A New Data Protection Law in Switzerland. Still the Weakest Privacy Law in Western Europe?

Michael Baltaian[1]

Abstract

On 1st September 2023, a new data protection law came into force in Switzerland. This article examines the practical implications of this new law for companies doing business in Switzerland. In particular, the article looks not only at the key components of the new law and how they compare with the equivalent law applying to the rest of western Europe (the EU's GDPR), but also what they mean in practice for companies, considering both international companies already subject to the GDPR and local Swiss businesses only operating in Switzerland. In addition, the article considers the broader implications of the new law for Switzerland in terms of its international competitivity and its protection of the privacy of people in Switzerland.

This article is **not** legal guidance.

Keywords: data privacy, personal data protection, FADP, GDPR

What has changed?

On 1st September 2023, the new Federal Act on Data Protection (FADP),[2] together with the associated Ordinance on Data Protection (DPO),[3] came into force. The ordinance supports the FADP by providing additional details on certain aspects of the law.

These replaced the previous Federal Act on Data Protection (FADP)[4] and Ordinance (DPO).[5]

Why the change?

The two primary drivers for replacing the previous act were:

- Bringing the law up to date

The previous law dated from 1992, the year when the World Wide Web was just being expanded beyond CERN but still largely limited to the scientific community.[6] As such, the law significantly pre-dated many of the most important personal data processing activities found in today's digital economy (e-commerce, smartphones, social media, cloud computing, Internet of Things, etc.).

[1] *Michael Baltaian is a Data Privacy Consultant and Adjunct Professor at the International Institute in Geneva.*
[2] New Federal Act on Data Protection (FADP) (unofficial English translation published by the Swiss Confederation): https://www.fedlex.admin.ch/eli/cc/2022/491/en
[3] New Ordinance on Data Protection (DPO) (unofficial English translation published by the Swiss Confederation): https://www.fedlex.admin.ch/eli/cc/2022/568/en
[4] Old Federal Act on Data Protection (FADP) (unofficial English translation published by the Swiss Confederation): https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en
[5] Old Ordinance to the Federal Act on Data Protection (DPO) (unofficial English translation published by the Swiss Confederation): https://www.fedlex.admin.ch/eli/cc/1993/1962_1962_1962/en
[6] CERN, "The birth of the World Wide Web": https://timeline.web.cern.ch/www-moves-prototype-production

Despite partial updates to the law in 2009 and 2019,[7] the Swiss Federation recognized that a comprehensive overhaul of the law was required.

- Retaining EU adequacy status

The EU maintains a list of countries it considers adequate in terms of data protection legislation and the rule of law. Countries on the list are considered by the EU to offer a level of personal data protection comparable to the protection enjoyed in the EU and, as a result, personal data can be transferred from the EU to such countries without the need for additional safeguards. EU adequacy status can be a major economic benefit for countries which do a significant amount of business with EU countries.

Switzerland was granted EU adequacy status in 2000 based on the old FADP from 1992.[8] However, this decision was taken when the EU's own data protection laws were based on the Data Protection Directive (DPD) from 1995.[9]

Since then, the EU has replaced the DPD with the General Data Protection Regulation (GDPR)[10] which raised the bar for personal data protection within the EU and, by implication, the expectations for other countries to be considered adequate. The EU indicated that it intended to revisit existing adequacy decisions and, without a significant overhaul of Switzerland's data protection law, there was a real risk that Switzerland could lose its EU adequacy status with the resulting impact on the Swiss economy.

The Swiss Confederation believe that the new FADP enhances data protection in Switzerland sufficiently that its EU adequacy status is no longer at risk.

The legislative environment

Most countries in the world recognize that people should be protected from the misuse of personal data about them and have enacted corresponding data privacy legislation.[11] A 2022 study identified 157 countries which now have some form of data privacy legislation.[12] Legislation typical takes the form of a comprehensive (or omnibus) data privacy law – a law that applies to any form of personal data – rather than sectorial laws – laws that apply to specific types of personal data or industry sectors (e.g. health, finance).

The global legislative landscape can be broadly divided into three categories:

- The GDPR

[7] Swiss Federal Council statement on the "New Federal Act on Data Protection (nFADP)": https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/digitization/data-protection/new-federal-act-on-data-protection-nfadp.html
[8] Swiss Federation information on "Adequacy of Switzerland by the EU": https://www.sem.admin.ch/bj/en/home/staat/datenschutz/internationales/angemessenheit-ch.html
[9] Old EU data protection law, the Data Protection Directive (DPD): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046
[10] Current EU data protection law, the General Data Protection Regulation (GDPR): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[11] Definitions for personal data vary but it is most commonly taken to mean any data relating to an individual who is or could be identified
[12] Graham Greenleaf (2022) "Now 157 Countries: Twelve Data Privacy Laws in 2021/22", University of New South Wales, Faculty of Law: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4137418

The General Data Protection Regulation (GDPR) is the EU's comprehensive data privacy law. It came into force in May 2018 and applies to all EEA countries (i.e. all 27 EU countries and the three EFTA countries Norway, Iceland and Liechtenstein). Even though the UK left the EU, the GDPR effectively continues to apply to the UK through the UK GDPR, a domestic UK law with minimal changes compared to the EU GDPR.[13]

In addition to applying directly to multiple countries, the GDPR is widely considered a mature and well thought through piece of legislation and, as a result, is often seen as the global "gold standard" for privacy laws. None-the-less, the GDPR has been criticised for introducing unnecessary bureaucracy for businesses to achieve compliance.[14]

- "GDPR Light" laws

As national data privacy laws are typically based on a common set of principles,[15] they often resemble each other. In addition, since the GDPR was introduced, other countries increasingly look to the GDPR when introducing or updating their own data privacy laws and, as a result, data privacy laws outside of the EEA increasingly resemble "GDPR Light" laws – laws that contain many of the same concepts and requirements as the GDPR but with some of the more onerous components watered down.

- The US

The United States remains an outlier in terms of data privacy law. It is the only G7 country without a comprehensive national data privacy law.[16] Instead, it has a patchwork of sectorial federal laws (e.g. HIPAA for entities processing health data) and comprehensive state laws (e.g. CCPA and CPRA for California).

The Swiss approach

Switzerland's new Federal Act on Data Protection (FADP) is a clear example of the "GDPR Light" approach. It borrows heavily from the GDPR but contains significant differences, seeking that "sweet spot" between being sufficiently close to the GDPR to protect people's personal data (and maintain Switzerland's EU adequacy status) and sufficiently different to limit the burden of compliance on businesses.

[13] The UK plans to replace the UK GDPR with a new data privacy law, the Data Protection and Digital Information (No. 2) Bill, which is currently progressing through the UK parliament: https://bills.parliament.uk/bills/3430

[14] For example, the UK government has criticized the GDPR for "pointless paperwork for businesses" and "annoying cookie pop-ups": https://www.gov.uk/government/news/british-businesses-to-save-billions-under-new-uk-version-of-gdpr . See also Chinchih Chen, Carl Benedikt Frey, and Giorgio Presidente (2022) "Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally" Oxford Martin School, University of Oxford: https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf

[15] Fair information Practice Principles: https://iapp.org/resources/article/fair-information-practices/

[16] The American Data Privacy and Protection Act (ADPPA), a proposed comprehensive data privacy law for the US, failed to progress through the US Congress in 2022

To whom does the FADP apply?

Like the GDPR, the FADP has an extraterritorial component, stating that it applies to activities which "have an effect in Switzerland, even if they were initiated abroad" (FADP Art. 3). In practice and applying similar rationale as for the GDPR, the FADP can be considered to apply to:

- Companies that are based in Switzerland; and
- Companies that are not based in Switzerland but offer goods or services to people in Switzerland
    - Simply having a website accessible from Switzerland would generally not be sufficient to trigger applicability of the FADP
    - However, the FADP would apply to companies which target people in Switzerland by for example allowing payment in CHF or shipping goods to Switzerland

Definitions

To a very large extent the FADP follows the same definitions (FADP Art. 5) as the GDPR. Personal data is any data relating to "an identified or identifiable" individual and sensitive personal data (data which could cause particular harm to individuals if misused) also basically aligns to the GDPR definition, with the addition of "data relating to social assistance measures."

The notable addition under the FADP is the definition of high-risk profiling (profiling that allows an assessment of "essential aspects of the personality") and uses this definition as the trigger for a number of additional obligations.

The key obligations of the FADP

The key obligations for companies arising from the FADP are outlined in this section.

Principles

The FADP requires companies to apply certain privacy principles when processing personal data. They generally correspond to the principles defined in the GDPR:

GDPR principle	**Corresponding principle under the FADP**
Lawful, fair and transparent	Lawful, good faith and transparent (FADP Art. 6 and Art. 19)
Purpose limitation	Purpose limitation (FADP Art.6)
Data minimisation	Proportionate (FADP Art. 6)
Accuracy	Accuracy (FADP Art. 6)
Storage limitation	Storage limitation (FADP Art. 6)
Security	Security (FADP Art. 8)
Accountability	No explicit accountability requirement

Companies should therefore follow the good privacy principles and, even though there is no explicit accountability requirement, companies should still maintain records to be able to demonstrate their compliance.

Like the GDPR, the FADP also contains a requirement to implement privacy by design and by default (FADP Art. 7). In practice this means companies need to have a process in place to ensure privacy principles and requirements are taken into account from the moment planning for a new activity starts.

Data protection officer (DPO) and registration

Unlike the GDPR, which requires companies to nominate a DPO in most cases, there is no requirement under the FADP for companies to have a DPO (FADP Art. 10). Companies should still consider whether nominating a DPO is beneficial (e.g. to manage communications with the data protection authorities and individual data subjects) and, in any case, need to ensure that accountability for compliance with data privacy requirements is clearly assigned within their organisation. If a company does appoint a DPO, that person should have sufficient knowledge and autonomy to fulfil the role.

There is no obligation to register processing activities with the authorities and, unlike the GDPR, companies outside of Switzerland do not need to designate a representative in Switzerland unless they carry out regular, large-scale, high-risk activities (FADP Art. 14).

Record of processing activities (RoPA)

The FADP introduces a requirement for companies to maintain an inventory of all their activities (RoPA) that involve the processing of personal data (unless the company has less than 250 employees and performs only low risk processing activities) (FADP Art. 12).

The information to be held in the RoPA closely resembles the corresponding requirements under the GDPR. Therefore, companies which already maintain RoPAs to satisfy GDPR requirements should be able to re-use the same format to satisfy the FADP.

Even small companies which fall below the RoPA requirement threshold are still recommended to maintain a RoPA to help them satisfy other privacy requirements (e.g. responding to data subject requests).

Legal basis and consent

Unlike the GDPR which requires an explicit justification or “legal basis” to process personal data, the processing of personal data is generally allowed under the FADP as long as the privacy principles and good security practices are respected, the individual has not explicitly objected and sensitive personal data is not shared with third parties (FADP Art. 30).

None-the-less, companies must obtain consent for processing sensitive personal data or performing high-risk profiling (FADP Art. 6). The requirements for valid consent generally align to those of the GDPR:

GDPR requirements	**Corresponding FADP requirements** (FADP Art. 6)
Freely given	Voluntarily
Specific and granular	Specific
Informed	Appropriately informed
Unambiguous	Explicit
Equally easy to withdraw	(This point is not explicitly mentioned)

The FADP relieves companies of the need to explicitly identify a legal basis for processing. However, companies should still ensure they follow the privacy principles, including for lawful, good faith and proportionate processing. Companies should be cautious about asking for consent when not necessary but, in case they decide to ask for consent, they should ensure they follow the GDPR requirements for valid consent.

Data protection impact assessment (DPIA)

The FADP introduces a requirement to perform a data protection impact assessment (DPIA) in cases of planned high-risk processing (FADP Art. 22). The triggers for a DPIA, the required contents and the requirement to consult with the data protection authority in case the high risk cannot be sufficiently mitigated all mirror the requirements in the GDPR.

In practice, a DPIA provides companies with a convenient mechanism to demonstrate that they have shown due caution, recognised risks and identified appropriate mitigating measures to sufficiently reduce these risks. Triggering a DPIA in the planning phase is also a way for a company to demonstrate that it is applying privacy by design.

Hence, it is advisable for companies to perform a DPIA if they are planning a processing activity that could result in a higher risk to individuals, including activities which involve large-scale processing of sensitive personal data or of vulnerable individuals, high risk profiling, systematic large-scale monitoring, automated decision making or novel technologies.

DPIAs must be retained for at least 2 years (DPO Art. 14).

Transparency

The FADP mirrors the GDPR in requiring organisations to inform individuals that their data is being processed at the time the data is gathered (if gathered directly from the individual) or within 30 days (if the data is obtained via a third party) (FADP Art. 19, 20 and 21).

In general, the FADP is less prescriptive than the GDPR in terms of what information needs to be provided and allows for more exceptions when information may not be provided. However, in the case of data transfers abroad, the FADP does go beyond the GDPR in requiring the company to list all countries to which that data may be transferred.

In practice, companies that are already subject to the GDPR may re-use their GDPR privacy notices to meet the requirements of the FADP, though they may need to enhance them with an explicit list of countries in case of international data transfers. Such information should be found in the company's record of processing activities (RoPA).

Security

Like the GDPR, the FADP contains a requirement for companies to implement appropriate technical and organisational measures for security (FADP Art. 8). However, unlike the GDPR, Swiss law spells out some specific and somewhat eclectic mandatory security measures in the ordinance (DPO Art. 3, 4 and 5).

These include application of least privilege access, logical access control, physical access control, protection of data at rest (including on portable media) and in motion, business and IT continuity plans and a requirement to keep systems up to date and patched. There are also requirements to log changes to and sharing of personal data (including who changed what and when) and to keep these logs securely for at least one year.

Procedures to identify and handle data breaches and, in case of higher risk processing, a broader policy on data security are required.

Whilst most companies will have such measures already in place as part of their general data security practices, it is worth reviewing the detailed requirements outlined in the ordinance to be sure to have procedures in place which address all of them and that these procedures are working in practice.

Data breaches

The GDPR requires notification to the relevant data protection authority of any personal data breach within 72 hours unless harm to individuals is unlikely and notification to individuals without undue delay if the risk to individuals is high.

By contrast, the FADP requires notification to the data protection authority as soon as possible only if the risk to individuals is high. Notification to individuals is necessary only if required for their protection or if instructed to do some by the authority (FADP Art. 24).

The definition of a data breach (a security incident leading to loss of confidentiality, integrity, or availability of personal data) as well as the reporting format closely match those in the GDPR.

In practice, companies need to have processes in place to detect and handle security incidents, including potential data breaches. These processes should include mechanisms to determine if notification is necessary, rapidly notify the authorities if needed and document the handling of each incident irrespective of whether notification was needed or not.

Third parties

Like the GDPR, the FADP requires companies to have a contract in place with third parties which process data on their behalf (processors) and to perform due diligence to ensure the processor's security practices are adequate (FADP Art. 9). Processors need approval to further delegate

processing to sub-processors but that can be given generically, rather than for individual sub-processors (DPO Art. 7).

However, in contrast to the GDPR, the FADP does not stipulate in detail the elements that a third-party contract must contain.

It is therefore a must for companies to have signed data processing agreements in place with all of its processors. Whilst, in theory, this agreement could be significantly simpler than those required under the GDPR, it must still contain sufficient obligations to adequately protect the company and, as a result, may well still include many of the aspects mandatory under the GDPR. Companies that are already working with data processing agreement templates which meet the GDPR requirements will most likely continue to use these.

The degree of due diligence required will vary depending on the risks associated with the processing. For lower risk processing, the contractual obligations to provide good data security contained in the data processing agreement may be sufficient.

International data transfers

The FADP adopts a similar approach to the international transfer of personal data as the GDPR does, with a list of "adequate" countries to which personal data can be transferred without additional safeguards and standard contractual clauses (SCCs) to be imposed in case of transfers to other countries (FADP Art. 16).

Switzerland's list of adequate countries (DPO Annex 1) closely follows that of the EU, though often with a slight lag (for example, Japan and South Korea are now recognised as adequate by the EU but not yet by Switzerland).

For transfers to countries which are not on Switzerland's adequacy list, the most common mechanism is to implement SCCs between the Swiss-based data exporter and the data importer abroad. The EU SCCs[17] are lengthy and complex contractual documents, leading to concerns about "paper-based compliance" where companies focus their efforts on getting the necessary contractual clauses in place at the expense of ensuring that personal data is actually adequately protected in practice. To their credit, the Swiss authorities have recognised the EU SCCs as being valid for exports out of Switzerland,[18] thereby at least sparing international companies the burden of negotiating two sets of SCCs when exporting data outside of adequate countries.

From a practical perspective, companies must be aware of all cases where they export personal data (including providing access to personal data to organisations outside of Switzerland) and ensure that such exports are either to countries on Switzerland's adequacy list or that they have signed SCCs in place with the data importers. Such SCCs should be the latest EU SCCs published by the EU on June 4, 2021, with suitably amended annexes (e.g. to describe the nature of the processing) and a "Swiss rider" to explain that references to the EU are to be read as including Switzerland. The identified data exports should of course match the corresponding data described in the Record of Processing Activities (RoPA) and privacy notices.

[17] EU Standard Contractual Clauses: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[18] Swiss data protection authority paper on standard contractual clauses: https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/datenschutz/Paper%20SCC%20def.en%2024082021%20(2).pdf.download.pdf/Paper%20SCC%20def.en%2024082021%20(2).pdf

The above actions can represent a significant amount of work, though thankfully no greater than that required of comparable companies based in the EU.

Data subject rights

Like to GDPR, the FADP spells out a number of rights for individuals which companies must be capable to satisfying. These largely correspond to the main data subject rights under the GDPR.

Data subject right under the GDPR	Corresponding right under the FADP
Right to be informed (transparency)	Right to be informed (FADP Art. 19)
Right to access (copy of data)	Right to access (FADP Art. 25)
Right to rectification (correction of data)	Right to rectification (FADP Art. 32)
Right to erasure (right to be forgotten)	Right to erasure (FADP Art. 32)
Right to object	Right to object (FADP Art. 32)
Right to portability	Right to portability (FADP Art. 28)
Right not to be subject to automated decision-making	No explicit right beyond right to object

The FADP defines a 30 day time deadline for access and portability requests (DPO Art. 18 and 22), in line with the GDPR's one month limit. However, the FADP allows for a slightly broader set of exceptions when a company may refuse a request. For example, under the GDPR, a company may refuse to provide a copy of data if the request is "manifestly unfounded or excessive"; under the FADP, it may refuse if it is "manifestly unfounded, namely if it pursues a purpose contrary to data protection or is manifestly of a frivolous nature" (FADP Art. 26).

The mishandling of data subject requests can undermine an individual's trust in an organisation and is a frequent trigger for complaints to data protection authorities. Hence, companies need to have reliable processes in place to identify and respond appropriately to data subject requests within the required time period. Typical causes for mishandling include a failure to recognise a data subject request has been made, failure to track a request through to completion and failure to provide a complete and good faith response. Companies that are already subject to the GDPR should be able to simply re-use their GDPR processes to satisfy the FADP.

Cookies

The GDPR is often incorrectly blamed for the "annoying cookie pop-ups", even though the requirements arise from a separate piece of EU legislation, the "e-privacy Directive,"[19] which requires users give their consent before non-essential cookies or other tracking technologies can be downloaded onto their devices. The impact of the GDPR was merely to specify what constitutes valid consent.

[19] The EU "e-privacy Directive": eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058

Similarly, under Swiss law, the FADP does not make any explicit reference to cookies or other tracking technologies. The cookie requirements arise from the Telecommunications Act (TCA)[20] which requires that "users are informed about the processing and its purpose and are informed that they may refuse to allow processing" (TCA Art. 45).
In practice, companies are taking the introduction of the new FADP as an opportunity to update their approach to cookies and bring their websites into line with the behaviour typical of other European websites, including a cookie preference pop-up on first arrival at the website informing users of the purposes for which cookies are used and offering the possibility to accept or reject non-essential cookies. This is typically complemented by additional information readily available through the privacy notice or a separate cookie notice and the ability to easily change cookie preferences at any time whilst using the site.

Sanctions and enforcement

This is an area where the FADP takes a significantly different approach from the GDPR.

	GDPR	**FADP** (FADP Art. 60-66)
Maximum penalty	EUR 20 mio or 4% of global annual turnover	CHF 250,000
Imposed against	A company	An individual
Imposed by	Data protection authority	Swiss cantonal authorities
Imposed for	Infringements of the GDPR	Wilful violations of the FADP
Other remedies	"Class action"-like lawsuits by not-for-profit organisations	

Fines under the GDPR are intended to be "effective, proportionate and dissuasive"[21] and EU national data protection authorities (coordinated, when necessary, through the European Data Protection Board or EDPB) have so far issued over 1,800 fines totalling over EUR 4 bio since the GDPR came into force in May 2018.[22] Put simply, the GDPR provides a big stick and EU authorities have not been reluctant to use it.

By contrast, the maximum fine under the FADP of CHF 250,000 appears quite modest and hardly dissuasive for larger organisations. The manner in which such a fine could be imposed has attracted some attention:[23]

- Fines imposed against individuals, rather than companies: it is anticipated that, in keeping with other data protection laws that impose fines on individuals, such fines would target key decision makers within an organisation rather than, for example, a data protection officer acting in an advisory role.

[20] Swiss telecommunications act (TCA)) (unofficial English translation published by the Swiss Confederation): https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/1997/2187_2187_2187/20180301/en/pdf-a/fedlex-data-admin-ch-eli-cc-1997-2187_2187_2187-20180301-en-pdf-a.pdf
[21] GDPR Art. 83(1)
[22] GDPR enforcement tracker: https://www.enforcementtracker.com/?insights
[23] See also for additional perspectives on FADP fines "How to avoid criminal liability under the revised Swiss DPA - 18 June 2023 – VISCHER": https://www.vischer.com/en/knowledge/blog/know-how/blog/how-to-avoid-criminal-liability-under-the-revised-swiss-dpa-1-1-1/

- Fines imposed by cantons, rather than by the national data protection authority: the Swiss data protection authority has no power to impose fines, though it can refer cases to the cantonal authorities. In general, this may further dampen the willingness to impose fines, though inconsistency in approaches across cantons cannot be excluded.
- Fines limited to wilful violations: whilst "there are no criminal penalties for negligent breaches of data protection obligations,"[24] wilful violations include transferring data to a processor without a contract, transferring data abroad without the necessary safeguards and failing to apply minimum security requirements.

How fines will be applied in practice will emerge over time, but all indications are that this new but limited power under the FADP will be used sparingly. Whilst the Swiss data protection regime is not entirely toothless (the Swiss data protection authority has the right to perform investigations and "may order that data processing activities be modified, suspended or discontinued, or that personal data be deleted"),[25] the sanctions and appetite for enforcement are likely to lag far behind those of the EU.

Impact of the new law

- **EU adequacy status maintained?**

A key objective of the new FADP was to ensure Switzerland maintained its status as an "adequate" country for personal data exports in the eyes of the EU.

Considering that the FADP includes all the key components found in the GDPR (even if the requirements are often watered down compared to the GDPR) and that, once granted, the EU has never withdrawn adequacy status from any country, there is nothing to indicate that Switzerland's adequacy status is any longer at risk.[26]

This will allow the continued free transfer of personal data between the EU and Switzerland, a major benefit for Swiss-based companies and the Swiss economy as a whole.

- **Compliance burden minimised?**

Whilst bringing Swiss data privacy law closer to the GDPR, Switzerland was also keen to keep the law business-friendly, limit the compliance burden and avoid the unnecessary bureaucracy that the GDPR is sometimes accused of.

This has led to the removal or softening of many requirements, including:

- No need to appoint a DPO
- No need for a legal basis to process personal data
- Greater freedom in drafting privacy notices and data processing agreements
- Higher threshold for reporting data breaches
- Broader exceptions for refusing data subject requests

[24] Swiss data protection authority statement on criminal law: https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/grundlagen/strafbestimmungen.html
[25] The role of the Swiss data protection authority: https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/grundlagen/rolle-edoeb.html
[26] Note that since this article was first drafted, the EU has confirmed that it continues to recognize Switzerland's adequacy status: Report on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC | European Commission (europa.eu)

For companies which operate internationally and already need to comply with the GDPR, the overhead of developing and implementing new Swiss-specific processes, procedures and templates is likely to exceed the benefits offered by Switzerland's lighter requirements. Hence, it is to be expected that international companies will chose to consistently apply their GDPR processes to EEA countries and Switzerland.

There are some very limited areas where the FADP requirements exceed those of the GDPR, e.g. in the more detailed specification of security requirements. These are however sufficiently minor that the risk of a company diligently following GDPR processes being sanctioned for missing a Swiss-specific requirement is low.

Therefore, for companies which operate internationally and already need to comply with the GDPR, the burden of compliance is likely to be the same as for an EEA country.

For local Swiss businesses only operating in Switzerland, the new FADP introduces many new obligations compared to the previous law. The lighter requirements of the FADP may provide some relief from this increased burden of compliance but this is likely to be limited in practice. For example, even though a company does not need to appoint a DPO, it must still ensure accountability for compliance with data privacy requirements is clearly assigned within their organisation. Similarly, even if requirements for reporting data breaches or responding to data subject requests are lighter, companies must still have processes in place identify and manage such events.

Therefore, for local Swiss businesses only operating in Switzerland, the burden of compliance is likely to be significantly higher than under the old FADP, though marginally lower than that for a comparable company operating in an EEA country.

- **Individuals' data better protected?**

The trade-off for a more demanding data privacy law should come, not only with the retention of EU adequacy status, but also with better protection of "the personality and fundamental rights" of individuals (FADP Art. 1).

Whilst the new FADP does impose additional requirements on companies, individuals are unlikely to see much of a change other than slightly more extensive privacy notices. The FADP does not require companies to identify a legal basis for processing an individual's data and we have not seen the flurry of consent requests that accompanied the introduction of the GDPR (when many companies realised they were holding data on individuals without any legal basis for doing so).

One challenge to better protection of individuals' data is simply lack of awareness. The GDPR received extensive media coverage when it came into force, the Internet is full of explainers regarding people's rights under the GDPR and a steady stream of significant fines has helped to keep the GDPR in the public spotlight. By contrast, the new FADP was introduced with typical Swiss discretion and information directed at the general public regarding their rights under Switzerland's lighter regime is very limited.[27] The nuanced deviations of the FADP from the GDPR have served to further "muddy the waters". As a result, individuals' understanding of what they can and should expect in terms of protection of their personal data generally remains limited.

[27] See for example the website of the Swiss data protection authority: https://www.edoeb.admin.ch/edoeb/en/home.html

The biggest difference between the FADP and the GDPR in terms of protection of individuals' data is however the enforcement regime. The Swiss data protection authority has limited resources[28] and is unable to directly impose even the limited fines foreseen under the FADP. This may undermine the protection of personal data through a) companies that cynically breach the law, believing that resulting profits will outweigh any eventual fine or other sanction, b) companies that decide to ignore or remain wilfully ignorant of the law, assuming that either this will never come to light or, if identified, will simply result in a request to "fix things" without other consequences and c) a reluctance of individuals to raise complaints to the authority, due to lower expectations that any significant actions will be taken.

Conclusions

The new FADP is a necessary (and maybe overdue) update to Switzerland's data protection landscape, a welcome step closer to the EU's GDPR and sufficient to assure that Switzerland will remain on the EU's "adequate country" list and can continue to enjoy the economic benefits that go with that.

Switzerland's "GDPR Light" approach of watering down certain requirements compared to the GDPR is, in practice, unlikely to significantly reduce the compliance burden on companies. Companies already subject to the GDPR will typically apply their existing GDPR practices to meet the Swiss requirements. However, local Swiss companies not subject to the GDPR now face similar challenges to those faced by comparable EEA companies when the GDPR was introduced.

The "GDPR Light" approach both weakens some requirements for protecting individuals' data and reduces individuals' clarity regarding their rights compared to their counterparts in countries subject to the GDPR. This, combined with a significantly weaker enforcement regime than the GDPR, means that Switzerland, as the only country not subject to the GDPR, still has arguably the weakest data privacy law in western Europe.[29]

Having only come into force on 1st September 2023, the revised FADP is still very new and, as was seen with the introduction of the GDPR, it may take several years for both companies and regulators to get comfortable with the new law and how it is to be applied. Actual enforcement activities (or lack of them) over the next 3-5 years are likely to frame some companies' attitudes to the FADP. This, together with evolving public concerns (or apathy) regarding data privacy, may determine how company privacy practices for Switzerland evolve and provide an interesting avenue for future research.

[28] The Swiss data protection authority has 33 employees according to its annual report of 2022/2023: https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/deredoeb/30.%20T%C3%A4tigkeitsbericht%202022-23_EN.pdf.download.pdf/30.%20T%C3%A4tigkeitsbericht%202022-23_EN.pdf

[29] In this context, western Europe is taken to mean all countries in the EU, EFTA and the UK. It does not consider the European microstates such as Andorra, Monaco, or San Marino