SMART SOLUTIONS
TO IMPROVE YOUR
DIGITAL EXPERIENCE

Privacy Compliance – the GDPR and the Swiss Data Protection Law

Hes·so

brix
more than software

TABLE OF CONTENTS

This document presents a brief overview of the EU's General Data Protection Regulation (**GDPR**) as well as the new Swiss data protection law: the Federal Act on Data Protection[1] (**FADP**). The purpose of these laws is to give control of personal data back to citizens by prohibiting organizations from processing personal data without a person's consent.

Though we review both the GDPR and FADP, more emphasis is placed on the GDPR than the FADP for two reasons. First, the GDPR has been in effect since 2018 whereas FADP only came into effect in September 2023. Second, FADP is inspired by the GDPR and arguably aims to give Switzerland a compatible law.

After our introduction, Section 2 defines key terms and Section 3 gives the principal requirements for organizations to become privacy compliant. Section 4 analyzes privacy compliance in the context of organizational scenarios like cloud usage, client onboarding, and the hiring process. Section 5 gives examples of fines already given out for violations of GDPR. Finally, Section 6 briefly compares the FADP to the GDPR.

[1] *Loi sur la protection des données* (LPD) in French, and *Datenschutzgesetz* (DSG) in German.

1 Introduction

What is the GDPR?

The GDPR, short for General Data Protection Regulation, is a Law from the European Union that specifies how companies must protect the personal data of EU citizens that they store and process. The law came into effect on May 26th, 2018.

What is the FADP?

The FADP, short for the new Federal Act on Data Protection came into effect on September 1st, 2023. The law is "new" since it replaces an existing privacy law that dates from June 1992, but which is no longer considered adequate in today's highly digitalized world.

As a Swiss organization, how does the GDPR impact you?

A Swiss organization needs to comply with the GDPR if:

- It has business operations within the EU, or
- It has access to personal data from EU customers, EU suppliers or EU employees. The *territorial scope* clause of the GDPR states that the law applies to companies operating outside of the EU, including Switzerland.

What happens if you fail to comply with the GDPR?

A company in blatant breach of GDPR can be fined up to 4% of its annual worldwide revenue, or 20 million EUR – whichever is greater.

Apart from legal reasons, why might it make sense for a Swiss organization to comply with the GDPR?

1. The new Swiss data protection law – FADP – is inspired by the GDPR. An organization in compliance with the GDPR is well positioned to be compliant with the FADP.
2. Your customers appreciate efforts to protect personal data. Indeed, the GDPR is the first of a worldwide trend towards the introduction of privacy regulations, e.g., the *California Consumer Privacy Act* and the Canadian *Protection of Personal Information and Electronic Documents Act* (PIPEDA).

3. Switzerland is a member of the European Free Trade Area, and the EU is Switzerland's largest trading partner. It is highly likely that a Swiss organization will eventually encounter personal data of an EU citizen.

Are there disadvantages in making your organization compliant to the GDPR?

Depending on the state of your data governance, implementing the GDPR can be costly since it requires resources to conduct an initial data cartography and possibly make changes to business activities and IT systems. However, the benefits in the long-term are important for data governance, organizational security, and mitigating the risk of fines.

Are there any differences between the FADP and the GDPR?

Apart from the fact that the FADP protects personal data originating in Switzerland, and the GDPR is designed to protect EU citizens, the essence of the two laws is the same. There are some small differences, so we return to this question later in the document.

What impact will the FADP have on Swiss organizations?

The FADP must be respected by all commercial and non-commercial organizations operating in Switzerland, or who process data that originates from Switzerland.

2 Key Definitions

According to the GDPR, **Personal Data** are any information which are related to an identified or identifiable natural person.

- Examples: name and surname, address, email address such as name.surname@company.com, identification card number, location data, IP address, cookie, advertising identifier of your phone.

One class of personal data is sensitive data. This is data that would not normally be in the public domain. It includes racial or ethnic origin, political opinions, membership of trade unions, religious beliefs, health conditions (both physical and mental), sexual orientation, and criminal offence history. If your organization requires such data, then extra-strong measures are required for protection. The penalty for not protecting sensitive data can be higher than for not protecting standard personal data.

A feature of the FDAP is to classify genetic and biometric data as sensitive data.

A **data subject** is an identified or identifiable living individual to whom personal data relates. A data subject can be a client, employee, supplier, contractor – so any individual with a relationship with your organization.

A **data controller** is a natural or legal person, public authority, agency, or other body which determines the purposes and means of processing of personal data. Controllers make decisions about processing activities. In practice, a data controller is any organization that stores or processes personal data.

A **data processor** is a natural or legal person, public authority, agency, or other body which processes personal data on behalf of a controller. Processors act on behalf of the relevant controller and under their authority. For instance, a cloud storage provider is a data processor for an organization that outsources its data storage.

Question: is your organization a controller or a processor?

If your organization uses a cloud service to store or process personal data, then you are a controller, and the cloud service is a data processor. We return to this question in Section 4.

3 Main GDPR Requirements

This section mentions the main requirements that an organization must respect to be compliant with the GDPR. It is based on the EU's GDPR checklist, broken down into four categories: 1) Lawful basis and transparency, 2) Data Security, 3) Accountability and Governance, and 4) Privacy Rights for citizens.

3.1 Lawful Basis and Transparency

The first step towards privacy compliance is to identify those organizational activities that process personal data and ensure that processing has a lawful basis.

3.1.1 List of Processing Activities

Organizations with over 250 employees or who conduct high-risk data processing must take the following steps. Other organizations are strongly encouraged to take these steps also.

- Keep an up-to-date and detailed list of processing activities and be prepared to show that list to regulators upon request. A processing activity corresponds to some business activity, e.g., newsletter, payroll, video surveillance.

- For each activity on the list, you should detail the purpose of the processing, the kind of data you process, who has access to data in your organization, any third parties with access (and where they are located), what you're doing to protect the data (e.g., encryption), and when you plan to erase it (if possible).

3.1.2 Legality of processing

For any of the identified activities, processing of data is illegal under the GDPR unless you can justify it according to one of the following conditions listed in GDPR. The conditions include:

- Receipt of consent from the data subject for storage and processing of that data.
- You can argue that the data is needed to conduct a contract with the subject. For instance, a school needs to keep student grades in its database to be able to give diplomas.
- The law of the host country requires that you process that data. For instance, bankers must do background checks on clients for AML due diligence which requires processing of data relating to origin of wealth.
- You can argue that processing the data is in the legitimate interests of the controller. An often-cited example is a commercial company that suspects some client of cheating the company, e.g., by claiming that delivered goods were not received, and therefore implements special processing to validate this suspicion.

For each business activity, your organization must choose a lawful basis for processing, and document your rationale.

- If consent is the lawful basis, know that consent can be revoked.
- Neither children nor those suffering from dementia can give informed consent.

3.1.3 Explain why you are collecting data.

You need to tell people that you are collecting their data and why (Article 12). You should:

- Explain how data gets processed, who has access, and how your organization is keeping the data safe.
- Include this explanation in a privacy policy, available on your website, in clear and plain language.

3.2 Data Security

This means implementing appropriate technical and organizational measures to protect data.

3.2.1 Data protection by default

- Technical measures include encryption, multi-factor authentication, and keeping software updated with the latest versions.
- Organizational measures include limiting the amount of personal data collected, deleting data you no longer need, and minimizing permissions accorded to employees for data.
- Employees must be aware of these measures.

3.2.2 End-to-end encryption

Tools like email, messaging, notes, and cloud storage should use encryption or pseudonymization whenever feasible. In the context of the Web for instance, *https* is an example of end-to-end encryption.

3.2.3 Security policy

Create a security policy and ensure team members are knowledgeable about data security.

- A policy should include directives about email security, passwords, two-factor authentication, device encryption, and VPNs.
- Technical and non-technical employees with access to personal data must receive GDPR training.

3.2.4 Data protection impact assessment

For each IT service, a data protection impact assessment aims to understand how your product or service could jeopardize personal data and minimize those risks. You should be able to show the results of the assessment to regulators. The reason for the assessment is to ensure that your organization fully understands the consequences of personal data processing and is convinced that the processing should take place despite any measured risks.

3.2.5 Notification of breach

In the event of a data breach, you must:

- Notify the data protection authority in your jurisdiction within 72 hours.

- Communicate data breaches to your data subjects unless the breach is unlikely to put them at risk (for instance, if the stolen data is encrypted).

3.3 Accountability and Governance

This theme considers how an organization oversees the implementation of GDPR.

3.3.1 Accountable person

Ensure some person in your organization is accountable for GDPR compliance – meaning he evaluates data protection policies and their implementation.

3.3.2 Data processing agreements

Services should have a standard data processing agreement available on websites for review.

- The agreement must mention any third-party services that handle the personal data, including analytics software, email services, cloud servers, etc.
- Agreement spells out rights and obligations of each party for GDPR compliance.
- Only use third parties that are reliable and give sufficient data protection guarantees.

3.3.3 Foreign representative

If you process data in an EU member state, you need to appoint a representative in that country who can communicate on your behalf with the local data protection authority.

3.3.4 Data protection officer

A Data Protection Officer (DPO) interacts with data subjects and surveys implementation of GDPR in the organization, assesses data protection risks, advises on data protection impact assessments, and cooperates with regulators and local data protection authorities.

- It is *recommended* that every organization have a DPO.
- Public authorities and organizations whose business model requires large scale processing of personal data are *obliged* to have a DPO.

3.4 Privacy Rights

GDPR is about handing control of personal data back to citizens. This is achieved through the provision of a series of rights that all citizens may exercise.

3.4.1 Right to consult

Data subjects have the right to see what personal data your organization has about them.

- They have a right to know how long you plan to store their information and the reason for keeping it.
- In response to a request from a data subject, you must respond with a copy of the personal data you hold. The first copy of this information must be free, but you may charge a reasonable fee for subsequent copies.
- You must comply with such requests within a month.
- Data must be sent in a commonly readable format (e.g., a spreadsheet).
- Data subjects can ask for data to be sent to a third party they designate, which may even be a competing business of yours.

3.4.2 Data accuracy

Keep data up to date by putting a data quality process in place and make it easy for data subjects to view and update their personal information for accuracy and completeness.

3.4.3 Right to forget

When consent is the legal basis of processing, citizens have the right to ask you to delete all the personal data you have about them.

- You must honor their request within a month.
- Grounds to deny the request include the exercise of freedom of speech or compliance with another legal obligation (e.g., salary data must be conserved for 10 years in some Swiss cantons).

4 Scenarios for Your Organization

Another approach to understanding the GDPR, and later FADP, is to consider how these laws impact on core activities that all organizations encounter.

4.1 The Hiring Process and Managing CVs

Your company will hire new people and publish job announcements on the Web in the hope of receiving CVs.

There are many interesting aspects about this activity:

- A CV will contain much personal data of the candidate: name, age, address, sex, education record, former employment, potential situation of health and handicap, driving license if the job requires mobility, etc.
- A CV can contain personal information of people other than the candidate, like the names and phone numbers of references and former employers.
- The employer may desire to share candidate information with other organizations, e.g., judicial authorities to know if the candidate has a criminal record. This means that the hiring company may collect more information about the candidate than the candidate includes in his CV.

Your organization must take the following steps:

- Ensure that only people who need to process CVs (HR department) or who take decisions about hiring (supervisors, etc.) have access to a CV.
- The Web portal through which candidates upload CVs should contain a privacy policy. Here is a good example of a privacy policy from the Pictet banking group: https://www.pictet.com/ch/en/legal-documents-and-notes/privacy-notice.
    - This policy clearly states that candidate information may be shared with outside organizations for background checks, that data is deleted or anonymized after 2 years, that the purpose of the data is to evaluate the candidate and ensure Pictet's diversity policy is maintained (which for instance justifies asking for the sex of the candidate), that automatic processing of CVs can take place, and that the candidate may ask for a copy of the data held by Pictet and ask to rectify this data.
- Special category information like religion, health, or political beliefs may never be shared.
- CVs of unsuccessful candidates should be deleted after the hiring process. If you wish to retain the CV of an unsuccessful candidate for a period after the hiring decision has been made, in case another position becomes available, then the candidate must give his explicit consent.

4.2 Client On-Boarding and Managing Prospect Data

Managing prospect and customer data is essential to a company's business.

Before the organization begins its privacy compliance journey, it must handle its existing customer databases. If these customer data were entered without explicit consent, then you cannot keep these data.

Many organizations use CRM software for this purpose, and today such software must help the organization be compliant to GDPR. For instance, the CRM should record all consent choices, provide a means for customers to update or withdraw consent and permit responses to subject access requests (where the customer asks for a copy of his or her personal data). The customer must understand how personal data is processed and how it is protected.

Often customer relations begin with the exchange of business cards. After receiving the business card, before you enter the client's contact data into a system, you must ask that client by email if he consents to this. The physical exchange of a business card is not enough to indicate explicit consent, principally because there is no auditable trace of consent being given.

Onboarding is a special kind of business relationship. It refers to the activities necessary to turn a prospect into a customer. In the finance domain, onboarding requires due diligence, identification, and verification. For wealthy clients for instance, anti-money laundering (AML) and Know-Your-Customer (KYC) checks must be made which entails collecting data relating to the prospect's nationality and origin of wealth. If your organization makes these checks, then you could consider such processing as a "legal obligation" that justifies processing of this personal data without explicit consent.

4.3 Marketing Campaigns & Data Repositories

Marketing emails remain a popular means of advertising your company products today.

Be aware that cold emailing is a form of "processing" under the GDPR, and it is only allowed if either the data subject has consented, or there is another legal basis. An example of the latter is a justified interest by the company for sending these mails; this can happen in the context of a B2B relation. Profiling prospective clients is another form of processing.

To become compliant with respect to mailing lists, one company (Litmus) suggests conducting an audit of your current email database. It is important to understand how you acquired the current emails. Current data practices should be disclosed (in the marketing emails for instance) and your organization must ensure that there is "freely given, specific, informed, and unambiguous" consent from all email receivers. Guidelines for obtaining consent include:

- Get consent from an opt-in, not pre-ticked boxes on Web forms.
- Keep consent requests separate from other terms & conditions. If subscribing to a newsletter is required to download a whitepaper, for example, then that consent is not freely given.

- Make it easy for people to withdraw consent—and tell them how to do it.

Question: should your company purchase a list of email addresses (under the GDPR)?

Probably not!

4.4 Cloud Services and Data Location

Your company may be a client of a cloud service provider, be these services IaaS, PaaS, or SaaS.

4.4.1 Cloud Service Provider

Cloud providers can demonstrate compliance with security in several ways: through a Data Protection Impact Assessment (DPIA) or by being ISO 27001 certified.

More recently, the EU has defined a Cloud Service Provider Code of Conduct for all types of cloud service providers that lays out a set of compliance requirements to "enable CSPs to demonstrate their capability to comply with GDPR". A monitoring authority can be mandated in a country to verify that a provider conforms to the code. The evaluation of the provider takes place once every year or whenever a complaint is made. Major cloud providers that adhere to the code include Cisco, Google Cloud, Dropbox, Salesforce, SAP, and IBM.

4.4.2 Cloud Service Client

Companies today can use many cloud providers, and many common services store data on the cloud, e.g., Zoom, Teams, WhatsApp, Dropbox, iCloud etc. Employees using personal devices, BYOD or not, might have installed other cloud-using services. Cloud services can therefore constitute a form of shadow IT.

Several of the most serious data breaches in recent years have been from cloud-based storage systems, including Apple, Microsoft, and Yahoo. Nonetheless, most cloud providers cannot, contractually, use the data for their own purposes. Thus, the cloud provider remains in the role of a data processor, and your company is the data controller. This means that your company remains responsible for personal data and must act in the event of cloud data leaks under the GDPR.

A crucial issue is the location of personal data that you store with the cloud provider. The provider may store copies of data in several countries (and therefore

legal jurisdictions). The laws in other countries may not be strong enough to protect user data to a level that satisfies the European Union:

- The EU has classified several countries as having an adequate level of legal protection for GDPR compliant cloud service providers to store their data there.
- The US is not on this list of countries with a recognized level of protection, essentially due to the US Patriot Act which enables law enforcement authorities to seize data provided a court warrant has been granted.
- **Switzerland is on the list of adequate countries since January 2024**. It was not on the list beforehand because the EU did not consider the 1992 Swiss data protection law to be sufficiently strong.

As a client, the right to audit your cloud provider should be part of the contractual agreement. The audit can be conducted as a Data Protection Impact Assessment (DPIA).

4.5 GDPR-compliant Websites

Company websites frequently offer services like white papers or proprietary content which users only have access to if they enter names or email addresses. Companies have used this practice in the past to build their mailing list. The practice is still possible, but it must comply with the GDPR.

The first step to make a website GDPR compliant is to publish a privacy policy on the site's pages. The policy should clearly *explain what data is being collected and what this data is used for*. The website policy must also make it clear how a person may contact someone in the organization with a request to see his or her personal data or to have it erased – formally called a subject access request (SAR) under the GDPR.

The website must be built using secure technologies. Indeed, several companies have been fined under the GDPR for collecting personal data through insecure websites. Among the measures that website owners are now expected to implement are i) use *https* instead of plain *http*, ii) use strong authentication methods for access to the database behind the website, and iii) ensure that the website software is kept up to date with the latest versions.

When websites do collect personal data, user consent must be sought for this. Consent forms on a web page must not be pre-ticked, meaning that the default option for a user is not to consent. Several consent options are possible, such as one consent option for receiving a newsletter and a second option for receiving marketing information.

A well-known issue for websites is cookies. A cookie is a small file that websites send to client Web browsers, and which browsers can send back to websites so that the site *remembers* users. Among the classes of cookies, we find:

- *Authentication* or *session* cookies. These allow browsers to remain "logged in" when the user returns to a website after having logged in earlier. Without these cookies, it would not be possible to implement features like shopping carts on e-commerce sites.
- *Layout* cookies. These handle user layout and presentation preferences. For instance, when a user returns to the website, he finds the same language and layout preferences that he chose on his first visit to the site.
- *Analytics* cookies. These are used to track the behavior of users on a site, e.g., to record the number of visits, type of device used to visit site (mobile or desktop, Windows, or Linux, …).
- *Advertising* cookies. These cookies record user characteristics such as age and location. They are used by marketeers to customize advertisements presented to users when they visit the site.

Most forms of cookie are considered privacy-invasive, and a website that uses these cookies must ask for explicit permission and must even offer the option to users of surfing the site with cookies disabled.

Modern websites are often built using frameworks like WordPress. These offer a core framework and a variety of plugins for different Web features. In WordPress for instance, there are plugins for newsletters, language translations, forms, etc. Each plugin can use its own cookies so the challenge for organizations is to verify that each plugin used on their website is GDPR compliant.

5 Example Fines

Many organizations have been fined for breaches of GDPR. We often hear of huge fines given to large US corporations but bear in mind that fines are proportional to the revenue of the organization. Many SMEs have been fined also.

Amazon received a 746 MEUR fine in 2021 for failure to get cookie consent; Facebook received a fine of 60 MEUR for the same reason.

WhatsApp received a 225 MEUR fine from the Irish data protection authority for not properly explaining its data processing practices in its privacy notice. If an organization claims "legitimate interests" for processing, then those interests must be clearly explained. Google received a 50 MEUR fine for not providing enough information in the privacy policies about how personal data is processed.

The Office of Housing in the French town of Rennes got a fine of 30 kEUR for use of a contacts file for purposes other than the initial purposes.

H&M was fined 35 MEUR for illegally processing employee data. Employee meetings were recorded and accessible to over 50 H&M managers, divulging "broad knowledge of their employees' private lives… ranging from rather harmless details to family issues and religious beliefs." A Paris SME was fined 20 kEUR for having cameras installed in their offices that continually filming employees.

The Italian phone operator TIM was fined 27.8 MEUR for making unsolicited promotional calls to people, some of whom were on non-contact and exclusion lists. Enel Energia was fined 26.5 MEUR for similar reasons. Many SMEs have been fined for the same reasons.

British Airways was fined 22 MEUR for not having sufficient security measures. After a data leak, the British data protection authority considered that the airline did not have sufficient security measures in place. Marriott Hotels was fined 20.4 MEUR for similar reasons. The Dutch Data Protection Authority (DPA) has imposed a 12,000 EUR fine on an orthodontic practice for allowing new patients to register on a website that used *http* instead of *https*.

6 The Swiss Law – the FADP

The new Swiss data protection law came into effect on September 1st, 2023. The FADP is very similar to the GDPR for two reasons:

a) The GDPR has become a standard for privacy laws across the world.
b) Switzerland is now on the list of countries that the EU considers as having adequate data protection measures. Not being on the list, as was the case prior to January 2024, was prejudicial to Swiss cloud providers, so a law that resembles the GDPR was needed to get Switzerland back on this list.

Though similar, there are some minor differences in the FADP. For instance:

- Biometric and genetic data is included in the categories of sensitive personal data.
- The maximum fine for an FADP violation is 250 kCHF – compared to up to 20 MEUR for a violation of the GDPR. Also, the FADP calls for a person in the organization to be fined, rather than the organization itself.
- A potential data leak must be declared "as soon as possible" under the FADP; the GDPR requires a leak to be declared within 72 hours.
- A data protection officer (called an adviser under the FADP) is not mandatory for the FADP – though it remains highly recommended in practice.

Despite the FADP text appearing les strict than the GDPR, it remains to be seen how strictly the authorities will enforce the law. For instance, if an organization fails to report a data leak within 72 hours, it is possible that a court will consider this a failure to declare the leak “as soon as possible”.

Sources:

https://www.enforcementtracker.com

https://termly.io/resources/articles/biggest-gdpr-fines/

https://gdpr-info.eu

https://gdpr.eu/checklist/

https://www.edoeb.admin.ch/edoeb/de/home.html

Authors: Ciarán Bryce (HES-SO), Kevin Lang (brix IT Solutions), Sojo Nagaroor (brix IT Solutions)

First version: March 2024.