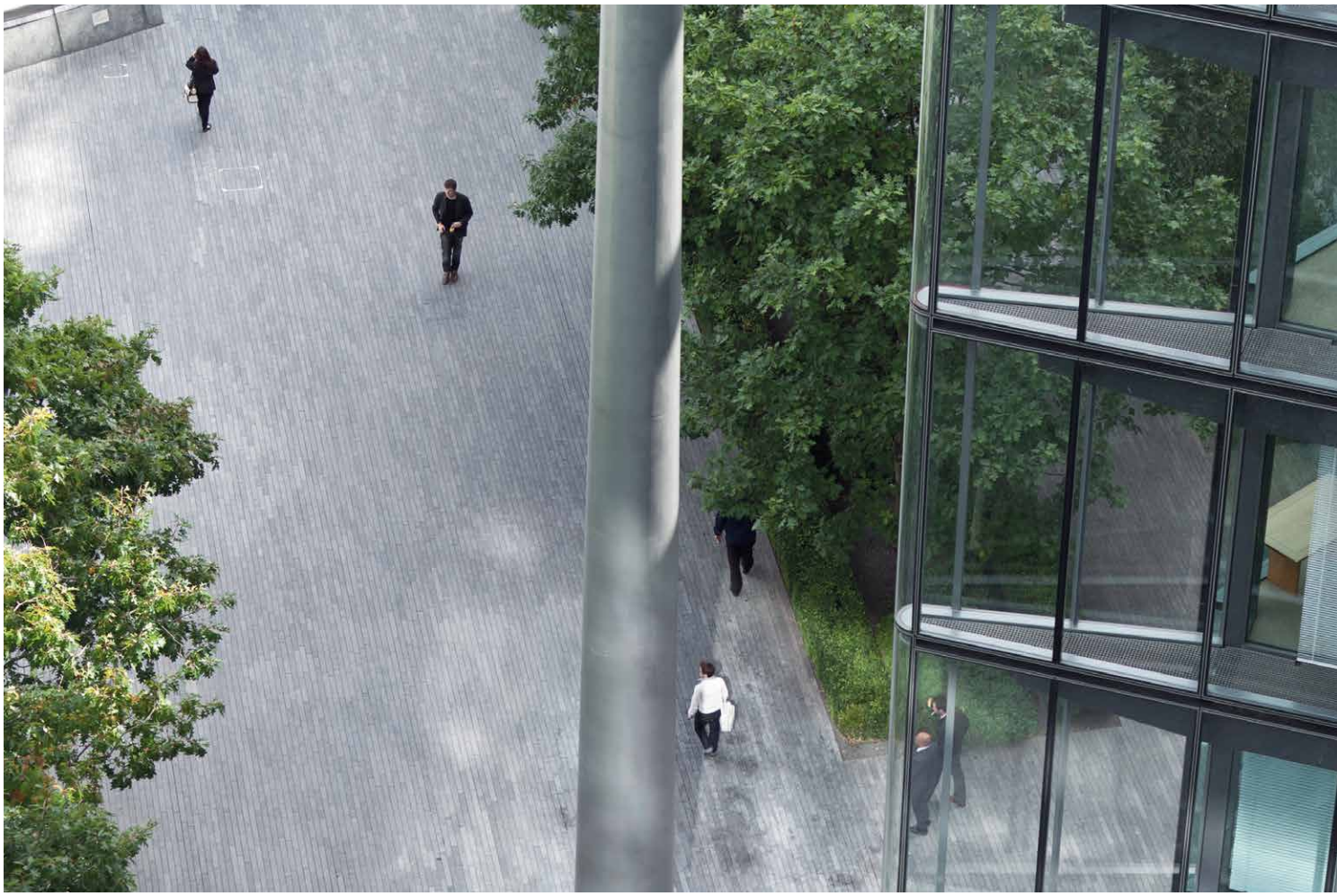
The EU General Data Protection Regulation (GDPR) in the banking industry

An impact analysis on banks and wealth managers with the focus on Switzerland

pwc



Executive Summary

"Banks and wealth managers need a clear plan and strategy as to how to best analyse the impact of the regulation and to implement the standards until May 2018."

Considered by many as a milestone in privacy regulation, the EU General Data Protection Regulation (GDPR) opens a new chapter on data protection. The regulation aims at empowering individuals with regard to controlling the use of their personal data and at harmonising the patchwork of national data legislation across the EU to lay the foundation for a thriving digital single market.

For these purposes, the regulation introduces complex and far-reaching rights for data subjects and new obligations for data processors, such as privacy impact assessments and data breach notifications. To take up this challenge, banks need a clear plan and strategy as to how to best analyse the impact of the regulation and to implement the standards if applicable until May 2018.

This white paper discusses the challenges faced by the Swiss banking industry with the GDPR and proposes a clear approach as to how best to analyse and implement the GDPR and avoid GDPR related risks. In addition to the necessity of implementing the regulation, PwC sees opportunities as to how GDPR compliance can contribute to operational excellence and good reputation, prepare for digitalisation and substantially reduce future regulatory adjustment costs in the light of pending amendments to the Swiss Data Protection Act.

The Key Takeaways

- The regulation can be considered a milestone in data protection regulation with far-reaching effects not only for technology but also for traditional companies.
- The GDPR also applies to the processing of personal data of EU residents by banks not established in the EU, where the processing activities are related to the offering of banking services.
- GDPR compliant Swiss banks will be mainly compliant with the future revised Swiss Data Protection Act.
- As the GDPR holds the controller accountable for compliance and requires the bank to demonstrate compliance, implementation substantially affects a bank's data protection organisation.
- Besides facing substantial fines, depending on the gravity of a data protection breach it cannot be ruled out that market access for a company concerned outside the EU may be temporarily restricted as a result of measures taken by national data protection agencies.
- The efforts required to implement the regulation differ among banking segments.
- Key determinants of GDPR impact on a bank are the type of customers, the basis of interaction, the services offered and the IT systems involved.
- GDPR implementation contributes to operational excellence and offers reputational benefits for banks. It may also uncover and provide opportunities for further digitalisation.
- Well-structured databases make it easier for banks to adapt their front office towards a state-of-the art customer-centred relationship management including an appropriate and efficient client on-boarding procedure.

Glossary

Binding corporate rules	A set of binding rules put in place to allow multinational companies and organisations to transfer personal data that they control from the EU to their affiliates outside the EU (but within the organisation).
Special categories of personal data	Sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Consent	Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
Data concerning health	Any personal data related to the physical or mental health of an individual or the provision of health services to them.
Data controller	The entity that determines the purposes, conditions and means of the processing of personal data.
Data erasure	Also known as the 'right to be forgotten', it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.
Data portability	The requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller.
Data processor	The entity that processes data on behalf of the data controller.
Data protection authority	National authorities tasked with the protection of data and privacy and monitoring and enforcement of the data protection regulations within the Union.
Data protection officer	An expert on data privacy who works independently to ensure that an entity adheres to the rules, policies and procedures set forth in the GDPR.
Data subject	A natural person whose personal data is processed by a controller or processor.
Encrypted data	Personal data that is protected through technological measures to ensure that the data is only accessible/readable by those who possess the encryption key.
Personal data	Any information related to a natural person (data subject) that can be used to directly or indirectly identify the person.
Personal data breach	A breach of security leading to the accidental or unlawful access to, destruction, misuse, etc., of personal data.
Privacy by design	A principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.
Privacy impact assessment	A process used to identify and reduce the privacy risks of entities by analysing the personal data processed and the policies in place to protect the data.
Processing	Any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.
Profiling	Any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.
Pseudonymization	The processing of personal data such that it can no longer be attributed to a single data subject without the use of additional data, so long as said additional data stays separate to ensure non-attribution.
Recipient	Entity to which the personal data is disclosed.
Regulation	A binding legislative act that must be applied in its entirety across the Union.
Representative	Any person in the European Union explicitly designated by the controller to be addressed by the supervisory authorities.
Right to access	Also known as 'subject access right', it entitles the data subject to have access to and information about the personal data that a controller has concerning them

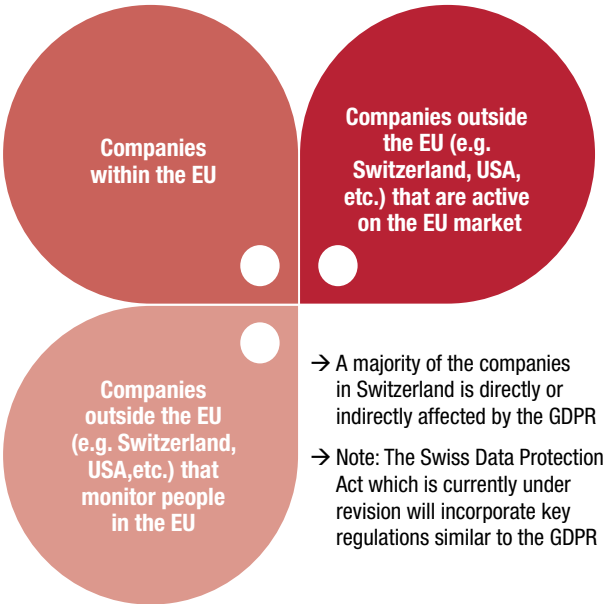
1. Introduction

"PwC's most recent experience shows that in the light of the extraterritorial reach of the GDPR and the large scope of data subjects affected, many banking executives in Switzerland are uncertain about the applicability and potential impact of the EU GDPR."

Financial institutions and financial industry service providers process a vast amount of personal data on a daily basis. Many of the data is confidential or even sensitive personal data. As a result of the EU's General Data Protection Regulation (GDPR), which was adopted in 2016 and will become directly applicable on 25 May 2018, banks will be subject to new legal-regulatory risks and will be increasingly in the focus of national data protection authorities (DPAs) in EU member states.

The GDPR aims to empower data subjects and it substantially expands their rights as a consequence. It also gives the DPAs new rights to audit banks and impose administrative fines which can amount to a maximum of EUR 20 million or 4 per cent of the global annual turnover of a company – whichever is higher.

Companies within the scope of the GDPR



→ A majority of the companies in Switzerland is directly or indirectly affected by the GDPR

→ Note: The Swiss Data Protection Act which is currently under revision will incorporate key regulations similar to the GDPR

A particular feature of the GDPR is its extraterritorial reach, which is stipulated in Art. 3. Besides applying to companies established in the EU, the regulation also applies to companies not established in the EU to the extent they target EU data subjects: *"[…] the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or […] the monitoring of their behaviour as far as their behaviour takes place within the Union."*[1]

Further, it is important to consider that the GDPR focuses on all data subjects. Hence, not only a bank's customers but all natural persons whose personal data a bank processes are within the scope of the regulation, even employees.

PwC's most recent experience shows that in the light of the extraterritorial reach of the GDPR and the large scope of data subjects affected, many banking executives in Switzerland are uncertain about the applicability and potential impact of the EU GDPR.

Reducing and managing uncertainty requires clear steps, such as identifying the data collected and processed as well as a proper legal assessment, embedding the specific business operations into the entire regulatory framework. And finally, a clear definition of requirements and risk mitigation strategies is essential.

[1] Reflecting decisions by the Court of Justice of the European Union (CJEU) related to the Data Protection Directive towards an increasingly strong extraterritorial application of EU data protection law.

2. The EU General Data Protection Regulation

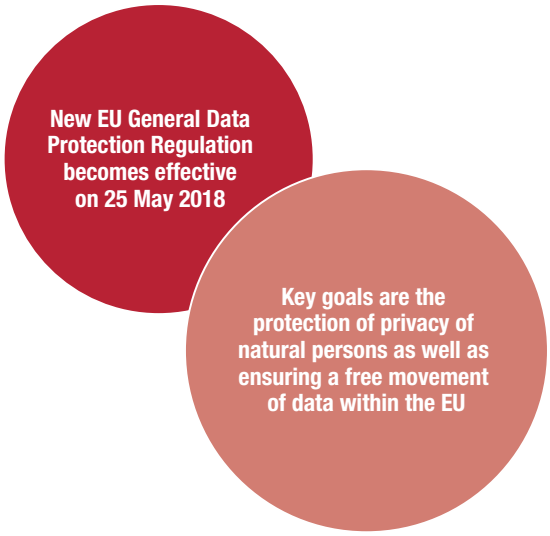
"The GDPR strongly impacts the digital industry, however reducing the relevance of the GDPR to tech-companies would also lead to missing the far-reaching effects on all other industries."

Considering the four years of negotiation involved and about 4,000 amendments made prior to its adoption, the GDPR can surely be considered a *milestone* in terms of data protection regulation; this also illustrates the substantial effects associated with this regulation. The regulation entered into force on 25 May 2016 and will become directly applicable on 25 May 2018.

The GDPR replaces the Data Protection Directive 95/46/EC and to a large degree harmonises the national data protection laws within the EU. It introduces a new *pan-European set of data protection rules* that are directly applicable in all EU member states. Due to its wide geographical scope, the GDPR will impact many companies outside the EU to the extent they target EU data subjects. Considering that Switzerland belongs to the world's leading financial hubs and – in that context – the importance of cross-border wealth management to Switzerland, the GDPR will substantially impact Swiss market players.

2.1. A Milestone in Data Protection Regulation

The GDPR strongly impacts the digital industry, however reducing the relevance of the GDPR to tech-companies would also lead to missing the far-reaching effects on all other industries.



The European Commission proposed the GDPR as an instrument to empower citizens and give them control over their personal data and to simplify the regulatory environment for *business in the course of digitalisation.* The regulation takes centre stage with regard to the realisation of the *digital single market,* a priority on the Commission's agenda. As a guardian of the single market and tasked with ensuring a level-playing field, the Commission is likely to closely monitor GDPR compliance by market participants domiciled inside and outside its territory. Although it is a regulation, the GDPR remains very vague, requiring careful interpretation and advice by data protection and legal professionals.

National Data Protection Authorities (DPAs) and the future European Data Protection Board will publish guidance to define best practices with regard to the application of the GDPR, which is likely to require ongoing legal impact assessments. With regard to sector specific guidance, for example financial services, the Commission and DPAs encourage drawing up of codes of conduct that should contribute to the proper application of the GDPR; these codes should take account of sector specific features when it comes to data processing and specific industry needs.

2.2. In the Aftermath: Focusing on the Right Spots

Although the GDPR has become an agenda point with high priority for companies across all industries, a recent PwC study showed that most firms are generally either not prepared or are still trying to make sense of the far-reaching ramifications of the GDPR related to concepts, such as data protection by design and default, data accuracy or data minimisation.[2]

Our experience in the Swiss banking environment shows that only recently has the GDPR become a topic on the regulatory radar of most Swiss banks. The applicability and scope of GDPR with respect to Swiss banks is the basic question, but banks also often ask for

[2] HP Enterprise/PwC - US - Survey and results.

more details on data privacy and data subject rights. We also often see that EU GDPR compliance is only handled in legal teams rather than as a cross-functional initiative. This is problematic due to the high impact on operations and the management of data processing as a daily business. Implementation of GDPR needs to be a joint initiative from all lines of service and all functions.

Another point is that many banks underestimate the effort required and the timeline they need to become compliant. We expect many banks will need a larger transformation initiative where several IT systems and the process landscape itself are affected and therefore wider change will be required. The deadline for compliance in May 2018 is tight in view of this.

Another hot topic among Swiss banks is the relationship between *banking secrecy* and the GDPR. In Switzerland, the financial privacy of citizens is legally protected by *banking secrecy.* Banking secrecy arises from banking legislation. Swiss banks are required to maintain confidentiality concerning the financial affairs of clients. Bank employees who violate that obligation are liable to prosecution. In light of that, some Swiss banks believe that they are already compliant with regard to data protection legislation. However, banking secrecy predominantly addresses the security of personal data within a bank in terms of confidentiality. Data protection legislation goes beyond preventing the disclosure of personal data. It governs the processing of personal data, provides rights to data subjects and confers duties on data controllers and processors. Therefore, complying with *banking secrecy* laws does not relieve Swiss banks from complying with data protection legislation.

3. The GDPR and Swiss Banking

"From 25 May 2018 on, the GDPR will apply without exception to Swiss banks and wealth managers actively offering cross-border services to customers domiciled in the EU."

The GDPR adds an additional layer of obligations to the already complex and highly regulated banking environment. Besides data protection legislation Swiss banks are subject to other regulations with strong personal data implications, such as Financial Market Supervisory Authority regulations on client data (i.e. FINMA Circular 2008/21 Annex 3), Know-Your-Customer (KYC) duties, record-keeping obligations (MiFID II) or the Automatic Exchange of Information (AEOI) in tax matters.

Documentation and archiving obligations constitute other tasks with a personal data dimension for banks. Hence, aligning regulatory initiatives is key to saving cost and effort when preparing with a solid foundation for upcoming regulations in the field of data protection and beyond.

Complying with the GDPR while observing all other obligations poses a significant challenge for banks in and outside the EU. Nevertheless, compliance will be a precondition to serve customers in the EU. Non-compliance will expose GDPR impacted Swiss banks to substantial legal risks and may ultimately trigger heavy administrative fines.

3.1. Applicability of GDPR

From 25 May 2018 on, the GDPR will apply without exception to Swiss banks actively offering cross-border services to customers domiciled in the EU. As a key pillar of the digital single market, it is unlikely that the Commission will tolerate a distortion of the level-playing field by companies domiciled outside the EU as a result of less strict data protection regulation. Thus, it can be expected that from 25 May 2018 on the Commission will put particular emphasis on GDPR compliance by foreign companies active on the EU market.

Although the powers of national DPAs in EU member states have been considerably broadened, doubts remain about the enforceability of the GDPR on businesses domiciled outside the EU. However, there is little doubt about its enforceability with regard to Swiss banks that in many instances have established subsidiaries in EU member states. A DPA could impose and collect GDPR related fines using a bank's assets in the EU. This may have repercussions on the legal setup of Swiss banks serving EU clients through subsidiaries in the EU.

3.2. Consequences of Non-Compliance with the GDPR

As already mentioned, the GDPR provides DPAs with new rights to audit and to impose administrative fines which can amount to a maximum of EUR 20 million or 4 per cent of the global annual turnover of a company – whichever is higher. In the case of Swiss banks with no physical presence or assets in the EU, DPAs in EU member states may find the enforcement of administrative fines for non-compliance with the GDPR particularly difficult, if not impossible. When issuing fines to companies in Switzerland, DPAs will have to rely on international mutual assistance in criminal matters from the Swiss State. Depending on the gravity of a data protection breach, market access for a company outside the EU could be temporarily restricted as a result of measures taken by national DPAs on an individual basis.

In any case, non-compliance with the GDPR by a Swiss bank is likely to trigger substantial reputational damage, especially with clients in the EU. Google's prompt compliance with the *Google Spain Decision* – stretching the reach of the EU Data Protection Directive in 2014 – suggests that even large international companies will generally prefer to comply with data protection enforcement notices, thus making the matter of practical enforcement irrelevant.[3]

Finally, while the procedure for enforcement of administrative fines for non-compliance is likely to remain uncertain and will have to be assessed on a case by case basis, claims by individuals will likely be treated differently. On the basis of private international law, application of the GDPR in proceedings against a Swiss bank is almost certain if the EU resident affected opts for the GDPR as the applicable law (and not the Swiss Data Protection Act). This option is also available to EU residents taking action in Swiss courts. While the applicability of foreign data protection law is not particularly new, given the much wider scope and new obligations that the GDPR entails compared to Swiss legislation, non-compliance with the GDPR entails high legal and financial risks.

[3] CJEU decision in Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12).

4. Avoiding GDPR Related Risks

"In most cases, Swiss banks and wealth managers aiming for compliance will be able to leverage on existing data protection mechanisms and IT security processes. However, an initial requirement for any GDPR compliance measures is a full picture of the personal data collected as well as of related data flows within a bank."

Given the *reputational and financial risks* that non-compliance with the GDPR involves, it is necessary for *Swiss banks and wealth managers* to assess their exposure to the regulation, and if results indicate the bank is within the scope of the GDPR they will have to assess their *readiness* to comply on the basis of their current data protection architecture.

In most cases, Swiss banks aiming for compliance will be able to leverage on existing data protection mechanisms and IT security processes. However, an initial requirement for any GDPR compliance measures is a full picture of the personal data collected as well as of related data flows within a bank. Given that the GDPR holds the controller accountable for compliance with the GDPR and requires it to demonstrate compliance (i.e. reversal of the burden of proof), GDPR implementation has far reaching effects on a banks' data protection organisation. In other words, a GDPR compliant bank will have to demonstrate that it has full control over the personal data it processes in the course of its business.

4.1. Identifying GDPR Impact on Banking

With regard to compliance and implementation, the GDPR impacts banking differently depending on the business segment. As far as customer data is concerned, much depends on the client segment, the basis of interaction and the services offered. All that determines the structure of personal client data

	Natural person client-related		Non-natural person client-related		
	Private Wealth/ Management Banking	Retail Banking	Corporate Clients	Asset Management	Investment Banking
Type of customer	Affluent & (ultra-)high-net-worth-individuals	Retail clients	Representatives of institutional clients, beneficial owners	Representatives of institutional clients, beneficial owners, potentially WM clients	Representatives of institutional clients, beneficial owners, potentially WM clients
Client interaction	Many direct client interactions, including sensitive data. For affluent clients more standardised/ digitalised than for the highly individualised (ultra-)HNW individuals	Standardised way of direct client interaction, more and more automated, standardised and digitalised	Very few and standardised information about natural persons	Mostly standardised and only limited information about natural person clients (except those banks that serve natural persons out of the AM division)	Mostly standardised and only limited information about natural person clients (except those banks that serve natural persons out of the IB division)
Services and products offered	Large variety of customised services and products	Standardised services and products	No services or products to natural person-based clients	No services or products to natural person clients (except those banks that serve natural persons out of the AM division). Potentially internal services for other segments	No services or products to natural person clients (except those banks that serve natural persons out of the IB division). Potentially internal services for other segments
Data type	Personal data and special categories of personal data (sensitive information)	Personal data (potentially limited sensitive data)	Personal data	Personal data	Personal data
Data structure	Many unstructured data	Structured and unstructured data	Structured data for natural persons	Structured data for natural persons	Structured data for natural persons
GDPR expected impact	**High**	**Medium**	**Low**	**Low to medium**	**Low to medium**

"The more complex the client's wealth structure, the more personal data banks will have."

processed by a bank. GDPR compliance is generally easier where data processing results in well-structured personal data. In addition, the larger the bank, the more complex its data structure is likely to be as a function of its legal setup (entities), diversity of operations and the data flows between and across divisions.

4.2. Impact of GDPR on Various Banking Segments

As the GDPR only affects natural persons, segments of business which are directly client related, such as *wealth management* and retail ranking, are more impacted by the regulation than other segments. While the focal point of this white paper is on customer data protection, it is important to remember that the GDPR applies to the processing of personal data of any EU resident. Thus, it may concern all sorts of personal data that can be found within a bank.

As a rule of thumb, *wealth management* with its high level of individualised services and client interaction will be most affected by the GDPR. A key feature of the *Swiss wealth management business model* and feel-good package is the broad selection of additional services, for example concierge services. Those services are provided by the actual client advisory and portfolio management sections. Inevitably, a substantial amount of sensitive data is collected in order to deliver such additional services; this includes information about a client's family, travel routes or health status. Moreover, it is a truism in banking that a relationship manager's assets are information about the client and the client's environment which is collected in order to best serve and meet the client's expectations. Here, banks face difficult legal questions, in particular with respect to special categories of personal data, such as health, religion or political affiliation.

As a consequence, the bank faces three key issues in the *wealth management segment*:

1. Currently, in most banks, data is spread across different systems and kept in various storage places. To comply with the GDPR, banks need to understand where and how the data is currently captured and saved and need to answer the question on how to structure processes for the future in order to have an easily accessible holistic view of client data.

2. It is assumed that wealth managers currently gather all kind of client information, even sensitive data, often unstructured. Banks have to decide how to deal with the data capturing and processing going forward, while retaining a comprehensive overview of data. Banks may implement a clear policy framework and further guidance in behavioural rules for client relationship managers to mitigate the risk of breaching GDPR.

3. How to handle collected personal data pertaining to the *client environment,* such as information about friends and a client's family?

In view of the significance of cross-border *wealth management* for Swiss banks, it is also important to address the transfer of personal data. This will involve interaction with a bank's other business divisions, mainly *investment banking* on the product side.

Retail banking faces similar challenges to *wealth management with respect to regular interaction with natural persons.* However, in contrast to the latter, *retail banking* – thanks to its service-channels – benefits from personal data collection that is much more standardised and less recurrent or individualised. Digitalisation can be expected to contribute to standardisation, in particular, with respect to how personal data is processed in *retail banking.* Finally, Swiss banks' retail clients are in most cases domiciled in Switzerland and are thus mostly outwith the scope of the GDPR.

To become compliant with the GDPR banks may have to substantially redesign business processes, in particular in the *retail banking* and *wealth management segments.* This is likely to have a considerable impact on client life-cycle management for a bank, i.e. the different phases of a client relationship: prospecting, on-boarding, servicing/ cross-selling, and up-selling and termination.

Therefore, any GDPR implementation measure in the context of client personal data should be carefully elaborated to reduce any negative effects on a bank's business to a minimum. The picture is different in the *corporate banking, asset management* and *investment banking* segments. These divisions only, or mainly, deal with *institutional clients* and thus, *legal persons.* Hence, for most banks, the interaction with natural persons is limited to representatives of institutional clients and ultimate beneficial owners, and such dealings are based on standardised, or even automated, processes. This data is generally limited to contact and identification details and is in a structured format. Implementing the GDPR in these banking segments would seem to be less complex.

Irrespective of banking segment, transaction data – the largest data set held by banks – is an important topic. It comprises inter-bank transactions, transactions to third parties and cross-border transactions. As transaction data can lead to identification of a client, it is considered to be personal data under the GDPR.

4.3. Impact of the GDPR on Data Protection Governance

GDPR implementation has far reaching effects on a bank's data protection organisation. Besides demonstrating that it has full control over the personal data it processes in the course of its business, a bank will have to demonstrate that it complies with the GDPR principles for data processing as well as with all other obligations required under the regulation.

Information duties	Rights of data subjects	Data protection by design and default	Consent to data processing
Banks will have to inform data subjects proactively and in detail on how their personal data is processed (e.g., by data privacy statement).	Banking clients will benefit from expanded rights, such as access to personal data, the right to object to processing, correction of inaccurate data, data portability and erasure of data.	Systems for data processing have to be designed to ensure best possible data protection from the outset (i.e., compliance with the principles of transparency, of data minimisation, of proportionality, etc.).	Where consent is required, it will become more difficult to obtain it. In addition, consent may be withdrawn at any time.

Documentation	**Data protection impact assessment**	**Technical and organisational security measures**	**Data protection officer**
Companies will have to document data processing comprehensively to show GDPR compliance ("data protection" and "run the bank" frameworks).	An impact analysis will be necessary if certain categories of personal data (e.g., health, racial and ethnic origin, political opinion, etc.) are processed or processing of personal data is used for profiling.	Companies have to apply measures to protect personal data (e.g., data protection procedure, including controls and use of encryption)	Some banks may have to designate a data protection officer, e.g., if they process special categories of personal data or systematically monitor people on a large scale.

Personal data breaches	**Outsourcing**	**Representative in the EU**	**Data protection governance**
Companies have to notify the loss or unauthorised disclosure of data, within 72 hours if feasible. On a case by case basis, this also requires notification of the individuals affected.	New responsibilities and stricter requirements for service providers (e.g., IT outsourcing, accounting, marketing, HR, etc.)	Some companies not domiciled in the EU may have to designate a representative in the EU if they process personal data of or monitor EU residents.	Banks will have to document compliance with the GDPR. This will require them to seek and implement various IT and organisational solutions to create a performing control framework to ensure compliance.

5. Turning the Regulation into a Benefit

The majority of banks serving customers residing in the EU will opt for compliance with the GDPR. It is a compliance journey which will not only affect how data processing is governed but may also alter business processes and require significant amendments on IT systems.

Thus, implementation of the GDPR may also contribute to operational excellence and uncover and provide opportunities for further industrialisation and digitalisation in the banking industry as well as opportunities for reshaping towards a state-of-the-art front-office.

5.1. Contributing to Operational Excellence, Cybersecurity and Reputation

An important aspect of GDPR implementation is the contribution it can make to operational excellence. A large problem that the majority of banks share across all business segments is IT legacy. To date, it seems to us that implementation of the GDPR would involve banks not only addressing implementation from a purely organisational and governance point of view, but also simultaneously addressing their IT legacy.

Many retail banks will have to optimise operational processes in the front office and shift towards state-of-the-art client relationship management and CRM solutions. Wealth management will have to decide on how to structure its data landscape to best address client relationship management in a digitalised world.

Besides contributing to operational excellence and cyber-defence capabilities, the GDPR provides an opportunity for Swiss banks to differentiate themselves from competitors and to be perceived as forerunners in terms of taking client data protection seriously, in particular after the reputational downturn experienced in connection with banking secrecy. In an increasingly digital world, in which banking has to move towards new business models and provide new value positions to clients, demonstrating true responsibility towards the treatment of personal data and customer rights is a key driver toward sustainable long-term growth as it will positively contribute to strong client-bank relationships. Third-party risk management is a related topic that can also be addressed within the GDPR context.

5.2. Uncovering Opportunities for Industrialisation and Digitalisation

A key side effect of GDPR implementation is that structuring data effectively will open up new opportunities for further industrialisation and digitalisation efforts. As a consequence, banks will be able to structure their processes more efficiently and effectively and avoid duplicated processes. Data will flow more smoothly within the bank, reaching the appropriate receiver quicker and allow for effective cost reduction as well as raise employee productivity and efficiency.

Today, banks collect a lot of data. However, substantial efforts are required for employees to obtain and process a bank's collected data. Structuring data and data flows permits to overcome that issue. In addition, well-structured databases make it easier for banks to adapt their front office towards a state-of-the art customer-centred relationship management including an appropriate and efficient client on-boarding procedure. This enables banks to gain a more holistic view of clients and to operate more efficiently on the sales side, not least with regard to client on-boarding and risk management.

Structuring data also raises the effectiveness of outsourcing which benefits of transparent and well-structured data flows as well as evident interfaces. This allows the implementation of agile applications. Thanks to the growing number of fintech and digital solution providers, banks will be able to offer a new variety of data-based services and products.

Finally, the reputation for security and integrity of established banks will remain a competitive advantage difficult to match by the new competitors from the fintech industry. Going forward, those banks will in the long-term substantially benefit of the GDPR as they reap the benefits of industrialisation and digitalisation in the banking industry and match them with their already strong reputation for security and integrity.

5.3. Complying with the Future Revised Swiss Data Protection Act

An additional side effect of GDPR implementation for Swiss banks consists in early compliance with the future amended Swiss Data Protection Act. The first draft of the revised Swiss Data Protection Act was published in December 2016. The proposed amendments are intended to adapt the existing law so as to align it with past and present developments at European level, in particular the amendments introduced into EU law by the GDPR.

Given that a substantial number of Swiss companies provide services to EU residents, it would be surprising if the revised Swiss Data Protection Act would deviate substantially from the provisions of the GDPR. With a data protection law granting data subjects served by Swiss companies the same rights as in the EU, the chances that the Swiss Data Protection Act will continue to benefit of an adequacy decision by the European Commission remain high. EU companies will be permitted to transfer personal data to companies in Switzerland without the need for additional safeguards.

6. The Right Approach to Tackle Complexity and Deliver

"PwC's five-step transformation framework has proven very efficient and effective in addressing GDPR implementation from a strategic and project management angle."

6.1. How to Meet GDPR Requirements Most Effectively

The GDPR is a complex piece of legislation which will put some banks under significant pressure to transform. The window of opportunity for implementation of the GDPR prior to 25 May 2018, when it will become directly applicable, is closing quickly. PwC suggests that banks combine decisive and bold steps with a risk-based approach to tackle GDPR implementation.

The starting point is an analysis of the bank's existing data protection setup, and personal data collected and processed, followed by a comprehensive analysis of gaps with regard to the requirements of the GDPR. This first phase is the heart of GDPR implementation and it can be performed separately from other steps. It includes an impact assessment and is essential to define the scope of the work required.

In PwC's experience the majority of banks require an end-to-end transformation and implementation approach to meet the conditions of the GDPR. It is important not to underestimate the complexity, e.g., with respect to a potential data structure transformation, organisational change and a larger contract amendment exercise for data subjects and third parties. However, several key factors define the effort for banks: the size, the complexity of services and products, the process and IT landscape, and the current compliance and regulatory set-up.

Thanks to our experience and to our many experts in the sector, we are able to keep costs low and minimise the risk of incompleteness, and are able to support your business in becoming compliant with the EU GDPR in an efficient and thorough way.

Executives designing GDPR compliance architecture should consider four critical building blocks: strategy, legal, data security and IT. PwC provides a holistic approach which consists of sustainable strategies that help your business adapt to the GDPR while reducing costs and leveraging talent, as well as tailor-made legal advice and outstanding IT solutions. In parallel, data security identify and mitigate risks around client and operational data. The proper combination of these four building blocks can help a bank to adapt to the complex challenge that GDPR compliance poses and exploit business opportunities to gain a competitive advantage.

PwC's five-step transformation framework has proven very efficient and effective in addressing GDPR implementation from a strategic and project management angle. It is a tested approach to performing large-scale transformation projects and smaller change initiatives, ensuring completeness and minimising risks. It brings transparency about what is required and what we do and gives you a complete overview that simplifies planning and budgeting. The framework can also be tailored easily to answer clients' specific needs.

6.2. Benefits from the PwC's Approach

The GDPR is a common regulation for all industries but is specifically meant to be implemented in various industries, and is even specific to single institutions. PwC has a clear strategy and approach so we can start immediately and efficiently work together with your people. Due to the complexity involved, an end-to-end approach is recommended, although for most banks an early assessment should be considered first.

Besides identifying specific impacts on the banking sector and the challenges it faces, PwC has identified several similarities across industries and institutions that lower the burden of implementation and ease complexity in application of the GDPR. Due to many GDPR engagements, we are committed to easing the process and aim at increasing efficiency and effectiveness.

This allows us to quickly identify ourselves with your needs, and we keep informed about potential upcoming regulatory amendments: we carefully analyse what is needed and what is not. In addition, PwC leverages your existing require-

ments listed into the GDPR standards and guidelines with other requirements (i.e., FINMA Circular 08/21 'Operational risk', FINMA Circular 08/07 'Outsourcing') to put them into the context of your risk environment and risk appetite.

You benefit from a broad spectrum of practical tools (specific work programmes) and pragmatic approaches on implementing the standards required. Most importantly, you get every service required from one source.

Our experts receive ongoing training on the GDPR and surrounding data protection regulations. They are used to managing operational excellence and IT transformation initiatives, delivering fast and precise results. But most importantly, our experts have practical experience on GDPR programmes that allows them to leverage the best approaches and tweaks. As a multi-disciplinary division, we are uniquely placed to help you adjust to the new environment. Our data protection team includes lawyers, consultants, cybersecurity specialists, auditors, risk specialists, forensics experts and strategists. If needed, our team is global, proposing innovative solutions with on the ground expertise in all the major EU economies.

1 Understanding and Assessment	2 Strategy and Set-up	3 Design	4 Implementation	5 Operating (Run-the-Bank)
Assessment of the current data protection governance, compliance set-up and legal entities to ensure completeness	Development of an action plan and strategy set-up, including a project charter and project plan	Development of a risk assessment programme, amended data structure and change design	Ensuring a seamless integration of new designs for all applications and processes	Conduct a completeness assessment to ensure GDPR compliance
Develop data inventory to understand the full scope of data affected and assessment of data subject types	Outline implementation-roadmaps in consideration of the right legal paths, incl. third-party risk management	Create data flow diagrams of business processes and overview of flows between the business processes and applications	Amendments of contracts, where applicable, e.g. to receive consent	Establish/enhance data privacy training and awareness programme for employees
Analysis of the (i) data structure, (ii) IT architecture, (iii) process structure and (iv) data transfers	Define design principles for changes required and desired by the bank as well as definition of change priorities	Outline organisational changes where applicable	Implementation of new policy compliance programme and frameworks	Develop a communication plan for all relevant stakeholders and an incident response process for data breach cases
Screening and grouping of unstructured data supported by existing PwC tools Dathena and Online Collaboration tool	Analysis of data processing purposes and their legal grounds	Design of a fully automated data subject right management process	Implement risk management frameworks	Ensure an ongoing compliance assessment and completeness of the compliance framework
Analysis of products und services offered in order to understand what kind of data is collected/processed in which area	Analysis of required contract amendments, including third parties	Develop and design frameworks concerning the (i) management of privacy, (ii) roles & responsibilities and (iii) governance & reporting	Implement or amend data transfer flows and amend interfaces to third parties, where required	Establish an emergency plan for data breaches and other potential violations of GDPR

Contacts

PwC
Birchstrasse 160
Postfach, 8050 Zürich

Susanne Hofmann-Hafner
Director, Tax and Legal
+41 58 792 17 12
susanne.hofmann@ch.pwc.com

Patrick Akiki
Partner, Advisory
+41 58 792 25 19
akiki.patrick@ch.pwc.com

Reto Häni
Partner, Cybersecurity
+41 58 792 75 12
reto.haeni@ch.pwc.com

Authors

Dr. Idir Laurent Khiar, Kristof Trautwein, Anna Huber, Johannes Stamm

We thank Nicolas Vernaz and Andrea Ullrich for the valuable contributions to this paper.