www.pwc.ch

What does the revision of the Swiss Data Protection Act entail, and how does it relate to the GDPR and the ePrivacy Regulation?

The E-FADP and the corresponding regulatory environment

"Freedom and self-determination in the digital world are crucially dependent on keeping sovereignty over our personal information"

Heiko Maas – German Minister for Foreign Affairs, 2015

pwc

Contents

The E-FADP and the corresponding regulatory environment

Summary

In September 2017, the Federal Council presented a draft for a fully revised Data Protection Act (E-FADP), which aims to increase transparency and strengthen the participation rights of data subjects whose data is processed. The draft is largely based on the General Data Protection Regulation (GDPR), which has been in effect since 25 May 2018. Similarly, the ePrivacy Regulation, which has also been adopted by the EU (not yet in force) and is intended to regulate privacy on the Internet and in electronic communications as lex specialis, is also closely linked with the FADP. This publication is intended to show what Swiss companies can expect from the FADP's revision, how far the legislation differs from the GDPR and what challenges could be faced during the implementation

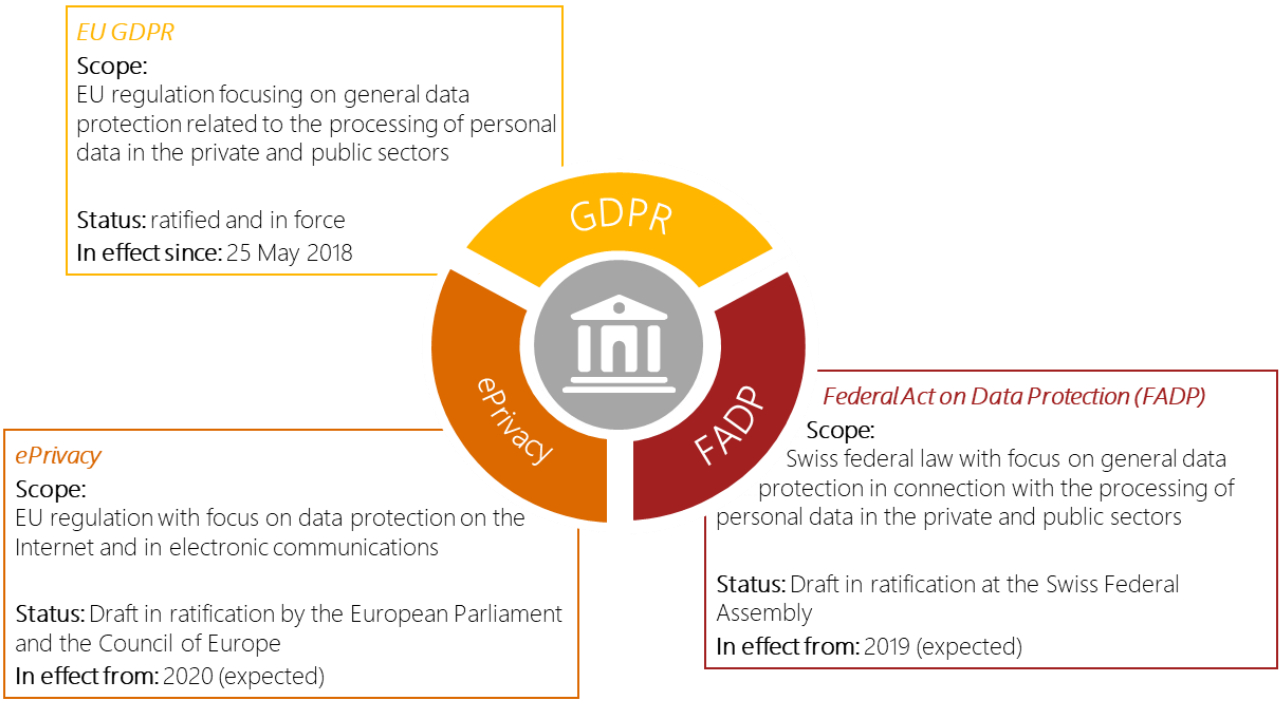
1. Overview of the current situation of data protection in Switzerland

With the proliferation of digital technology over the past three decades, data protection requirements have steadily increased. The implementation of the European regulation (GDPR) in May 2018 and the ePrivacy Regulation (expected in 2020) represent a wave of European measures aimed at protecting the personal freedoms of data subjects. With the rapid development of communication and distribution channels, as well as the advanced capacity of companies to collect and process personal information, the protection of data subjects is at the heart of the new regulations.

The Federal Council decided in 2011 to revise the Data Protection Act (FADP), which came into force in 1992. Due to the publication of the GDPR in 2016, the Swiss National Council decided to carry out the revision of the FADP incorporating the GDPR. This affects all Swiss companies that process personal data (such as customer or employee data). Any handling of personal data constitutes processing, in particular the collection, storage, safe keeping, use, modification, disclosure, archiving, deletion or destruction of data. Due to the broad scope, there will probably be very few companies in Switzerland that are not affected by the revision.

Affected companies' experiences with the GDPR, as well as the draft revision of the FADP, show that the implementation of the new regulations represents a major challenge for companies. Therefore, there is an urgent need for action. A holistic understanding of the coming regulations is central to maximising cost-efficiency and market-conformity. The market experience shows that the technical and temporal dependencies between the revised Data Protection Act (E-FADP), ePrivacy Regulation and GDPR should be taken into account during the implementation.

In the following chapters, we will cover what the new laws on the protection of personal data mean for Swiss companies in concrete terms, what measures must be taken and what needs to be taken into account in the forthcoming development. The focus of this document is primarily on the E-FADP and its dependencies on the GDPR.

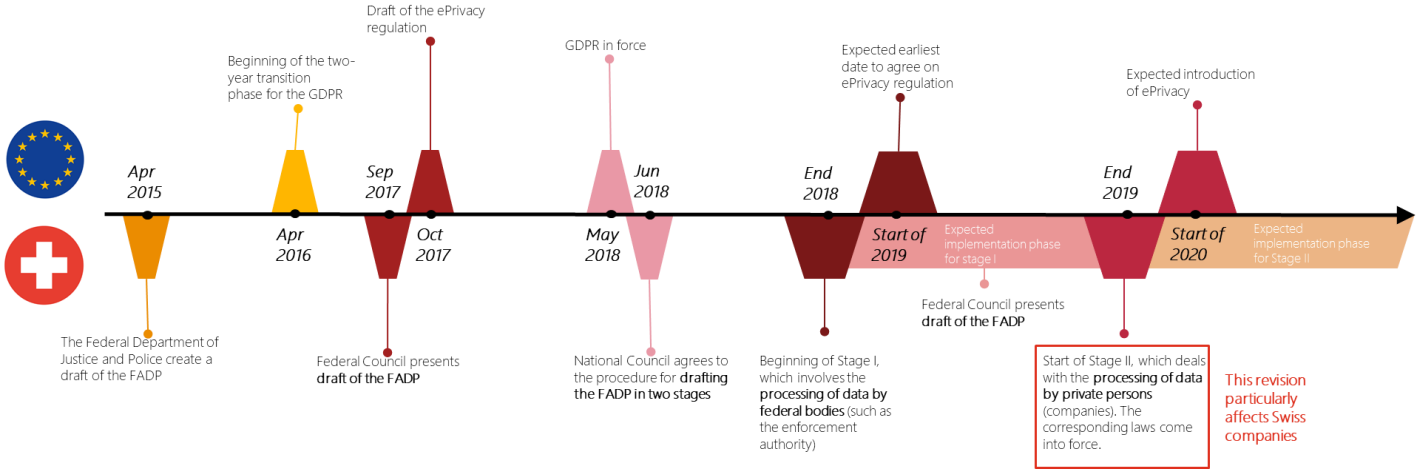


2. The revision of the Swiss FADP

The revised Data Protection Act is intended to replace the existing Swiss Data Protection Act (FADP). It should take into account technological progress and strengthen the protection of personal data of natural persons1. The revision will be based on the content of the GDPR.

2.1 The timeline of the total revision

The original intention was to comply with both the Schengen acquis and the GDPR in a single step by totally revising the FADP. Strictly speaking, Switzerland is only obliged to take over the data protection provisions resulting from the Schengen agreements. However, in order to be recognised as a third country with a level of data protection comparable to the EU, the relevant adaptations to European law should also be made. Otherwise, there is a risk that data between Switzerland and the EU can only be exchanged under complex conditions. However, it was then decided to divide the total revision into two stages. The division should first allow for the necessary prior consultation on the implementation of the EU law (Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data in the criminal field), which is required by the Schengen agreements. Subsequently, the total revision of the Data Protection Act can be addressed "without time pressure". For Swiss companies, the second stage, which is expected to be completed by the end of 2020, is particularly relevant.



2.2 The E-FADP and how it differs from the current FADP

This document is based on the draft of the Data Protection Act (E-FADP) presented in September 2017. The E-FADP reinforces many of the existing rights of data subjects, introduces various new requirements and, in a few cases, restricts existing articles. The new draft differs from the existing legislation (FADP) in the following key points:

Protection object: natural persons
While the FADP of 1992 regulated the protection of data of both natural and legal persons, the E-FADP confines itself to data of natural persons.

Sanctions
Unlike the FADP, the draft of the new legislation defines clear sanctions. Thus, individuals who intentionally violate the E-FADP can be fined up to CHF 250,000.

Particularly sensitive personal data
The E-FADP extends the existing list of data that falls into this category. Thus, genetic and biometric data that uniquely identify a natural person (e.g. fingerprints) have also been taken into account.

Data protection through technology design and data protection by privacy-friendly default
Data processors will be subject to increased due diligence requirements, which are also more precisely

[1] See glossary

defined. Data controllers and processors must reduce the risk of a breach of privacy by taking appropriate measures when planning data processing. In addition, they are obliged to ensure, by means of suitable default settings, that they only process personal data that is necessary for the purpose in question.

Privacy impact assessment
Under the E-FADP, data controllers or data processors are obliged to carry out a data protection impact assessment if the intended data processing leads to an increased risk to the privacy or the fundamental rights of the data subjects. Both risks and appropriate measures must be described.

Notification of data protection breaches
Data controllers must notify the Federal Data Protection and Information Commissioner (FDPIC) of a data breach as soon as possible if there is a high risk to the privacy or fundamental rights of the data subject. If necessary, the data subjects must also be informed

2.3 How is the E-FADP different from the GDPR?

The E-FADP is closely based on the GDPR, which came into force in May 2018. This is essential from an economic point of view, since data exchange with companies and state authorities from countries that do not have comparable protection of personal data can only be carried out under difficult conditions.

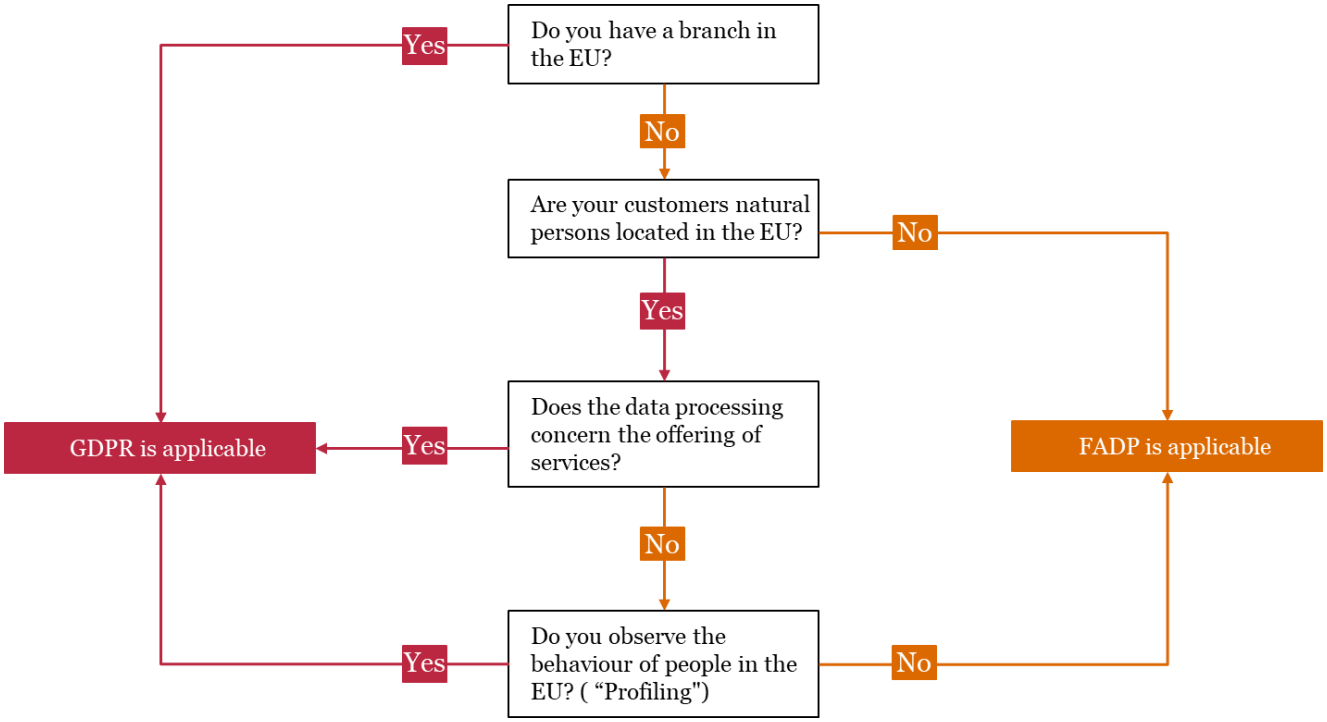
Although the content of the E-FADP is based on the GDPR, there are differences between the two. The main differences between the E-FADP and the GDPR are listed below:

Main criteria		GDPR	E-FADP
Category	Specifications		
General rules	Geographical range	Entities in the EU and/or entities processing data of natural persons within the EU	Entities based in Switzerland
	Fines	Up to EUR 20 million or 4% of sales (the higher of the two amounts constitutes the maximum penalty)	Up to CHF 250,000 (individuals)
Principles for processing personal data		The processing of personal data is generally prohibited, unless there is a legal basis	The processing of personal data is generally allowed, unless the privacy of an affected person is violated
		The following processing principles should be considered for all personal data being processed: 1. Purpose 2. Data minimisation 3. Accuracy 4. Storage limitation 5. Integrity and confidentiality 6. Accountability	The following processing principles should be considered for all personal data being processed: 1. Purpose 2. Data minimisation 3. Accuracy 4. Storage limitation 5. Integrity and confidentiality
Directory of processing activities		Management of a data inventory for the GDPR and E-FADP	
Data breach	Deadline	Within 72 hours	"ASAP"
	Receiver	Supervisory authority and, under certain conditions, the data subjects	Swiss supervisory authority and, upon request, the persons concerned
Privacy rights		A data subject has the right to transfer personal data	There is no right of transferability
		1. Right to rectify inaccurate personal data 2. Right to notification 3. Right to restrict processing 4. Right to be forgotten – erasure 5. Right to object 6. Right to revoke consent 7. Right not to be the subject of exclusively automated processing	Only right to information (the remaining rights are not explicitly formulated in the E-FADP, but are otherwise regulated and enforceable by the Swiss legal system)

3. What the revision means for Swiss companies

3.1 Decision tree – where is your company?

Depending on the specific market activities of Swiss companies, the provisions of either the E-FADP alone or of both the E-FADP and the GDPR apply. The following graphic gives you an overview of which data protection regulations are especially relevant for your company.



3.2 Challenges in implementing the new Privacy Act

For several years, PwC has been supporting numerous companies in Switzerland and within the EU in the analysis, concept definition and implementation of GDPR. In parallel, PwC conducted a benchmarking exercise for various financial service companies to gain market insights into the design and progress of the GDPR implementation.

We observed the following areas in which market players have made progress in the context of the GDPR:

1. Management of personal data and creation of a directory of processing activities

- The challenges in managing personal information are:
  - to create a list of processing activities;
  - to integrate the directory into the business and keep it up to date.

Depending on the business model and diversity of the data landscape, the following challenges remain in defining the directory of processing activities:

1. Identify personal data attributes/categories and define their purpose and legal basis to form a taxonomy of personal data. In addition, the taxonomy is centred around maintaining “business as usual – BAU” by implementing processes and controls. These are to ensure that the taxonomy is reflected in any change in the processing of personal data within the business.
2. Keep directories up to date so that changes in the system are reflected in the processing directories.
3. Identify personal data that is transferred to

third parties and reflect it in the taxonomy. The maintenance and integration of BAU also presents a key challenge for financial service providers.

2. Data protection through technology design and data protection by privacy-friendly default

Privacy through technology design refers to the implementation of organisational and technical measures to comply with the principles of regulation. It is essential to protecting the rights of data subjects before the start of, and during, the processing of personal data. Data protection can be achieved by privacy-friendly pre-setting, which by default only collects and processes the data that is required for a particular purpose. New products, or changes to existing products, require a risk assessment. But even with existing data and processes, there must be a clear understanding of what data is used for what purpose.

To verify compliance with the principle of data minimisation, it is anticipated that the industry standard for data mining will be used. There is currently no such industry standard. In this situation, GDPR compliance is guided by external consultants and service providers who already have experience in the industry and can provide such benchmarks qualitatively.

Another challenge experienced during the GDPR implementation is the design and enactment of concepts, policies and controls that ensure an update of safety standards and plans in order to continuously comply with GDPR principles. This challenge is also to be expected from the E-FADP.

Especially when defining the requirements and when implementing the E-FADP, care should be taken to ensure that the measures to be implemented include a concrete audit trail, in order to ensure continuous compliance with regulations. Cyber security is playing an increasingly important and complementary role in data protection. The technical and organisational measures to be taken to protect the data and the associated compliance with data protection laws can only be achieved and adhered to with a secure IT system.

IT security thus becomes an integral part of compliance with legislation. The compliance officer will not be able to handle the task alone, but will need the support and cooperation of the IT specialist.

Privacy rights for data subjects

Depending on a company's business model, customer segmentation and risk appetite, the degree of automation of processes to comply with the rights of data subjects may vary widely. Experience with the GDPR shows that existing solutions such as e-banking can be used to manage the right of access within an automated procedure. Companies that elect to manage data subject queries manually typically build a single centre of excellence to receive and process all requests. These activities can be managed by existing units, for example those typically handling customer complaints (whose scope is being extended to cover data privacy requests).

Experience shows that currently companies have established limited end-to-end processes that take into account the handling of the extended data protection requirements, as well as the requests of data subjects. Typically, it is recommended that companies create working groups and provide training to cover general privacy requests for the GDPR, E-FADP and ePrivacy Regulation, such that they are responded to in a consistent format. The training should consider the level of processing automation.

In order to be as cost-efficient as possible in responding to requests, standardised reports could be developed. The experience gained from implementing the GDPR shows that standardised reports facilitate an efficient response process. In developing standardised reports, companies need to determine how to delineate between their structured and unstructured data, and how to integrate both metadata and transaction data.

Predicting the volume of expected enquiries from data subjects is a major challenge, where any such prediction is linked to numerous key business considerations. Experience with the GDPR shows that regular inquiries can be expected, peaking at the go-live period.

3. Specific compliance challenges regarding data deletion requests (the right to be forgotten)

3.1 Compliance with data deletion requests

The right to erasure is an absolute right under the GDPR that can only be exercised if the relevant personal data is no longer needed for the purpose for which it was collected and if no other requirements oppose the right (e.g. mandatory archiving or reporting requirements). Businesses need to document why they collect and process personal data and record the legal basis for doing so.

If the right to erasure can be exercised, companies need to erase the relevant data immediately. In this context, companies often face the challenge of limited system capabilities. Existing systems are often limited in respect of data deletion, particularly data supporting a master data integrity model. In the financial sector, it is expected that only a small number of individuals will exercise the right to erasure.

Companies should consider the current and expected number of manually processed requests, the complexity of their system architecture and the number of affected systems.

3.2 Expansion of systematic deletion capacity

The expansion capacity for the principles regarding storage limitation is a major challenge in the industry. Most institutions have fragmented system landscapes which create major challenges to identifying:

i. which data attributes are stored/edited in which applications;
ii. which data sources are needed;
iii. what the purpose of data editing is on the attribute level;
iv. how and when the data is archived for each system.

An automatic deletion functionality is recommended because the manual work to achieve the same outcome is more expensive. A strategic automated deletion functionality requires a clear analysis showing:

1. Which applications process which attributes.
2. The data taxonomy attributes required to determine the purpose and legal basis of personal data collection.
3. Data source by application.
4. Clean up of the archives (legacy).
5. Updates of the data policies.
6. Defined requirements that ensure that the data is deleted once archived in a main application.
7. Defined requirements for the archive, under which the legal data retention period of the specific attributes is considered and adapted to the purpose and legal basis for data collection and processing.
8. Defined requirements for the deletion of personal data in the archive system, in that there is no overlap of personal data between archive and operational applications. In this regard, in consideration of the ePrivacy Regulation, companies should avoid working with personal data but instead work with data field/attributes names or dummy data sets. In testing, companies may replace their actual data with pseudonyms and encrypt the resulting combination.

4. Handling unstructured data

As mentioned in the previous chapter, it is important to consider unstructured data in the design and concept definition of the erasure capacity. Experience shows that companies find locating unstructured data challenging and complex. Handling unstructured data is a crucial part of the GDPR. Certain elements of "unstructured data" (e.g. customer lists for marketing events maintained in Excel) are essentially managed outside of structured systems, such that it is important to define the scope and approach at an early stage.

In addition, experience from the GDPR shows that requests from data subjects regarding unstructured data require manual retrieval and review, leading to considerable additional effort. To reduce this effort, litigation teams and forensic teams can assist companies with disproportionate numbers of requests from data subjects.

To guarantee a comprehensive approach that includes unstructured data, the system landscape and operational business model must be extensively analysed. Policies, procedures and codes of conduct need to be revised and enforced to ensure compliance with data protection principles. This substantially facilitates the identification of unstructured data. In addition, third-party support may also be considered for a tactical solution. Scanning tools can also be implemented to detect or outsource discrepancies in terms of unstructured data policies and procedures.

5. Management of personal data with respect to third parties

Personal data is transferred to a third party if it is made available to a third party outside of the company's infrastructure, systems or networks (including those within the same group of beneficially owned companies – i.e. intra-group). There is, however, no transmission of personal data if the data is sent anonymously (and re-identification is not possible).

The main challenges that companies encounter are identifying that data is being transferred and determining the purpose for which a third party is processing personal data. Processes and controls are needed to identify the data processed by third-party providers and the contractual arrangements in place, and to monitor compliance. The processes should also establish the link to the processes concerning the rights of data subjects (e.g. right to erasure).

In addition, existing contracts with third parties must be updated in order to:

1. determine the way in which data is processed;
2. define the type of data and categories of data subjects concerned and define control measures;
3. define the requirements and obligations in preparation for any data subject requests.

Companies must also ensure that third parties adopt the new guidelines or amendments and adhere to them thereafter.

Sometimes companies struggle to identify the existence of relevant third parties to which personal data is transferred, for example, when creating a website, development typically requires multiple third-party and advertising providers.

6. Information and cyber security: challenges and opportunities

"It's no longer a question of whether… it's about when…" is a familiar adage. Attacks on the infrastructure of large organisations appear weekly on newspaper front pages. Acknowledging that not all attacks can be prevented and that there will never be

100% security, companies should improve their ability to detect attack incidents in order to effectively and rapidly detect, contain and respond. Companies' responses should include the notification of the data breach to the appropriate supervisory authorities within 72 hours, as required by the GDPR. The GDPR refers to a "personal data breach", which is to be understood as a breach of security that leads to the destruction, loss, alteration or unauthorised disclosure of personal data, whether by error or unlawfully. Unauthorised access to personal data is also covered.

Data breaches have significant implications for companies, including in circumstances where unauthorised individuals obtain access to confidential information. Outcomes of data breaches may include significant financial damage, legal risk and reputational damage. Furthermore, at the centre is any negative impact on the affected person(s). Post data breaches, data entrusted to the company may be circulating through the World Wide Web and thus providing a platform for cyber-attacks.

Absolute security cannot be guaranteed; however, firms can strengthen their cyber resilience to significantly reduce the likelihood of an attack against them being successful and improve their response times, limiting damage. Strengthening cyber resilience is achieved through enhancing preventative and detective controls, e.g. penetration testing, and response processes.

To effectively manage cyber risks, companies need to consider a number of different factors. Firstly, companies should have consistent cross-departmental cyber risk processes, procedures and practices. Security concepts should be integrated into projects, products and processes (security by design). Special attention should be given to the threat landscape and the threat actors that might target the companies' infrastructure. Such knowledge and know-how should be operationalised cost-efficiently in the security architecture of a company.

Companies should perform frequent disaster recovery exercises according to the principle that "practice makes perfect". Doing so will train, strengthen and optimise the overall operational readiness within the company. Training should be provided on a regular basis to increase competency and awareness. The best IT security infrastructure is of little use in the absence of informed and trained staff, as it requires only one individual to create a vulnerability for threat actors (e.g. by clicking on a link in a phishing attack).

4. Outlook

4.1 The ePrivacy Regulation

The ePrivacy Regulation protects the right to privacy and communication and is one of the cornerstones of the EU's Digital Single Market Strategy.
This new regulation has been positioned as "future-proof": it refers to existing and future communication technologies. The ePrivacy Regulation will have a disruptive effect on companies' digital strategies, which will need to be redefined to meet the new requirements.

The ePrivacy Regulation will replace the existing ePrivacy Directive, last revised in 2009. The new regulation has been amended to reflect current digital markets and therefore includes a significant extension in scope and application. The main objective of the ePrivacy Regulation is to protect the electronic communications of natural and legal persons and the information stored on their electronic devices. The cornerstones2 of the proposed rules on privacy and electronic communications are:

- ***All electronic communications require a high degree of confidentiality***
  Listening, intercepting, scanning and storing text messages, emails, voice calls, etc. is not permitted without the user's consent. The principle applies to current and future means of communication – including all devices connected to the Internet of Things.

- ***Confidentiality of users' online behaviour and devices must be ensured***
  The user's consent is required to access information on their device. For example, users must also submit their agreement to websites, prior to accessing them, permitting the website to use cookies or other technologies to access information stored on the users' computers or to track the users' online behaviour.

- ***The processing of communication content and metadata requires the consent of the person concerned***
  Data protection is afforded to both the content of a communication and its metadata – for example in respect of a phone call, metadata includes the caller, the party called, and the time, place and duration of the call.

- ***Spam and direct marketing communications require prior approval***
  Regardless of the technology used (e.g. automated calling systems, SMS or email), users must give their consent before being contacted for commercial purposes. Advertisers must show their phone number or use a specific (identifying) area code that indicates that the call is a marketing call.

The objective of the ePrivacy Regulation is to supplement the requirements of the GDPR. However, the two regulations may overlap. In case of conflict, the provisions of the ePrivacy Regulation take precedence (provided they do not reduce the level of protection that natural persons enjoy within the framework of the GDPR). The ePrivacy Regulation thus represents a lex specialis for the GDPR, and as such is relevant to Swiss companies. It is recommended that companies consider interfaces with the ePrivacy Regulation based on the existing design when analysing the E-FADP.

Based on the latest information, the following parallels exist between the E-FADP and the ePrivacy Regulation:

[2] Based on the ePrivacy Regulation draft of December 2017

Criteria		GDPR/E-FADP	The ePrivacy Regulation
General rules	**Affected**	Natural persons	Natural and legal persons
	Scope	General data protection in connection with the processing of personal data by legal persons of the private sector and legislative bodies (public sector)	Processing of electronic data and information relating to electronic devices
	Geographical range	Entities in the EU and/or entities processing data of individuals within the EU (Switzerland: only entities domiciled in Switzerland)	Locations where the user accesses the service: provision of online communication services, online tracking technologies or electronic marketing
Personal data inventory	**Legal basis**	(i) consent of the persons concerned, (ii) contractual obligation, (iii) compliance with the legal obligation, (iv) public and/or legitimate interests	Consent is required for any type of data processing if the processing goes beyond the requested service (e.g. processing allowed without consent if required for communication transmission)
Rights of the persons concerned		Right to erasure (GDPR), no right to erasure under the E-FADP	Immediate deletion of certain data (e.g. contents of the communication), other data will not be stored longer than necessary (e.g. metadata)
		Right to object to processing	Right to control electronic communication including the prohibition of unwanted communication/advertising
		Right to access data, right to transfer, right to rectification, right to object to consent, right to object to automated decision-making, right to restriction of processing	Two rights are protected: Everyone's right to respect for their private and family life, their home and their communication Right to privacy and confidential communication

5. Need for action

Swiss companies need to take immediate action on the GDPR/E-FADP and the ePrivacy Regulation, moving away from tactical temporary solutions and towards long-term strategic solutions. The automation of inquiries must be promoted in order to accomplish timely processing and case management and the deletion or archiving of personal data in an efficient, faster and cost-saving way.
A significant challenge is the management of corporate regulatory conflicts, e.g. E-FADP vs. GDPR vs. the ePrivacy Regulation. At the same time, managing the uncertainty surrounding the final version of the regulations and the cost/effort of any estimation are key aspects to achieving efficient compliance. A gap analysis on the GDPR/E-FADP and the ePrivacy Regulation, tailored to the individual company, is an important step in identifying any need for action and developing company-appropriate measures.
Regarding the ePrivacy Regulation policies, companies need to analyse applicability to their company and, if necessary, adapt the company's data privacy and electronic communications processes. A company-wide analysis should ask (not exhaustive):

- What personal data is processed?
- For what purposes is personal data collected and processed?
- What sensitive data is processed?
- What is the legal basis for the data processing? Is there consent?
- What data traffic exists with EU foreign countries and/or third countries, and on what legal basis?
- How are the rights of data subjects processed?
- Are data processors (currently "service providers") involved?
  - Are there written agreements for order processing?
  - How are the notification obligations fulfilled?
  - How are the affected rights fulfilled?
- Who is responsible for data protection within the company? Whom should affected persons contact to exercise their rights?
- What data security measures are available?
- Is there a privacy impact assessment for data processing?
  - What risks arise from data processing and what rights and freedoms are affected?
  - How can risk be prevented or minimised?
  - Is prior consultation with the regulator necessary?
- Does the company require a data protection officer?
- What precautions against data breaches already exist?
- How are notification obligations fulfilled? (e.g. privacy statements)
- Is there a documentation requirement for data processing? How is the documentation obligation fulfilled?

The topic of data protection will continue to occupy compliance and legal functions, as well as the IT function, in the coming years. Efficient IT solutions are becoming increasing available and are of greater focus, especially in the areas of data management, data archiving and data classification. For example, emerging technologies such as machine learning and AI have the potential to automate data classification processes, reducing manual processes.
Emerging technologies can further support today's IT infrastructure and applications for universal indexing and searching in order to quickly locate personal data, e.g. deletion requests can be processed successfully. Other rights enjoyed by a data subject include free access to content, correction of data and the right to object to data processing. To efficiently handle the requests of data subjects, efficient IT solutions can offer a system-based workflow that supports the process from receipt to completion of a request.
Innovative IT solutions combined with effective data governance reduce the risk of unwanted data leakage and enhance anomaly detection.

Glossary

Data subject	A person about whom data is processed
Data controller	A company or person who decides on the purposes and means of processing personal data
Data processor	A natural or legal person, agency, institution or other body that processes personal data on behalf of the data controller
DPO	Data protection officer
Legal person	A company
Natural person	An individual or user who makes use of online services
Portability	Transferring data from one data controller to another
Structured data	Data from which specific information can be read
Transfer	Transfer of data between data controller and processor
Unstructured data	Data without identifiable structure (e.g. images, text, voice message)

Notes

For more information please contact:

Regulatory Transformation

Patrick Akiki
Partner, Finance Risk and Regulatory Transformation
+41 79 708 11 07
akiki.patrick@ch.pwc.com

Marc Lehmann
Director, Finance Risk and Regulatory Transformation
+41 79 785 69 93
marc.lehmann@ch.pwc.com

Morris Naqib
Senior Manager, Finance Risk and Regulatory Transformation
+41 79 902 31 45
morris.naqib@ch.pwc.com

Legal

Susanne Hofmann
Director, Leader Legal Compliance & Data Protection
+41 79 286 83 67
susanne.hofmann@ch.pwc.com

Michael Taschner
Director, Legal FS Regulatory & Compliance Services
+41 79 757 95 53
michael.taschner@ch.pwc.com

Philipp Rosenauer
Manager, Legal FS Regulatory & Compliance Services
+41 79 238 60 20
philipp.rosenauer@ch.pwc.com

PwC Digital Services

Wolfgang Schurr
Partner, Cybersecurity and Privacy
+41 79 545 77 71
wolfgang.schurr@ch.pwc.com

Sascha Sandragesan
Manager, Cybersecurity and Privacy
+41 58 792 50 56
sascha.sandragesan@ch.pwc.com

Key contributors:
We would like to thank Daniel Winteler, Philipp Schwarz, Chris Müller and Caroline Gigger for their valuable contributions to this publication.