European Journal for Security Research (2019) 4:243–264
https://doi.org/10.1007/s41125-019-00042-z

ORIGINAL PAPER

A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises

Martin Brodin[1]

Received: 25 March 2019 / Accepted: 4 June 2019 / Published online: 8 June 2019

Abstract
The EU's General Data Protection (GDPR) is an EU regulation that affects everyone in the EU and all organisations outside the EU that wants to do business with the EU. GDPR introduces tougher requirements for processing personal data, which may be difficult for many small- and medium-sized enterprises (SMEs) to follow without major adjustments. This work uses design science to develop a framework for SMEs to adapt to GDPR. The framework was empirically evaluated in three different types of organisations, resulting of GDPR compliance according to their Data Protection Officers. It was also theoretical evaluated against scientific literature including the identified implications of GDPR. In this paper the framework is presented, from initial analysis and design to implementation and future work, with advice on how to work with each part to achieve compliance. The paper also highlights some of the most important changes in GDPR compared to its predecessor, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (DIR95).

Keywords General Data Protection Regulation · GDPR · Information management · SME · SMEs

1 Introduction

The EU's General Data Protection Regulation (GDPR) has been in place since May 2018, replacing existing data protection laws in all EU countries. GDPR affects all organisations in the EU and every company outside the EU that wants to do business within the EU. The purpose of GDPR is "…the protection of natural persons with regard to the processing of personal data and on the free movement of such data" (the European Commission 2016). For most organisations GDPR requires

✉ Martin Brodin
martin.brodin@his.se

[1] University of Skövde, Box 408, 541 28 Skövde, Sweden

significant changes in many parts of the organisation; unfortunately, many small- and medium-sized enterprises (SMEs) do not have resources or knowledge to manage this by themselves (Hashim 2015; Schulze 2018). SMEs typically have simple planning and control systems with informal rules and procedures. They also tend to have less standardisation of work processes, which is a problem since GDPR demands full control of every process that contains personal data (Supyuenyong et al. 2009). In Europe more than 99% of all businesses are SMEs (defined as an enterprise with less than 250 employees (Harris et al. 2012; The European Commission 2018). If an organisation does not comply with GDPR it may be expensive, and the chances of discovery are significant, since anyone can file a complaint. In the first 8 months of GDPR around 60,000 complaints were received, resulting in fines up to $57,000,000 (Olenick 2019).

For SMEs with limited resources and information management system, this means a great deal of work, so there is a need for a structured approach to make sure they do not miss anything (Hashim 2015; Supyuenyong et al. 2009). A report from the Irish SME Association shows that, although most SMEs are aware of and concerned about GDPR, only 30% of business have identified the steps needed to be GDPR compliant (ISMEs 2018). With just 2 months to the regulation coming into force, a major study revealed that 63% of all organisations in the study estimated that they will not be ready in time, and 26% believe it will take at least 4 years for them to get fully compliant with GDPR (Schulze 2018). The aim of this paper is therefore to illustrate a way for small- and medium-sized enterprises (SMEs) to comply with GDPR, without jeopardise the economy or spend a tremendous amount of time.

The paper is structured as follows: section one introduces GDPR and presents what is new in GDPR compared to its predecessor—directive 95/46/EC of the European Parliament and of the Council of 24 (October 1995) on the protection of individuals with regard to the processing of personal data and on the free movement of such data (DIR95). Section two explains the method that is used, and section three presents the framework. Sections four and five show the empirical and theoretical evaluation, and section six concludes the work with a discussion and thoughts about further research.

1.1 Changes from DIR95

GDPR is built upon a previous regulation, DIR95 (The European Commission 1995), maintaining considerable continuity but also introducing many new protections. GDPR is a European regulation which is immediately enforceable as law, which looks the same across the EU/EEA without different national implementations. DIR95 was a directive that had to be adapted to national law. It is also a law that applies to those outside the EU who wish to do business within the EU/EEA. Furthermore, GDPR applies to all processing of personal data, not just to structured data as was the case with DIR95. Examples of unstructured data are e-mails, spreadsheets, Word and PDF files, videos, pictures, social media posts and other types of data not organised in a defined manner.

In this section we go through some of the most important implications for SMEs.

1.1.1 Principles (Article 4–11)

GDPR introduces some new important principles related to the processing of personal data; *Pseudonymisation, transparency, data minimisation* and *consent of minors (children)*. *Pseudonymisation* means the processing of personal data in a way that it cannot be related to a specific data subject without the use of additional information (the additional information must be stored separately and protected). In DIR95 we had anonymisation. DIR95 states that personal data shall be processed lawfully and fairly, whereas GDPR adds in a transparent manner in relation to the data subject. Both DIR95 and GDPR state that the personal data used in the processing shall be adequate, relevant and necessary in the light of the purposes for which they are processed. GDPR makes this even clearer by introducing data minimisation. GDPR also introduce a special section for processing of children's personal data.

1.1.2 Rights of the Data Subject (12–23)

Important rights of the data subject are: *Right of access, Right to rectification, Right to erasure, Right to restriction of processing* and *Right to object*. These rights also exist in DIR95 but have been clarified and extended in GDPR. In GDPR, the data processor also has to inform the data subject about the legal basis for the processing, time the personal data will be kept, the source of the data and the rights of the data subject. When it comes to the right to erasure (also known as the right to be forgotten), GDPR moves closer to the data subject and makes it easier to be forgotten. In GDPR, personal data does not need to be incomplete, inaccurate or not processed in accordance with the regulation to be forgotten. It may also be forgotten if it not needed for the purpose it was collected anymore, consent has been withdrawn, or if the data subject objects and there is no stronger legal ground. A new right in GDPR is the *Right to data portability which* allows the data subject to obtain and reuse their personal data for their own purposes across different services if the processing is carried out by automated means and the legal ground is consent or contract. Data shall be handed over in a structured, commonly used and machine-readable format.

1.1.3 Controller and Processor (24–43)

There are some important implications when it comes to the responsibilities of controllers and processors. First, they must base their work on the principle: data protection by design and default. This means that all software development must be shipped with data security measures turned on as default and as a part of the design. Furthermore, when a controller processing personal data they must ensure, by technical and organisational measures, that only personal data which are necessary for each specific purpose of the processing are processed. If a data breach occurs, the controller has to report it to the supervisory authority within 72 h and they also need to inform the data subject.

A Data Protection Impact Assessment (DPIA) is something that many SMEs need to perform, or at least reflect over. When data processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller must perform a

DPIA prior to the start of any processing. Some SMEs must also assign a Data Protection Officer (DPO), if their core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or processing on a large scale of sensitive personal data or personal data relating to criminal convictions and offences. The DPO is an independent role.

1.1.4 Transfers of Personal Data to Third Countries or International Organisations (44–50)

With GDPR, the rules for transferring personal data outside the EU/EEA have been tightened up. This is only allowed under certain conditions; adequacy decision, appropriate safeguards, binding corporate rules, legal assistance treaty and specific situations. Adequacy decision is where the Commission has decided that the area (country, territory or sector within the country) or organisation in question ensures an adequate level of protection. If there is no adequate decision a transfer may occur if the controller or processor has provided appropriate safeguards, and enforceable rights and effective legal remedies are available for data subjects. For companies established in the EU or belonging to an international group of companies located outside the EU/EEA area, binding corporate rules are a possible route. These are rules that a group of companies develops to regulate their personal data processing across national borders.

If none of the above applies, personal data may still be transferred with a judgment of a court or tribunal in a third country, or if a specific situation appears such as; the data subject has explicitly consented to the proposed transfer, the transfer is necessary to (a) a contract with the data subject or regarding their interest, (b) public interest, (c) the of defence of legal claims, or (d) to protect vital interests of the data subject, or if the data is public and open for consultation.

1.1.5 Actions for SMEs

Many things remain the same (however, the changes that SMEs must perform may differ between the countries in EU, since GDPR is regulation and DIR95 was a directive that was adapted into different national laws). Anyhow, there are several changes that all SMEs must consider (Table 1).

1.2 Research State of the Art

There are many opinion-based articles about GDPR from practitioners, but at his point the number of scientific articles is limited. This section presents the most relevant existing research.

GDPR has 99 articles whilst DIR95 only has 34, which indicates that there is a lot of work involved in compliance (Lindqvist 2018). Most problem with compliance are found in SMEs (with the exception of companies with an existing security focus), since they have more limited resources (Lindqvist 2018; Sirur et al. 2018). Some researchers focus on a specific article in GDPR, for instance data portability,

Table 1 News in GDPR and corresponding actions for SMEs

News in GDPR	Actions for SMEs
Personal data shall be processed in a transparent manner in relation to the data subject	Determine what personal information is processed and where. Classify information and update personal data policy
Data minimisation	Determine what personal information is processed and where. Clarify the legal ground for all personal data processing. Remove all unnecessary data
Processing of children's personal data	Perform an extra security analysis if children's personal data is processed
The processor must inform the data subject about the legal basis for processing, time personal data will be kept, source of the data and the rights of the data subject	Update personal data policy and the template for consent
Strengthen right to be forgotten	Create a process and routines to meet data subjects demands and to terminate personal data processing
Right to data portability	Create a process and routines to meet data subjects demands
Data protection by design and default	Update routines for purchase and configuration of software and hardware
Ensure that only personal data which are necessary for each specific purpose of the processing are processed	Update work routines
Report data breaches within 72 h	Create/update process and routines for incident response
Perform Data Protection Impact Assessment (DPIA) when data processing is likely to result in a high risk to the rights and freedoms of natural persons	Create a process for managing new personal data processing and routines for DPIA
Data Protection Officer (DPO)	Assign a DPO if core activities are of the required nature
Transfers of personal data to third countries or international organisations	Determine what personal information is processed and where. Make agreements when a transfer is necessary

certification and privacy (Ataei et al. 2018b; Bu-pasha 2017; De Hert et al. 2017; Graef et al. 2018; Lindqvist 2018; Rodrigues et al. 2016; Urquhart et al. 2018; Vanberg and Ünver 2017) or a specific sector/business (Erdos 2016; Grundstrom et al. 2019; Lopes and Oliveira 2018; Stanciu and Rîndașu 2018).

There are some studies that deal with challenges that come with GDPR. Ataei et al. (2018a) identified three challenges with GDPR, after interviewing six GDPR experts. The first is user-friendliness—implementing GDPR in a way that does not place unmanageable burdens on users. The second challenge is awareness—the need to think about data protection during deployment. The final challenge is technical considerations and how to guarantee anonymisation. Grundstrom et al. (2019) identified 13 challenges for GDPR compliance for insurance companies, which they

sorted into four categories of personal data access; Procedure, Protection, Privacy, and Proliferation. Tikkinen-Piri et al. (2017) identified several important changes in the GDPR compared to DIR95, which they summarise in twelve practical implications for organisations. Each implication is something that every organisation must take care of. The twelve implications are shown in Table 2 and later used in the theoretical evaluation.

2 Method

The research is a close collaboration with practitioners, since the problem is common to all SMEs in Europe and needs a comprehensive solution that is not too resource-intensive. The solution must work for practitioners from day one. The work aims to design an artefact (the framework presented in Sect. 3) in collaboration with practitioners involved in the cases, so the research method called design science (Hevner and Chatterjee 2010; Peffers et al. 2007; Sein et al. 2011; Vaishnavi and Kuechler 2007) is a good choice. The designed artefact may be a method, model or design principle (Gregor and Hevner 2013). Design science deals with two challenges; to address a practical problem in a specific organisational setting and to construct and evaluate an artefact (in this case a low-cost method, with accompanying tools) that addresses the class of problems identified (complying with a new data protection law). To scientifically design something that practice would benefit from requires a problem identified in practice (Hevner and Chatterjee 2010; Nunamaker et al. 1991; Peffers et al. 2007; Rossi and Sein 2003; Vaishnavi and Kuechler 2007; Walls et al. 1992). Furthermore, the problem should not have a well-known solution; hence, a literature review may be suitable to start with. Looking into an adjacent discipline may provide ideas for new findings to the researcher's field (Vaishnavi and Kuechler 2004). Before designing the solution, a proposal or objective for the solution should be presented (Gregor and Jones 2007; Hevner and Chatterjee 2010; Peffers et al. 2007; Vaishnavi and Kuechler 2007; Walls et al. 1992). The proposal or objective is then further developed to a tentative design or the first draft of the artefact. As the name design science implies, design is the central part of the research process and the development of the artefact take place in a design search or development process (Gregor and Jones 2007; Hevner and Chatterjee 2010; Nunamaker et al. 1991; Peffers et al. 2007; Rossi and Sein 2003; Vaishnavi and Kuechler 2007; Walls et al. 1992). Hevner and Chatterjee (2010) point out that development is an iterative search process. When the artefact is designed it must be evaluated (Hevner and Chatterjee 2010; Nunamaker et al. 1991; Peffers et al. 2007; Rossi and Sein 2003; Vaishnavi and Kuechler 2007; Walls et al. 1992). The evaluation of the artefact may be in terms of validity (that it works), utility (gives value outside the development environment), quality, and efficacy. Evaluation can be in the form of final summative tests in case studies, or expert review (Vaishnavi and Kuechler 2004). The final version of the artefact has to be communicated, both to practitioners and to the research community (Hevner and Chatterjee 2010; Peffers et al. 2007).

There are several suggested design science processes, but for this work the chosen process is the one by Vaishnavi (Fig. 1), which is similar to Peffers et al. (2007).

Table 2 Twelve practical implications for organisations (Tikkinen-Piri et al. 2017)

Practical implications (Tikkinen-Piri et al. 2017)	Explanation
Specifying data needs and usage	A data processor is not allowed to collect more personal data than needed for the processing and must specify the legal basis for all personal data processing
Considering conditions for data processing in international context	If any personal data is transferred to a third country or an international organisation, the organisation must ensure that their current safeguards comply with the GDPR otherwise they need to develop new ones
Building privacy through data protection by design and default	Every personal data processor must implement technical and organisational measures and procedures to ensure compliance with GDPR. Privacy must be considered in every process all the time and shall be by default and design
Demonstrating compliance with GDPR requirements	Controllers are obligated to demonstrate that their personal data processing complies with GDPR and must have a plan for how to do it
Developing processes to deal with data breaches	A data breach with personal data must be reported to the supervisor authority within 72 h. To be able to do that a process for it needs to be in place
Reckoning with sanctions for non-compliance	If an organisation does not comply with GDPR, the supervisory authorities may impose administrative fines (up to €20 million or 4% of the annual global turnover). Therefore, it is important to include all procedures related to personal data processing in the GDPR preparation
Designating a Data Protection Officer (DPO)	Some organisations must assign a DPO, it is up to each organisation to find out if they need one and if so, assign one
Providing information to data subjects	The controller is obligated to inform the data subject about the processing of personal data when it comes to how, when and where it is processed, the legal basis, security measures and the subject's rights
Obtaining consent on personal data usage	When the legal basis demands a consent from the data subject prior to processing it must be collected and accordance to GDPR
Ensuring individuals' right to be forgotten	The data subject has a right to be forgotten, if this right is invoked, the data connected to the subject must be deleted. To be able to ensure that all data is erased all documentation of the data needs to be up to date
Ensuring individuals' right to data portability	Individuals have a right to obtain and reuse their personal data for their own purposes across different services. Organisations needs to make sure that the personal data can be transmitted to other service providers' processing systems
Maintaining documentation	Documentation that shows GDPR compliance must be kept up to dated

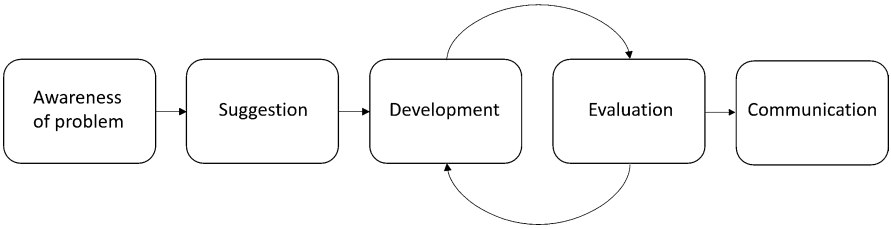

Fig. 1 The design science process in this work (Vaishnavi and Kuechler 2004)

The process was applied in the way described in the following sections.

2.1 Awareness of Problem

The problem is well-known all-over Europe since it is a new EU regulation that will affect most SMEs in some way. All organisations must follow the regulation, but it is not clear to everyone what they must do to be fully compliant. To get a picture of the which challenges organisations face when getting ready for GDPR, we met with different organisations to find out how their road to compliance looked. These were open discussions to see if there was a common way or method that most will use. It turned out that everyone had their own method and approach, but there was no common approach, and none had the complete picture or was sure of success.

2.2 Suggestion

In suggestion phase, which usually results in the first draft of the artefact, a checklist was created by analysing the regulation and categorising all identified actions. The checklist consisted of measures that an organisation needs to carry out in order to be compliant, such as analyses that need to be done and documents and routines that need to be created or updated. The researchers then followed an organisation in their preparation for GDPR for 6 months. During this period, several discussions with legal experts and GDPR experts in the organisation and at government agencies took place. The checklist was constantly updated and the need for a framework or model to structure the compliance process became clearer during meetings. Since there was no existing framework or model for GDPR, it needed to be either brand new or adapted from a similar field. Managing information on mobile devices is close to GDPR and something that a lot of SMEs dealt with lately, so it became natural to adopt a framework from this area. It is also an area where several frameworks has been developed lately (Brodin

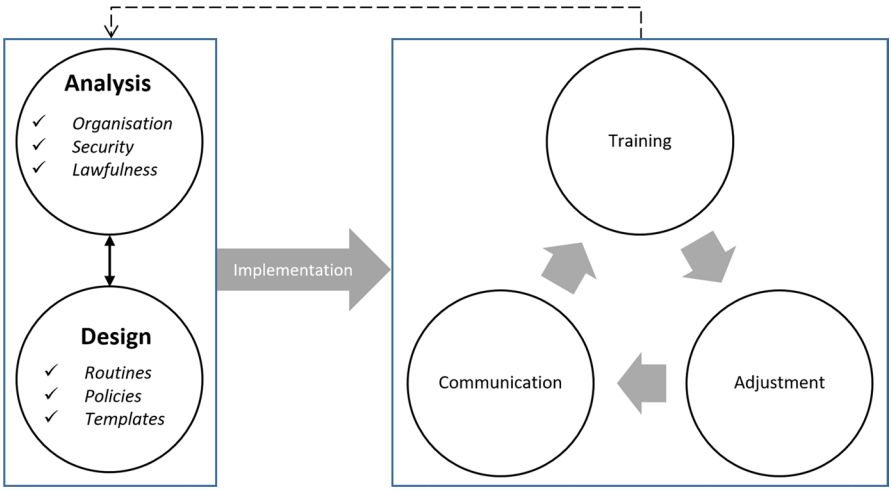

Fig. 2 A framework to help SMEs to adapt to GDPR. Adapted from Brodin (2015)

2017). Each category in the checklist was matched to each category in the framework (Fig. 2). The updated version of the framework was the first version of the artefact for GDPR.

2.3 Development

The artefact was developed during an iterative process with evaluations in practice followed by adjustments of the framework. The development process took place in three organisations in cooperation with GDPR experts in each organisation, both internal and external, and at least one of the following roles: CIO, CEO or DPO.

2.4 Evaluation

There were two types of evaluation in this work, empirical and theoretical. The empirical evaluation was set in three different organisations; one public organisation whose task is to serve the citizens of a major Swedish city, one in a private midsize management consulting firm with 50–100 employees and one in an event planning company with 10–20 employees. Secondly, the artefact was evaluated against scientific literature and twelve identified implications with GDPR, see Table 2.

2.5 Communication

It is important to communicate the final result (Hevner and Chatterjee 2010; Peffers et al. 2007), and the final version of the framework was communicated to interested organisations and to the research community through this article.

3 Framework

The framework used for the GDPR compliance projects is an adaptation of Brodin (2015). The framework was originally devised to help SMEs to gain the benefits of mobile devices without compromising security. Its theoretical background is in strategic management (Johnson et al. 2015) and ISO/IEC 27,000-series (ISO/IEC 2016). Managing information on mobile devices is close to the work that is needed for GDPR, since both are about achieving control of the organisation's data and protecting it at all times.

The original framework looks at expectations, environment and resources and capability in the analysis phase to determine which strategy road to take. GDPR offers one road for all, which gives another focus for the analysis, but when it comes to information security the necessary analysis it is very similar for GDPR and mobile devices. The design phase differs when it comes to focus areas—where the original framework looks at options, development and selection, we focus on what is needed to be created to be compliant with GDPR. The road from design to the future is, on the other hand, almost the same.

Each phase in the framework was re-designed to orient it towards GDPR compliance, before contact with the organisations was made. The eventual components are described in more detail in the following sections.

3.1 Analysis

The framework starts with analysis to determine the current state of the organisation when it comes to information control and security. In this phase the model for information classification is also updated to be prepared for GDPR' and information is re-classified.

The first analysis is information analysis, which is conducted in one or more workshops, to get an overview of all personal data processing in the organisation. Each participant in the workshop writes down all personal data processes that they encounter, one process per Post-it. Each Post-it is then connected to the location where the information is processed, for example, on paper or in an IT system. Data processing by external processors, which might need a data processing agreement, are also documented. Although SMEs are not obliged under article 30 to hold a register of all personal data processing; a simple register or use case diagram could be a useful result from the workshop to take the work further. If the personal data processes are complex, or many different systems are involved, the next step is an information flow analysis to identify how personal information moves inside the organisation. The information flow analysis focuses on personal data and how the data moves between systems. When the organisation knows what kind of personal data they process and where it is stored it is time for information classification followed by an information security analysis. At this point, the legal ground for each item of personal data must be clear.

To sum up the analysis phase, we can say that when it comes to GDPR the analysis phase has five important points. *Information analysis*—a method to get an overview of what personal information that are processed and where. *Information flow analysis*—creating an understanding of how personal information moves inside the organisation. *Information classification*—requiring the classification scheme to be updated to include personal data according to GDPR, and some information needs to be re-classified. *The legal ground for personal data processing*—making it clear why personal data is processed and to what extent. Redundant additional information must be removed. *Information and IT security analysis*—ensuring appropriate security for personal data (Fig. 3).

3.2 Design

The design phase focuses on routines, policies, and templates. There are two types of routines; derived from GDPR, and internal work routines. Routines that are directly linked to GDPR concern the rights of the data subject (meeting requests about an individual's right to access, rectification, erasure, restriction of processing, data portability and object) or responsibilities of the data controller (how and when to conduct a Data Protection Impact Assessment (DPIA) and

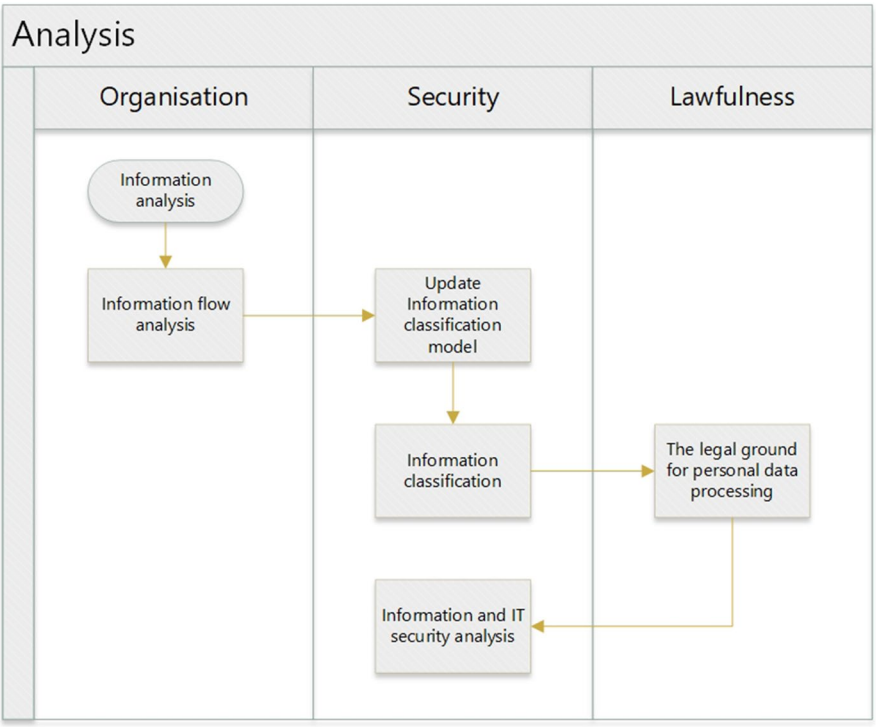

Fig. 3 The analysis phase

how to act when a data breach occur). Work routines concern the handling of personal data during a regular working day for all employees. The templates are connected to routines directly linked to GDPR. Policies that manage processing of personal data needs to be updated, for instance the personal data policy; which clarify what kind of information that is collected, how it is collected and how it is used and stored. It also tells the data subject how to exercise their rights. Another document that is updated in this phase is the one which explains how documents are stored and when data must be erased.

There are five key points in the design phase of the GDPR work that everyone needs to consider. *Updating routines where personal data are processed*—since personal data is the central point in GDPR it is extremely important that all personal data is handled correctly in all respects. *Creating routines for managing requests from data subjects, for instance to be forgotten*—GDPR strengthens the individual's rights, so it is important that organisations have procedures to accommodate individuals' requests. *Create or update process for data breaches*—according to GDPR, all personal data incidents that pose a risk to the registrant must be notified to the regulatory authority within 72 h. *Update personal data policy*—policies prior to 2018 follow the old data protection law and needs to be updated to GDPR. *Create templates connected to routines and policies*—to ensure that everyone does the same and to avoid individual solutions around the organisation. One of the more important templates is the one for data processing agreement, which also needs to be updated and signed for all cases where external personnel might process personal information on behalf of the controller (Fig. 4).

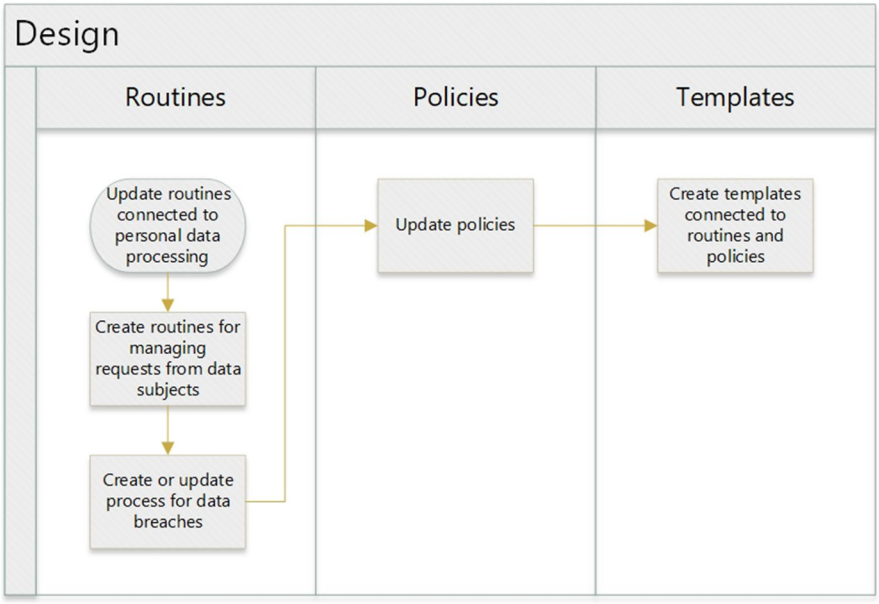

Fig. 4 The design phase

3.3 Implementation

After working with management and experts, it is time for implementation throughout the organisation. Focus in the implementation is on:

1. Creating conditions for continued compatibility with GDPR by introducing the new routines and creating a reporting system for incidents.
2. Appointing people to the new roles and giving them the conditions for their work.
3. Cleaning up existing data processing; deleting unnecessary personal data; and removing all data processing that is not compatible with the new law.

During the implementation is it also important to set a structure that will survive for a long time. The organisation needs to make sure that all changes reach all relevant personnel. This makes *communication* important. Organisations need to ascertain that all information about the changes reach everyone.

It is not only the changes that need to reach out to everyone, GDPR requires a new way of thinking and working. This makes *education* important. Organisations need to ascertain that everyone has the right competence to comply with GDPR and to play their individual part. Appropriate training can be within working procedures, GDPR and information security. This is also something that should recur annually. Finally, the people in charge for the strategy and corresponding documents need to pay attention to signals from the business that point to deficiencies in policies and instructions. If anomalies/deficiencies are found in procedures, instructions or documentation, they need to be addressed. *Adjustments* need to be communicated, and training materials may need to be updated.

When the implementation project comes to its end it is time to plan for the rest of the time that the law will apply. It is important that all employees adapt to the new work routines and keep the registry of personal data processing alive—GDPR compliance is not a one-time event. As times go, policies and routines probably need to be adjusted. It is also a good to plan for periodic compliance audits.

4 Empirical Evaluation

The GDPR compliance framework was evaluated in three organisations. The organisations were chosen to represent both private and public sectors, medium and small, as well as with and without the requirement of assigning a Data Protection Officer (DPO). The compliance result was reviewed and approved by internal or external GDPR experts in each organisation and at least one of the following roles CIO, CEO and DPO. Data was collected through practitioners' workshops, which were documented.

4.1 Case One

The first case took place in a public organisation whose task is to serve the citizens of a major Swedish city. The organisation has its own IT department with

several servers, but they also run services on servers controlled by others. In some cases, they process sensitive data and are obligated to appoint Data Protection Officer (DPO).

4.1.1 Analysis

The work was divided into several full day work meetings. During the first meeting, the researchers presented the framework and the organisation reported about its status in their work with GDPR compliance and introduced the resources that will be available. Further work was planned with the framework as a basis—the first work meetings managed the first part of the framework, *analysis*. The organisation had previously identified all (135) of their work processes but found it difficult to get an overall picture of the remaining work. "My employees have neither the time nor the interest to familiarise themselves with what GDPR means for us and what is required.", said the IT manager who felt very reassured by the framework. First out of the analysis was a GDPR risk assessment on each process, which was conducted in two half day workshops with 15 participants in each. The workshops resulted in an action list for each process and a common list of risks that concern all processes. On the common list a lot of the actions from *design* in the framework are found. Each process owner was made responsible for addressing the risks on their list. A separate project was formed to manage the risks on the common list. The analysis phase continued with a drawing of a system map and an information flow analysis where all personal data were mapped to the systems and then the personal data flow was drawn. Next, a register of all personal data processing was created with the help of previous work and an information analysis. The register also included the legal ground for each personal data processing and where a data processing agreement is needed. Previous information classification had not, for obvious reasons, considered the GDPR. To get a clearer picture of whether data protection is at the right level, an information classification for each process and IT system was conducted in accordance to GDPR. An IT and information security analysis, with the new information classification as a basis ended the analysis section.

4.1.2 Design

The next step was to design all the necessary documents. First out was to update work routines where personal data are processed to make sure that all personal data are processed in accordance with GDPR. At the same time routines for managing requests from data subjects, for instance to be forgotten and access, was created by a subproject in the organisation. The subproject was also responsible to create templates connected to the new routines and a process for data breaches. In cooperation with the IT manager, all data processing agreements were updated and signed, and a personal data policy was created.

4.1.3 Implementation

The implementation project was handed over to the organisation to manage by themselves without the help of the researchers.

4.2 Case Two

The second case takes place in a private midsize management consulting firm with 5–100 employees. The organisation has no legal demand to designate a Data Protection Officer (DPO), but some of the consultants are appointed to DPO in other organisations. The work was carried out together with experts from the organisation, the CIO, and with support from the CEO and the management team.

4.2.1 Analysis

The *analysis* phase started with stakeholder analysis to find out which of the employees needed to be considered during the work. Next up was the system map, which was updated, and systems with personal information were identified. Then the information analysis was carried out with the help of two workshops, one with business support and one with five consultants. The result of the two workshops was a register over all personal data processing, including where an agreement between controller and processor is needed. The information analysis also revealed that there is no need for a Data Protection Impact Analysis (DPIA) at this point. An information security analysis, with the focus on personal data and GDPR, concluded the *analysis* phase.

4.2.2 Design

In the *design* phase new routines, a personal data policy, and forms and templates were created. The existing model for information classification was updated with information containing personal data. The CIO explained that they have an information classification model that is used, but people probably do not have any understanding of where each information class should be stored. "We have several places to store documents, including cloud services, and people store wherever it is most suitable for them. Most people do not reflect on whether it is okay from a classification perspective. It may largely be because of lack in communication, we had all our documents stored on a secure internal surface only a few years ago, but the change came quickly." A plan was made to communicate the updated information classification model, with a directive on where each class may be stored.

The next task was to create or updated processes, routines, and policies are that are affected by GDPR—for instance, processes in the information management system regarding how to start a new data processing that contains personal data, and procurement of IT systems. Routines were created for conducting a Data Protection Impact Assessment (DPIA), meeting the registered request (for instance to be

forgotten and access) and how to act if a personal data breach occurs. The data storage policy, ISIT policy and personal data processing policy were updated. The final action was to create forms and templates related to the new routines and policies: request for change, correction, and deletion, request for registry extract and a template for data processing agreement. Finally, a new role was appointed: Data Protection Officer.

4.2.3 Implementation

The foundation of the implementation was to execute what was created during the design phase, primarily through communication and education. Communication was intranet-based (where a news item was published and templates uploaded), and through the information management system (where the process regarding personal data processing was updated according to decisions in the design phase). An in-house GDPR training was held, and an online information security course was created. The online course was planned as a recurring annual event. Finally, a yearly GDPR revision was included in the annual calendar.

4.3 Case Three

The third organisation is an event planning company with 10–20 employees. Although the company is small, they process a lot personal information for their many events. Unlike the first two organisations, the researchers did not have any active role in the work. The purpose of this case was to find out whether the framework was also useful for people who were not involved in creating it. Though the researchers did not take part in the actual work in the organisation, they answered questions about the framework and about GDPR. The researchers also monitored progress. The project manager at the organisation felt that the framework helped them, and the work gave them a better understanding of the new regulation. "Before this project we knew that GDPR would force us to some changes, but we had a problem to see where to start, and what needed to be done by us to comply."

4.3.1 Analysis

The organisation has all their IT outsourced. The IT partner has ensured that everything related to IT is GDPR compliant. GDPR compliance cannot be delegated to an external partner to avoid legal responsibility, but the analysis phase concentrates on the organisation's own work. The IT partner will, however, make the analyses on their side and then report back to the organisation. The organisation focused their analysis on what information they got and where it is stored. They created a record of all personal data processing, to get a good overview. The register had, among other things, records of the type of processing, the legal ground for the processing and the type of personal data processed. The records in the registry were then analysed for where data processing agreement is needed.

4.3.2 Design

The design phase was a lot about creating new documents since most of the necessary ones were missing. "Since we are a relatively young company with quite few employees, we have not had much focus on developing policies and other formal documents, our focus has been on our deliveries. Therefore, this was a useful exercise for us." said the project manager. Two new policies were created: Personal Data Processing Policy and Policy of the processing, storage and deletion of personal data. Routines for meeting the registered request (for instance to be forgotten and access) and how to act if a personal data breach occurs were created. Finally, a template for consent and forms for Request for change, correction and deletion and, Request for registry extract were created.

4.3.3 Implementation

During the implementation, all employees received an GDPR education to get a basic understanding of the regulation and how the organisation has chosen to work with personal data processing from now on. All new routines and policies were communicated during an internal GDPR meeting and everyone was informed of where to turn if they got some questions in the future. After the GDPR came into force, the organisation's compliance has been tested several times without demonstrating any shortcomings.

4.4 Case Summary

The main purpose of the three case studies was to evaluate the GDPR compliance framework in live settings, in different types of organisations. Initially, the organisations outlined very different challenges, but as they began to understand the framework the picture slowly changed. In organisation one and three, the biggest concern was initially that they felt that compliance was overwhelming, and that they had no idea where to start or what the eventual goal looked like, but the framework helped them to visualise the road they were about to take and the goal the must reach. The common picture helped the different groups, but it did not resolve all the remaining challenges.

A common picture was that we do not have much personal data and the one we have is stored in the same place. But the information analysis showed quite quickly that there are considerably more personal data than expected and in several different places. With that new insight, a lot of new questions appeared in all three organisations:

- Do we need consent for everything?
- Are we allowed to continue do this?
- Do we need any data processing agreements?

- What is the legal basis for our processing of personal data?

Most of the questions raised during information analysis were solved when the legal basis for each personal data processing where determined. With the new insights, more questions were born. Some specific while others are more general, Table 3 highlights the questions that appeared in all three organisations.

5 Theoretical Evaluation

As mentioned in the introduction, there have been some theoretical evaluations in the literature where GDPR has been compared to its predecessor, DIR95 (Ataei et al. 2018a; Grundstrom et al. 2019; Tikkinen-Piri et al. 2017). Ataei et al. (2018a) has their focus on the user interface level for Location-Based Services rather than issues that SMEs face. Grundstrom et al. (2019) focuses on challenges for the organisation in a specific sector, insurance. These challenges are of interest for SMEs that manages a lot of sensitive personal data and with the same structure as insurance companies, but not all SMEs. There is one study that look at GDPR compliance challenges for all organisations: Tikkinen-Piri et al. (2017). Each identified implication by Tikkinen-Piri et al. (2017) was

Table 3 Common challenges in the three organisations

Common challenges	Framework solutions
What do we need to do in order to get compliant with GDPR?	The complete framework
What personal data processing do we have?	Analysis—information analysis
Do we need any data processing agreements?	Analysis—information analysis
What is the legal basis for our processing of personal data?	Analysis—the legal ground for processing
Do we need consent for everything?	Analysis—the legal ground for processing
Are we allowed to do this?	Analysis—the legal ground for processing
What information shall we give to data subject´s? (With this question specific situations were mentioned all the time)	Analysis—the legal ground for processing Design—policies Implementation—creating conditions for continued compatibility with GDPR
What information become more sensitive with GDPR?	Analysis—updated information classification scheme and information classification
Which level is good enough for data protection?	Analysis—information and IT security analysis
Do we already today manage personal information in accordance to GDPR?	Design—routines Design—policies
What shall we do if a personal data breach occurs?	Design—routines
What shall we do if we got a request for registry extract?	Design—routines Design—templates
What information shall we give to data subject´s and how?	Design—policies Everyday business—communication

Table 4 The framework in relation to the twelve practical implications for organisations

Implication (Tikkinen-Piri et al. 2017)	The framework
Specifying data needs and usage	Analysis—information analysis
Considering conditions for data processing in international context	Analysis—information analysis
Building privacy through data protection by design and default	Design—routine
Demonstrating compliance with GDPR requirements	Implementation
Developing processes to deal with data breaches	Design—routine
Reckoning with sanctions for non-compliance	Analysis—information and IT security analysis
Designating a Data Protection Officer (DPO)	Implementation
Providing information to data subjects	Design—policy
	Everyday business—communication
Obtaining consent on personal data usage	Implementation
Ensuring individuals' right to be forgotten	Design—routine
	Design—policy
	Design—template
Ensuring individuals' right to data portability	Design—routine
	Design—policy
	Design—template
Maintaining documentation	Design—routine

mapped to the framework and the result is shown in Table 4, and explained in Sects. 5.1, 5.2 and 5.3, where the implications are in *italics*. An organisation following the framework will deal with all twelve implications identified by Tikkinen-Piri et al. (2017).

5.1 Analysis

Specifying data needs and usage is the first implication, which is addressed in the first analysis, information analysis. The challenge for SMEs is to get a picture of all personal data processing, its legal basis and that the processing is in accordance to GDPR. Information analysis results in a list of all personal data processing and the answer to the implication for each process, it also shows if there is any *data processing in international context* (the second implication). An important aspect of *demonstrating compliance with GDPR requirements* is to ensure security by technical and organisational measures. To know what level that is needed an Information and IT security analysis has to be performed. *Reckoning with sanctions for non-compliance* is the last of the twelve implications—this is managed during the analysis phase. It is about risk management and should be a factor during the Information and IT security analysis and managed during risk mitigation.

5.2 Design

Building privacy through data protection by design and default is about implementing technical and organisational measures and procedures to ensure protection of the rights of all data subjects and compliance with the GDPR. Every process and routine needs to be designed with data protection as a central part, not an option. Some of the more important new routines are the once that deal with the rights of data subjects: *ensuring individuals' right to be forgotten* and e*nsuring individuals' right to data portability*. Both need routines and templates for subjects to fill in when they want to exercise their rights. It is also important for organisations to p*rovide information to data subjects* about their rights, for instance by a personal data policy. Since controllers are obligated to inform supervisory authority about data breaches within 72 h, it is important to d*evelop processes to deal with data breaches*. Other things that the organisation need to do in accordance with supervisory authority is *demonstrating compliance with GDPR requirements* and, on request, provide documents that strengthen their compliance with GDPR. The routine for *maintaining documentation* is then an important task during the design phase to make sure all documents are kept alive.

5.3 Implementation

The last two implications, *obtaining consent on personal data usage* and *designating a Data Protection Officer (DPO)* are tasks for the implementation phase.

6 Conclusion

For most organisations, GDPR requires significant changes in many parts of the organisation; unfortunately many SMEs do not have resources or knowledge to manage this by themselves. If they do not comply, it may risk expensive penalties. This paper has presented a framework for SMEs to use in their work with GDPR compliance. The framework was developed using design science, and the compliance results was reviewed and approved in each of the organisations by both experts and senior management. The result was also evaluated against the twelve practical implications for organisations in their road to GDPR compliance identified in scientific literature (Tikkinen-Piri et al. 2017).

The result suggests that the framework can be of great help to SMEs and provide a secure, low-cost process for GDPR compliance. Although the framework has only been evaluated in three organisations, the result indicates that it is effective. However, it needs to be validated further in more organisations and with subsequent external reviews. It would also be interesting to go back to the organisations in this study if they receive any external reviews, for instance from the Data Protection Authority, to analyse the result once again.

GDPR applies throughout the EU/EEA but this framework is only tested in Sweden. GDPR compliance will look the same in all EU/EEA but the road to compliance may differ depending on how the national law that was replaced by the GDPR was designed. With that background, it may be interesting to also test the framework other EU/EEA countries. Furthermore, the focus in this research is primarily on analysis and design; the implementation part may need to be further examined.

References

Ataei M, Degbelo A, Kray C (2018a) Complying with privacy legislation: from legal text to implementation of privacy-aware location-based services. Int J Geo-Inf 7(442):1–28

Ataei M, Degbelo A, Kray C (2018b) Privacy theory in practice: designing a user interface for managing location privacy on mobile devices. J Locat Based Serv 12(3–4):141–178

Brodin M (2015) Combining ISMS with strategic management: the case of BYOD. In: IADIS international conference information systems, pp 161–168

Brodin M (2017) Security strategies for managing mobile devices in SMEs: a theoretical evaluation. In: 2017 8th International conference on information, intelligence, systems and applications, IISA 2017, pp 89–94

Bu-pasha S (2017) Cross-border issues under EU data protection law with regards to personal data protection. Inf Commun Technol Law 26(3):213–228

De Hert P, Papakonstantinou V, Malgieri G, Beslay L, Sanchez I (2017) The right to data portability in the GDPR: towards user-centric interoperability of digital services. Comput Law Secur Rev 34(2):193–203

Erdos D (2016) Statutory regulation of professional journalism under European data protection: down but not out? J Media Law 8(2):229–265

Graef BI, Husovec M, Purtova N, Journal GL (2018) Articles data portability and data control: lessons for an emerging concept in EU law. Ger Law J 19(06):1359–1398

Gregor S, Hevner AR (2013) Positioning and presenting design science—types of knowledge in design science research. MIS Q 37(2):337–355

Gregor S, Jones D (2007) The anatomy of a design theory. J Assoc Inf Syst 8(5):312–335

Grundstrom C, Väyrynen K, Iivari N, Isomursu M (2019) Making sense of the general data protection regulation—four categories of personal data access challenges. In: Proceedings of the 52nd Hawaii international conference on system sciences, pp 5039–5048

Harris M, Patten K, Regan E, Fjermestad J, Harris M (2012) Mobile and connected device security considerations : a dilemma for small and medium enterprise business mobility? In: AMCIS 2012

Hashim J (2015) Information communication technology (ICT) adoption among SME owners in Malaysia. Int J Bus Inf 2(2):221–240

Hevner A, Chatterjee S (2010) Design research in information systems, vol 22. Springer, New York

ISME (2018) Businesses unprepared for GDPR. Retrieved 5 June 2018, from https://www.isme.ie/report-businesses-unprepared-gdpr/

ISO/IEC (2016) ISO/IEC 27000:2016—information security management systems—overview and vocabulary

Johnson G, Whittington R, Scholes K, Angwin D, Regnér P (2015) Fundamentals of strategy, 3rd edn. Pearson Education, Harlow

Lindqvist J (2018) New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? Int J Law Inf Technol 2018(26):45–63

Lopes IM, Oliveira P (2018) Evaluation of the implementation of the general data protection regulation in health clinics. J Inf Syst Eng Manag 3(4):28
Nunamaker J, Chen M, Purdin T (1991) Systems development in information systems research. J Manag Inf Syst 7:89–106
Olenick D (2019) 60,000 EU data breaches filed under GDPR. Retrieved 10 Feb 2019, from https://www.scmagazine.com/home/security-news/privacy-compliance/60000-eu-data-breaches-filed-under-gdpr/
Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S (2007) A design science research methodology for information systems research. J Manag Inf Syst 24(3):45–78
Rodrigues R, Barnard-wills D, Hert P De (2016) The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR. Int Rev Law Comput Technol 30(3):248–270
Rossi M, Sein MK (2003) Design research workshop: a proactive research approach. In: 26th Information systems research seminar in Scandinavia (IRIS), Haikko, Finland
Schulze H (2018) GDPR compliance report. Retrieved 3 May 2018, from https://crowdresearchpartners.com/portfolio/gdpr-compliance-report/
Sein MK, Henfridsson O, Rossi M, Lindgren R (2011) Action design research. MIS Q 35(1):37–56
Sirur S, Nurse JRC, Webb H (2018) Are we there yet ? Understanding the challenges faced in complying with the general data protection regulation (GDPR). In: MPS'18, pp 88–95
Stanciu V, Rîndaşu S (2018) The impact of general data protection regulation in the accounting profession—evidences from Romania. J Inf Assur Cyber Secur 2018(2018):1–9
Supyuenyong V, Islam N, Kulkarni U (2009) Influence of SME characteristics on knowledge management processes: the case study of enterprise resource planning. J Enterp Inf Manag 22(1/2):63–80
The European Commission (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Off J Eur Union 281(23/11/1995):31–50
The European Commission (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC General Da. Off J Eur Union 119(1):1–88
The European Commission (2018) What is SME? Retrieved 20 June 2018, from http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en
Tikkinen-Piri C, Rohunen A, Markkula J (2017) EU general data protection regulation: changes and implications for personal data collecting companies. Comput Law Secur Rev 34(1):134–153
Urquhart L, Sailaja N, Mcauley D (2018) Realising the right to data portability for the domestic Internet of things. Pers Ubiquitous Comput 22:317–332
Vaishnavi V, Kuechler W (2004) Design science research in information systems. http://www.desrist.org/design-research-in-information-systems/
Vaishnavi VK, Kuechler W (2007) Design science research methods and patterns: innovating information and communication technology. Taylor & Francis Group, New York
Vanberg AD, Ünver MB (2017) The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? Eur J Law Technol 8(1):1–22
Walls JG, Widmeyer GR, El Sawy OA (1992) Building an information system design theory for vigilant EIS. Inf Syst Res 3(1):36–59

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH ("Springer Nature").

Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users ("Users"), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use ("Terms"). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.

These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.

We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.

While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval , sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.

These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.

To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.

Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.

If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com