EPFL Center for Digital Trust

FOCUS 8

Data protection in the EU and Switzerland

Key differences and shared principles

Featuring interviews with

Paul Nemitz
European Commission

& **Sylvain Métille**
UNIL

Written by Leila Ueberschlag

Data protection in the EU and Switzerland

Key differences and shared principles

Nearly seven years after the entry into force of the General Data Protection Regulation (GDPR) in Europe, what impact has it had on data protection? What are the main legislative differences between the European Union and Switzerland? And how will the situation evolve as the rise of generative AI in our daily lives further exacerbates privacy challenges?

This edition of C4DT Focus explores these questions by providing an overview of the situation in Europe and Switzerland, highlighting the similarities and differences, particularly through two interviews with data protection specialists.

100,000 complaints received annually

In July 2024, the European Commission published its second report on the implementation of the GDPR. The report shows, among other things, that since 2018, data protection authorities have launched more than 20,000 investigations on their own initiative. Collectively, they receive over 100,000 complaints annually (see the related commentary in the interview with Paul Nemitz below), and have imposed over 6,680 fines to date, totalling approximately 4.2 billion euros. According to the report, data protection authorities have, in general, made extensive use of their corrective powers, although their numbers vary considerably from one authority to another. On an individual level, awareness of the GDPR and data protection authorities (Eurobarometer 549 of 2024 on justice, rights, and values) shows that 72% of respondents across the European Union have heard of the GDPR, with 40% knowing what it is.

As a reminder, the GDPR, which came into effect in May 2018 in Europe, also applies to non-European entities that process data of European residents to whom they offer goods or services. In 2015, in order to align Swiss law with the new European rules to come, Switzerland undertook a revision of its Federal Act on Data Protection (FADP) which had been in place since 1992. After several developments, the new Federal Act on Data Protection (nFADP) finally came into effect in September 2023. Furthermore, it was recognized by the European Commission in January 2024 as being aligned with the GDPR, allowing data to continue to flow freely between Switzerland and the European Union.

Key provisions of the GDPR

In detail, the GDPR strengthens the “right to be forgotten” and facilitates access to personal data, notably by establishing a right to data portability, enabling free transfers from one service provider to another. Companies and organizations must also comply with the principles of “data protection by default” and “by design” to ensure the security of information collected throughout its lifecycle, from creation to deletion.

Individuals’ consent must be obtained through a clear statement or an unambiguous affirmative act. Additionally, the appointment of a data protection officer is mandatory for entities whose core activities involve processing sensitive data or large-scale data. Any security breach must be reported to the competent authority within a maximum of 72 hours.

The GDPR also grants additional rights to individuals, such as the right of access, the right to rectification, the right to object to data processing, and the temporary limitation of its use. Moreover, citizens and pressure groups can file class actions for compensation in case of violations of the regulation. Data transfers to countries outside the European Union are strictly regulated and require specific safeguards.

Finally, in case of non-compliance, the GDPR provides for significant administrative penalties, which may reach 20 million euros, or, in the case of a company, up to 4% of the total annual global turnover of the previous financial year, whichever is higher.

A swiss law considered less strict

The nFADP, which takes inspiration from the GDPR, is considered less formalistic and imposes lower compliance requirements compared to the European regulation. Similar to the GDPR, it enhances individuals' rights, including access, rectification, and erasure of personal data, while introducing obligations for businesses and institutions, such as transparency in data processing and breach notifications to competent authorities. However, the nFADP adopts a more flexible approach: consent can be implicit in certain situations, penalties are criminal in nature and target responsible individuals rather than companies, and there is no explicit right to data portability. Penalties can reach up to 250,000 francs, and if no responsible individual can be identified, a subsidiary fine of up to 50,000 francs may be imposed on the company. Additionally, fines are imposed only when unlawful intent is proven

“It is crucial for data protection authorities to take a more proactive approach in their investigations”

Paul Nemitz is the principal advisor in the Directorate-General for Justice and Consumers of the European Commission. Before, he was the director responsible for fundamental rights and Union citizenship, the lead director for the reform of the EU data protection legislation, the “Snowden” follow up, the negotiations of the EU—US Privacy Shield and the EU Code of conduct against hate speech on the internet.

He reflects on the GDPR’s impact six years after its implementation, its effectiveness, the evolving challenges posed by emerging technologies like AI, and the future of data privacy in Europe.

What is your assessment six years after the General Data Protection Regulation (GDPR) came into force?

The report issued by the European Commission in July 2024 shows that, overall, the implementation of the GDPR has been positively assessed. However, there are areas where improvements can still be made. For instance, we have found that over 100,000 complaints are filed annually with data protection authorities. On one hand, this indicates that people in Europe are aware of their rights and are eager to exercise them. On the other hand, the high volume of complaints, coupled with research showing that in some member states up to 80% of websites fail to meet

even the most basic GDPR requirements – such as having an accessible Privacy Policy – demonstrates that compliance needs to be improved.

No law is perfectly complied with, but the effectiveness of compliance is determined by the likelihood of detection for noncompliance, multiplied by the potential fines. This combination creates a deterrent effect, which is central to ensuring adherence to the law. GDPR allows for significant fines, but it is clear that, with data being used everywhere, the chances of a Data Protection Authority (DPA) detecting noncompliance are still low.

In my view, it is crucial for data protection authorities to take a more proactive approach in their investigations, especially with large companies that process data from a significant number of people. Additionally, DPAs should continue to impose substantial fines. The goal is for fines to have a broad deterrent effect – not just on the company fined, but also on others.

How could this situation be improved?

It is crucial for DPAs, in their policy on fines, to ensure that penalties are both proportional and effective in deterring future noncompliance. We have already seen an increase in fines across many member states, which is a positive trend. I encourage data protection authorities to continue raising fines, as this would strengthen the deterrent effect of their activities and help improve overall GDPR compliance.

How is the GDPR perceived and understood by companies in Europe and abroad?

Perceptions of GDPR compliance vary widely. A majority of companies, particularly those that respect their clients – especially individual consumers – make the necessary efforts to ensure they fully comply with the GDPR. However, some business models in the data economy, like those of Meta (Facebook) or Alphabet (Google), regularly test the limits of GDPR and operate on the edge of compliance. Unsurprisingly, these companies frequently criticize the regulation in place and seek to rally opposition to proper GDPR implementation. Still, we should not overlook the fact that most companies recognize the importance of protecting personal data – not just to comply with the law but to safeguard individuals and uphold democratic values.

Are the sanctions significant enough for large corporations, for which, as you said, breaking the law often remains economically more advantageous than complying with it?

The full extent of binding powers, including penalties of up to 4% of global turnover, must be systematically enforced against major companies. Fining can be cumulative to other measures, for example, a halt in data processing

and deletion of data. I am confident that with those measures held out in a credible way, the rate of compliance will increase.

The issue of all-encompassing profiling in the data market is particularly concerning. This goes far beyond a Spotify playlist or an airline loyalty program; it involves personality profiles with thousands of parameters, created through the extensive collection of personal data by companies like Meta and Alphabet. These profiles reveal sensitive information such as people's religious orientation, political preferences, sexual orientation, dreams, aspirations, and desires, making them fundamentally incompatible with democracy. The mere knowledge that such profile exists, whether held by private entities or public authoritiess has a chilling effect on individual behaviour. We must collectively aim to eliminate such all-encompassing personality profiles. This could be achieved through stricter enforcement of the GDPR or, should that prove insufficient, through a specific law. Such a law, similar to the AI Act's initial articles, should prohibit the use of AI for mass social scoring, which is effectively equivalent to these overarching profiles. Establishing a dedicated legal framework is essential to end the creation and misuse of such intrusive data practices.

Is the increasing use of generative AI making GDPR's application more complicated?

The implications of AI on data protection are multifaceted. First, personal data has been used to train AI models recklessly, often without valid legal grounds – an issue still requiring thorough investigation. Second, the compliance of AI with GDPR when processing personal data is far from assured, raising numerous ancillary challenges.

For example, AI could make it easier to identify individuals in ways that were previously not possible. Data considered non-personal may now be classified as personal due to AI's ability to identify individuals. These are critical issues that require our attention.

Moreover, the approach to risk taking by companies who are producing major AI programs – such as Microsoft, Meta or Alphabet – often appears quite careless. Recently, press reports have revealed that some of these companies are considering using nuclear power to fuel their AI operations. The world has witnessed the catastrophic dangers of nuclear power through past accidents. If these companies' approach to nuclear power reflects their broader attitude toward risk – particularly in relation to AI and compliance with the law – then it raises serious concerns. In light of this, it is essential for data protection authorities to adopt a very rigorous approach to ensuring AI compliance with data protection laws.

Do you think the GDPR alone is sufficient to address the challenges posed by AI, or is there a need for additional legislation?

The European Union already has a specific law in place —the AI Act— but it doesn't exclusively focus on the protection of personal data. The GDPR remains fully applicable to AI, and I believe it will continue to be the more relevant law for a long time, especially since it can be directly invoked by individuals.

At this stage, it is unclear whether the AI Act gives individuals the right to bring direct actions against companies or authorities in cases of noncompliance. the GDPR, however, makes it clear that people can take direct action in cases of noncompliance, including compelling data protection authorities to act by taking them to court.

For this reason, and due to the substantive nature of the law, I would argue that the GDPR will remain the more relevant piece of legislation for the foreseeable future. In fact, I would go as far as to say that it is legally inconceivable for data processing to be considered legal under the GDPR if the AI Act is not fully complied with. As a result, we may find that noncompliance with the AI Act could give individuals the right to take legal action based on the GDPR, particularly under the principle of legality of processing.

How do you see things evolving in the coming years in Europe?

I believe the willingness of data protection authorities (DPAs) to enforce the GDPR and impose significant fines is growing. That being said, Europe still lags behind when it comes to the scale of its fines compared to the Federal Trade Commission in the United States, which, for example, imposed a $5 billion fine on Facebook. There is certainly room for larger fines in Europe.

I also see DPAs becoming more tech-savvy, and their increasing cooperation across borders will make enforcement more efficient. Soon, the European Union will likely adopt new procedural regulations that will improve collaboration between DPAs across borders. This will enable them to handle complaints more effectively and respond more quickly, which will significantly enhance the overall enforcement of the GDPR.

“Data protection in Switzerland could benefit from a framework as robust as FINMA’s supervision”

Sylvain Métille is a professor specializing in data protection and cybercriminal law at the University of Lausanne, and a practicing attorney at HDC. He provides an analysis of how Switzerland has adapted its data protection framework in response to the GDPR and technological advancements, discussing the impact of these changes, the differences between Swiss and EU approaches, and the challenges of enforcement in Switzerland.

What is your assessment six years after the GDPR came into force in Europe and its impact on Switzerland?

It is important to remember that data protection did not begin with the GDPR. The GDPR replaced the 1995 Data Protection Directive, which established similar principles but allowed for varying interpretations among European member states. As a regulation, the GDPR ensures a more uniformed application of data protection laws across the EU, which benefits businesses – including those outside Europe, like in Switzerland – that process EU residents’ data. The consistency of rules simplifies compliance for these businesses.

Switzerland revised its Data Protection Act (FADP) to align with the GDPR and strengthen individuals' rights in response to technological advancements. What other effects has the GDPR had in Switzerland?

The GDPR, coupled with the risk of substantial financial penalties, and Switzerland's lengthy, complex legal revision process, has significantly raised awareness about data protection and related legal obligations.

On one hand, individuals are now more conscious of their rights. On the other hand, businesses increasingly understand their obligations. Many companies clearly strive to do the right thing. In the past, some aimed to succeed without being fully aware of the rules. Now, these companies not only seek success but are also conscious of the regulations and are making their best efforts to abide by the law.

What are the major differences between Switzerland and Europe?

Jurisdictional differences and distinct legal frameworks play a role. When the GDPR was adopted in 2016, it generated significant attention in Europe and Switzerland. By 2018, many Swiss businesses, fearing sanctions, began aligning their practices with GDPR requirements. Even those not directly subject to the GDPR made adjustments, anticipating that similar regulations would come to Switzerland. By the time Switzerland revised its law, many major players were already compliant, requiring only fine-tuning to meet Swiss-specific requirements.

A key difference lies in the legal basis for processing data. In the EU, data processing requires justification under strict criteria, creating a significant burden for data controllers. In Switzerland, as long as principles like proportionality, security, transparency, purpose limitation and good faith are respected, no justification is required unless these principles are breached. This flexibility simplifies compliance without substantially weakening protection.

Switzerland also takes a pragmatic, risk-based approach. For instance, the obligation to maintain a record of processing activities applies only to companies with over 250 employees or those processing high-risk data. In the EU, small companies with regular processing activities may still require to maintain a record. This pragmatic approach does not necessarily reduce protection but reduces paperwork for lower-risk activities.

What is your opinion on the sanctions stipulated by Swiss law?

Swiss law imposes limited penalties, focusing on criminal offenses by individuals (including when data is processed by a company). Fines can reach up to 250,000 francs, which is not insignificant. However, when businesses weigh the potential benefits of non-compliance against the penalties to be paid by an employee, the deterrent effect is limited.

Penalties apply only in specific cases requiring proof of intent, which can be challenging. These are minor offenses and not a priority for overburdened criminal prosecution authorities. Unlike the EU, where organizations are held accountable, Swiss law holds individuals responsible, potentially encouraging greater compliance. However, the smaller fines reduce its impact.

For those genuinely aiming to comply, Swiss law is relatively manageable, with fewer formalities than EU regulations. But for businesses whose core operations involve non-compliant practices – like opaque data brokering or creditworthiness assessments – weak enforcement reduces the law's effectiveness.

The most significant sanction is the prohibition of data processing, which can be imposed by a civil court or the Federal Data Protection and Information Commissioner (FDPIC) officer. However, enforcement is limited due to the office's understaffing and conciliatory approach, leaving Switzerland without a strong enforcement authority like COMCO in competition law.

Have any fines been issued in Switzerland since the Federal Act on Data Protection has been revised?

To my knowledge, no fines have been issued yet. This is partly because offenses under the new law are misdemeanours rather than administrative fines and are handled by authorities not specialized in serious offenses. In some cantons, the same authorities handle minor issues like parking tickets, which limits their capacity to enforce data protection laws offenses.

Additionally, breaches subject to penalties are narrowly defined, and proving intent is difficult. For example, failing to implement adequate security measures constitutes a breach, but proving it was intentional is challenging. Political decisions to use criminal sanctions mean enforcement relies on cantonal systems, which are not well-equipped for such cases. Moreover, the FDPIC cannot impose fines directly, further weakening enforcement.

Individual lawsuits against non-compliant businesses have been somewhat effective but place a significant burden on individuals. While the process is free, losing a case could lead to covering the opposing party's legal costs, discouraging consumers from pursuing claims against large corporations.

Does AI threaten compliance with the GDPR and the FADP?

We are at a turning point with AI, which demands vast amounts of data for training, often exceeding what can be anonymized without identification risks. This creates tension between advancing AI and upholding data protection laws.

AI also introduces new risks, including manipulation through deepfakes and reputational damage. While the general public remains unaware of many of these risks, their potential for harm is immense, highlighting the need for stronger application of existing laws. Some countries, like Italy, have acted swiftly against violations, but Switzerland has been less proactive.

Why has Switzerland been slower to act?

It comes down to resource allocation and prioritization. The FDPIC is legally required to address all cases but lacks the resources to do so effectively. This forces selective enforcement, which courts may later review.

In summary, while the existing rules offer substantial protection, gaps remain — especially in commercial contexts where companies with extensive resources can easily outmatch regulators. Comparing data protection enforcement to banking oversight, Switzerland's Financial Market Supervisory Authority (FINMA) has a large, respected staff and clear authority. Data protection in Switzerland would benefit from a similar framework.

Pragmatism also has its place. Not all data processing poses significant risks, so reducing formalities for low-risk activities is sensible. However, for high-risk areas like medical data, stronger safeguards are essential.

Takeaways and conclusions

The GDPR has significantly reshaped the data protection landscape, offering a uniform framework across Europe and serving as a model for many countries, including Switzerland. Its strengths lie in empowering individuals with robust rights and providing data protection authorities with strong corrective powers. However, the sanctions, while substantial, often remain manageable for large corporations, raising questions about their true deterrent effect.

One key criticism of the GDPR is the significant administrative burden it places on businesses. While large corporations like Meta or Google have the resources to navigate compliance with relative ease, smaller businesses often find the regulatory requirements daunting and costly, highlighting the tension between universal application and proportionality. As Sylvain Métille explains, “The GDPR is one of the rare regulations that apply uniformly to all businesses, regardless of their size or resources.” Moreover, the European Commission’s 2024 report notes that divergent interpretations of the GDPR by national authorities create legal uncertainty, which raises compliance costs and disrupts the free flow of personal data.

Switzerland, inspired by the GDPR, has opted for a more “pragmatic” approach. The new Federal Act on Data Protection strengthens individual rights but imposes lower compliance costs. This reflects the country’s preference for a flexible, risk-based approach, though it raises concerns about enforcement effectiveness, given limited resources and the absence of significant penalties.

As digital technologies continue to evolve, and with the advent of generative AI, existing legal structures are facing ever greater challenges. The need for a harmonised yet adaptable approach is becoming more urgent than ever. Growing public awareness of the risks associated with the processing of personal data is driving demands for stricter laws globally, while data profiling and targeted advertising practices are coming under increasing scrutiny.

Looking forward, a combination of rigorous enforcement, international cooperation and practical flexibility will be essential. The GDPR has enabled significant advances in data protection harmonisation, but continued adaptation, innovation and a more effective global framework will be needed to address emerging risks, while fostering trust and innovation in the digital space.

About

C4DT Focus

The digital world is evolving at high speed, and not a day goes by without the subject making headlines. With targeted interviews of international experts and a survey of the most relevant articles on the subject, the C4DT Focus offers you valuable insights into a digital topic that was recently in the news.

Center for Digital Trust

Housed at the Swiss Federal Institute of Technology Lausanne (EPFL, epfl.ch), the Center for Digital Trust (C4DT, c4dt.epfl.ch) brings together academia, industry, not-for profit organizations, civil society, and policy actors to collaborate, share insight, and gain early access to trust-building emerging from state-of-the-art research being undertaken at EPFL. C4DT also supports the public sector by facilitating technology transfer in domains such as privacy protection and security, democracy and humanitarian assistance and critical infrastructures.

EPFL C4DT
Building BC
Station 14
1015 Lausanne
Switzerland