

Swiss Privacy Law Reforms Present Divergences From GDPR

By **Kim Roberts** and **Vanessa Alarcon Duvanel** (September 14, 2023, 12:14 PM BST)

Most organizations are now very familiar with the General Data Protection Regulation, the European Union regulation that governs how an individual's personal data is managed and controlled.

However, for those entities in Switzerland, there is a new system with which to get to grips. From Sept. 1, further privacy law compliance obligations for businesses need to be met, and all eyes will now be on the country as it ushers in its own data privacy reforms to see how they compare and contrast to the GDPR.

In this article we plan to explain where the new Swiss law diverges from the existing privacy law regime and what those divergences mean in practice.

To briefly recap, the GDPR was a set of provisions effective from 2018 that harmonized the data privacy laws across Europe. It standardized issues around requirements for securing personal data, reporting data breaches, identifying lawful bases for processing personal data and managing obligations when sharing personal data outside of an organization.

The new Swiss law obligations require Swiss-based organizations to follow the reformed Federal Act on Data Protection. The act is not new; in fact, it is more than 30 years old, having first been introduced back in the analogue era of 1992.

However, as the Swiss Federal Council stated in a press release last month, a complete overhaul of the data protection law was needed "to ensure that the population has adequate data protection adapted to the technological and social developments of our time."^[1]

The council points out that the new Federal Act on Data Protection, or DPA, has a challenge when it comes to compatibility with the GDPR. While Swiss companies were under no requirement to comply with the GDPR, since Switzerland is not bound by its rules, many global organizations have in fact taken an international approach to compliance based on the GDPR's gold standard.

The council therefore claims that companies that have already complied with the GDPR will have minimal changes to make.

The DPA is applicable to processing — essentially any use of personal data of Swiss individuals by any



Kim Roberts



Vanessa Alarcon Duvanel

organization around the world, which due to the country's historic and ongoing international links will affect a large number of entities.

Likewise, there are many international companies and bodies registered or with operations in Switzerland, such as the numerous companies structured as a Swiss-registered *verein* — a legal structure recognized by the Swiss Civil Code — that will need to look closely at the obligations that may apply to them, which do have some notable differences.

Be Afraid, Be Fairly Afraid

A reminder that some companies will not need to hear is that one of the biggest concerns for companies under the GDPR has been the extent of the liability on corporates for security incidents that qualify as data breaches under the GDPR.

The regulator's ability to fine an organization hefty sums of up to €10 million (\$10.7 million) or 2% global turnover, or €20 million (\$21.5 million) or 4% global turnover, depending on the severity of the breach — for a security incident that amounts to a personal data breach and causes harm to individuals — is probably the most notorious risk factor the GDPR poses.

It is fair to say that data regulators were somewhat slow to wield the stick when it came to large fines. Early breaches were mainly focused on smaller infringements. The first U.K. GDPR penalty from the Information Commissioner's Office was a £275,000 (\$344,000) fine handed to a London pharmacy in 2019, Doorstep Dispensaree, for failing to comply with data protection rules, rather than a high-profile breach that compromised millions of people's personal data.[2] Moreover, this fine was later reduced on appeal to £92,000 (\$115,000) in 2021.

In the Doorstep Dispensaree matter, the fine was a result of a correspondence to the ICO from the Medicines and Healthcare products Regulatory Agency after a search had found a cache of personal data, including names, addresses, dates of birth and National Health Service numbers stored in a rear courtyard.

Even so, since then, regulators have been flexing their muscles in recent years and will continue to do so, with the major trend being to focus on international Big Tech companies.

The EU's largest fine was levied at Meta with a €1.2 billion (\$1.29 billion) penalty on May 22,[3] off the back of the Irish Data Protection Authority investigation that commenced in August 2020 and reported back on May 12 this year.[4] This followed Meta's transfers of personal data to the U.S. on the basis of standard contractual clauses.

The 2020 European Court of Justice case that prompted the sanction, *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems*, found that Meta Ireland infringed Article 46(1) of the GDPR.[5]

Organizations know that regulators are becoming increasingly aggressive and focused on scenarios where harm is caused to individuals as a result of an organization's failure to protect personal data.

It is becoming increasingly clear for businesses that regulatory investigations cost a great deal of time and money, creating additional financial and logistical headaches.

The risk of reputational harm to organizations that are publicly slated as not able to protect consumer personal data, or not capable of continuing business as usual in the immediate aftermath of a personal data breach, has also been a significant sea change, and has required a high-level corporate response to manage those risks.

Entities in Switzerland, however, will not have the specter of such painful regulatory scrutiny. The DPA does not have the same degree of corporate responsibility. Welcome relief, albeit at an institutional level.

But management should not get complacent. The new reforms make it clear that culpability is a criminal offense, and it will be the management, not the companies, that the regulator goes after, with fines of up to 250,000 Swiss franc (\$280,000) for intentional breaches of the DPA.

This move could be an effective strategy in sharpening management's data compliance protocols. If management undertakes a tick box approach to data compliance — say simply running an annual training session to refresh individuals about their obligations when managing personal data — and a serious breach were still to happen, there appears to be no corporate process to hide behind.

Compact Risk

Despite the increased pressure on individuals, one apparent respite in the DPA is that the reporting obligations seem, on the face of it, more relaxed than the GDPR. Under the EU regime, there is an obligation to report any data breaches that pose any risk within a 72-hour timeframe.

The EU's blanket approach, and relatively tight timescale, mean organizations must implement internal processes for both the thorough monitoring of cybersecurity and mechanisms in order to report within days.

The DPA obliges entities to report high-risk data breaches as soon as possible to the Swiss Federal Data Protection and Information commissioner. On the one hand, this can be viewed as providing some flexibility in terms of what needs to be reported and on what time frame. Alternatively, it can be seen as a potential stumbling block for data privacy compliance.

After all, without clearer parameters than exactly what constitutes the difference between a high-risk and non-high-risk breach becomes subjective.

While some information may be available from guidance issued in the EU following the introduction of the GDPR, the Swiss regulator itself has not yet clarified the meanings of these terms or issued analogous guidance to help organizations understand how this new obligation affects them.

Likewise, the requirement to report a personal data breach as soon as possible can also be viewed subjectively and has been a topic of considerable debate for organizations when assessing reporting requirements under the GDPR.

Does it mean soon as a breach occurs? Or as soon as a breach has been investigated and assessed for its risk level and the extent of the impact on the individuals concerned?

As anyone who has been involved in managing the fallout from a personal data breach knows, these types of investigations are both extremely technical and time-consuming. The requirement to report as

soon as possible is highly likely to be interpreted very differently, depending on the nature and extent of the personal data breach concerned.

The authorities say that these issues are likely to be clarified in subsequent guidance, but it creates an interesting point of divergence to the obligations on an organization to only report a personal data breach if the risk of harm test under the GDPR is met. It will be important to tighten these definitions to avoid confusion and potential exposure to criminal fines.

The expectation is that the applicable fines will most likely be levied against C-level executives and those responsible for an organization's data protection program, i.e., data protection officers. The stated focus for imposing fines under the new regime is willful failings to comply with the new obligations.

The remit for fining includes failing to provide correct information to consumers about how their personal data is processed or failing to cooperate with an investigation undertaken by a regulator. The DPA also provides that if an individual's failure to comply with the requirements of the law cannot be determined, the organization may face a fine, not exceeding 500,000 Swiss franc (\$560,000).

The threat of personal accountability and criminal liability is certainly sending shivers down the spine of those in the boardroom. However, like the enforcement action under the GDPR, we wait to see the extent of how the new regime will be applied in practice.

A Swiss Representative

The DPA also introduces a change to the extraterritorial scope of the original Federal Act on Data Protection, a somewhat unusual move in Swiss legislation.

Inspired by the GDPR, the DPA now requires that any organization that processes personal data of individuals in Switzerland must have a corporate seat in Switzerland — read a registered office — or appoint a representative in the country.

In other words, any entity offering goods or services to Swiss individuals or monitoring their behavior, and any entity that regularly carries out large-scale data processing and poses a high risk to data subjects, must now have someone representing them with respect to privacy matters in Switzerland.

Unlike the GDPR however, a mere establishment in Switzerland is not sufficient to escape the obligation to nominate a Swiss representative to serve as the local and accessible point of contact.

Conclusion

The reformed DPA is a necessary new law to adjust to recent technological and social developments. It brings a few challenges that will require an adjustment by companies in and outside of Switzerland.

While many of the requirements of the new law, such as the appointment of the representative and the extraterritorial effect are very similar to the GDPR, the new Swiss law also has key differences, principally around data breach reporting obligations and the liability of officers of the company.

These differences will need to be carefully managed in practice, especially by multinationals that may have competing obligations under different laws that apply to them. Perhaps the most far-reaching impact of the new law is the liability for officers.

It remains to be seen how this will play out in practice and how it might affect the way in which personal and legal responsibility for compliance with privacy law obligations shapes the culture of businesses that are within the scope of the new law.

Kim Roberts and Vanessa Alarcon Duvanel are counsel at King & Spalding LLP.


The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] <https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/digitization/data-protection/new-federal-act-on-data-protection-nfadp.html>.

[2] <https://ico.org.uk/media/action-weve-taken/enforcement-notice/2616741/doorstop-en-20191217.pdf>.

[3] https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en.

[4] <https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland>.

[5] Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems : Case C-311/18 Judgment of the Court (Grand Chamber) on 16 July 2020.