The global footprint of data protection regulations

Data protection is shaping industries around the globe

"I really believe that we don't have to make a trade-off between security and privacy. I think technology gives us the ability to have both."

John Poindexter

pwc

Table of Contents

Personal data protection – introduction

The world is going through its fourth industrial revolution, one that is driven by extreme social and economic connectivity. Digitalisation and data availability have been and still are key enabling factors of such a revolution, and the amount of information being processed is growing exponentially by the day. Most activities nowadays result in the production of some sort of data, starting from a simple phone call all the way to less obvious examples like buying groceries with your credit card and your store loyalty card. This constantly growing amount of information needs to be stored and managed by organisations, which in turn have to grow more complex to survive in the modern, digitalised world.

Given its importance, personal data processing is currently a top priority on many government agendas around the world. The EU initiated a regulatory standard when it published the General Data Protection Regulation (GDPR), and it set the bar for the update and review of most global personal data protection laws. After GDPR, companies all over the globe should expect a wave of new or updated regulations, and should be prepared to comply with increasingly strict requirements. In this document we describe in great detail how some of these regulations are changing, and what companies need to do in terms of processing personal data in order to survive in this highly regulated world.

Why data protection matters

People in the current era manage their personal data in ways that would have been unthinkable just a couple of decades ago. Would a person in the 1980s reveal their address, phone number and annual income to a total stranger met on the bus? Most certainly not. Today, though, people share an unimaginable amount of information with companies – essentially with total strangers – and most of the time we do so because we are confident that our data will be processed legally and in line with basic data protection principles. We assume that our data will be kept safe and confidential, that no third party will have access to it, and that the company to which we entrusted our data will use it only for the purposes for which we provided it. We can confidently make this assumption because strong data protection regulations are being enforced and companies have real incentives to make sure our data remains protected.

Despite their best efforts, however, this doesn't always work, as the recent Facebook-Cambridge Analytica data scandal demonstrated: millions of Facebook's personal data profiles were allegedly analysed without authorisation and used for illegal political purposes. Cases like this highlight the need for stronger and more transparent regulations – like the EU's GDPR, which entered into force in May 2018, after the events linked to the Cambridge Analytica data misuse scandal.

A milestone in Data protection: the EU GDPR

Demand for the new European Union General Data Protection Regulation (EU GDPR) arose out of a need for stronger regulatory requirements regarding personal data protection. GDPR needed to embrace a much wider scope of requirements compared to the previous Data Protection Directive 95/46/EU adopted in 1995. The GDPR was published on 24 May 2016 with a transposition period of two years until May 2018 (when it came into force). It was a new regulatory framework designed to strengthen the data privacy and protection of all EU citizens, across the EU member states and abroad.

Any organisation, regardless of geographical location, that collects or processes personal data on EU residents needs to comply with GDPR, including organisations with no business facilities in the EU but that offer goods and services into the EU or that monitor European citizens. Non-compliance from such organisations has severe financial consequences, with fines either up to 4% of total global annual turnover or 20 million euros, whichever is higher.

GDPR is seen by many as a milestone in the context of data protection, as it sets a level of protection for the data subject that was unheard of before. Not only does it define strict principles of compliance when it comes to the processing of personal data, but also grants data subjects a set of rights that give them more control over how their personal data is processed. The most noteworthy of such rights is definitely the right to be forgotten: in a digitalised society where any information seems destined to be stored forever on some server, this right grants data subjects the possibility of having their data deleted once it is no longer needed for the purpose for which it was collected. More specifically, organisations need to have the capability of deleting data from all their systems upon request (including the systems of other companies to which data was transferred).

The EU GDPR framework for compliance

The articles of the EU GDPR include eight key topics that need to be covered operationally from three different perspectives: business (which data is processed), IT (where is personal data processed) and third parties (to whom is personal data transferred).

1

Data inventory
Organisations need to create and maintain a data inventory to identify which personal data is processed and for which purpose.

2

Principles
Personal data processing should always be performed in adherence with personal data protection principles (e.g. it has to be lawful, for a specific purpose, etc.)

3

Standards
To ensure that personal data is processed in compliance with GDPR requirements, companies need to develop processes and enforce behavioural standards with their staff.

4

Data subject rights
Under GDPR, natural persons have a series of rights (data subject rights), to which organisations need to be ready to answer (e.g. right of data access, or right to be forgotten).

5

Data processing records
The regulation requires organisations to maintain a detailed record of all the personal data processing activities.

6

Personal data breaches
Companies must minimise the risk of data breaches, and need to implement processes to inform the supervisory authority within 72h of a breach (when certain conditions are met).

7

Data Protection Officer
When certain conditions are met, organisations need to nominate a Data protection Officer to monitor compliance with GDPR requirements.

8

Data Protection impact assessment
For processing activities which present a risk to the rights and freedom of the individuals, an impact assessment is required, to identify and implement adequate mitigation measures.

Current status of GDPR implementation

Complying with GDPR has resulted (and still is) in massive investments for organisations in Europe and throughout the world, but some companies have also managed to look at the bright side. Compliance with the regulation also brought new opportunities for organisations that had already consistently redefined their approach to privacy, allowing them ultimately to benefit from the value of the data they hold. They have been able to develop a setup better suited to the new digital economy and the associated trust among data subjects by giving them more transparency and control over their own data.

Many companies, both in the EU and in other countries like Switzerland, have adopted a risk-based approach for the implementation of compliance measures with GDPR. This has often manifested itself in a wave approach, where certain measures have been prioritised over others. Where some companies completed the implementation of compliance measures by the GDPR go-live date in May 2018, most organisations are working on the subsequent steps, including:

1. Ensuring the efficacy of the implemented measures. This is especially important in terms of the procedures related to personal data processing records and personal data breaches
2. Automating the implemented processes, where possible, to reduce compliance costs. Many organisation have implemented processes through tedious manual efforts, but these can often be automated over the long term (e.g. regarding data subject rights, where the generation of data subject rights reports can be easily automated)
3. Reviewing data protection efforts from a strategic perspective, by including data management within the company's strategic orientation. In light of the efforts already undertaken to create the data inventory, the next logical step is to make sure to use this information strategically by making the best possible use of the data that companies already hold and process (always keeping in mind compliance with data protection principles, particularly in relation to the purpose limitation).

Key data protection laws in Europe and the world

Data protection has become a hot topic in many countries around the world. Whether your company is based in Europe or in a remote region of China, you will have to deal with some sort of personal data protection regulation – and things may get complicated for corporations with a global footprint. So much so that it may be more efficient for a US-based company to simply comply with the European GDPR in all of the locations in which it operates – as most other regulations would typically be equivalent or less strict than the GDPR.

In this section we aim to give you a detailed overview of the key data protection regulations in some of the most important regions in the world.

EU: local derogations to the GDPR

The GDPR is a regulation, and as such it automatically applies equally in all EU member states without the need to transpose it into national laws. Nevertheless, these states can still exercise a degree of discretion on certain areas of the regulation. In fact, the text allows for national derogations on specific sections (e.g. processing of special categories of personal data or data transfers).

In practice, where GDPR allows for derogations, national laws can be more or less strict than the GDPR in defined areas. Here we list some examples of these differences for the biggest European countries. However, the full scope of derogations is too extensive to be covered here and we suggest companies initiate a full analysis of the national derogations published within the countries they operate.

Country	Derogation to GDPR
UK	With Brexit coming soon, UK data protection law will be monitored closely, as it may lead the way to a UK-specific data protection law (to the extent that the GDPR will not be directly applicable anymore). The Data Protection Act, applicable from May 2018, contains an extensive lists of derogations to the GDPR, but here are the most noteworthy: • UK derogations set stricter conditions for the processing of special categories of personal data (such as biometric information, or data on sexual orientation) where explicit consent is required. The processing of these special categories of personal data needs to meet specific conditions in order to be considered lawful. • The UK Data Protection Act also requires that appropriate safeguards and policies are in place for processing special categories of personal data, and that these are adequately documented as part of keeping processing records (c.f.r. Art. 30 GDPR).
Germany	In Germany the new Federal Data Protection Act (FDPA) entered into force in May 2018, thereby setting additional and stricter requirements for processing personal data: • Specific requirements are stipulated for processing video recordings: not only do companies need to ensure that the activity does not raise a risk to the rights and freedoms of individuals, but such processing is also only permitted under a strict set of conditions. Considering the widespread use of closed circuits cameras, this is bound to be one of the most challenging requirements to meet. • Where the GDPR requires the mitigation of risks to the individuals in the context of automated decision-making and profiling, German derogations only allow the processing of personal data for scoring purposes under a set of specific conditions.

Country	Derogation to GDPR
Austria	Austrian derogations (listed in the Datenschutzgesetz, updated in 2018) are limited in scope, but mostly stricter than the respective requirements in the GDPR, for example: • As in Germany, specific requirements are set for the processing of video recordings: also in this case, processing is only permitted under a strict set of conditions. • Where GDPR mainly focuses on the obligations of the controllers and processors as legal entities, the Austrian Datenschutzgesetz sets specific requirements for the employees of such entities, who are in turn liable in case they do not treat as confidential any personal data processed in the context of their employment.
France	The Revised French Data Protection Act (in force since May 2018) sets a number of requirements that are stricter than the respective articles from the GDPR, for example: • French law explicitly prohibits processing of special categories of personal data, unless the conditions set in the derogation are met. This provision is mainly aligned with the GDPR dictate, but it becomes stricter when it comes to the processing of biometric information in the context of employment. • Where the GDPR sets the minimum age at 16 for a kid to provide consent for the offering of online services, under French law that minimum age is lowered to 15 (with additional local requirements).
Italy	Italy only published the revised version of its privacy regulation in September 2018, with some months of delays compared to other European countries. Worth noting are the following: • Italian law is introducing stricter criminal sanctions for instances where personal data is unlawfully processed • In Italy the age for child consent for the offering of online service has also been lowered, in this case to 14 years.

Data protection around the world

While the EU GDPR is already enforced, other countries have begun working on their own data protection laws – often trying to align them with the GDPR's requirements. Here we provide an overview of how other data protection laws currently under review align with the GDPR, followed by a more detailed description on the current status of the regulation in such countries.

Country	Key privacy regulation	New or updated law	Similarity to the GDPR	Timeline
Switzerland	Federal Act on Data Protection	Updated	High degree of similarity	Expected to be fully applicable by end of 2020
US	Varies per state	New and updated	Varies per state	n/a
Canada	Digital Privacy Act	Updated	Updates in line with GDPR requirements	Expected to be applicable by end of 2019
China	Chinese National Standards on Information Security Technology – Personal Information Security Specification	New	Some require-ments are even more rigorous than the GDPR	Came into force from May 2018
India	Draft of the Personal Data Protection Bill	New (draft)	In its current state, lower protection of personal data compared to the GDPR	Draft was submitted in July 2018

Country	Key privacy regulation	New or updated law	Similarity to the GDPR	Timeline
Thailand	Draft of the personal data protection act	New (draft)	Designed to be aligned with GDPR	Draft was approved in May 2018
Singapore	Personal Data Protection Act	Existing (no changes)	Similar level of protection as the GDPR	n/a
Jersey	Data Protection Law	Updated	Imitates requirement of the GDPR	Came into force from May 2018

Data protection in Switzerland: FADP

On 9 December 2011, the Federal Council approved the report on the evaluation of the Data Protection Act and instructed the Federal Department of Justice and Police (FDJP) to examine legislative measures to strengthen data protection in the light of the results of the evaluation and current developments in the EU and the Council of Europe. Furthermore, the revision of existing laws was necessary due to the Schengen Convention.

The alignment of FADP to GDPR 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 (different levels of requirements applicable to the same company, restrictions on doing business with certain companies, etc.).

In September 2017, the Federal Council presented a draft for a significantly revised data protection act, the Federal Act on Data Protection (FADP), which aims to: (i) increase transparency (e.g. data controllers are obliged to ensure, by means of suitable default settings, that by default only personal data is processed that is necessary for the respective purpose); (ii) strengthen the participation rights of data subjects (e.g. data controllers shall notify the Federal Data Protection and Information Commissioner of a data breach as soon as possible if there is a high risk to the personality or fundamental rights of the data subject); (iii) and take into account technological progress (e.g. genetic as well as biometric data that uniquely identify a natural person has also been taken into account).

The revision is divided in two stages. The first is to allow for prior consultation regarding the implementation of the EU law (Directive 2016/680 on the protection of individuals related to the processing of personal data in the criminal field), which is required by the Schengen agreements. Thereafter, the data protection act can be revised without time pressure. The second stage, expected to be completed by the end of 2020, is particularly relevant for Swiss companies. Additional and more detailed information on the FADP and its link to the GDPR can be found in our publication "What does the revision of the Swiss FADP entail, and how does it relate to the GDPR and the ePrivacy Regulation?"

Data protection in the United States

The United States has over 20 industry-specific data security laws on the federal level. Besides that, there are hundreds of state laws to regulate the collection and use of personal data, and that number is growing each year. In some cases, federal privacy laws override state privacy laws on the same topic. For example, the federal law regulating commercial e-mail and the sharing of e-mail addresses overrides most state laws regulating the same data. On the other hand, there are many federal privacy laws that do not override state laws, which means a company can get into situations where it has to be compliant with different federal and state privacy laws that regulate the same types of data, such as medical or health records.

Most states have implemented some form of privacy legislation, but California is leading on data protection topics. The state has put multiple privacy laws into place, some of which have far-reaching effects at a national level. As an example, California was the first state to enact a security breach notification law in 2002 (California Civil Code §1798.82). However, a number of bills that would establish a national standard for data security breach notifications have been introduced in the U.S. Congress, but none have been passed so far.

Data protection in Canada

Canada has four private sector privacy statutes that govern the collection, use, disclosure and management of personal information: (i) the Federal Personal Information Protection and Electronic Documents Act, S.C. 2000, (PIPEDA); (ii) Alberta's Personal Information Protection Act, S.A. 2003 (PIPA Alberta); (iii) British Columbia's Personal Information Protection Act, S.B.C. 2003 (PIPA BC); and (iv) Québec's An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q. (Québec Privacy Act).

PIPEDA, the federal privacy law, is less stringent compared to the GDPR, but has been amended in 2018 to partially align to GDPR requirements.
The PIPEDA updates introduced mandatory data breach reporting provisions, however many shortcoming still remain in comparison to GDPR, mainly in the area of Data Portability, Right to Erasure, and Consent.

Data protection in China

The long anticipated first Chinese National Standards on Information Security Technology – Personal Information Security Specification GB/T 35273-2017 has been released and came into force on 1 May 2018. It serves as the new de facto standard for practical data protection handling, which complements and clarifies many existing data protection laws, such as the Cybersecurity Law and the Consumer Protection Law, and describes practical compliance steps.

However, how the standards will be implemented is still not clear. Despite uncertainty about its effect, the language in the standard is broad and includes more rigorous requirements than even the GDPR. As example, while the GDPR focuses only on some specific types of data, the Chinese standard is more far-reaching in terms of sensitive personal information. The Chinese standards cover any personal data that would cause harm to persons, property, reputation, and mental and physical health if lost or abused.

Data protection in India

In July 2018, India got closer to its first data privacy law by submitting a draft of the Personal Data Protection Bill, which forms a framework and prescribes how organisations, including the state, should collect, process and store citizens' data. However, the bill still has many loopholes that might weaken the privacy and security of citizens' personal data. As example, the requirement to store a copy of all personal data at a server centre in India creates extensive permissions for the government to use the personal data. Therefore, the bill still needs many further rounds of review before becoming a law that is comparable to the GDPR.

In the meantime, the Information Technology Act from 2000 includes specific provisions intended to protect electronic data and considers issues like paying compensation and imposing punishment in the case of wrongful disclosure and misuse of personal data as well as in the event of a violation of contractual terms related to personal data. However, the IT Act lacked provisions for the protection of and the procedures to be followed to ensure the safety and security of sensitive personal information of an individual. As a consequence, several amendments and finally Section 43A was inserted in the IT Act, which became the Information Technology Rules, 2011. The privacy rules force corporate entities to collect, process and store personal data, including sensitive personal information, in order to be compliant with certain procedures.

Data protection in Thailand

Currently there is no specific law protecting personal data in Thailand, but the country has been working for years on a regulation related to this topic. A draft of the Personal Data Protection Act (Draft Act) was approved by the Thai Cabinet in principle on 22 May 2018. A revised version of the document is now under consideration by the Council of State.

This new regulation has been drafted to align data protection in the country to the minimum requirements set by many data protection laws in the world, particularly by the GDPR. The act now needs approval from the Council of State, but no official timeline has been set for when the new law will be published and come into force.

Data protection in Singapore

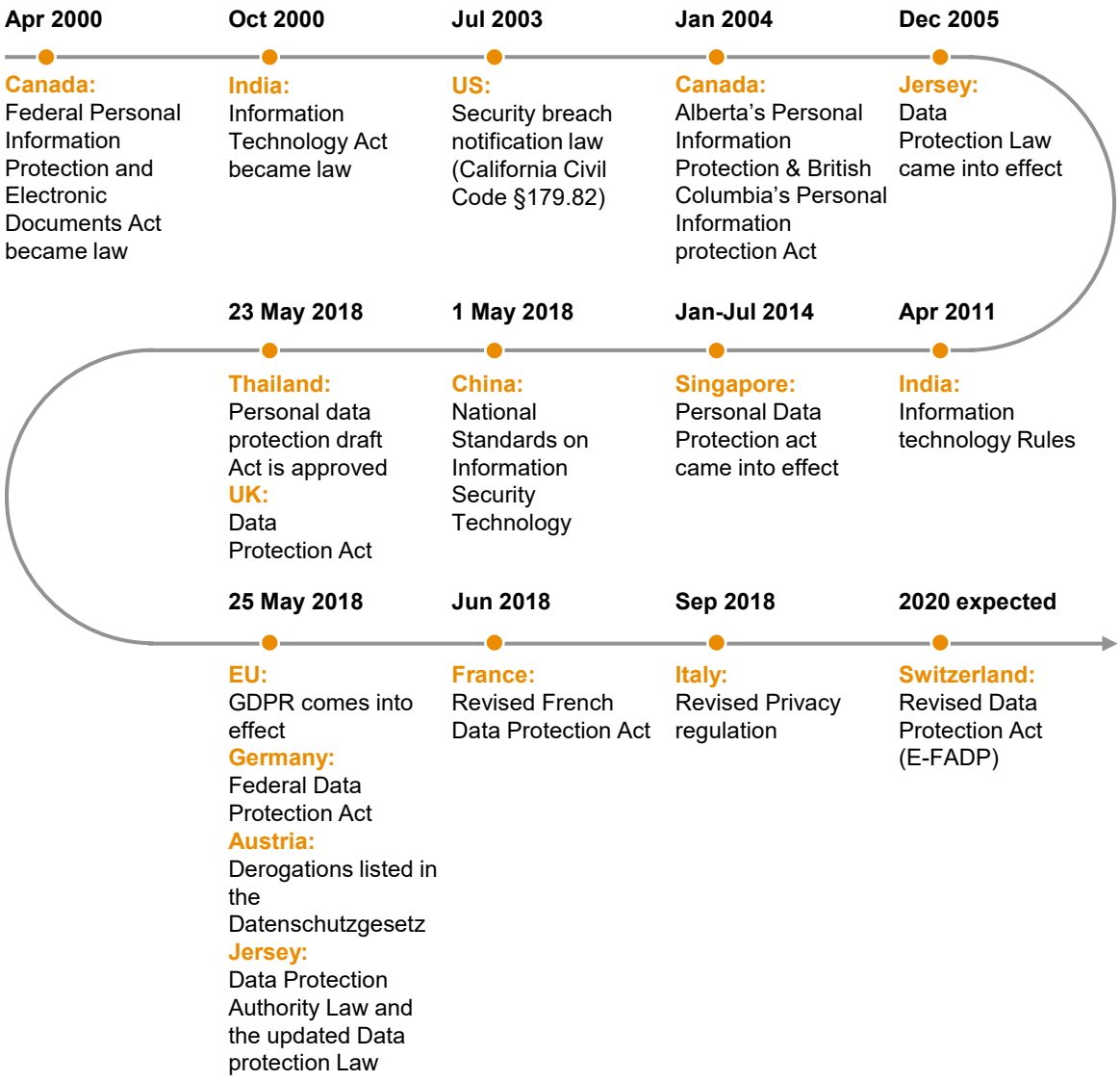
The Personal Data Protection Act was enacted in Singapore in 2012, and it entails extraterritorial scope, i.e. it applies to any company processing data from natural persons located in the country, regardless of the location of the company itself.

Currently, Singapore has initiated a series of public consultations to review the act with regard to important topics such as Managing Personal Data in the Digital Economy or Managing Unsolicited Messages and the Provision of Guidance to Support Innovation in the Digital Economy."

Data protection in Jersey

The Data Protection (Jersey) Law came into effect on 1 December 2005 and was modelled on the UK Data Protection Act of 1998. Jersey makes great effort to ensure that their data protection regulations provide the same standards of protection for personal data as the ones in force in the EU, since historically a large amount of the personal data processed in Jersey belongs to EU citizens.

The Data Protection Authority (Jersey) Law 2018 and the Data Protection (Jersey) Law 2018 was enacted in order to imitate the enhanced requirements of the GDPR. The new law in both jurisdictions came into force on 25 May 2018. The data protection legislation in Jersey is considered equal to the European Data Protection Directive (Directive 95/46/EC) by the European Commission. This equality will remain in force until the European Commission reviews it, latest by 2022.


Apr 2000
Canada: Federal Personal Information Protection and Electronic Documents Act became law
Oct 2000
India: Information Technology Act became law
Jul 2003
US: Security breach notification law (California Civil Code §179.82)
Jan 2004
Canada: Alberta's Personal Information Protection & British Columbia's Personal Information protection Act
Dec 2005
Jersey: Data Protection Law came into effect
Apr 2011
India: Information technology Rules
Jan-Jul 2014
Singapore: Personal Data Protection act came into effect
1 May 2018
China: National Standards on Information Security Technology
23 May 2018
Thailand: Personal data protection draft Act is approved
UK: Data Protection Act
25 May 2018
EU: GDPR comes into effect
Germany: Federal Data Protection Act
Austria: Derogations listed in the Datenschutzgesetz
Jersey: Data Protection Authority Law and the updated Data protection Law
Jun 2018
France: Revised French Data Protection Act
Sep 2018
Italy: Revised Privacy regulation
2020 expected
Switzerland: Revised Data Protection Act (E-FADP)

What's next for your organisation?

Some of the strongest data protection requirements have been set forth in the GDPR, but as we have seen there are a number of other data protection regulations that companies in Europe and in the world have to consider. Also, many countries are still working on reviewing, updating or creating their laws on data protection. Although no final text is available in many cases (e.g. in Thailand or Switzerland), one may expect a high degree of similarity with the EU GDPR.

Data protection is a complex topic, and even more so when your business is present in multiple countries and thus subject to a number of different laws. Organisations in this situation need to consider which regulations are applicable to them, when to act, and which processes to implement. It would often be easier to simply apply to your entire organisation the standards set by the strongest applicable regulation, rather than trying to set up different processes in different locations.

A holistic approach will ensure that clients in different locations do not perceive any difference in the service provided, thereby projecting a more coherent image – on top of often being the most efficient approach. This type of holistic approach does not need to be strict: a risk-based approach is often the best solution. Such an approach allows companies to identify which gaps tin regulatory requirements need to be filled with urgency, which gaps can be filled at a later stage or which ones are even considered as acceptable for the organisation. When dealing with draft regulations, companies applying a risk-based approach can decide to either start implementing processes on the basis of what the requirements will most likely be, or wait until the final text is ready. The latter would entail the risk of not having the processes implemented once the regulation has gone into effect (this is especially true for big organisation that need long lead times for transformation projects, as the experience with implementation of GDPR-compliant processes has shown).

Data protection has become so important nowadays that most organisations can no longer afford to treat it as just another compliance topic. An increasing number of processes within an organisation involve some form of personal data processing, and the requirements from a regulatory perspective are becoming stricter by the day. Companies need to start looking at the protection of personal data from a strategic perspective: knowing which personal data they process, in which systems; defining adequate safety measures; and ensuring adequate training for employees should all become part of the strategy of any big organisation. Having a solid data management system in place when it comes to the processing of personal data will be of help in complying with any regulation on the topic.

From a practical perspective, to ensure compliance, companies should set up adequate monitoring for applicable regulations and decide how to deal with upcoming new laws. It is important that processes are implemented as soon as possible given the importance of data protection for customers. Also, companies subject to the GDPR that have already implemented the respective processes for compliance should keep their guard up: Additional local derogations can be expected, and a new ePrivacy regulation is on its way (for more details, you can read our publication Is ePrivacy defining the future standard of data protection for the banking industry?).

How can PwC help?

As a multi-disciplinary practice, we are uniquely placed to help our clients adjust to this new environment. Our data protection team includes lawyers, consultants, cybersecurity specialists, auditors, risk specialists, forensics experts and strategists. Our team is truly global, proposing innovative solutions with on-the-ground expertise in all the major EU economies.

PwC is best suited to support you in your journey to compliance, from the readiness assessment to the implementation of required actions (see picture on the right).

1 Readiness assessment and gap analysis

We can help you understand where do you stand in terms of compliance with current and upcoming regulations

2 Personal data inventory

We can help you in facilitating the streamlined collection of key data inventory information and in defining the data processing efforts across your organisation

3 Action plan development

We can help you develop an adequate action plan to define and implement the necessary processes, with a focus on prioritisation and with risk-based approach

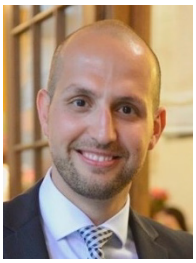
4 Implementation of compliance actions

Once all gaps and respective measures for compliance have been defined, we can help you implement the processes to ensure an effective transition to Business as Usual

Notes

For additional information, please contact our Regulatory Transformation experts:

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

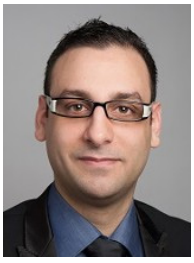


Morris Naqib
Senior Manager,
Risk and Regulatory Transformation
Mobile: +41 79 902 31 45
Email: morris.naqib@ch.pwc.com

Mark Hussey
Senior Manager,
Risk and Regulatory Transformation
Mobile: +41 79 549 0759
Email: mark.hussey@ch.pwc.com

Isabella Sorace
Manager,
Risk and Regulatory Transformation
Mobile: +41 79 742 37 16
Email: isabella.sorace@ch.pwc.com

Legal expertise:



Yari Antonio Iannelli
Assistant Manager,
Legal, FS Regulatory & Compliance Services
Mobile: +41 58 792 28 54
Email: yari.iannelli@ch.pwc.com

Key contributors:
We would like to thank Dat Huynh and Enrico Zurkirchen for their valuable contribution to this publication.