# New data protection regulations

## Key elements

Ochsner & Associés
1, place de Longemalle
1204 Geneva

Tel. +41 22 786 88 66
Fax +41 22 786 88 67

cung@oalegal.ch
fgillioz@oalegal.ch
www.ochsnerassocies.ch

# Table of Contents

# Introduction

The European regulation 2016/679 of April 27, 2016, commonly called « General Data Protection Regulation » (**GDPR**) is repealing the European directive 95/46/EC of October 25, 1995, which was the reference in the European Union on data protection of natural persons. The GDRP will be applicable throughout Europe on May 25, 2018.

Due to this new regulation, Switzerland had to review its own provisions regarding data protection in order to be in line with the European requirements. The Federal Act on Data Protection of June 19, 1992 (FADP) is currently being revised. The date of its entry into force is still unknown, but it shall be expected for 2019 or 2020. A preliminary draft of the new act (**PD-FADP**) has been published.

Regardless of the status of the revised FADP, the main elements arising from its revision are known and should be implemented by companies affected by it as soon as possible, even before its entry into force. The reasons behind this is because many companies located in Switzerland are also concerned by the GDPR and the implementation of these new regulations may take a lot of time.

This Guide has the purpose of highlighting the key elements that have to be taken into consideration by companies collecting and processing personal data.

For the purpose of this Guide, the PD-FADP and GDRP will be jointly called "**Data Protection Regulations**".

# General

## Scope of application

### ❖ FADP

The FADP applies to the processing of data pertaining to natural persons and legal persons in Switzerland by:

- Private persons;
- Federal bodies.

This Guide will solely deal with the processing of data by private entities.

### ❖ GDPR

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not.

The GDPR applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to:

- The offering of goods or services;
- The monitoring of their behavior.

### Type of data

The Data Protection Regulations apply to the processing of "personal data", i.e. any information to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to:

- An identifier such as a name
- An identification number
- A location data
- An online identifier such as an IP address
- Factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity

As an example, any company who keep HR records, customer lists or contact details are concerned by the Data Protection Regulations.

### Notions

**Controller** : Natural or legal person, alone or jointly with others, determines the purposes and means of the processing of personal data. The controller says how and why personal data is processed.

**Processor** : Natural or legal person, which processes data on behalf of the controller. The processor acts on the controller's behalf.

## Principles

### Accountability principle

The key element emphasized by the new regulations is the **accountability principle**. The regulations require from companies to show how they comply with the principles, for example by documenting the decisions taken about a processing activity.

In order to demonstrate that a company complies with this principle, it must:

- Implement appropriate technical and organizational measures that ensure and demonstrate that it comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies;
- Maintain relevant documentation on processing activities;
- Appoint a data protection officer ;
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
    - Data minimization;
    - Pseudonymisation;
    - Transparency;
    - Allowing individuals to monitor processing; and
    - Creating and improving security features on an ongoing basis;
- Use data protection impact assessments where appropriate.

### Lawful processing

For processing to be lawful, the company needs to identify a lawful basis before it can process personal data. The Data Protection Regulations require that personal data shall be:

- **Consented** by the data subject;
- Processed **lawfully**, **fairly** and in a **transparent** manner;
- Collected for **specified**, **explicit** and **legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
- **Adequate**, **relevant** and **limited to what is necessary** in relation to the purposes for which they are processed;
- **Accurate** and, where necessary, **kept up to date**;
- Kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed;
- Processed in a manner that ensures **appropriate security** of the personal data.

## Key areas to consider

### Consent

Consent of the data subject must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action, i.e. a positive opt-in. Consent cannot be inferred from silence, pre-ticket boxes or inactivity.

Consent must also be separated from other terms and conditions. The company will need to provide simple ways for people to withdraw consent, such as by providing a contact information within the company to whom he may address such concerns or by providing this option on the person's online account.

### Individual's rights

The Data Protection Regulations creates some new rights for individuals and strengthens some of the rights that currently exist:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

## Data protection impact assessment

Data protection impact assessment (**DPIA**) is a tool, which can help companies identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow companies to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

A DPIA must be carried out when:

- A new technology is used;
- The processing is likely to result in a high risk to the rights and freedoms of individuals.

Overview of the key elements that the DPIA should contain:

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller;
- An assessment of the necessity and proportionality of the processing in relation to the purpose;
- An assessment of the risks to individuals;
- The measures in place to address risk, including security and to demonstrate that the companies complies.

## Appointment of a Data Protection Officer

The companies shall appoint a Data Protection Officer (**DPO**) in any case where:

- The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- The core activity of the company consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- The core activity of the company consist of processing on a large scale of special categories of data (sensitive data) and personal data relating to criminal convictions and offences.

The DPO's tasks are:

- To inform and advise the company and its employees about their obligations to comply with the Data Protection Regulations;
- To monitor compliance with the Data Protection Regulations, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits;
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers, etc.).

The DPO operates independently and reports to the highest management level of the companies (i.e. board level).

### Designation of a representative in the EU

Companies who are subject to the GDPR and that are not established in the EU must designate a representative in the EU (e.g. internal or external representative, such as a law firm).

### In case of data breach

All companies have a duty to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

The DPO must inform the supervisory authority of the data breach within 72 hours of the companies becoming aware of it.

In Switzerland, the supervisory authority is the Federal Data Protection and Information Commissioner (Préposé federal à la protection des données et à la transparence, PFPDT).

## Financial risks

In case of violation of any requirements under the Data Protection Regulations, the company may face criminal sentences in the form of a fine:

- In the European Union :
    - Up to **10 million Euros** or **2% of the company's global turnover**;
    - For the most serious violations : **up to 20 million Euros or 4% of the company's global turnover**;
- In Switzerland: up to **500'000.- Swiss francs**.

In Switzerland, in case of breach of professional confidentiality, the person may be sentenced to serve custodial time up to three years.

# How can you start now : steps to take

The following checklist highlights a few steps that a company can take now to prepare for the Data Protection Regulations:

1. Identify the internal and external key players regarding data processing;
2. Raise awareness;
3. Identify the information the company holds and the purposes;
4. Identify the risks;
5. Proceed with a risk assessment;
6. Set up a process;
7. Document and update.

# Conclusion

The entry into force of the GDRP and the revised FADP has an important impact on many companies, which have to revise their organization and policies regarding data protection.

It is strongly advised to bring awareness to the higher level of the company that the data protection laws are changing. They indeed need to appreciate the impact this is likely to have and identify the areas that could cause compliance problem.

It will thus be important for Swiss companies to thoroughly identify and review their specific data processing activities and evaluate respective risks. Targeted measures will be necessary to ensure and maintain compliance within the company.

* * *

# Contacts


**Fabien GILLIOZ**
Attorney-at-law, Partner
fgillioz@oalegal.ch

**Cindy UNG**
Attorney-at-law
cung@oalegal.ch


*This Guide presents the main elements related to the Data Protection Regulations and does not have the purpose to be exhaustive. The information contained in this Guide is of general nature and does not constitute legal advice. Please do not hesitate to contact us for further information. Our law firm may assist companies in order to assess their data processing procedure and to set up a process compliant with the Data Protection Regulations.*