The General Data Protection Regulation in Financial Services Industries: How Do Companies Approach the Implementation of the GDPR and What Can We Learn From Their Approaches?

Manuel Holler
Zurich University of Applied Sciences
Institute for Marketing Management
manuel.holler@zhaw.ch

Benjamin van Giffen
University of St.Gallen
Institute of Information Management
benjamin.vangiffen@unisg.ch

Seth Benzell
Massachusetts Institute of Technology
Initiative on the Digital Economy
sbenzell@mit.edu

Matthias Ehrat
Zurich University of Applied Sciences
Institute for Marketing Management
matthias.ehrat@zhaw.ch

Abstract

This research study sets out to explore the General Data Protection Regulation in financial services industries grounded on the pivotal question: "How do companies approach to General Data Protection Regulation and what can we learn from their approaches?". Regarding the former, a three-stage iterative and risk-based implementation approach was unveiled, regarding the latter, good practices for implementation at a strategy-, organization-, management-, process-, and technology-related level were identified. Notwithstanding the inherent limitations by the applied case study research at leading companies in finance and insurance business, it can be concluded that companies strive with the utmost effort to ensure compliance with the General Data Protection Regulation, yet there exists a gap between strategy and implementation.

1. Introduction

In our digital and global world, the amount and flow of data is growing exponentially. Recent statistics by management consultancy McKinsey & Company [1] demonstrate this growth. The flow of data has risen by the factor 45 from the year 2005 to 2014 [1]. Thereby, personal data which means "any information relating to an identified or identifiable natural person" [2:111] represent particularly relevant and sensitive data. This dramatic increase has fostered legislation to create adequate policies to cope with this development [2,4]. With the General Data Protection Regulation of the European Parliament and the Council of the European Union introduced as harmonized regulation officially passed in Brussels on April 6, 2016, companies were expected to be compliant as of May 25, 2018 [2].

While the question "Why to be compliant with the General Data Protection Regulation?" is widely acknowledged, the issue "How to be compliant?" currently leaves several open questions in research [3,4] and practice [5,6]. The implementation of such a multi-faceted regulation is highly complex, so how should companies arrange their strategies, organizations, processes, and technologies? In this sense, this research study adopts an information systems perspective, focusing on technology in use [7,8]. Despite the timeliness and relevance of data privacy regulations in general and furthermore the recency of the General Data Protection Regulation in particular, little empirical work and insights from the field are available [3,4,9].

Thus, the objective of this research is to study the General Data Protection Regulation in different financial services industries in the DACH region. In particular, we aim to have a look behind the scenes in a first step and strive for the identification of good practices for implementation in a second step. The central research question is: "How do companies approach the implementation of the General Data Protection Regulation and what can we learn from their approaches?" This question is answered leveraging in-depth insights by case study research [10,11,12] at leading companies in finance and insurance business. Particularly, interactions with stakeholders (e.g., Data Privacy Officers, Program Managers GDPR) brought new facts to light.

This research study exhibits the following structure: Section 2 provides the background in terms of the General Data Protection Regulation and related work. Section 3 sketches methodical details on data collection and data analysis. Section 4 presents insights from the implementation approach and derives good practices for implementation. Section 5 features the conclusion in terms of discussion, limitations, and future work. Section 6 closes by an appendix.

2. Background

2.1 General Data Protection Regulation

The General Data Protection Regulation is a complex set of individual rules [2]. At a glance, "this regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data" [2:108]. From a temporal perspective, the General Data Protection Regulation was passed on April, 6 2016 given a time frame of two years to be compliant: May, 25 2018 [2]. Thereby, the Data Protection Directive 95/46/EC [13] can be considered as antecedent. Contextually, the General Data Protection Regulation can be regarded as cornerstone among other regulations [2,4]. From a structural viewpoint, the regulation comprises eleven chapters and 98 specific articles [2]. Figure 1 illustrates the structure of the General Data Protection Regulation. In the following, a brief summary of each chapter with focus on key characteristics and central alterations is given, based on the original document [2] and a well-established interpretation [4].

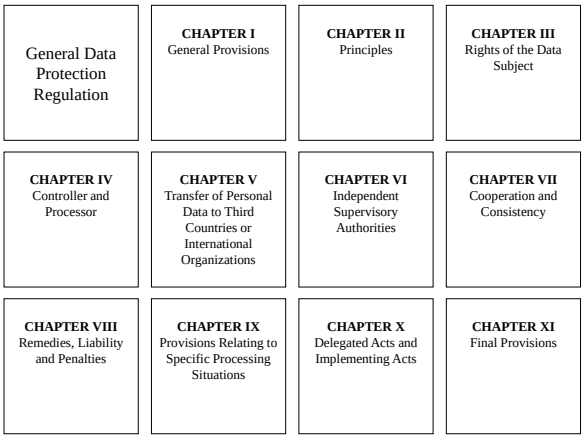

Figure 1. Structure of the General Data Protection Regulation [2]

Chapter I "General Provisions" contains general provisions such as objectives, scope, and definitions. In this context, the objective as comprehensive and harmonized regulation for the member states, the material scope of data processing and the territorial scope of EU citizens as well as EU companies can be considered as main characteristics. In Chapter II "Principles" fundamental principles related to the handling of personal data are introduced. Here, the topic of lawfulness and aspects of consent of the data subject for processing stand in the center as novel topics. Over all details of the regulation, the handling of personal data should follow "lawfulness, fairness and transparency, purpose limitation, accuracy, data minimization, storage limitation, integrity and confidentiality" [2:117].

Chapter III "Rights of the Data Subject" strengthens the rights of the data subject (i.e., natural person). Beside a reframing of existing rights, particularly novel rules such as the "Right of access by the data subject", "Right to rectification", "Right to erasure (Right to be forgotten)", "Right to restriction of processing", and "Right to data portability" can be highlighted. In Chapter IV "Controller and Processor" further obligations are imposed on the controllers and processors (i.e., companies). In organizational terms, the mandatory introduction of Data Protection Officers represents a novelty. Furthermore, in technological terms, Privacy-by-Design and Privacy-by-Default are innovative principles. In processual terms, enhancements such as an assessment of potential privacy impacts in early stages and an obligatory notification of data breaches at later stages are introduced. Insofar, the accountability over the lifecycle becomes more relevant. Beyond, the role of Codes of Conduct is strengthened.

Chapter V "Transfer of Personal Data to Third Countries or International Organizations" regulates the transnational data processing. Although some minor modifications in terms of data transfer to countries out of the European Union are adopted, no major changes compared to the previous regulation exist. In Chapter VI "Independent Supervisory Authorities" the regulatory authorities are empowered. This refers on the one hand to the creation of novel authorities, but also to the strengthening of existing ones. In this context, the "One-Stop-Shop" represents a novelty which aims at a distinct distribution of responsibilities for the sake of improving efficiency and effectiveness of data protection activities.

Chapter VII "Cooperation and Consistency" addresses the relationship of the different authorities. In this sense, the communication and interworking between the inter- and intra-country supervisory authorities are stipulated. Beyond, for example, the European Data Protection Board is created as novel body to "ensure the consistent application of this regulation" [2:229]. In Chapter VIII "Remedies, Liability and Penalties" effects of non-compliance are referred. In order to leverage compliance with the General Data Protection Regulation to the top management level, revenue-dependent administrative fines up to four percent of the group sales are introduced. In contrast, compensations for the data subjects in the case of rule-breaking are defined as well.

Chapter IX "Provisions Relating to Specific Processing Situations" offers specifications regarding individual situations. As example, for the purpose of science or art, minor derivations from the regulation are nominated. Finally, the last two chapters X "Delegated Acts and Implementing Acts" and XI "Final Provisions" refer in a great measure to administrative matters.

2.2 Related work

As a matter of principle, the area of data privacy can be viewed from different scientific angles, such as legal, psychological, or technological perspectives [14,15]. As a socio-technical phenomenon, the information systems community also exhibits a well-established tradition on data privacy research [14,15]. In their seminal work, Smith et al. [14] present the APCO model which depicts the antecedents (e.g., privacy experiences, privacy awareness, and personality differences) and outcomes (e.g., regulation, behavioral reactions, and trust) of the privacy concern concept. This model and its further development [14,16] served many empirical studies as foundation. To summarize the reviews by Smith et al. [14] and Bélanger and Crossler [15], data privacy is a multi-layered concept with the companies' responses to it as important area of research [17].

The announcement of the General Data Protection Regulation has led to another wave of interest in and publications on the topic in domains such as law [18,19,20] and management [3,21,22]. Particularly for the information systems domain, aspects of Privacy-by-Design [23], the communication of compliance [24], and the management of data privacy breaches [25] have been subjects of interest. With the purpose to identify literature which guides organizations in the implementation of the General Data Protection Regulation, a review according to established guidelines [26,27,28] was performed. After the scope determination, we conceptualized the topic (e.g., General Data Protection Regulation, GDPR; implementation, realization) and searched, analyzed, and synthesized the literature (e.g., Google Scholar, Scopus, Web of Science; time period of five years, inclusion and exclusion criteria) [26,27,28].

As main results, Voigt and von dem Bussche [4] present a process model on General Data Protection Regulation implementation comprising a gap analysis, risk analysis, project conception, and implementation. Similarly, a technically oriented privacy engineering methodology [29] has been proposed which differentiates between goal-oriented and risk-based privacy requirements elicitation. Furthermore, literature suggests some frameworks supporting the transitioning towards compliance [9,30]. Such works typically show a rather static, informing than a dynamic, action-oriented character [9,30]. Also in this context, Tikkinen-Piri et al. [3] list guidelines for the practical implementation of the General Data Protection Regulation purely derived from the law itself (e.g., "Specifying data needs and usage" [3:147]). Additionally, from the perspective of risk minimization, Bauer [52] suggests a six-step approach for the implementation (e.g., "Raise awareness enterprise-wide" [52:14]).

In summary, these research works show a methodical research gap [31]. Most works are based on conceptual deliberation [3,4,9], far too little attention has been paid to empirical work on this novel phenomenon. In particular, practice-based qualitative research [10] has been neglected. Such research however is highly relevant as Almeida Teixeira et al. name the "lack of practical guides or standard procedures" [53:416] as critical barrier in the successful implementation of the General Data Protection Regulation.

3. Research methodology

The objective of this research is to study the implementation of the General Data Protection Regulation in financial services industries in the DACH region. Accordingly, case study research to understand how companies approach this highly contemporary and interwoven phenomenon can be seen as an advantageous scientific method [10,11,12]. Thereby, the companies act as cases of the multiple-case study, the activity of implementing the regulation serves as embedded unit of analysis [10].

Concerning the data collection, the context of the European DACH region as highly successful economy and role model in terms of digitalization and data privacy in the sense of a purposeful sampling [32] was selected. Especially the financial services industries are characterized by strong regulation and well-experienced in compliance, thus offer insightful views [10]. Our sample merged in two main industries, namely finance and insurance [32]. Both High Street Banks are credit institutions with significant size and international relevance. The Private Bank offers financial services to wealthy individuals. All General Insurances offer a portfolio to privates and corporates, whereby Insurance & Bank extends its offer to additional financial services. Furthermore, additional companies and organizations were involved [32]. Machinery Financial Services deals with renting and leasing of heavy industrial equipment. The Specialized Consultancy offers customized help, while the

Economic Organization deals with the overarching role of data privacy in the economy. Finally, the Start-up Company is active in the domain of eCommerce. The General Data Protection Regulation also represents a major challenge for countries outside the EU, as the Switzerland- and Liechtenstein-based enterprises hold customers and employees with EU nationality which fall under this regulation [2,4].

Business	**Interviewee**	**Head-quarters**	**Employees**
High Street Bank **	Lead GDPR Implementation Program	SUI	40,000+
High Street Bank **	Program Manager DP Initiatives	SUI	50,000+
Private Bank **	Head of GDPR Implementation Project	LIE	3,000+
Insurance & Bank **	Head of GDPR Implementation Project	SUI	7,000+
General Insurance **	Compliance Counsel	SUI	5,000+
General Insurance **	Program Manager GDPR	SUI	4,000+
General Insurance **	Head of Corporate Security	SUI	3,000+
Machinery Financial Services **	Chief Information Officer	GER	25,000+
Specialized Consultancy °	Senior Privacy Consultant	SUI	10+
Start-up Company **	Chief Executive Officer	GER	10+
Economic Organization °	Attorney	SUI	100+
GDPR implementation maturity		Just started * Work in progress ** Fully implemented *** Not applicable °	

Table 1. Foundations of the research study

In detail, semi-structured interviews [33,34] with project leads responsible for the realization of the General Data Protection Regulation provided the main evidence. These were mainly rooted in IT departments, but also in legal or compliance departments. Table 1 visualizes these foundations of the research study. More precisely, this interviewee sample comprised a balanced ratio of five female and six male experts with at least five years of experience in the data privacy area. During the interviews iterated interview guidelines [33,34] including a study overview, interviewee and company background, trends and challenges, organization, process, and technology perspective, reflection, and conclusion directed the conversation. The complete final version of the guidelines can be found in the appendix. The duration of the interviews was between 32 and 65 minutes with an average of 46 minutes. Subject to availability internal documents were used for triangulation [10]. In this context, all implementing companies (i.e., except Specialized Consultancy and Economic Organization) provided at least one management presentation or strategy paper. Private Bank even supported the triangulation by supplying analysis tools and preliminary results.

Concerning the data analysis, the audio records and written transcripts of the interviews [35,36] built the foundation for the qualitative text analyses [37,38,39]. Particularly, the analysis steps open, axial, and selective coding [37,38,39] were conducted to carve out the outcomes on a systematic basis. In this process, the focus lay on the identification of the implementation approach and good practices. Therefore, the data reducing activities were informed by established frameworks [40,41,42]. An initial round of coding was conducted by the first author, another round was accomplished by the second author. Both coders used the software tool NVIVO [36]. The code book showing the data reduction is available upon request. Ultimately, the findings of the research study were validated with further practitioners from financial services industries in the methodological setting of a focus group [43,44,45]. Involving iterations, the study conception took place from November to December 2017, the data collection and data analyses from January to May 2018, with the validation workshop held in July 2018.

Qualitative research is susceptible to sparse scientific rigor [46,47,48]. To counter this weakness, we leveraged entrenched case study guidelines [10,48]. In particular, in the data collection phase we applied techniques like audio recording [35] and triangulation of sources of evidence [10]. In the stage of data analysis steady sense making [48] and multi-coding [49] was employed.

4. Results

4.1 Implementation approach

Although the General Data Protection Regulation can be considered as a milestone in data privacy, corresponding activities have been pursued before and

after this regulation. Thus, the implementation approach can be understood as a major cycle in recurring data protection activities. Generally, this approach consists of three iterative phases "Stage I Appraise", "Stage II Strategize", and "Stage III Realize". As a matter of principle, the implementation of the General Data Protection Regulation is approached in a risk-based manner. Hence, companies focus on the parts of the regulation which entail the largest impact – from a monetary and non-monetary perspective. Subsequently, after this first cycle the maturity is enlarged and the risk is reduced in an iterative manner. In brief, Figure 2 visualizes this implementation approach of the General Data Protection Regulation which emerged from the data. Below, each stage is detailed with emphasis on distinguished matters from the cases.

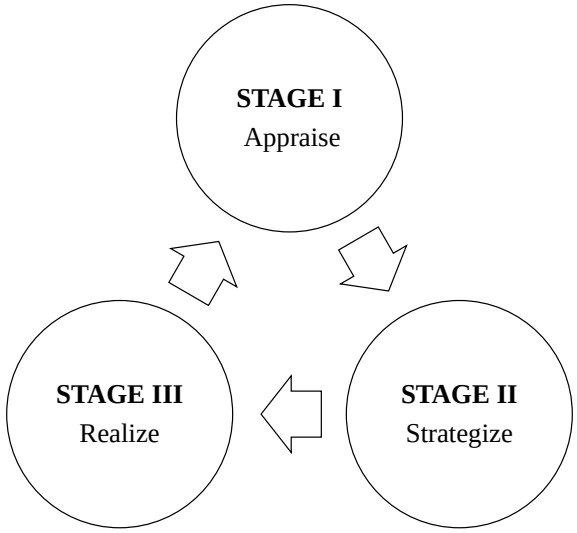

Figure 2. Implementation approach of the General Data Protection Regulation

4.1.1 Stage I "Appraise"

The first stage "Appraise" comprises aspects of grasping the General Data Protection Regulation and furthermore understanding its impact on the enterprise. Fundamentally, this phase begins with a simple reading and work-up of the regulation by a corresponding project team. This is followed by an initial assessment focusing on the gap between the as-is and to-be situation within the organization. Overall, the attitude towards data protection is clear, yet executives consider this evaluation as essential step: "It is a compliance project, it is a must-do project, nevertheless the first step is to convey decision makers to make decisions." (Compliance Counsel, General Insurance).

Regarding the organizational structure, legal-driven, compliance-driven, and information technology-driven data protection activities are dominant. For example, a Swiss insurance assigned the data protection project to the compliance department with the CEO as direct sponsor. In contrast, more unconventionally, the project is managed by the marketing department with the CTO and CIO as co-sponsors at another Swiss insurance. In any case, a highly interdisciplinary and collaborative approach between compliance, legal, business, and technology becomes nascent: "The subject matter makes it absolutely necessary to work highly interdisciplinary." (Senior Privacy Consultant, Specialized Consultancy).

Principally, the role of partners is considered as divergently. For one, some companies – particularly rather medium-sized and non-digital ones – consider external partners such as consultancies and law offices as essential support. In this sense, one manager even pointed out: "In the case of a law suit, we will have American circumstances, the companies with the best attorneys will win." (Head of GDPR Implementation Project, Insurance & Bank). For another, some enterprises fend for themselves: "Even established consulting companies need to pass through the learning curve, and beyond that, data protection needs to come from the innards." (Compliance Counsel, General Insurance).

Challenges in this initial stage arise from several sides. First, from a regulatory perspective obstacles emerge from the novelty of the regulation: "The GDPR is pretty new, had several evolution steps, and features several ambiguities." (Lead GDPR Implementation Program, High Street Bank). Second, from the company viewpoint obstacles arise from the fact that the understanding of data protection, but also the corresponding infrastructure is not very developed: "The process and application landscape is highly heterogeneous in the different subsidiaries." (Lead GDPR Implementation Program, High Street Bank).

In sum, most organizations in the finance and insurance domain are confident: "The customers are approaching us on a basis of trust. Other industries have more challenges than the banking industry." (Lead GDPR Implementation Program, High Street Bank).

4.1.2 Stage II "Strategize"

The second stage "Strategize" exhibits issues of working out a suitable strategy to approach the General Data Protection Regulation. This usually comprises the translation of the regulation into a data protection governance framework at a macro level and into detailed requirements at a micro level. Grounded on

the initial assessment and in line with the risk-based approach commonly focal areas are defined: “We defined a “cook book” which is an interpretation aid to translate the articles into a list of requirements. Then, we broke down our activities into 22 main areas.” (Head of Corporate Security, General Insurance).

Referring to the cognition as an opportunity or threat, the perspectives are ambivalent. On the one hand, enterprises are discernible that solely aim for compliance with the General Data Protection Regulation: “Our company simply accomplishes the things it is forced to, no further investments to fuel positive ancillary effects are placed.” (Compliance Counsel, General Insurance). On the other hand, more and more companies leverage the initial efforts to foster digitalization: “We see that as an absolute opportunity to do our homework.” (Program Manager GDPR, General Insurance).

A major mistake is the estimation that the General Data Protection Regulation covers “everything”, all areas of the company and every country: “Initially our scope was far too wide, a scope reduction of areas and countries was necessary.” (Program Manager DP Initiatives, High Street Bank). For one, for example, clients, employees, shareholders, beneficial owners in a retrospective, current, and prospective manner are defined as main data subjects. For another, in the highly global business structures, commonly frameworks are defined as a Swiss company can be a subsidiary of a European company or can have own subsidiaries in Europe.

In order to operationalize the strategy, commonly a variety of working packages are initiated: “Furthermore, we set up a (1) core stream, (2) business requirements stream, (3) legal stream, (4) IT stream, (5) data transfer process stream, (6) data breach incident handling stream, (7) group policy and control processes stream, and (8) sourcing stream.” (Program Manager DP Initiatives, High Street Bank).

To summarize, companies are making strong efforts to conceptualize and plan the implementation approach of the General Data Protection Regulation: “Meanwhile, we have implemented our governance framework – the approach how to do it.” (Head of GDPR Implementation Project, Private Bank).

4.1.3 Stage III “Realize”

The third stage “Realize” features facets of implementing the actions defined of the General Data Protection Regulation at a technological level. The technology is often not paid much attention, as companies expect major technology vendors to provide ready-made IT solutions: “We focus on the activities related to customers, employees, and regulatory authorities.” (Head of GDPR Implementation Project, Private Bank). During the whole implementation process continuous exchange – for example in the form of workshops with universities – is indispensable: “What are you doing? What methods and technologies do you use? How far are you?” (Program Manager DP Initiatives, High Street Bank).

In this stage, the challenging alignment between business and IT becomes nascent: “The IT raises the claim to requirements from the business, and in contrast the business demands for the technological possibilities by the IT.” (Compliance Counsel, General Insurance). More deeply, the obstacles are in the details: “How to deal with a Swiss person living in the EU and having an accident? How to handle a member of the EU applying for a job in Switzerland?” (Head of Corporate Security, General Insurance). Beyond, particularly the heterogeneous legacy IT in the different countries poses challenges: “We are not a start-up which can implement data protection by-design.” (Compliance Counsel, General Insurance). Insecurities regarding the feedback emerge as well: “We cannot estimate how many requests we will have. Will we be swamped? Will there just be a few?” (Head of GDPR Implementation Project, Private Bank).

In total, instead of concrete solutions at a technological level, in the first instance strategic and conceptual elements are developed: “We work hard until May 2018, but we have to admit that we will not have addressed all our applications.” (Head of GDPR Implementation Project, Insurance & Bank).

4.2 Good practices for implementation

With a common implementation process at a macro level and company-specific nuances at a micro level, the studied cases provide lessons learned at different dimensions. In this sense, Table 2 nominates good practices [40,41] for the implementation of the General Data Protection Regulation. Thereby, the practices are organized along the well-established business engineering dimensions [42]. Several models were screened to suitably structure these. In line with the socio-technical character, the holistic representation, and the established nature in the information systems domain [42,54,55], we finally selected the business engineering approach. This research stream is rooted in the design of enterprise solutions differentiating the levels strategy, processes, and technology [54,55]. Further versions addressed shortcomings and included additional aspects such as organization and management [42].

Furthermore, the validation workshop held in July 2018 reinforced such a systematization: “As for any topic with major business relevance, you need a

strategic direction, proper organizational and managerial set-up, structured approaches, and supporting technology." (Data Privacy Manager, General Insurance).

Practice dimension	Good practice
Strategy	• Risk-based approach to data protection implementation [**] • Generic strategy formulation for future-proofness of data protection [**] • Exploitation of data protection efforts for push of digital transformation [*]
Organization	• Fit of data protection organization to organization [**] • Set-up of an interdisciplinary team with clear responsibilities [**] • Intra- and inter-organizational industry exchange [**]
Management	• Assurance of top management commitment [**] • Establishing a data protection culture [**] • Implementation of a data protection governance system [**]
Process	• Systematic macro level process with micro level sprints [**] • Intensive analysis and late implementation phase [**] • Iterative approach to data protection implementation [**]
Technology	• Prioritization of IT and applications [*] • Development of novel data protection architectures [*] • Scalability and automation of processes [*]
Sources of the good practices	Evidence from selected cases [*] Evidence from all cases [**]

Table 2. Good practices for the implementation of the General Data Protection Regulation

At a strategy-related level, several decisions can support the effectivity and efficiency of the implementation efforts: First, in order to cope with the threatening risk of fines and reputation loss, companies should apply a risk-based approach to data protection implementation. In this sense, a clear prioritization of activities according to the potential impact and criminal relevance is pivotal. Second, a generic strategy formulation for future-proofness of data protection beyond the General Data Protection Regulation enables a future-oriented approach. Implementation plans should be designed to enable modifications, specifications, and additions with regard to further regulations in a manageable way. Third, to use the drive, an exploitation of data protection efforts for the push of digital transformation is desirable. With little further investment, companies can create a digital competitive advantage beyond pure compliance with the law.

At an organization-related level, different organizational measures and set-ups can lead to success of the implementation: First, with the goal to embed the topic of data protection in the remaining enterprise, it is necessary to ensure the fit of the data protection organization to the organization. More than the manifestation such as compliance- or IT-driven data protection, the joint efforts and deep business integration count. Second, a set-up of an interdisciplinary team with clear responsibilities addresses the interwoven task. In the long term, IT and legal capabilities need to be built up as these represent critical abilities of a company related to data privacy. Third, in order to benefit from one another, the set-up of intra- and inter-organizational industry exchange is a success factor. Steady conversations help to overcome challenges arising from the novelty of the regulation and define quasi-standards.

At a management-related level, the leadership represents a sound measure to negociate the complex implementation challenge: First, with the objective to lay the foundation it is pivotal to assure top management commitment. Such profound interventions involve various stakeholders and areas across the enterprise, and thus need strong support. Second, establishing a data protection culture across the whole organization fosters comprehensive reach beyond particular activities. Data protection is too critical to cede it to the data protection team. Third, in order to address the complex interdependencies, companies should initiate the implementation of a data protection governance system. In contrast to the actual management, such systems describe the structures like the relationship between group and subsidiary regulations.

At a process-related level, methodical aspects support the success of the implementation efforts: First, to cope with the complexity of the General Data Protection Regulation and the uncertainty in the daily operations, a systematic macro level process with micro level sprints is recommended. For one, the systematic macro level process enables a structured change control process, for another, the micro level sprints provide a pragmatic approach based on feedback. Second, an intense analysis and late implementation phase implies a sound understanding of the novel regulation before taking action. The General Data Protection represents a virgin territory

and legal practice for all stakeholders involved. Third, for meeting the brief deadlines, an iterative approach to data protection implementation is valuable. The maturity can be augmented at a later stage.

At a technology-related level, the technological implementation represents the base: First, as foundation of any compliance, the prioritization of IT and applications is essential. While organizational and governing capabilities are soft success factors, IT and applications can be regarded as hard success factors. Second, the development of novel data protection architectures becomes necessary. Among others, modules of data classification, data portability, data deletion, and data monitoring are considered as key requirements. Third, to ensure an effective and efficient processing of requests, scalability and automation of processes becomes increasingly relevant. This is especially important against the backdrop of the unsecure request numbers to be expected.

5. Discussion and conclusion

This research study sets out to explore the General Data Protection Regulation in financial services industries grounded on the pivotal question: "How do companies approach to General Data Protection Regulation and what can we learn from their approaches?" Regarding the former, a three-stage iterative and risk-based implementation approach was unveiled, regarding the latter, good practices for implementation at a strategy-, organization-, management-, process-, and technology-related level were identified.

It can be concluded that companies strive with the utmost effort to ensure compliance with the General Data Protection Regulation, yet there exists a gap between strategy and implementation. This gap particularly gets obvious as enterprises conduct assessments, create strategies, and develop frameworks, however seem to neglect the actual information technology. There is evidence that this shortcoming is caused by the prioritization of communication activities, missing technological capabilities, and simply the lack of time for the actual implementation (see section 4.1). At a more abstract level, the emergence of the General Data Protection Regulation may be understood as an external stimulus to which the enterprise reacts in an appraising, strategizing, and realizing manner. In this sense, the regulation stands in a line with other external stimuli such as new technologies or changing markets where companies react in similar ways. Another important aspect refers to the generalizability of the results. In the DACH region, the General Data Protection Regulation and further local regulations need to be considered. In this context, the current Swiss privacy law is less challenging, and also its new version is expected to follow the European role model [51]. So, currently no dual systems are established. Similarly, for other non-EU-countries also multiple regulations apply. Depending on the difference of these laws, dual systems are conceivable. Hence, our results need to be generalized with care. For pure EU-countries, however, the implementation may be less complex as no other regulations are in effect.

Regarding the implementation approach, prior studies (e.g., [4,9]) have noted aspects of risk management and stage-based processes. Our empirical work confirms this character, but also shows their different manifestations. While some enterprises focus on the "Stage I Appraise" and introduce more sub-phases, others differentiate the subsequent "Stage II Strategize" in a more fine-grained manner. The iterative character of the implementation in turn can be assessed as novel. Compared to the conceptual reflections (e.g., [3,4]) on the implementation, empirical evidence from the cases indicates high complexity which in turn demands these iterations. Referring to the good practices for implementation, little empirical research [3] was found in the scientific literature. The case study findings show that various levels of the enterprise – from organizational culture to information technology architectures – need to be addressed to support compliance with the General Data Protection Regulation. While this empirical study can reinforce existing guidance (e.g., "Raise awareness enterprise-wide" [52:14]), it also brings out further recommendations such as the generic strategy formulation for future-proofness and the exploitation of efforts for push of digital transformation. Beyond this short-term view, there are many open points in the medium- and long-term. For example, it is heavily discussed how beneficial the General Data Protection Regulation and other data privacy laws are for the economy in terms of digital innovation: "A company can be organized in a very structured way to be conform, but this kills creativity – a company is a living organism. Beyond, start-ups will leave the EU and move to the less restricted regions." (Chief Executive Officer, Start-up Company).

We hope that this research study adds to our understanding of the General Data Protection Regulation in financial services industries. To practice, we make a contribution by delivering helpful, actionable advice. To science, we contribute by the generation and dissemination of knowledge on this complex phenomenon. However, extant limitations should be made transparent: First, the study at hand is

exploratory and qualitative in character [10,48], thus affords insightful views, but cannot generate all-embracive, generalizable results. Here, a quantitative survey would add value. Second, we set out for an information systems perspective – which postulates a socio-technical paradigm [7,8] – hence it does not reflect a legal viewpoint. It needs to be discussed how these equally important views can be aligned. Third, the insights were collected up the best of the participating companies, yet the mid- and long-term success will turn out in certain time. Periodic assessments (e.g., in a six months rhythm) could address this restriction.

In terms of future research it needs to be expected that further regulations in the privacy domain are upcoming in the next few years. In this sense, on the one hand, for example with the overarching ePrivacy regulation [50] another highly relevant law is currently under development. On the other hand, novel – either supplementary or even contrasting – country-specific regulations are in emergence, for the case of Switzerland the drafted "Bundesgesetz über den Datenschutz" [51]. Beyond, further industries such as MedTech and HealthCare as well as more theory-informed research can serve as valuable avenues for further research.

Acknowledgements. This research study was supported by the ZHAW Product Management Center, the HSG Competence Center Data Privacy, and swissnex Boston.

6. Appendix: Interview guidelines

Interviewee and company background
- What is your current position within your organization?
- Please specify briefly your job position und responsibilities.
- Which product/service portfolio is developed and managed within your organization?
- Please describe briefly the strategic vision of your organization.
- What is the impact of digitalization on your organization?

Trends and challenges
- What are specific trends in data protection in your region/industry/organization?
- What are specific challenges in data protection in your region/industry/organization?
- What is the role of the GDPR for your organization? How do you assess its importance?
- Which opportunities and threats linked with the GDPR do you see in general?

Organization, process and technology perspective
- Which department in your organization is leading the GDPR compliance efforts?
- What is the role of internal/external partners in the industry ecosystem at that point?
- How does your organization principally approach to comply with the GDPR? Methods? Tools?
- How do the sub-phases "Appraise", "Strategize", and "Realize" look like?
- How do you deal with aspects of information and communication technology?
- What is the status quo of the project? What is the accomplished/planned timeline?

Reflection
- What are good practices and strategies for implementation?
- What are lessons learned and dead ends?
- What are incalculable factors and bottlenecks?
- Which changes/new capabilities are required?

Conclusion
- Can you provide us supporting documents or reports?
- Would you like to add any comments or ideas regarding the GDPR?
- Would you like to add any comments or ideas regarding the GDPR study?
- Could we get back to you in case we have some further questions from our data analysis?

7. References

[1] McKinsey Global Institute, Digital Globalization: The New Era of Global Flows, Working Paper, 2016.

[2] European Parliament and Council of the European Union, General Data Protection Regulation, Brussels, Belgium, 2016.

[3] Tikkinen-Piri, C., A. Rohunen, and J. Markkula, "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies", Computer Law & Security Review (34:1), pp. 134–153, 2018.

[4] Voigt, P., and A. von dem Bussche, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer, Cham, Switzerland, 2017.

[5] Tankard, C., "What the GDPR Means for Businesses", Network Security (6), pp. 5–8, 2016.

[6] Miglicco, G., "GDPR Is Here and It Is Time to Get Serious", Computer Fraud & Security (9), pp. 9–12, 2018.

[7] Bostrom, R. P., and J. S. Heinen, “MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes”, MIS Quarterly (1:3), pp. 17–32, 1977.

[8] Chen, D. Q., M. Mocker, D. S. Preston, and A. Teubner, “Information Systems Strategy: Reconceptualization, Measurement, and Implications”, MIS Quarterly (34:2), pp. 233–259, 2010.

[9] Calder, A., EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide, IT Governance Ltd., Ely, Great Britain, 2017.

[10] Yin, R. K., Case Study Research – Design and Methods, Sage Publications, London, Great Britain, 2003.

[11] Eisenhardt, K. M., “Building Theories from Case Study Research”, Academy of Management Review (14:4), pp. 532–550, 1989.

[12] Benbasat, I., D. K. Goldstein, and M. Mead, “The Case Research Strategy in Studies of Information Systems”, MIS Quarterly (11:3), pp. 369–386, 1987.

[13] European Parliament and Council of the European Union, Data Protection Directive, Brussels, Belgium, 1995.

[14] Smith, H. J., T. Dinev, and H. Xu, “Information Privacy Research: An Interdisciplinary Review”, MIS Quarterly (35:4), pp. 989–1015, 2011.

[15] Bélanger, F., and R. E. Crossler, “Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems”, MIS Quarterly (35:4), pp. 1017–1041, 2011.

[16] Dinev, T., A. R. McConnell, and H. J. Smith, “Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the ‘APCO’ Box”, Information Systems Research (26:4), pp. 639–655, 2015.

[17] Greenaway, K. E., Y. E. Chan, and R. E. Crossler, “Company Information Privacy Orientation: A Conceptual Framework”, Information Systems Journal (25:6), pp.579–606, 2015.

[18] De Hert, P., and V. Papakonstantinou, “The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals”, Computer Law & Security Review (28:2), pp. 130–142, 2012.

[19] De Hert, P., and V. Papakonstantinou, “The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?”, Computer Law & Security Review (32:2), pp. 179–194, 2016.

[20] De Hert, P., V. Papakonstantinou, G. Malgieri, L. Beslay, and I. Sanchez, “The Right to Data Portability in the GDPR: Towards User-centric Interoperability of Digital Services”, Computer Law & Security Review (34:2), pp. 193–203, 2018.

[21] Mertens, P., “Die Datenschutz-Grundverordnung – Eine kritische Sicht”, Wirtschaftsinformatik & Management (11:1), pp. 6–17, 2019.

[22] Suhling, P., “Eine Retrospektive auf den Datenschutz seit Einführung der EU-DSGVO: EU-Datenschutz-grundverordnung – Vom Papiertiger zum Berglöwen”, Wirtschaftsinformatik & Management (11:1), pp. 35–36, 2019.

[23] Kurtz, C., M. Semmann, and T. Böhmann, “Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors”, Proceedings of the 24th Americas Conference on Information Systems (AMCIS), New Orleans, United States, 2018.

[24] Fox, G., C. Tonge, T. Lynn, and J. Mooney, “Communicating Compliance: Developing a GDPR Privacy Label”, Proceedings of the 24th Americas Conference on Information Systems (AMCIS), New Orleans, United States, 2018.

[25] Petkov, P., and M. Helfert, “Identifying Emerging Challenges for ICT Industry in Ireland: Multiple Case Study Analysis of Data Privacy Breaches”, Proceedings of the 23rd Americas Conference on Information Systems (AMCIS), Boston, United States, 2017.

[26] Webster, J., and R. Watson, “Analyzing the Past to Prepare the Future: Writing a Literature Review”, MIS Quarterly (26:2), pp. xiii–xxiii, 2002.

[27] Vom Brocke, J., A. Simons, K. Riemer, B. Niehaves, R. Plattfaut, and A. Cleven, “Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process”, Proceedings of the 17th European Conference on Information Systems (ECIS), Verona, Italy, 2009.

[28] Vom Brocke, J., A. Simons, K. Riemer, B. Niehaves, R. Plattfaut, and A. Cleven, “Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research”, Communications of the AIS (37:1), pp. 205–224, 2015.

[29] Notario, N., A. Crespo, Y. S. Martín, J. M. D. Alamo, D. L. Métayer, T. Antignac, A. Kung, I. Kroener, and D. Wright, “Pripare: Integrating Privacy Best Practices into a Privacy Engineering Methodology”, IEEE Security and Privacy Workshops, pp. 151–158, 2015.

[30] Russell, K. D., P. O’Raghallaigh, P. O’Reilly, and J. Hayes, “Digital Privacy GDPR: A Proposed Digital Transformation Framework”, Proceedings of the 24th Americas Conference on Information Systems (AMCIS), New Orleans, United States, 2018.

[31] Müller-Bloch, C., and J. Kranz, “A Framework for Rigorously Identifying Research Gaps in Qualitative Literature Reviews”, Proceedings of the 36th International Conference on Information Systems (ICIS), Fort Worth, United States, 2015.

[32] Coyne, I. T., “Sampling in Qualitative Research. Purposeful and Theoretical Sampling; Merging or Clear Boundaries?”, Journal of Advanced Nursing (26:3), pp. 623–630, 1997.

[33] Schultze, U., and M. Avital, “Designing Interviews to Generate Rich Data for Information Systems Research”, Information and Organization (21:1), pp. 1–16, 2011.

[34] Rubin, H. J., and I. S. Rubin, Qualitative Interviewing: The Art of Hearing Data, Sage Publications, Thousand Oaks, United States, 2004.

[35] Alam, I., “Fieldwork and Data Collection in Qualitative Marketing Research”, Qualitative Market Research: An International Journal (8:1), pp. 97–112, 2005.

[36] Sinkovics, R., E. Penz, and P. N. Ghauri, “Analysing Textual Data in International Marketing Research”, Qualitative Market Research: An International Journal (8:1), pp. 9–38, 2005.

[37] Strauss, A. L., and J. M. Corbin, Grounded Theory in Practice, Sage Publications, Thousand Oaks, United States, 1997.

[38] Charmaz, K. C., Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis, Sage Publications, London, Great Britain, 2006.

[39] Wiesche, M., M. C. Jurisch, P. Yetton, and H. Krcmar, “Grounded Theory Methodology in Information Systems Research”, MIS Quarterly (41:3), pp. 685–701, 2017.

[40] O'Dell, C., and J. Grayson, “If Only We Knew What We Know: Identification and Transfer of Internal Best Practices”, California Management Review (40:3), pp. 154–174, 1998.

[41] O'Dell, C., J. Grayson, and N. Essaides, If Only We Kew What We Know: The Transfer of Internal Knowledge and Best Practice, Free Press, New York, United States, 1998.

[42] Brenner, W. et al., “User, Use & Utility Research – The Digital User as New Design Perspective in Business and Information Systems Engineering”, Business and Information Systems Engineering (6:1), pp. 55–61, 2014.

[43] Morgan, D. L., Focus Groups as Qualitative Research, Sage Publications, Newbury Park, United States, 1988.

[44] Nielsen, J., “The Use and Misuse of Focus Groups”, IEEE Software (14:1), pp. 94–95, 1997.

[45] Tremblay, M. C., A. R. Hevner, and D. J. Berndt, “Focus Groups for Artifact Refinement and Evaluation in Design Research”, Communications of the AIS (26), pp. 599–618, 2010.

[46] Sarker, S., X. Xiao, and T. Beaulieu, “Qualitative Studies in Information Systems: A Critical Review and Some Guiding Principles”, MIS Quarterly (37:4), pp. iii–xviii, 2013.

[47] Keutel, M., B. Michalik, and J. Richter, “Towards Mindful Case Study Research in IS: A Critical Analysis of the Past Ten Years”, European Journal of Information Systems (23:3), pp. 256–272, 2014.

[48] Yin, R. K., “Validity and Generalization in Future Case Study Evaluations”, Evaluation (19:3), pp. 321–332, 2013.

[49] Lombard, M., J. Snyder-Duch, and C. C. Bracken, “Content Analysis in Mass Communication: Assessment and Reporting of Intercoder Reliability”, Human Communication Research (28:4), pp. 587–604, 2002.

[50] European Parliament and Council of the European Union, Regulation on Privacy and Electronic Communications, Brussels, Belgium, 2017.

[51] Bundesversammlung der Schweizerischen Eidgenossenschaft, Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) Vorentwurf, Bern, Switzerland, 2016.

[52] Bauer, D., “6 Steps to GDPR Implementation”, Risk Management (65:3), pp. 14–15, 2018.

[53] Almeida Teixeira, G., M. Mira da Silva, and R. Pereira, “The Critical Success Factors of GDPR Implementation: A Systematic Literature Review”, Digital Policy, Regulation and Governance (21:4), pp. 402–418, 2019.

[54] Österle, H., Business Engineering: Prozeß- und Systementwicklung - Band 1: Entwurfstechniken, Springer, Berlin/Heidelberg, Germany, 1995.

[55] Österle, H., W. Brenner, C. Gaßner, T. Gutzwiller, and T. Hess, Business Engineering: Prozeß- und Systementwicklung - Band 2: Fallbeispiel, Springer, Berlin/Heidelberg, Germany, 1996.