

Data protection Brochure



OA LEGAL

SWISS INNOVATIVE LAW FIRM

Swiss Data Protection Overview

TABLE OF CONTENTS

- Introduction
- Swiss and/or EU data protection rules
- Processing “sensitive” personal data
- Data protection actors
- Processing of employees’ personal data
- Outsourcing and transfers abroad
- Distributed Ledger Technology challenges
- Check list example
- Rights of data subjects

Introduction


Data protection is a fundamental right of data subjects.

The purpose of data protection law is to protect the personality and fundamental rights of data subjects. Such protection in Switzerland is embedded in the Swiss Constitution (Art. 13 para. 2) and is also provided in particular at Art. 28 of the Swiss civil code.

In Switzerland, personal data is subject to the Swiss Federal Act on Data Protection (the “FADP”) as well as in certain circumstances the European General Data Protection Regulation (the “GDPR”). Since the entry into force of the GDPR, the FADP has been under revision (the “R-FADP”). However, no date of entry into force was set to date.

Swiss and/or EU data protection rules

It is important to assess which data protection rules apply to you. Depending on the activity of the entity processing the data, the FADP might apply alone or both the FADP and the GDPR may apply. This requires a case-by-case analysis.



If an entity solely processes personal data within the territorial scope of Switzerland, the FADP shall solely apply. In other words, if a company only offers its services in Switzerland and does not target European ("EU") clients with online services, the GDPR should not apply. Also, processing the personal data of employees who work in Switzerland but reside in the EU (i.e. "frontaliers") does not trigger alone the application of the GDPR. Compliance with the GDPR is also required in addition to the FADP when:

- The company (controller/processor) processes personal data in Switzerland but has an establishment in the EU; or
- The company (controller/processor) has processing activities in Switzerland related to the offering of services to data subjects located in the EU (i.e. targeting of the EU market); or
- The company (controller/processor) monitors the behavior of data subjects located in the EU.

If the GDPR applies to your activity and you do not have an office in the EU, you will need to appoint a representative based in the EU where you process personal data unless you only process personal data on occasional basis and such processing does not include, on a large scale, the processing of sensitive personal data (as referred to in the GDPR) or relating to criminal convictions and offences, 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.

In addition, you may have to appoint a data protection officer (DPO) depending on the nature, scope and/or purpose of your core activities, in particular if they imply, on a large scale, the regular and systematic monitoring of data subjects or the processing of sensitive personal data. A DPO can be an existing employee or externally appointed, insofar as said person has the proper knowledge / qualifications. The DPO is in charge in particular of ensuring the proper application of data protection laws to the processing of personal data within the company.

Processing "sensitive" personal data?

Personal data that qualifies as "**sensitive**" (i.e. special categories under the GDPR) requires additional attention as it is subject to increased protection.

The FADP and GDPR make a distinction for certain categories of personal data that are qualified as "**sensitive**" such as personal data on a person's health, intimate sphere, racial or ethnical origin, political views, religious or philosophical convictions, trade union related views, social security measures (under the FDAP/R-FDAP), genetic data and biometric data for the purpose of uniquely identifying a natural person (under the GDPR and R-FDAP) and administrative or criminal proceedings and sanctions (under the FDAP/R-FDAP; separate category under the GDPR).

Please note that certain categories of personal data that a company may consider as sensitive do not qualify as such under the FDAP, R-FDAP or GDPR. This is for instance the case of financial information.

This does not mean that you should not effectively protect said personal data with additional measures as they may be considered as "sensitive" by your clients because of your activity.

Data protection actors

Under data protection laws, the following actors co-exist:

A data subject:

The person which personal data is collected / processed. The data subject is entitled to certain rights / protection under the FADP / GDPR and is entitled to make certain claims in the event of a breach.

A data processor:

A data processor is the service provider to a data controller who processes the personal data according to the data controller's instructions (no autonomy on decisions taken in relation to the data processing). The data processor is legally responsible for breaches of the law and/or contract. Under both the FADP and the GDPR, outsourcing the processing of personal data to a data processor requires a proper processing contract.

A data controller (or joint-controller):

The entity (no matter if a private company, a non-for-profit or a public authority) that collects and processes personal data of data subjects and determines the purpose and means of the data processing / data file (alone or jointly with another joint controller). The data controller is responsible for its compliance with the FADP / GDPR and legally responsible for breaches of the law.

A data protection authority:

The data protection authority is the personal data protection supervisory authority, per country.

In Switzerland, the Federal Data Protection and Information Commissioner are for instance responsible for supervising private entities.

Processing of employees' personal data

Employers have databases full of personal data of employees. This includes employment contracts or evaluations, as well as sensitive personal data such as data on health or religion of employees.

An employer has obligations towards its employees, in particular the protection of the employee's personal rights (Art. 328 of the Swiss Code of obligations ("CO")). Art. 328b para. 2 of the CO provides that the employer may handle data concerning the employee only to the extent that such data concerns the employee's suitability for his job or are necessary for the performance of the employment contract. In all other respects, the provisions of the FADP apply. This means that an employer should carefully assess the extent of the processing of the personal data of its employees. In particular, any monitoring of employees and the legitimacy of such actions must be assessed on a case-by-case basis (including surveillance of emails, security cameras, etc). A balance of interests is important and any measure should remain proportional.

Furthermore, in some circumstances, there may be tensions between various duties of the employer towards employees. A balance of interests is important. For instance, the employer has the duty to protect its employees' health. This duty however does not allow the employer to collect any health data of employees as employees are also entitled to protection against abusive processing of their personal data. The COVID-19 pandemic raised the issue on the processing of health data (i.e. sensitive data) such as symptoms of the virus, temperature, diagnosis.

Outsourcing and transfers abroad

Whenever a data controller decides to outsource the processing of personal data to a data processor, the data controller should make a careful assessment, in particular of the following issues:

- Who is the data processor and does the data processor comply with applicable law? Remember that the data controller remains liable for the processing of personal data by the data processor.
- Is the outsourcing contract compliant with applicable FADP and/or GDPR? For financial services providers, are financial regulations complied with?
- Is the data processor entitled to any sub processing (i.e. sub contractors)?
- Is the data processor located abroad, i.e. will the personal data be transferred abroad?

In particular, cloud computing can raise various issues in terms of outsourcing and transfers abroad when personal data transferred to a cloud system does not entirely belong to the data controller. In fact, a cloud can be administered by a third party located in Switzerland, Europe or any third country and may entail for instance a transfer to a data processor and/or a transfer abroad.

In terms of transfers abroad, both Switzerland and the EU hold a list of countries that are deemed “adequate” in terms of personal data protection. In such case, the transfer abroad as such is authorized. If the country to which the personal data is not on the adequacy list(s), then further modalities will be required on a case-by-case basis (various tools exist that are not described here). To give an example, determining the location of the servers used by the data controller, as well as the location of the servers used by any data processors and contractors (i.e. digital tools used to process personal data, incl. cloud) is crucial as the servers could be located anywhere.

Distributed Ledger Technology challenges

The technical / digital infrastructure used for collecting and processing personal data is important for the analysis of personal data protection.

For instance, the use of blockchain technology raises points of tension in terms of data protection compliance. There is still not clear answer on how blockchain should be designed in order to be entirely compliant with the applicable data protection regulations in Switzerland and/or in Europe.

Challenges lie inter alia in the control over the personal data (i.e. who is a data controller, who is a data processor, who has access to the data) and how to protect the right to be forgotten of the data subject. Blockchain projects thus require a case-by-case analysis in terms of data protection compliance.

Checklist example

Before entering into a project or when making a data protection compliance assessment, one should assess multiple questions, for instance:

1. What personal data do you need to run your business? Are you collecting more data than necessary? Is any of this data qualified as “sensitive”?

Will you be processing personal data of minors (e.g. specific rules for minors)?

2. What will you be doing with this personal data?

e.g. will you be doing any profiling, automated decision making, behavioural monitoring

3. Are you allowed to process such personal data? On which basis?

e.g. is the processing proportional to the purpose / balance of interests, based for instance on legal requirements, a contractual relationship or the consent of the data subject

4. Where the processing is based on the data subject's consent, is this consent valid?

5. In which capacity are you processing personal data?

e.g. are you a controller, joint controller or processor?

6. Are you transferring personal data to a third party?

e.g. processors, cloud infrastructure, another group company.

If you are transferring personal data to a processor, did you execute a proper processing agreement?

7. Are you transferring personal data abroad?

e.g. are your servers or processors located abroad or are you part of an international group?

Have you verified if the third country is on a CH and/or EU adequacy list?

If not, are you properly relying on an alternative measure (i.e. The European Court of Justice invalidated the EU-US shield framework which may no longer be used as a basis for transfers to the US.

Checklist example (2)

8. For how long do you need to store the personal data? Have you set retention periods?

9. Have you complied with your duties of transparency / information towards data subjects?

10. Where applicable: Are you keeping the proper processing records?

11. Where applicable: have you applied with your duties of privacy by design and privacy by default?

12. Is the personal data properly secured? Who has access to the data within your business?

Have you thought of proper technical and organizational methods?

e.g. anonymization, pseudonymization, internal segregation of data, cyber security, physical security

Have you thought of organizing training sessions for your employees?

13. Are you equipped to answer claims brought forward by data subjects?

14. Do you know what to do in the event of a breach? Have you implemented internal processes?

Rights of data subjects

Data subjects have multiple rights in terms of the protection of their personal data, for instance where applicable.

- Right to lawful processing
- Right to information (transparency)
- Right to access personal data
- Right to object to the processing or to request a restriction of processing
- Right to rectification and erasure

- Right to restriction of processing
- Right to data portability (GDPR)
- Right to not be subject to a decision based solely on automated processing, including profiling (GDPR)
- Right to data security

Sanctions for a breach of data protection can be based on civil law, criminal law or administrative law.

**For more information on how OA Legal can assist you,
please contact one of our data protection specialists.**



Fabien Gillioz



fgillioz@oalegal.ch



Deborah Lechtman



dlechtman@oalegal.ch



Chloé Hasler



chasler@oalegal.ch

OUR OFFICE

1, place de Longemalle

1204 GENEVA

Phone: +41 22 786 88 66

eFax: communications@oalegal.ch

email: info@oalegal.ch

Disclaimer

This Data Protection Brochure (hereafter: “Brochure”) is published for informational purposes only and should not be construed as legal advice on any specific facts or circumstances. You should not act upon the information in this Brochure without seeking prior advice from a qualified lawyer licensed in your country or jurisdiction. OA Legal does not guarantee the timeliness, accuracy, or completeness of the information, opinions and analysis contained herein. All information, analysis and opinions may be amended at any time without any prior notification. No part of this Brochure is legally binding or enforceable and is made without express or implied warranties or representations of any kind. OA Legal will not accept any liability whatsoever for any loss or damage resulting from the use of, or reliance on, the Brochure. The information contained in this Brochure may not be used or reproduced - even in parts – in any other context.
