

# New Federal Act on Data Protection (nFADP)

**Switzerland is implementing new legislation to better protect its citizens' data. Swiss companies will have to comply with this legislation from September 1, 2023.**

In its fall 2020 session, Parliament passed the new Act on Federal Data Protection (nFADP). It improves the processing of personal data and grants Swiss citizens new rights. This important legislative change also comes with a number of obligations for companies. Implementation through the Data Protection Ordinance is on September 1, 2023.

## A necessary new law

The first Federal Data Protection Act dates back to 1992. The Swiss population has since introduced into daily life the use of the Internet and smartphones and is increasingly using social networks, the Cloud or the Internet of Things. In this context, a complete overhaul of the data protection law - and not just a partial one as was the case in 2009 and 2019 - is essential to ensure that the population has adequate data protection adapted to the technological and social developments of our time.

Swiss law's compatibility with European law, and in particular with the European General Data Protection Regulation (GDPR), is the nFADP's other challenge. The nFADP should make it possible to maintain the free flow of data with the European Union (EU) and thus avoid a loss of competitiveness for Swiss companies.

## What are the main changes?

The nFADP introduces the following eight major changes for businesses.

1. **Only data of natural persons**, and not those of legal persons, are now covered.
2. **Genetic and biometric data** fall under the definition of sensitive data.
3. **The principles of "Privacy by Design" and "Privacy by Default"** are introduced. As its name implies, the principle of "Privacy by Design" requires developers to integrate the protection and respect of users' privacy into the very structure of the products or services that collect personal data. The principle of "Privacy by Default" ensures the highest level of security as soon as the products or services are released, by activating by default, i.e. without any intervention from users, all the measures necessary to protect data and limit their use. In other words, all software, hardware and services must be configured to protect data and respect the privacy of users.
4. **Keeping a register of processing activities** is now mandatory. However, the ordinance allows exemptions for SMEs whose data processing presents limited risk of harm to the data subject.
5. **Prompt notification** to the Federal Data Protection and Information Commissioner (FDPIC) is required in the event of a data security breach.
6. **The concept of profiling** (i.e. the automated processing of personal data) is now part of the law.