preconditions that must be met:

- **Consent freely given**
  The consent is only valid if the person concerned has issued it freely. The person concerned must have a genuine choice, i.e. it is not permissible for them to be faced with a fait accompli when asked to give their consent or for their decision to be restricted in any other way. In this context, we draw attention in particular to the so-called "prohibition on tied provisions", which forebids making the conclusion of a contract dependent on the processing of additional data that is not needed for the actual performance of the contract.
- **Detailed, recognisable and determinate information**
  The person concerned must be informed before they issue their declaration of consent about the purpose for which their personal data is to be collected and processed. The information provided must contain all the particulars of relevance for the decision in the specific case, and these must be sufficiently to-the-point. Consent is thus always tied to a particular purpose, which it is not permissible to formulate in excessively broad terms. The person concerned must finally be put in the position to recognise the items of information easily and also to recognise that their action will be qualified as consent.
- **Form and positive action**
  According to the GDPR, it is sufficient for the controller to be able to document the consent. The consent is therefore not bound to be in a particular form and can also be issued electronically or verbally. Nonetheless, the consent ought only to come into being through an unambiguous act. That means that, as a general rule, it is necessary for the person concerned to take positive action; other variants, such as tacit consent, pre-ticked boxes or inaction by the person concerned would thus not constitute consent. If the consent is in written form, then the request to issue it must be in an understandable and readily accessible form, expressed in clear and simple language and clearly distinguished from other subject-matters.
- **Right of withdrawal**
  The person concerned has the right to withdraw his or her consent at any time. It must be guaranteed that this withdrawal is as simple to perform as issuing the consent itself.

B. "Privacy by design" and "privacy by default"
The principle of "privacy by design" (data protection through technical means) signifies that at the time that data processing is being planned already (for instance the deployment of a new IT system or process), the controller must reduce the risk of personal data breaches or violations of fundamental rights and must avert such occurrences. Examples would be making provision for the regular deletion of data or for having it anonymised as a default prac-

tice. One point stressed in each instance as being particularly significant for the technically supported protection of data is to minimise the volume of data.

The principle of "privacy by default" (protection of data through pre-settings militating in favour of protection) means that the controller or processor has the duty to ensure through default settings that the only personal data that can be processed is the data that is needed for the particular intended purpose. One example of that is that a website must basically permit purchases to be made without it being necessary to create a user profile.

C. Appointment of a representative in the EU
Those Swiss controllers or processors who fall within the scope of the GDPR must designate a representative within the EU. This obligation lapses in particular if the processing only takes place occasionally, if no special data categories are processed and if the processing does not lead to a risk for the rights and freedoms of the natural person.

D. Records of processing activities
Controllers are required to keep records of the processing activities within the company. Processors must keep a similar record of all the categories of processing activities carried out under contract from a controller. The records are to be in the form of documentation or an overview of all the processes and procedures within the company in which personal data is processed. They must indicate the salient aspects of the data processing, such as the data categories, the circle of persons affected, the purpose of the processing and any recipients of the data that there may be.

A company must first of all establish those cases in which it collects and processes personal data, for instance of its customers, suppliers or employees. An appropriate way of doing that is to begin by drawing up a list of all the applications and tools used throughout the company's system landscape (for example time-and-attendance system, CRM system and HR information system) in which personal data is saved. At the same time, that helps in establishing the data flows inside the company and serves as a basis for the record kept of processing activities. Quite apart from that, Swiss companies are going to have to conduct stock-taking as their first step in order to work out if they fall within the scope of the GDPR or not.

E. Data breach notification
Breaches in the protection of personal data must be notified to the supervisory authority within 72 hours if possible. The notification duty is only waived if there is unlikely to be a risk for the rights and freedoms of individuals. It is often the case that breaches must be communicated to the persons concerned as well.

F. Data protection impact assessment
If a particular form of processing is likely to cause a high risk, especially in the case of new technologies or on account of its nature, its scale, its context or its purposes, then a data protection impact assessment must be performed. If the finding of such an assessment is that data processing in the absence of particular measures constitutes a high risk, then the supervisory authority must be consulted.

G. Consequences of data protection infringements
The maximum fine is up to 20 million euros or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is the higher. What counts is the annual turnover of the entire group of undertakings, not the individual legal entity. The GDPR furthermore provides for a right of collective action, which is going to make it possible in future for consumer protection associations to enforce the rights of data subjects.

Conclusion and important notice

Revision of the Swiss Federal Act on Data Protection
The scope of the GDPR is very broad, and Swiss companies must check if they are required to comply with these new provisions. The first precondition for that is for companies, whatever their size, to acquire a certain competence in data protection and to determine the internal responsibility for it. The examples of a company's obligations arising out of the GDPR presented briefly above will hopefully convey an initial impression of the consequences of this EU legislation. Considering the severity of the sanctions, Swiss companies would be well advised to take compliance with the new provisions seriously. Companies affected will have to review in particular their internal processes, guidelines, contracts and data protection declarations and may also need to adapt the way in which their IT systems function.

The efforts to comply with the new GDPR ought to produce returns in two respects at one and the same time. The preliminary draft for a new Swiss Federal Act on Data Protection (PD-FDPA) has just gone through the formal consultation procedure. A revised draft is expected to be published already this fall. The intention is for data protection to be tightened up in Switzerland too (along similar lines to the provisions contained in the GDPR and to satisfy the obligations arising out of the corresponding Council of Europe convention (ETS 108)), in particular by increasing processing transparency and the possibility for data subjects to check up on their data. With its Swiss Finish, the Federal Council's preliminary draft is going too far. Although it may be assumed that it will not survive in the presented form, compliance with data protection regulations is nevertheless going to become more important for all Swiss businesses in future.

We shall provide you with information about the revision of the Swiss Federal Act on Data Protection.

Zurich, 25 May 2017

Dr. Daniel Alder
daniel.alder@kellerhals-carrard.ch

Dr. Nicolas Mosimann, LL.M.
nicolas.mosimann@kellerhals-carrard.ch

Virginie A. Rodieux, LL.M.
virginie.rodieux@kellerhals-carrard.ch

Dr. Cornelia Stengel
cornelia.stengel@kellerhals-carrard.ch