State: March 2018

The GDPR and its consequences for Switzerland[1]

Contents

[1] *NB: This text will be subject to additions and amendments in the light of developments and reflections at national and European level. Indeed, the position of the reference and supervisory authorities and their interpretation of the GDPR is currently being clarified (G29, European Commission, supervisory authorities of the member states of the Union).*

Introduction: revision of the EU legal framework for data protection

In January 2012, the European Commission put forward a package of legislative measures designed to update and modernise the regulations of the 1995 Directive on Data Protection (Directive 95/46/CE) and of the 2008 Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Framework Decision 2008/977/JAI). The aim of this reform is to create a series of common standards for the whole of the EU which are adapted to the digital era, to improve legal certainty and increase the confidence of citizens and businesses in the digital single market. The reform includes a communication setting out the Commission's objectives and two proposed pieces of legislation: a General Data Protection Regulation and a directive relating specifically to the police and law enforcement.

On 14 April 2016, the European Parliament approved the submitted texts, thereby finalising more than four years of work. The rules deriving from the General Data Protection Regulation will be directly applicable in all member states from 25 May 2018. The EU countries have until 6 May 2018 to transpose the provisions of the Directive into their national legislation.

The General Data Protection Regulation (GDPR)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/CE (General Data Protection Regulation or GDPR) was approved by the European Parliament on 14 April 2016 and will enter into effect on **25 May 2018**. From this date onwards, the GDPR will be directly applicable to all active players in the European Union. Under EU law, a regulation applies in its entirety as soon as it enters into effect (it cannot be applied selectively). Unlike a directive, it is directly applicable throughout the EU without the need for transposition in the member states. The new rules give citizens more control over their personal data, place more responsibility on enterprises while reducing their reporting burden, and strengthen the role of the data protection authorities. **This reference text for Europe will have direct repercussions on a large number of Swiss businesses**.

Material scope (Art. 2 GDPR)

Generally, the material scope of Directive 95/46/CE has not been changed in this regulation. The GDPR applies to "*the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*" (Art. 2(1) GDPR). It applies to all personal data relating to identified or identifiable natural persons and does not differentiate between processing by a natural person or by a public or private legal entity. Article 2(2) of the GDPR states four exceptions; the GDPR "*does not apply to the processing of personal data:*

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."

The GDPR covers the processing of personal data concerning natural persons, whatever the nationality or residence. This means that when personal data of a natural person domiciled in Switzerland is processed in a member state of the European Union, it will fall under the scope of the GDPR.

Territorial scope (Art. 3 GDPR)

Compared to Directive 95/46/CE, the territorial scope has been extended and now contains the **criterion of targeting data subjects (extraterritorial application)**. This extended scope coheres with a 2014 judgment by the Court of Justice of the European Union (CJEU) in favour of the extraterritorial application of the Directive in the Google Spain case (C-131-12).

Article 3 GDPR states:

1. *This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*
2. *This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
   a) *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; **or***
   b) *the monitoring of their behaviour as far as their behaviour takes place within the Union.*
3. *This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.*

Application of the GDPR thus depends on the following two connecting factors:

1. **Establishment criterion** (= place of establishment of a data controller or processor; Art. 3(1): the data controller or processor is established **in the European Union**. In this case, the Regulation applies regardless of whether processing takes place in the Union or not. In the case of Weltimmo c. NAIH (C-230/14), the CJEU interpreted the concept of establishment in a relatively broad and flexible way.

2. **Targeting criterion** (= whereabouts of subjects of data processing; Art. 3(2): the data controller is established **outside of the European Union** but its processing activities involve offering goods or services to data subjects located within the Union or monitoring behaviour

of these data subjects insofar as this behaviour takes place within the European Union. In this latter case of behaviour monitoring, European legislation refers to the monitoring of internet users in general. **In practice, the GDPR should apply when a resident of the EU, regardless of his nationality or his domicile, is directly targeted for data processing.**

When considering whether the Regulation applies, the specific case should always be taken into account, in particular whether the data controller intends to offer goods or services to subjects in the Union or to monitor their behaviour.

Rights of the data subject

One of the aims of the EU reform is to **grant greater control and visibility to data subjects**. Article 12 GDPR requires the data controller to set up procedures and mechanisms which allow data subjects to exercise their rights. It establishes the principle of transparency: any information addressed to the public or the data subject must be in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular where addressed specifically to a child. In general, information must be provided in writing and free of charge. The Regulation also provides for maximum response times in providing information. All the modalities listed in Article 12 GDPR apply to all rights provided for by the Regulation, notably:

- **The right to information** (Articles 13 and 14 GDPR). When a data subject's personal data is collected, the data controller provides them with a range of information at the time that the data in question is obtained. The data controller must also provide information when data has not been obtained from the data subject.

- **The right of access** (Article 15 GDPR)
  The data subject has the right to obtain from the data controller confirmation as to whether their personal data are being processed, and where this is the case, they have the right to obtain access to the data and to certain additional information as given in letters a) to h). This right includes access to a copy of the personal data undergoing processing.

- **The right of rectification** (Article 16 GDPR)
  The data subject has the right to ask for their data to be rectified or completed without undue delay.

- **The right to erasure or the 'right to be forgotten'** (Article 17 GDPR)
  The data subject has the right to ask for their data to be erased without undue delay if one of the grounds in § 1 applies. If the data subject's personal data has been made available to third parties, then the 'right to be forgotten' applies: the data controller is required to take all reasonable measures to inform these other entities that the data subject has requested the erasure of any links to, copy or replication of those personal data.

- **Right to restriction of processing** (Article 18 GDPR)

The data subject has the right, in certain cases provided for by law, to have the data controller restrict the processing of their personal data. When such restriction is requested, the data controller may only continue to store the data. In principle, no other operation may be carried out with this personal data.

- **Controller's notification obligation** (Article 19 GDPR)
  This article establishes a notification obligation requiring the data controller to communicate any rectification or erasure or restriction of processing to each recipient of personal data.

- **Right to data portability** (Article 20 GDPR)
  The data subject has the right to receive the personal data provided to the data controller in a structured, commonly used and machine-readable format, and has the right to transmit those data to another controller, for example in order to change service provider. This right may only be exercised if the data processing takes place with the consent of the data subject or on the basis of a contract.

- **Right to object** (Article 21 GDPR)
  The data subject has the right to object on grounds relating to his or her particular situation at any time to processing of personal data concerning them which is based on public interest or legitimate interests pursued by the data controller, including profiling. The data subject also has the right to object to the processing of their data for direct marketing purposes.

- **Right to automated individual decision-making** (Article 22 GDPR)
  The data subject has the right not to be subject to a decision based solely on automated processing which produces legal or similar significant effects concerning them. This expressly includes profiling.

- **Right to communication of a personal data breach** (Article 34 GDPR).
  The data controller is required to notify the data subject of any personal data breach likely to result in a high risk to their rights and freedoms.

The Regulation also provides specific protection for children, who are less aware of the risks, consequences and of their rights regarding data protection. Under Article 8 of the GDPR, when information society services are offered directly to a child, the holder of parental responsibility over the child must authorise or give their consent to data processing (the member states may set an age limit between 13 and 16 years).

Applicability to Swiss businesses (Arts. 3 and 27 GDPR)

It follows from the Regulation and its recitals that the GDPR applies to Swiss businesses in cases provided for by the criterion:

Of establishment (Article 3(1); recital 22):

- Processing of personal data in the context of the activities of a European branch or a subsidiary with a legal personality[2] of a Swiss company in the Union;

- **Processors[3]:** Processing of personal data carried out by a Swiss company[4] acting as processor on behalf of a European company.

A processor in the Union (e.g. IT service provider) who processes personal data for a Swiss company will be subject to the Regulation regardless of whether it is the data of data subjects in Switzerland or the Union (art. 3 § 1 GDPR). It shall be bound to comply with the specific obligations of the processor laid down by the Regulation (cf. Articles 28, 30 § 2 and 37 GDPR) and the requirements imposed by the Swiss law (cf. Article 10*a* FADP). In case of a breach, his responsibility is likely to be engaged. However, this does not mean that the controller in Switzerland will therefore be subject to the Regulation.

Of targeting (Article 3(2); recitals 23 and 24:

- The processing of personal data of data subjects who are in the Union by an enterprise based in Switzerland where the processing activities are related to offering goods or services in the Union, whether payment is required or not (Art. 3(2) (a) GDPR);

> Example 1: A company based in Switzerland sells watches to persons domiciled in France, Belgium, Portugal, Finland and Greece via an online boutique. The GDPR applies because the Swiss company offers goods to persons in the Union.

The GDPR does not provide a precise definition of the concept of "offering goods and services". Recital 23 suggests that it should be ascertained *"whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union"*. In order to ascertain this intention, a number of factors should be taken into account, including *"the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union"*.

[2] Recital 22 of the GDPR specifies that an establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements is not the determining factor in that respect.
[3] The ICO created a checklist for data processors: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/data-processors/
[4] Provided that the Swiss company intends to offer goods or services to EU residents.

In a different context (cf. cases C-585/08 and C-144/09), the CJEU has already addressed the issue of how to establish whether the offering of goods and services can be considered as being directed at a particular member state of the European Union. In this context, it also identified the following factors: the mention of a telephone number with an international dialling code, the description of the route from a member state to the place where the service is offered (e.g. a Swiss hotel indicating the route to take from abroad); the mention on a website of international clients in different EU member states; the use of a top-level internet domain other than that of a member state where the service is offered (e.g. the site www.exemple.ch also accessible at www.exemple.se and www.exemple.eu).

However, *"the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention".*
It should be stressed that the list of factors given here is not exhaustive and that the issue should always be analysed on a case-by-case basis.

- Processing of personal data of EU residents by a company based in Switzerland where the processing activities relate to the monitoring of the behaviour of data subjects in the Union (Art. 3(2) (b) GDPR).

  With regard to behavioural monitoring and ascertaining whether a processing activity can be considered as such, recital 24 states that *"it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes".*

This refers in particular to behavioural advertising, which is defined by the Article 29 Data Protection Working Party in its Opinion on online behavioural advertising as *"advertising that is based on the observation of the behaviour of individuals over time. Behavioural advertising seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests".*

> Example 2: A hotelier in Gstaad creates profiles of his Italian, Swedish, German and Polish clients in order to make them special offers. The GDPR would apply as long as the profiles were established on the basis of behaviour in the Union.

> Example 3: A website operator who uses webtracking to monitor the activities of visitors or to observe their surfing behaviour could also draw conclusions about their interests, preferences or online habits. The GDPR would certainly be applicable.

Obligations of enterprises affected by the Regulation[5]

One of the major new features compared with Directive 95/46/CE is the establishment of the principle of the data controller's accountability (cf. Article 5(2) GDPR) i.e. the data controller is actively responsible for ensuring the compliance of data processing. The data controller is responsible for compliance with general principles and must also be able to give proof of this compliance. This principle gives rise to the principle of reverse onus. The Regulation provides in particular for the following obligations:

- Article 24 GDPR makes clear that the principle of responsibility goes hand-in-hand with the risk-based approach, according to which the controller will in future have to assess in an objective manner the likelihood and severity of risk for the rights and freedoms of natural persons when processing is performed. Controllers must therefore implement monitoring measures and systems in their organisation to ensure and to be able to demonstrate that processing is performed in compliance with the GDPR.

- Article 25 GDPR introduces the principles of data protection by design and by default[6]. They require that the data protection guarantees are integrated into products and services from the initial phase of their design.

- Article 30 GDPR states that each data controller or representative should maintain a record of processing activities under its responsibility. The content of the record is set out in detail in Article 30(1) GDPR. This record must be made available to the supervisory authority on request. The obligations do not apply to an enterprise employing fewer than 250 persons, with exceptions (cf. Art. 30(5) GDPR).

- Article 35 GDPR provides for a data protection impact assessment[7] to be carried out when processing is likely to result in a high risk to the rights and freedoms of natural persons.[8] Where an analysis leads to the identification of particular risks, the controller is obliged to consult the independent supervisory authority before processing; if a data protection officer has been designated, the data controller is obliged to consult them. An impact analysis is compulsory in certain cases (cf. Art. 35(3)) and its minimum content is set out in Article 35(7).

In the Regulation, security of processing is established as a fundamental principle of data protection:

- Article 32 GDPR requires the data controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In doing so, it

[5] The ICO created a checklist for data controllers : https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/data-controllers/

[6] The ICO has published guidance on privacy by design

[7] The ICO has published some helpful information on this topic: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

[8] In order to help data controllers conduct data protection impact assessments, the CNIL provides free DPIA software on its website: https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil . An English version is also available: https://github.com/LINCnil/pia/tree/master/src/assets/i18n ; the Irish DPC published a guide to learn more about how and when to carry out a DPIA: http://gdprandyou.ie/data-protection-impact-assessments-dpia/

must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as risks of varying likelihood and severity to the rights and freedoms of natural persons. The Regulation cites pseudonymisation, encryption and the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems as examples. Furthermore, the controller *"shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law"* (see Article 32(4)).

This security obligation gives rise to the new obligation to notify the supervisory authority of personal data breaches. In certain cases, the data subject must also be notified of any breach:

- Article 33 GDPR creates a system of notification of data breaches[9]. A personal data breach is defined in Article 4.12 GDPR as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*. In the case of a personal data breach which is likely to result in a risk to the rights and freedoms of natural persons, the data controller must notify the supervisory authority as soon as possible, if possible within 72 hours (cf. Article 33(1)). The processor must inform the controller without undue delay after becoming aware of a personal data breach. The content of the notification is set out in Article 33(3). Finally, the controller must document any personal data breaches, comprising the facts relating to its effects and the remedial action taken. This documentation should enable the supervisory authorities to implement their tasks and powers.

- Article 34 GDPR sets out the modalities and conditions for the communication of a personal data breach to data subjects. In this case, no time limit is set. The underlying idea is to allow data subjects to take appropriate measures, if necessary, to stop or mitigate the negative effects that may result from a personal data breach.

In three specific cases (cf. Article 37 GDPR), it is now compulsory to designate a data protection officer.[10] This is necessary for: 1) a public authority or body, 2) companies whose processing operations require regular and systematic monitoring of data subjects on a large scale and 3) companies, which process sensitive data. Moreover, the Regulation allows Union or member state law to require the designation of a data protection officer in cases other than those provided for in the GDPR. A group of undertakings may also appoint a single date protection officer, as may public authorities and bodies, taking account of their organisational structure and size (Article 37(2) and (3)). The qualities the data protection officer must possess are given in Article 37(5).

[9] See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

[10] See "Guidance on appropriate qualifications for a Data Protection Officer" and http://gdprandyou.ie/data-protection-officer/ from the Irish DPC.

Finally, the Regulation encourages the drawing up of codes of conduct[11] intended to contribute to the proper application of the Regulation (Arts. 40 and 41). They should be drawn up according to the specific features of the various processing sectors and the specific needs of the enterprises. These codes are submitted to the data protection authority, which is competent pursuant to Article 55 GDPR, which provides an opinion on whether the code complies with the Regulation. Article 42 and the articles following establish a certification mechanism.

Obligation to designate a representative of controllers or processors not established in the Union (Art. 27 GDPR)

Where Article 3(2) GDPR applies, Article 27 GDPR requires data controllers and also processors not established in the Union to designate in writing a representative when the Regulation applies to their processing activities. This representative must be established in one of the member states in which the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are resident (Art. 27(3)).

According to recital 80 of the GDPR, the representative may be addressed by the supervisory authorities (cf. Article 58 GDPR) and the data subjects on any matter relating to the processing of personal data. The representative shall maintain a record of processing activities under its responsibility (cf. Article 30 GDPR). The designated representatives are also subject to enforcement proceedings in the event of non-compliance with the GDPR by the controller or processor. It is important to stress that this does not in any way affect the responsibility of the controller or processor towards the authorities and data subjects, since the designation of a representative is without prejudice to legal action which could be initiated against the controller or the processor themselves.

Article 27(2) explains that this obligation to designate does not apply to:

a) *"processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or*
b) *a public authority or body".*

[11] See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct-and-certification/

GDPR sanctions

The Regulation, unlike Swiss law, recognises the power of the supervisory authorities to impose administrative fines under certain conditions. Each supervisory authority should ensure that any administrative fine imposed for a breach of the GDPR is effective, proportionate and dissuasive. Indeed, it should not be forgotten that the Regulation provides for a whole series of dissuasive measures (see e.g. Article 58(2) GDPR) such as warnings, formal notice, a temporary or permanent ban on processing and reprimands. From all of these instruments, the data protection authorities should select that which is most effective in establishing compliance.

Controllers should only as a last resort be given fines in excess of EUR 20 million or corresponding to 4% of their annual global turnover. Article 83 GDPR lists the factors to be taken into account when determining the size of a fine.

It should also be borne in mind that any damages for loss suffered resulting from legal proceedings must also be paid.

Contact:

Since the Regulation is a piece of European legislation, should you have any questions regarding its application we advise you contact a European data protection authority such as the ICO[12] in the UK and the DPC, the Irish Data Protection Commissioner[13]. We also recommend that you consult their websites, which contain practical guides, factsheets and practical tools on conforming to the Regulation.

[12] The ICO has created a guide to the GDPR for the organisations: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr as well as a guide to the GDPR for

[13] The DPC has launched a GDPR-specific website www.GDPRandYou.ie with guidance to help individuals and organisations