EU General Data Protection Regulation: Changes and implications for personal data collecting companies

Christina Tikkinen-Piri[a]
Anna Rohunen[a,*]
Jouni Markkula[a]

[a]University of Oulu, Finland
[*]University of Oulu, Faculty of Information Technology and Electrical Engineering (ITEE), Empirical Software Engineering in Software, Systems and Services (M3S) research unit, P.O. Box 4500, FI-90014, University of Oulu, Finland. E-mail address: anna.rohunen@oulu.fi

Abstract

The General Data Protection Regulation (GDPR) will come into force in the European Union (EU) in May 2018 to meet current challenges related to personal data protection and to harmonise data protection across the EU. Although the GDPR is anticipated to benefit companies by offering consistency in data protection activities and liabilities across the EU countries and by enabling more integrated EU-wide data protection policies, it poses new challenges to companies. They are not necessarily prepared for the changes and may lack awareness of the upcoming requirements and the GDPR's coercive measures. The implementation of the GDPR requirements demands substantial financial and human resources, as well as training of employees; hence, companies need guidance to support them in this transition. The purposes of this study were to compare the current Data Protection Directive 95/46/EC with the GDPR by systematically analysing their differences and to identify the GDPR's practical implications, specifically for companies that provide services based on personal data. This study aimed to identify and discuss the changes introduced by the GDPR that would have the most practical relevance to these companies and possibly affect their data management and usage practices. Therefore, a review and a thematic analysis and synthesis of the article-level changes were carried out. Through the analysis, the key practical implications of the changes were identified and classified. As a synthesis of the results, a framework was developed, presenting 12 aspects of these implications and the corresponding guidance on how to prepare for the new requirements. These aspects cover business strategies and practices, as well as organisational and technical measures.

Keywords: General Data Protection Regulation, GDPR, Data Protection Directive, Personal data

1. Introduction

The European Parliament voted on the General Data Protection Regulation (GDPR) in May 2016. The GDPR will come into force and replace the current Data Protection Directive 95/46/EC (hereinafter DIR95) in May 2018. It will improve data subjects' privacy protection and facilitate organisations' and companies' work through its clarified rules, more concretised requirements and even direct instructions on the provisions' implementation. On the other hand, the GDPR's new obligations bring considerable changes to companies' privacy protection implementation. All companies handling EU residents' personal data or monitoring data

subjects' behaviour within the EU, regardless of where they are based, will be governed by the GDPR. This indicates that non-EU and international companies will have to comply with both their national legislation and the GDPR. Since its adoption in 1995, DIR95 has been the central legislative, personal data privacy instrument in the European Union (EU). The GDPR has been under development since 2009, and the European Commission officially published a proposal for the data protection reform in early 2012 (de Hert and Papakonstantinou, 2016). In 2018, the GDPR will finally come into force after this multiphase law-making process. The GDPR aims to improve the level of personal data protection and harmonisation across the EU as DIR95 no longer meets the privacy requirements of the present-day digital environment.

Data privacy legislation has been evolving with the development of personal data collection and processing technologies since the rapid progress in electronic data processing began in the 1960s. In Western countries, legislation on personal data privacy was established at that time, in both Europe and the United States (US). The first means of ensuring data privacy were the data protection act passed by the German federal state of Hessen in 1970, the Swedish data protection act adopted in 1973 and the Fair Information Practices (FIPs) formulated by the US government in 1973. Since then, several other initiatives on privacy regulation have been launched. Many of them have applied and further developed FIPs, such as the Organisation for Economic Co-operation and Development (OECD) guidelines, DIR95 and now the GDPR, with the FIP-based Privacy by Design and Privacy by Default (PbD) principles.

Rapid technological development due to the convergence of calculation power progress, increased storage capacity and advanced network technology makes it possible for companies to collect, process and interlink data in an expanded way. They increasingly tend to use these data for various purposes, such as personalised services and marketing. As a result of technological development, along with globalisation, new and increased challenges for personal data protection have emerged (Reding, 2010). Although new technologies and services benefit both businesses and consumers, they also generate serious privacy risks. This situation may decrease people's trust in companies that collect data for their service production. The lack of trust can slow down the development of the innovative use and adoption of new technologies (Reding, 2010), and many new business opportunities may be missed if appropriate data protection practices are not implemented.

The GDPR aims to meet the current challenges related to personal data protection, strengthen online privacy rights and boost Europe's digital economy. It specifically aims to provide individuals with better capabilities for controlling and managing their personal data (Mantelero, 2013), hence striving to reinforce the data subjects' trust in personal data collecting companies. Within the new data protection framework, individual service users may also benefit from the free movement of data if it results in growing businesses with improved and personalised services.

The companies collecting, processing and utilising personal data are required to comply with the data privacy legislation. They should now proactively prepare for the changes that the GDPR brings and adapt to these changes within a given time span. Implementing data privacy in business operations is often challenging as such. For example, PbD rests on a proactive approach to privacy and privacy assurance as the organisation's default mode of operation (Cavoukian, 2009). It promotes embedding privacy into the design of information technology systems and business practices by default in a data-minimising way. The adoption of PbD principles in systems design has proven demanding, although there are specified means for achieving PbD goals (Spiekermann, 2012). Data privacy implementation also deals with a complex whole, covering different aspects, including company-level awareness raising and training, adoption of organisational and technological data protection measures, and documentation of processing operations. In parallel with putting these into practice, personal

data utilisation and processing should be enabled in a way that benefits companies. In this light, companies clearly need substantial amounts of time, resources and guidance to implement data privacy.

A major challenge related to the implementation of the GDPR is the companies' lack of awareness and understanding of the forthcoming changes and requirements that the GDPR imposes through its new rules. These requirements have various practical implications for organisational processes and practices, technological system design, as well as personnel training and assignment of new responsibilities in the organisations. Such demands bring out the need to review and revise current data privacy practices and technological data protection measures, as well as possibly plan new ones to ensure compliance with the GDPR. Some companies understand the need for changes, but research indicates that the information about the GDPR and its provisions is not necessarily diffused to them in a timely manner. According to London Economics (2013), Mikkonen (2014) and a TRUSTe survey (2015), less than half of the companies were aware of the GDPR changes. Learning about and understanding legislative requirements as such are often cumbersome and time consuming, resulting in difficulties in the implementation of the legislation's provisions. As for the GDPR, a comprehensive reform with coercive measures (such as substantial sanctions for infringements) is expected to take place. This makes the situation even more challenging and requires from companies additional actions and responsibilities to achieve compliance. The implementation of the GDPR necessitates changes that have diverse implications for companies and the usage of their resources. For example, complying with the GDPR will strongly affect information-intensive, small- and medium-sized enterprises (SME) that drive their revenue growth from online advertising (Thüsing and Traut, 2013). These companies also cannot necessarily afford juridical help to comply with the new rules of the GDPR. As non-compliance with the GDPR poses financial, legal and reputational risks to companies, they may want to deal with the GDPR requirements through their risk management policies and risk analyses. In this way, data privacy issues can be managed by means of companies' established risk management procedures.

This paper aims to help with the GDPR implementation by providing information on its changes and their practical implications, specifically for personal data intensive companies. These companies extensively collect and process personal data for their service production and largely base their business and service provision on these data. They include social media, healthcare, mobility and financial services, for example. These companies need to take into account the new GDPR requirements when they develop their business strategies and policies, in which personal data usage plays a central role. To tackle this issue, the research question was set: *What are the strategic, business practice, organisational and technical implications of the GDPR for personal data intensive companies?*

We answer this problem based on a systematic review and analysis of the key changes introduced by the GDPR and their practical implications for companies' current data protection practices. These implications are discussed and elaborated, and approaches to their implementation are outlined. Based on this information, companies can be educated on how to prepare for the GDPR and apply its rules in their everyday actions. It can help them ensure their personal data management and usage practices' compliance with the new requirements and manage a successful transition. It may also ease the timely management of the GDPR requirements' implementation, which is a strategic-level issue demanding substantial financial and human resources, including employee training. Early adoption of the required changes not only guarantees compliance with the GDPR but can also bring competitive advantage to the companies.

The rest of this paper is organised as follows. Section 2 presents a brief history of data protection, describing the development of privacy legislation over the previous decades. Section 3 discusses the research methodology, and Section 4 covers the identified changes introduced by the GDPR. Section 5 explains the GDPR's practical implications and outlines approaches for implementing its requirements. Finally, Section 6 concludes this paper.

2. History of data protection

The development of automatic processing of personal data, together with businesses' increasing tendency towards personal data collection and usage, implies various societal benefits (both at the organisational level and in individual persons' lives), such as efficiency, quality and productivity. On the other hand, it is evident that this evolution also poses privacy challenges. Privacy belongs to fundamental human rights in Western countries and is controlled by legislation that responds and adapts to data subjects' privacy needs.

The European Convention for the Protection of Human Rights and Fundamental Freedoms (referred to as the European Convention on Human Rights [ECHR]) was drafted by the Council of Europe in 1950 and entered into force in 1953 (Council of Europe, 1950). Its Article 8 guaranteed member states' citizens the right to the respect for private and family life, home and correspondence, according to the Universal Declaration of Human Rights that was proclaimed and adopted by the General Assembly of the United Nations in 1948 (United Nations, 1948). Even in the 1960s, the rapid progress in the electronic data processing field enabled public administrations and large enterprises to set up extensive data banks and to improve and increase the collection, processing and interlinking of personal data (Council of Europe, 2017). This situation soon evoked discussions on information privacy and brought out the need for personal data protection (cf. Westin, 1967; European Union Agency for Fundamental Rights & Council of Europe, 2014). As the then existing legislation with an uncertain scope of private life and the emphasis on protection only against public authorities' interference was no longer considered adequate, the Council of Europe initiated the establishment of a framework of specific principles and norms to prevent unfair collection and processing of personal data in both private and public sectors (Council of Europe, 2017; European Data Protection Supervisor, 2005).

The growing use of automated personal data systems resulted in the establishment of data privacy regulation in the US as well. Personal data privacy protection principles were formulated by the US government first. The US Department of Health, Education, and Welfare (1973) proposed and named FIPs as a set of principles for protecting the privacy of personal data in record-keeping systems in 1973. One year later, the US Privacy Act was passed (United States of America, 1974 [5 U.S.C. § 552a]). This act applies the FIPs to federal agencies' record systems and governs their collection, maintenance, use and dissemination of information about individuals. Subsequently, different versions of FIPs have been developed, for example, by the Federal Trade Commission (FTC, 1998). They have also been widely applied in the legislation of different countries.

Meanwhile, the development of data protection principles in Europe resulted in the introduction and adoption of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) in 1981 (Council of Europe, 1981). Its implication was that necessary measures should be taken regarding contracting parties' domestic laws to implement the principles laid down in the convention (Council of Europe, 2017). As stated by the European Data Protection Supervisor (2017), Convention 108 set minimum standards for protecting individuals' personal data against abuses, possibly associated with the collection and processing of these data. Another objective was to regulate

the transborder flow of personal data. Around the same time as the introduction of Convention 108 and similar to it, the OECD (2011) issued and adopted the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Both Convention 108 and the OECD Guidelines relied on FIPs as their core principles, revising and extending the FIPs' original statement but not using the term (Gellman, 2015). The work in the Council of Europe and in the OECD resulted in many European countries' enactment of national-level legislation for balancing an individual's right to data protection with the need of public authorities, employers, and so on, to process data (European Data Protection Supervisor, 2005).

In the beginning of the 1990s, an EU-level initiative was taken to harmonise data protection, based on Convention 108. Consequently, in 1995, the EU adopted the European Commission's DIR95, to be implemented in EU member states through national laws (European Commission, 1995). This directive regulates the protection of individuals with regard to personal data processing and its free movement within the EU. The directive relies on the OECD's FIP-based core principles, resulting in their implementation throughout Europe. In 2002, the European Commission introduced the Directive on Privacy and Electronic Communications (EC Directive 2002/58/EC) (European Commission, 2002). This directive concerns the processing of personal data and the protection of privacy in the electronic communications sector, and it complements DIR95. For example, the directive regulates confidentiality, unsolicited communications, and processing of billing, traffic and location data.

Compared with the EU, in the US, no such national omnibus legislation regulating personal data collection and use has been developed. Instead, the US approach to data protection relies on a sector-by-sector basis regulation and self-regulation, also having different statutes for the public and the private sectors (Schwartz, 2013). For example, the US industry-specific legislation incorporates the Health Insurance Portability and Accountability Act (United States of America, 1996 [43 U.S.C. § 1320d-9]) and the Fair Credit Reporting Act (United States of America, 1970 [15 U.S.C. § 1681]). The US privacy legislation also consists of state-level privacy laws, such as the regulations of the Massachusetts General Law with the prescription of comprehensive information security programmes by companies (Commonwealth of Massachusetts, 2010). To bridge the differences between the US and the EU data protection approaches and to provide US organisations with streamlined means to comply with DIR95, the US Department of Commerce developed (in consultation with the EU) the US-EU Safe Harbor program (European Commission, 2000; US Department of Commerce's International Trade Administration, 2015), which was launched in 2000. It allowed US companies to obtain a voluntary certification, and compliance was overseen by US federal agencies, specifically the FTC (Schwartz, 2013). The European Commission approved its draft of the standard contractual clauses (i.e., model contract provisions) in 2001. These contractual clauses can be used by US organisations, as an alternative to joining the Safe Harbor program, to meet the adequacy requirement of DIR95 for privacy protection (Schwartz, 2013). As another alternative to Safe Harbor, binding corporate rules (BCRs) were developed by the EU Article 29 Working Party and adopted in 2003 (Article 29 Data Protection Working Party, 2003). The BCRs can be used when international personal data transfer occurs within a single multinational company or within the members of a corporate group. In October 2015, the Court of Justice of the EU (the Court) declared the European Commission's Safe Harbor decision (2000/520/EC) invalid because it enabled US public authorities' interference with the fundamental rights of persons by accessing their data (Court of Justice of the EU, 2015). The Court also found that the Safe Harbor decision denied the national supervisory authorities their powers. In February 2016, the European Commission and the US government agreed on the establishment of a new framework for personal data exchanges for commercial purposes. In July 2016, the European Commission adopted the EU-US Privacy Shield to fulfil the requirements set out by the Court's ruling (European Commission, 2016a). The Privacy Shield imposes obligations on US companies to protect personal data, including regular updates and reviews by the US

Department of Commerce, as well as sanctions in case of non-compliance with the rules. It also requires written assurance from the US that public authorities' access to personal data will be subject to clear limitations, safeguards and oversight mechanisms. Although in use since August 2016, challenges have been found regarding the Privacy Shield's validity and associated overall assessment of the US legal order (Tracol, 2016).

DIR95 has been a central legislative, personal data protection instrument in the EU. Currently, 20 years after its implementation, the directive does not provide the degree of harmonisation that is required among the EU member states or the efficiency to ensure the right to personal data protection in the present-day digital environment (European Commission, 2012a). Due to the inadequate harmonisation, Europe remains at a disadvantage in the global competition with other countries, such as the US and China (Dix, 2013). The European Commission is tackling the situation by proposing a fundamental reform of the EU's data protection framework, to come into force in May 2018 (European Commission, 2016b). The reform consists of two instruments – the GDPR and the Directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities. The reform will emphasise the GDPR, which is proposed to replace DIR95. The GDPR points out the role of the FIP-based PbD principles (Cavoukian, 2009) and obliges companies to integrate these principles into their business processes (European Commission, 2012b). The economic impact of this unified regulation will be significant because currently, European and non-European market participants have to deal with 28 separate legal frameworks.

3. Methodology

The main research question of this study was set to be: *What are the strategic, business practice, organisational and technical implications of the GDPR for personal data intensive companies?* To answer this question we decomposed it into two more specific research questions.

The first research question is:

- What are the changes introduced by the GDPR compared to DIR95?

Through this research question, we aimed to identify the GDPR's imposed changes with practical relevance from the companies' perspective, as well as the corresponding key aspects that they need to focus on when preparing to implement the GDPR requirements.

The second research question is:

- What are the main practical implications of the GDPR's imposed changes for personal data intensive companies?

Through this research question, we aimed to identify the practical implications of the GDPR changes regarding personal data intensive companies' strategic and business practice-level, organisational and technical privacy protection measures.

In our systematic review, analysis and synthesis of the GDPR changes, we identified the GDPR articles with implications for personal data intensive companies' data management and usage processes and practices, as well as their technological systems. We then searched for and identified the articles with corresponding contents in DIR95. We compared the GDPR articles with the corresponding DIR95 articles and extracted the changes introduced by the GDPR. In

the analysis, we included only the GDPR articles with changes that were relevant to the research questions (i.e., those concerning personal data intensive companies) and omitted some of the relevant GDPR articles with no significant changes with respect to this research.

We used the extracted changes as themes of the analysis, using the GDPR's article structure as the basis and combining the articles about similar subjects under the themes. The themes were general provisions and principles, transparency and modalities, information and access to personal data, rectification and erasure, right to object and automated individual decision making, general obligations, security of personal data, data protection impact assessment and prior consultation, data protection officer (DPO), codes of conduct and certification, transfer of personal data to third countries or international organisations, and remedies, liability and penalties. We conducted the analysis at the article level to facilitate finding a more detailed description of the GDPR requirements that would be of interest to readers. In the analysis, we specified the changes to present the new, specified and clarified obligations, principles and provisions of the GDPR. We described and explained these changes to provide a clear understanding of their requirements from the perspective of personal data intensive companies.

Based on the analysis of the changes, we identified and classified their key practical implications for personal data intensive companies. We compiled these implications into a framework with 12 aspects that the companies should consider when preparing to implement the GDPR requirements. We formed and discussed these aspects, instead of the GDPR article-level changes, as some of the GDPR requirements cover several articles (e.g., the information provision aspect covers articles of the following GDPR sections: *Transparency and modalities*, *Information and access to personal data*, and *Right to object and automated individual decision making*). We elaborated on the 12 aspects and outlined suggestions on how to consider them in practice. In this way, the GDPR's implications for companies can be understood, and they can prepare for and manage the practical changes that the GDPR will bring to their everyday operations and activities.

4. Changes introduced by the GDPR

The results of the thematic analysis of the changes introduced by the GDPR were compiled according to its articles. As some of the new articles of the GDPR build on the articles of DIR95, their differences are explained, and the changes are described in relation to the articles of DIR95. The analysis does not cover the GDPR restrictions (Article 23) that provide for the EU's or its member states' possibility to restrict the scope of the GDPR's obligations and rights (Article 5, Articles 12–22 and Article 34) when needed, for example, to safeguard national security, defence or public security in a democratic society. Subsections 4.1–4.12 specify and describe the changes identified in the analysis. Each subsection starts with a summary of the GDPR's key changes regarding the themes. These summaries aim to present the main results of the analysis in a clear and concise form, to be specified and described in greater detail below.

4.1. General provisions and principles

GDPR Articles 1–11

Corresponding articles in DIR95: Definitions (Article 2), national law applicable (Article 4), principles relating to data quality (Article 6), criteria for making data processing legitimate (Article 7) and processing of special categories of data (Article 8)

- Extended territorial scope: applies to EU-based controllers and processors regardless of where the processing takes place, personal data processing related to goods or services

offered to the data subjects in the EU, and monitoring of the data subjects' behaviour within the EU
- New definitions: pseudonymisation, genetic data, biometric data, data concerning health, binding corporate rules and personal data breach
- New provisions and principles: transparency of data processing, accountability, and processing which does not require identification
- Clarified or specified provisions and principles: data minimisation principle, conditions for consent, and lawful data processing (especially the conditions for the lawfulness of processing children's personal data)
- Added conditions concerning a child's consent in relation to information society services: consent or authorisation by the child's parent or custodian is required if the child is younger than 16 years old.

The GDPR includes an *extended territorial scope* for personal data processing operations under its governance (Article 3). In addition to the activities of the controller's establishment and the personal data processing in an EU member state, as specified in DIR95, the GDPR also applies to the processing by controllers or processors that are not established in the EU if they offer goods or services to the data subjects in the EU or monitor the data subjects' behaviour within the EU.

The GDPR introduces new definitions relevant to personal data intensive companies and their processing operations (Article 4). Under the GDPR, the principles and the provisions for the processing are largely the same as those of DIR95, but the GDPR has the following additions: *transparency of data processing* (Article 5), *accountability* (Article 5) and *processing which does not require identification* (Article 11). The GDPR further clarifies and specifies some of the principles that are already present in DIR95, as follows: *data minimisation principle* (Article 5), *conditions for consent* (Article 7) and *criteria for lawful processing* (Article 6).

The GDPR's general provisions include new definitions for pseudonymisation, sensitive personal data types, data protection policies and data breach, as follows. *Pseudonymisation* refers to personal data processing in such a way that the data cannot be attributed to a specific data subject without any additional information; this requires keeping such additional information separately and subject to technical and organisational measures ensuring non-attribution. *Genetic data* is defined as any data relating to an individual's characteristics that are inherited or acquired during early prenatal development. *Biometric data* denotes any data relating to an individual's physical, physiological or behavioural characteristics and allowing a unique identification (e.g., facial images or dactyloscopic data). *Data concerning health* means any information related to an individual's physical or mental health or the provision of health services to the individual. *Binding corporate rules* involve personal data protection policies that are adhered to by a controller or a processor for personal data transfers to third countries for processing and using the data. *Personal data breach* means a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data that are transmitted, stored or otherwise processed.

The GDPR's new principles and provisions are *transparency of data processing*, *accountability* and *processing which does not require identification*. The GDPR requires *personal data to be processed in a transparent manner* in relation to the data subject, in addition to lawful and fair processing provided in DIR95. As the GDPR specifies that personal data must be processed under the controller's responsibility and liability, the controller is obliged to ensure and demonstrate its processing operations' compliance with the GDPR provisions. The GDPR introduces the concept of *accountability*, referring to the controller's responsibility for

demonstrating this compliance. Regarding the principle of *processing which does not require identification*, the GDPR stipulates that the controller is not obliged to maintain, acquire or process additional information to identify the data subject if the purposes for which the data are processed do not require identification by the controller. If the controller is able to demonstrate that it cannot identify the data subject, it has to communicate this to him or her.

DIR95 stipulated that personal data should be adequate, relevant and not excessive in relation to the purposes of its collection and processing. The GDPR's clarified *data minimisation principle* further requires limiting personal data to the minimum necessary for processing purposes and processing personal data only if (and as long as) the purposes cannot be fulfilled without personal data. The GDPR includes notable developments regarding *consent to be valid for lawful processing*. DIR95 provided for the data subject's unambiguous consent, whereas the GDPR requires that a data subject's consent be given freely and be a specific, informed and explicit indication of his or her wishes. Under the GDPR, the controller bears the burden of proof of the data subject's consent to the processing of his or her personal data. If the data subject's consent is to be given in a written declaration concerning other matters as well (such as contracts), the request for consent must be presented so that it is clearly distinguishable from the other issues. Under the GDPR, the data subject also has the right to withdraw his or her consent at any time. However, the withdrawal does not affect the lawfulness of processing based on the consent before its withdrawal. The GDPR complements the *prerequisites of lawful processing* required by DIR95, providing that the data subjects' interests or fundamental rights and freedoms (requiring protection of personal data) are not overridden by the controller's legitimate interests, particularly when the data subject is a child (this does not apply to the processing carried out by public authorities in the performance of their tasks).

The GDPR sets the conditions for processing children's data in relation to information society services offered directly to children. The processing of a child's personal data is lawful if the child is at least 16 years old (member states may by law require a lower age but 13 years at the minimum). If the child is younger, processing is lawful only if consented to or authorised by the child's parent or custodian. In this case, the controller is obliged to make reasonable efforts to obtain verifiable consent, considering the available technology.

4.2. Transparency and modalities

GDPR Article 12

Corresponding article in DIR95: The data subject's right of access to data (Artcile 12)

- New obligations of controllers: provision of transparent and easily accessible and understandable information about personal data processing, provision of procedures and mechanisms to extend the modalities for exercising the data subject's rights (including the means for electronic requests, responding to the data subject's request within a defined deadline and providing information about the reasons for possible refusals)

The GDPR obliges the controller to provide the data subject with any information and communication on personal data processing in an intelligible form. DIR95 required this as well but did not mention any specific format requirements for the information. The GDPR specifies that clear and plain language, adapted to an understandable format for a variety of data subjects, has to be used. This is especially essential when the information is addressed to a child. Standardised icons can also be used to provide overview information on the intended processing. The GDPR extends the data subject's right to obtain information on his or her personal data processing by stating that if the personal data are processed by automated means,

the controller has to provide the means for requests (and for corresponding information provision) to be made electronically. Under the GDPR, the controller must respond to the data subject and provide the requested information within one month from the request, whereas DIR95 only required responding 'without excessive delay'. If the controller refuses to respond to the request, it has to inform the data subject of the reasons for the refusal and the possibilities for lodging a complaint to the supervisory authority.

4.3. Information and access to personal data

GDPR Articles 13–15

Corresponding articles in DIR95: Information to be given to the data subject (Articles 10–11) and the data subject's right of access to data (Article 12a)

- Specified obligation of the controller: new information requirements for providing the data subject with additional information about the controller, the data subject's rights and data transfers to third countries
- Added informational requirements related to the data subject's right of access to his or her personal data: If the data subject's personal data are being processed, he or she has the right to receive additional information on the data processing and his or her related rights.

The GDPR brings new and notable additions regarding the information provision to the data subject. In addition to the information required by DIR95 (controller and representative identity, purposes of processing, data recipients, voluntariness or obligatoriness of the data disclosure, possible consequences of the failure to provide the data, and the right to access and rectify the data), the GDPR obliges the controller to provide the data subject with the following information about the controller and its data processing: the contact details of the controller, the controller's representative (if any) and the DPO; legal basis for the processing; the controller's or a third party's legitimate interests based on which the processing is carried out; information about the source of the personal data (if not collected from the data subject) and whether it originates from publicly accessible sources; and the period during which the personal data will be stored (if this is not possible, then the criteria used to determine the storage period have to be presented). Furthermore, the controller is obliged to inform the data subject about the latter's rights to the following: obtain erasure of the personal data, obtain restriction of the processing, object to the processing, have data portability, lodge a complaint with the supervisory authority and withdraw consent to the processing at any time (this does not affect the lawfulness of processing based on the consent before its withdrawal). The controller also has to inform the data subject if it intends to transfer data to a third country or an international organisation. In such an event, information on the corresponding level of data protection has to be provided by referring to an adequacy decision by the European Commission or to appropriate safeguards. The GDPR maintains the possible derogations in DIR95; for example, there is no information obligation if the law expressly provides for personal data recording or disclosure. If the controller intends to process the personal data for a purpose different from the original one, it has to provide the data subject with information on this new purpose prior to processing.

The GDPR adds new rules regarding the data subject's access to personal data. Similar to DIR95, the GDPR stipulates the data subject's right to obtain from the controller, on request, confirmation on whether or not personal data relating to him or her are being processed. If so, the controller is obliged to provide the following information, in addition to the information required by DIR95 (purposes of the processing, categories of processed data and data recipients): the storage period (or the criteria for determining this period); the right to request rectification or erasure of personal data or to restrict or to object to its processing; the right to lodge a complaint with the supervisory authority; and the existence, logic and envisaged

consequences of automated decision making, including profiling. If the data have not been obtained from the data subject, any available information on its source should be provided. In case the personal data are transferred to a third country or an international organisation, the data subject has the right to obtain information on the appropriate safeguards (Article 46) relating to the transfer.

4.4. Rectification and erasure

GDPR Articles 16–20

Corresponding article in DIR95: Right of access (Article 12b–c)

- Data subject's specified rights to rectification, erasure and restriction of processing of personal data: the conditions of the data subject's right to be forgotten, the conditions of the data subject's right to restriction of processing
- Data subject's new right: data portability from one system to another

The GDPR guarantees the data subject's right to obtain *rectification, erasure and restriction of processing* of his or her personal data, similar to DIR95 (Articles 16–18). The GDPR specifies this right by setting new conditions for the *right to erasure (right to be forgotten)* (Article 17). In this way, the GDPR provides for the data subject's right to erasure without the grounds required by DIR95 (such as incompleteness or inaccuracy of the data). The GDPR also specifies the conditions for the restriction of the data processing and introduces *the data subject's right to data portability* (Article 20).

The GDPR further specifies *the right to erasure* by providing the conditions for the *right to be forgotten principle*. Under the GDPR, the data subject has the right to obtain from the controller the deletion of his or her personal data and its abstention from further dissemination on the following grounds: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; the data subject withdraws consent on which the processing is based and where there are no other legal grounds for the processing; the data subject objects to the processing of personal data for specific purposes (Article 21(1)), and there are no overriding legitimate grounds for the processing; the data subject objects to processing for direct marketing purposes; the data are unlawfully processed; or the personal data have been collected for the purpose of offering information society services to a child. If the controller has made the personal data public and is obliged to erase these data, it has to inform other controllers about the data subject's request for the erasure of any link, copy or replication of the data.

Under the GDPR, in certain cases, instead of erasure, the *restriction of the personal data processing* is sufficient. DIR95 already guaranteed the data subject the right to obtain blocking of data if the processing does not comply with its provisions, particularly in case of incomplete or inaccurate data. However, the GDPR specifies the following grounds for restriction: the accuracy of the personal data is contested by the data subject (in this case, restriction is set for a period, enabling the controller to verify the accuracy of the data); the processing is unlawful, and the data subject opposes the erasure and requests the restriction instead; the controller no longer needs the personal data for the accomplishment of its task, but the data are required by the data subject as proof for legal reasons; and the data subject has objected to the processing, and the verification is pending on whether the legitimate grounds of the controller override those of the data subject. When the personal data processing is restricted, the controller must inform the data subject before lifting the restriction.

According to the new principle of the *right to data portability*, the data subject is entitled to receive the personal data that he or she has provided to a controller for automated processing based on consent or a contract. These data have to be provided to the data subject in a structured, commonly used and machine-readable format. The data subject also has the right to have these data transmitted directly to another controller. The controller is required to ensure that the *right to data portability* will not adversely affect the rights and freedoms of others and that the exercise of portability will not prejudice the *right to be forgotten*.

4.5. Right to object and automated individual decision making

GDPR Articles 21–22

Corresponding articles in DIR95: The data subject's right to object (Article 14) and automated individual decisions (Article 15)

- Specified right to object to personal data processing, including profiling: The right to object has to be presented clearly and separately from any other information. The controller is required to demonstrate compelling legitimate grounds for the processing, which override the interests or fundamental rights and freedoms of the data subject (i.e., the controller bears the burden of proof).
- Specification relative to the data subject's right not to be subject to a decision based on automated processing: Subjecting the data subject to a decision is allowed only based on a contract between the data subject and the controller or on the grounds of the data subject's explicit consent.

The GDPR specifies the *right to object* to the processing of personal data by requiring the communication of this right to the data subject and adding the *burden of proof* principle (Article 21). The GDPR also specifies the data subject's right not to be subject to a measure based on automated decision making and extends this right to *profiling* (Article 22).

Similar to DIR95, the GDPR provides for the data subject's *right to object* to the processing of his or her data for certain specified purposes at any time, on grounds relating to his or her particular situation. This processing is related to public interest, the exercise of official authority or the controller's legitimate interests. The GDPR also obliges the controller to present the *right to object* to the data subject, clearly and separately from any other information. When the data subject objects to the processing, the controller has to quit processing unless it demonstrates compelling legitimate grounds, which override the interests or fundamental rights and freedoms of the data subject (i.e., the controller bears the *burden of proof* to demonstrate these grounds). Compelling legitimate grounds can be related to the establishment of legal claims, for example. The GDPR guarantees the data subject the right to object to personal data processing for *direct marketing purposes*, similar to DIR95; if the data subject objects, his or her personal data cannot be processed for these purposes anymore. In the GDPR, processing of this kind also covers profiling related to direct marketing. The GDPR obliges the controller to provide the data subject with automated means to object to the processing of his or her data for the information society services.

The GDPR specifies the data subject's *right not to be subject to automated individual decisions* that are based solely on automated processing of data and intended to evaluate the data subject's personal aspects, such as performance at work, creditworthiness, reliability and conduct (Article 15). The GDPR adds the data subject's right not to be subject to a measure based on *profiling*, which can be used as the basis of decisions, whether or not these are automated. *Profiling* means automated personal data processing that is used for evaluating personal aspects to analyse or predict a person's performance at work, his or her economic situation, health,

personal preferences, interests, reliability, behaviour, location or movements. The GDPR also specifies cases in which the right not to be subject to automated decisions does not apply, as follows: the processing is based on a *contract* between the data subject and a data controller, the data subject has given his or her *explicit consent* to the processing, or automated decision making is authorised by the EU or a member state's law. If the automated decision making takes place on the grounds of a contract or consent, the controller has to implement measures to safeguard the data subject's rights and freedoms and legitimate interests. At the minimum, the data subject has to be provided with the right to be in contact with a natural person so that he or she can express his or her point of view and to contest the automated decision. Automated individual decision making cannot be based on special categories of personal data (defined in Article 9), unless the data subject has given explicit consent for processing, and the EU or the member state's law does not stipulate that the prohibition of the processing of these data may not be lifted by the data subject.

4.6. General obligations

GDPR Articles 24–31

Corresponding articles in DIR95: Confidentiality of processing (Article 16), security of processing (Article 17), notification (Article 18) and contents of notification (Article 19)

- New grounds for the controller's obligations: principles of data protection by design and by default
- Clarifications concerning responsibilities and obligations: controllers' responsibilities in situations with several joint controllers, and position and obligations of processors related to personal data processing under the controllers' authority
- New obligations of controllers and processors: maintain records of processing activities under their responsibility and co-operate with the supervisory authority; for the controllers and the processors that are not established in the EU, obligation to designate a representative in the EU under certain conditions

The GDPR's stipulated *general obligations of the controllers and processors* of personal data (Articles 24–31) cover the corresponding DIR95 obligations, namely, *confidentiality of data processing* (Article 16), *security of data processing* (Article 17), the controller's obligation to *notify the supervisory authority* of its processing operations, and specified *contents of this notification* (Articles 18–19). General obligations (Article 24, responsibility of the controller) require the controller to implement appropriate technical and organisational measures to ensure data protection and accountability concerning these measures. The GDPR sets out the new principles of *data protection by design and default* (Article 25). It clarifies the *responsibilities of joint controllers* (Article 26) and the *position and obligations of the controllers and data processors* (Articles 28–29). The GDPR also introduces two new obligations, as follows: controllers' and processors' obligation to maintain records of processing activities under their responsibility and to co-operate with the supervisory authority (replacing the DIR95 obligation to notify the supervisory authority) (Article 30) and controllers' and processors' obligation to *designate a representative* in the EU if they are established elsewhere (Article 27).

According to the general obligation concerning the *responsibility of the controller*, the controller has to adopt data protection policies and implement appropriate technical and organisational measures to ensure that personal data processing is performed in compliance with the GDPR. The controller should also be able to demonstrate this compliance. Technical measures include pseudonymisation or encryption (Article 32), for example. Organisational measures include maintaining a record of processing activities (Articles 30–31) and performing a data protection impact assessment (Article 35), among others. The GDPR obliges the

controller to implement mechanisms to ensure the verification of the effectiveness of the implemented measures. Approved codes of conduct (Article 40) or approved certification mechanisms (Article 42) can be used for this purpose.

The PbD principles are incorporated into the GDPR through its new principles of *data protection by design and default*. These oblige the controller to implement appropriate technical and organisational measures and procedures in a way that the data processing will meet the GDPR requirements and ensure the protection of the data subjects' rights. The implementation of these measures has to be done by considering their cost and state of the art. *Data protection by design and default* should be handled when the means for processing are determined, as well as during the processing itself. The controller must implement mechanisms to ensure by default that only the personal data necessary for each specific purpose of the processing is actually processed. These mechanisms should ensure that any data are not collected, processed or retained beyond the minimum necessary, in terms of the amount of the data, their storage time and accessibility. Particularly, such mechanisms must ascertain that by default, personal data are not made accessible to an indefinite number of persons without the individual's intervention.

The GDPR determines the *joint controllers' responsibilities* that were not included in DIR95. Joint controllers are those who determine the purposes and the means of personal data processing together with other controllers. Controllers of this kind must transparently determine their respective responsibilities for compliance with the GDPR. These particularly concern the procedures and the mechanisms for exercising the data subject's rights and the controllers' duties related to information provision (Articles 13–14). The arrangement among the joint controllers has to be made available to the data subject.

Under the GDPR, the controller's obligations related to the data processing to be carried out by a processor are similar to the corresponding DIR95 obligations. These obligations require the controller to choose a processor that provides sufficient guarantees with respect to the technical and organisational measures for ensuring data protection. The GDPR still adds some clarifications to the position and obligations of processors. The processing carried out by a processor must be governed by a contract (or another legal act binding the processor to the controller) that determines the processing details, such as its duration, purposes and the processed personal data types. Particularly, the requirements for the processor under the contract are as follows: act only on instructions from the controller (especially when the transfer of the personal data is prohibited), employ only the staff members who have committed themselves to confidentiality or are under a statutory obligation of confidentiality, take all required measures (pursuant to Article 32) for the security of processing, enlist another processor only with the controller's prior permission, assist the controller in responding to requests for exercising the data subject's rights, and assist the controller in ensuring compliance with the obligations for personal data security and the data protection impact assessment. When the processing has ended, the processor has to delete or hand over all the personal data to the controller and not process it otherwise; to ensure compliance, the schedule and the means for deletion or return should be defined in the data processing contract. The processor should also make available to the controller and the supervisory authority all the information necessary to demonstrate its compliance with the obligations stated in the GDPR.

The GDPR obligates each controller, processor and the controller's representative to maintain *a record of processing activities* under its responsibility (Article 30), instead of requiring a notification of the processing operations to the supervisory authority, which is the corresponding DIR95 obligation. This record has to be made available to the supervisory authority on request. *A record of processing activities* is not required of an enterprise or an organisation employing less than 250 persons, unless the processing will likely result in a risk

to the rights and freedoms of data subjects, the processing is not occasional, or it includes special categories of data (Article 9(1)) or personal data relating to criminal convictions and offences (Article 10). The GDPR also obligates the controller and the processor to co-operate with the supervisory authority in the performance of their duties (Article 31).

The GDPR requires the controllers that are not established in the EU to designate a representative in case the GDPR applies to their data processing activities. The representative is required in the EU if the data processing activities relate to the offering of goods or services to the data subjects residing in the EU or to the monitoring of their behaviour (Article 3(2)). However, this obligation does not apply to a controller that is established in a third country if the European Commission has decided that this country ensures an adequate level of protection. Neither does it apply to enterprises with less than 250 employees, to a public authority or body or to a controller that only occasionally offers goods or services to data subjects residing in the EU.

4.7. Security of personal data

GDPR Articles 32–34

Corresponding articles in DIR95: Security of processing (Article 17); DIR 2002/58/EC also includes associated provisions: Security (Article 4)

- Extended obligation to cover processors: The implementation of measures for the security of data processing is clarified regarding the data processors' obligations.
- New obligation of the controller: notification of a personal data breach to the supervisory authority and to the data subject
- New obligation of the processor: notification of a personal data breach to the controller

The GDPR sets out data security, where it obliges both the controller and the data processor *to implement appropriate measures for the security of processing.* The GDPR clarifies the processor's obligations (Article 32) and introduces the obligation of both the controller and the processor to provide *notifications of personal data breaches* (Articles 33–34).

The GDPR extends the controller's obligation to implement appropriate technical and organisational measures to ensure the security of personal data processing so that it also covers the processor. Following an evaluation of the privacy risks, the controller and the processor must take the necessary measures to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, particularly any unauthorised disclosure, dissemination or access, or alteration of personal data. The GDPR extends the controller's obligation to directly cover data processors, irrespective of the contract with the controller, whereas under DIR95, processing by the processor had to be governed by a contract (or a legal act).

Regarding the *personal data breach notification*, built on Article 4(2) of e-privacy Directive 2002/58/EC, the GDPR stipulates that the controller and the processor have to meet the following requirements. In case of a personal data breach, the controller has to notify the supervisory authority without undue delay and where feasible, not later than 72 hours after becoming aware of it. If not made within this time limit, the notification has to be accompanied by reasons for the delay. Correspondingly, the data processor is obliged to alert and inform the controller without undue delay after becoming aware of a personal data breach. The controller must document any personal data breaches, and this documentation must comprise the relevant facts, the effects of the breach and the remedial action taken.

The GDPR obliges the controller to communicate the personal data breach also to the data subject when it will likely adversely affect the protection of his or her personal data or privacy. This notification must be done without undue delay, using clear and plain language. However, the communication of a personal data breach to the data subject is not required if the controller has implemented appropriate protection measures or taken subsequent measures so that the personal data remains unintelligible, and the privacy risks are no longer likely to materialise.

4.8. Data protection impact assessment and prior consultation

GDPR Articles 35–36

Corresponding article in DIR95: Prior checking (Article 20)

- New obligation of the controllers: a data protection impact assessment prior to likely risky processing operations
- Simplification relative to controllers' obligation to obtain authorisation to process personal data: Prior consultation with the supervisory authority is required only if the data protection impact assessment indicates a high risk related to the data processing or if the supervisory authority judges it necessary.

The GDPR introduces the controllers' new obligation to carry out a *data protection impact assessment* prior to likely risky personal data processing operations (Article 35). Under the GDPR, the controller or the processor is required to consult the supervisory authority prior to the processing only if the *data protection impact assessment* shows high privacy risks (Article 36).

Under the GDPR, the controller has to conduct *a data protection impact assessment* prior to processing operations that present specific risks to the data subject's rights and freedoms due to their nature, scope or purposes (particularly if the data subject's personal aspects are systematically and extensively evaluated for automated decisions, if special categories of personal data (defined in Article 9) are processed on a large scale or if a publicly accessible area is systematically monitored on a large scale). The *data protection impact assessment* must include the following at the minimum: a general description of the envisaged processing operations and the purposes of the processing, an assessment of the processing operations' necessity and proportionality in relation to the purposes, an assessment of the risks to the data subjects' rights and freedoms, and the measures to address the risks (i.e., safeguards, security measures and mechanisms to ensure personal data protection and to demonstrate compliance with the GDPR). When conducting a *data protection impact assessment*, attention should be paid to the compliance with approved codes of conduct (Article 40, presented in Subsection 4.10. Codes of conduct and certification), the data subjects' or their representatives' views on the intended processing, and the possible need for a review to assess if processing operations are in accordance with the *data protection impact assessment*. A *data protection impact assessment* is not necessarily required if it has already been carried out as part of a general impact assessment required by law (e.g., in case of data processing by public authorities with a legal basis in the EU or a member state's law).

Prior consultation builds on the concept of *prior checking* in DIR95. These prior checks were carried out by the supervisory authority before starting likely risky personal data processing operations, based on a notification received from the controller or the DPO. The GDPR instead requires the controller or the processor to consult the supervisory authority prior to the risky processing operations. They are also required to provide the supervisory authority, on request, with the data protection impact assessment and any other information needed for making an assessment of the compliance and the risks and related safeguards. The consultation with the

supervisory authority is required only if the data protection impact assessment indicates high risks to the data subject's rights and freedoms or if the supervisory authority judges it necessary. In case of non-compliance with the GDPR and insufficiently identified or mitigated risks, the supervisory authority may prohibit the intended processing and make proposals to remedy the processing operations.

4.9. Data protection officer (DPO)

GDPR Articles 37–39

Corresponding article in DIR95: Obligation to notify the supervisory authority (Article 18)

- New obligation of the controller and the processor: designation of a DPO if the data processing operations require regular and systematic monitoring of data subjects or when special categories of data are processed. The core tasks of the DPO are provided in the GDPR.

The GDPR introduces the controller's and the processor's new obligation to designate a DPO in the following situations: the personal data processing is carried out by a public authority or body, the controller's or the processor's core activities consist of processing operations requiring regular and systematic monitoring of data subjects on a large scale, or the core activities consist of processing special categories of data on a large scale (defined in Article 9). In other cases, the designation of a DPO is voluntary unless required by the EU or a member state's law. A group of companies may designate a single DPO; likewise, public authorities or bodies may designate a single DPO for several entities of the controller or the processor, according to their organisational structures. The DPO has to be designated based on his or her professional qualities, expert knowledge of data protection laws and practices, and ability to fulfil the DPO's tasks (described at the end of this subsection). The DPO may be employed by the controller or the processor or may perform the tasks based on a service contract.

The GDPR sets out the DPO's position by defining the controller's and the processor's obligations in relation to the DPO's performance, as well as by defining the DPO's own obligations related to his or her tasks. The controller and the processor must ensure that the DPO is properly and timely involved in all issues relating to personal data protection. They have to provide the DPO with access to personal data and processing operations, along with the resources necessary to carry out the tasks defined in GDPR Article 39 and to maintain his or her expert knowledge. The DPO must be able to perform his or her duties and tasks independently, without receiving any instructions (regarding the exercise of the function) and without being dismissed or penalised for performing the tasks. If the DPO has tasks and duties other than those defined in Article 39, the controller or the processor should ensure that these are compatible with his or her tasks and duties as a DPO and do not result in a conflict of interests. The DPO is bound by confidentiality in the performance of his or her tasks and is required to directly report to the controller's or the processor's highest management level. The GDPR guarantees the data subjects the right to contact the DPO on all issues related to the processing of their data and to request to exercise their rights.

The DPO has the following core tasks: informing and advising the controller or the processor and their employees of their obligations; monitoring the controller's or the processor's compliance with the GDPR, other EU member states' data protection provisions and their own data protection policies (including the assignment of responsibilities, awareness raising and training of the staff involved in the processing operations, and the related audits); providing advice regarding the data protection impact assessment (Article 35) and monitoring its

performance; and cooperating with and acting as the contact point for the supervisory authority (e.g., when obtaining the prior consultation described in Article 36).

4.10. Codes of conduct and certification

GDPR Articles 40–43

Corresponding article in DIR95: Codes of conduct (Article 27)

- Simplifications relative to approval of codes of conduct: National-level codes of conduct can be directly approved by the supervisory authority.
- New means to demonstrate the processing operations' compliance with the GDPR: data protection certification mechanisms, seals and marks

The GDPR builds on DIR95, which promoted encouraging trade associations and other bodies to draw up sector-specific *codes of conduct* for contributing to the implementation of the national provisions pursuant to the directive. DIR95 provided for the procedures for approving the *code of conduct* drafts by the national authority and the Working Party composed of the national-, community- and commission-level authorities or their representatives. The GDPR builds on this but points out the importance of taking into account the needs of micro enterprises and SMEs, as well as the need for specifying the GDPR's application. The supervisory authority provides an opinion on the draft code's compliance with the GDPR and approves it upon finding it appropriate. If the approved draft code only concerns processing activities in the member state in question, any further action is not needed, and the supervisory authority can register and publish it. In other cases, a procedure is followed, where the European Commission may finally decide that the approved *code of conduct* has general validity within the EU. Monitoring compliance with a *code of conduct* may be carried out by a body accredited by the supervisory authority. Despite the approaching GDPR enforcement, it seems that no information is available on bodies of this kind yet.

The GDPR introduces *certification mechanisms* and *data protection seals* and *marks* as new, voluntary means to demonstrate the processing operations' compliance with it, specifically at the EU level. These certificates will possibly be similar to the trustmarks and labels that are provided by certification authority companies today, such as Symantec (formerly VeriSign), TRUSTe and Comodo. Similar to drawing up codes of conduct, the importance of considering the needs of micro enterprises and SMEs is emphasised regarding *certification mechanisms* and *data protection seals* and *marks*. Certifications will be issued and renewed by accredited certification bodies. The controller or the processor that seeks certification is required to provide the certification body with all information and access to its processing activities that are necessary for conducting the certification procedure. In case the certification requirements are no longer met, the certification will be withdrawn.

4.11. Transfer of personal data to third countries or international organisations

GDPR Articles 44–49

Corresponding articles in DIR95: Principles (Article 25) and derogations (Article 26)

- New conditions for personal data transfers: BCRs, approved code of conduct and approved certification mechanism are new means of appropriate safeguards for personal data transfers to third countries or international organisations.

The GDPR sets out the conditions that the controller and the processor must meet for personal data transfers to third countries or international organisations. These conditions are the *adequacy decision* and *appropriate safeguards*, such as *BCRs*. The *adequacy decision* was already included in DIR95, whereas new conditions for transfers are incorporated into *appropriate safeguards*.

The GDPR builds on DIR95 regarding the European Commission's possibility to make an adequacy decision about the level of data protection of a third country (or a territory or a processing sector in that country) or an international organisation. To make the decision, the commission has to assess the level of protection regarding the rule of law, the independent supervisory authority and the international commitments entered into by the third country or the international organisation (the detailed criteria for the adequacy decision are presented in Article 45(2)). If an adequacy decision has been made, a transfer may take place, and any further authorisation to transfer is not required from the supervisory authority.

If the commission has not adopted an adequacy decision, the GDPR requires from the controller or the processor *appropriate safeguards*, in a legally binding instrument, for transfers to third countries or international organisations. Two types of appropriate safeguards are determined, as follows: the safeguards that do not require any specific authorisation from a supervisory authority and the safeguards that can be used based on an authorisation. The appropriate safeguards that do not require authorisation are *standard data protection clauses adopted by the European Commission*, *standard data protection clauses adopted by a supervisory authority* (these have to be approved by the commission), *BCRs* for multinational groups of companies (the requirements for these rules are defined in Article 47), an *approved code of conduct* (Article 40) and an *approved certification mechanism* (Article 42) (an *approved code of conduct* and an *approved certification mechanism* are required to be used together with binding and enforceable commitments of the controller or the processor in the third country to apply the appropriate safeguards). An authorisation from the supervisory authority is required for a transfer (or a set of transfers) if it is based on *contractual clauses between the controller or the processor and the data recipient* or *provisions of administrative arrangements between public authorities or bodies*.

The GDPR clarifies the DIR95 derogations for a data transfer in the absence of an *adequacy decision* or *appropriate safeguards*. These specifically concern data transfers that are necessary for the protection of important reasons of the public interest. A data transfer may also be justified, under limited circumstances, by a legitimate interest of the controller or the processor. This requires the controller to assess the circumstances of the transfer operation in question, providing suitable data protection safeguards and informing the supervisory authority and the data subjects of the transfer.

4.12. Remedies, liability and penalties

GDPR Articles 77–84

Corresponding articles in DIR95: Remedies (Article 22), liability (Article 23) and sanctions (Article 24)

- Specifications concerning the data subject's right to a judicial remedy: The data subject can lodge a complaint with a supervisory authority if he or she considers that processing of his or her data infringes the GDPR. The GDPR also specifies the bodies, organisations and associations that may lodge a complaint on behalf of the data subject.
- Extended liability to cover processors: Both the controller and the processor are liable for the damage caused to the data subject by processing that infringes the GDPR.

- Clarified liability of joint controllers and joint processors: Each controller and each processor are held liable for the entire damage caused to the data subject.
- Administrative fines imposed on the controller and the processor: Supervisory authorities are entitled to impose fines up to maximum amounts as sanctions for infringements of the GDPR.

The GDPR provides the data subject with *the right to lodge a complaint* with a supervisory authority and *the right to an effective judicial remedy* against a controller or a processor, building on the right to a judicial remedy for the infringement of the data subject's rights, under DIR95. It extends the liability for the damage to the data subject to cover processors and clarifies the liability of joint controllers and joint processors. The GDPR also entitles supervisory authorities to impose fines for its infringement.

Under the GDPR, the data subjects have *the right to lodge a complaint* with a supervisory authority if they consider that the processing of their personal data infringes it. The bodies, organisations or associations that may lodge a complaint on behalf of the data subjects, aiming to protect the data subjects' rights and interests, are also specified in the GDPR. Parties of this kind have the right to lodge a complaint with a supervisory authority, independently of a data subject's complaint, if they consider that his or her rights have been infringed.

Under DIR95, the controller was liable for the damage caused to the data subject as a result of an unlawful processing operation or any act incompatible with the national provisions adopted pursuant to the directive. The GDPR extends this liability to cover the processors as well and obliges them to pay the data subject compensation for the damage in case they have not complied with its obligations or the controller's instructions. The GDPR also clarifies the liability of joint controllers and joint processors, providing that each controller or processor is held liable for the entire damage caused to the data subject.

The GDPR specifies the member states' obligations to adopt measures for implementing the provisions similar to DIR95 and to lay down the sanctions for their infringement. The member states' supervisory authorities are entitled to formulate rules for the administrative fines imposed on the controller, its representative or the processor as sanctions for infringements. The supervisory authorities shall ensure the imposition of these fines up to maximum amounts, with due regard to the circumstances of each case. For example, infringement of the GDPR principles (such as the data minimisation principle) is subject to a fine up to €20 million or 4% of the total annual turnover worldwide in the case of an undertaking (whichever is greater). Correspondingly, fines of different amounts are also imposed on the controller or the processor, for example, when they fail to provide data subjects with their rights or do not maintain written records of the processing operations as required by the GDPR.

5. Practical implications of the GDPR

Due to the new GDPR obligations, all companies handling EU residents' personal data or monitoring data subjects' behaviour within the EU should review and revise their current organisational and technical privacy protection measures and possibly develop new policies that ensure compliance with the GDPR. To help with these tasks, we have identified the GDPR changes with the most practical relevance to personal data intensive companies. The 12 aspects of the GDPR implementation, identified in the analysis of the GDPR changes, are summarised as a framework (Table 1). Each aspect's implications are then elaborated in separate subsections. The corresponding actions demanded of the companies, as well as possible solutions for the requirements' implementation, are described.

Acquisition of knowledge about the GDPR is the starting point for the GDPR requirements' implementation in companies. Companies should also train their employees who perform tasks related to data processing so that they are aware of the changes introduced by the GDPR and can adapt to its practical implications. Overall, the implementation of the GDPR indicates the need for various actions, planning and assignment of new responsibilities, which may have substantial impacts on the companies' usage of their resources and may demand the acquisition of new expertise. As the GDPR incorporates the accountability principle requiring the companies to demonstrate compliance with it, data privacy policies and processes that can be documented well also need to be developed. Companies will possibly find it useful to consider the GDPR requirements through their risk management policies, specifically as the GDPR introduces substantial sanctions for non-compliance, resulting in obvious financial risks.

Table 1. The GDPR's practical implications for personal data intensive companies.

GDPR's practical implications	**Requirements for implementation**
Specifying data needs and usage	The clarified GDPR data minimisation principle requires limiting personal data processing to the minimum necessary. The GDPR also introduces new obligations to be taken into account when planning data collection and processing. If the data are collected from children for information society services, their ages have to be verified, and possibly, consent has to be obtained from their parents or custodians. A company that plans to profile its customers has to inform the data subjects accordingly, including the reasons and the need for it. For the processing conducted by a processor, companies need to review their data processing contracts to make sure that the required provisions will be included in them.
Considering conditions for data processing in international context	The GDPR provides for new conditions for personal data transfers to a third country or an international organisation. Companies have to check if their current safeguards for personal data transfers comply with the GDPR conditions and when necessary, put into practice new ones. Non-EU companies and international companies handling EU residents' personal data or monitoring data subjects' behaviour within the EU will have to comply with both their national legislation and the GDPR. In case the GDPR provisions apply to a non-EU established controller, it has to designate a representative in the EU.
Building privacy through data protection by design and default	Companies are obliged to implement technical and organisational measures and procedures to ensure by default the processing operations' compliance with the GDPR and the protection of the data subjects' rights. Therefore, privacy must be considered in every process and at every level of the business and enforced throughout the organisations' systems. This should be done when the means for processing are determined and during the processing itself.
Demonstrating compliance with GDPR requirements	The GDPR obliges controllers to demonstrate that their personal data processing complies with the regulation. For this reason, companies are advised to consider adherence to *codes of conduct* and possible participation in their preparation through associations representing their respective fields. The application of data protection *certifications, seals* and *marks* is recommended as well.

Developing processes to deal with data breaches	As controllers are obliged to notify data protection authorities and data subjects about data breaches as early as possible, clear and well-practised procedures need be established in organisations to deal with possible breaches and related reporting.
Reckoning with sanctions for non-compliance	Under the GDPR, supervisory authorities are entitled to impose administrative fines on non-complying companies. Non-compliance could cost a company a fine of up to €20 million or 4% of the annual global turnover, whichever is greater. Thus, all procedures related to personal data processing should be planned to ensure compliance.
Designating a DPO	Companies with processing operations based on regular and systematic monitoring of data subjects or the use of special categories of data are each required to designate a DPO as the contact point for all data protection activities. Companies may thus need to obtain new expertise.
Providing information to data subjects	Companies are obliged to inform data subjects about processing operations, data security measures, the legal basis for the processing, the data subjects' rights and the companies' legitimate interests. This information has to be transparent, easily accessible and understandable, especially when the data subject is a child. Procedures and mechanisms for exercising the data subjects' rights are also required (i.e., companies have to arrange for the means of responding to information requests according to the GDPR requirements).
Obtaining consent on personal data usage	The data subject's consent is required for personal data usage. The controller should be able to demonstrate that the data subject has consented to the processing. The request for consent must contain all relevant information about the processing and present it clearly. The request has to be clearly distinguishable from other information (e.g., contracts) presented to the data subject. Procedures are needed for obtaining consent and for its withdrawal.
Ensuring individuals' *right to be forgotten*	Companies are obliged to delete the data subject's personal data anytime he or she wants it. This requirement demands implementing processes and technical means for the deletion within established time limits. These include ways of informing third parties that process personal data about the deletion request. Ensuring the *right to be forgotten* requires documentation of the data, how it is stored and what parties it is shared with.
Ensuring individuals' *right to data portability*	Companies are obliged to provide the data subject with an electronic copy of his or her data on request. They must ensure that the personal data collected for processing is in a consistent format to facilitate its further use by the data subject and its transmission to other service providers' processing systems.
Maintaining documentation	Companies are obliged to maintain a *record of processing activities* and make it available to the supervisory authority on request. They are also required to conduct a *data protection impact assessment* prior to likely risky processing operations. This documentation has to be available to the supervisory authority as well.

5.1 Specifying data needs and usage

The GDPR requires companies to limit the personal data processing to the minimum necessary through its clarified data minimisation principle. To comply with this principle, companies have to decide what *data types* are needed for their business operations. They also have to ensure that the purposes for using personal data are specified because collecting any excess data is not allowed. Specifically, the data subjects' consent is now required separately for each purpose. For example, the usage of a specific service may not be contingent on the collection of personal data that is not needed for offering this service. When deciding on the data types to be collected, increased transparency requirements and sanctions for non-compliance with them have to be taken into account. A major question brought by the new GDPR obligations is whether and how data about children will be collected for business operations under the requirements concerning the verification of the data subjects' ages and the parents' or the custodians' consent (Subsection 5.9 presents more information on verifiable parental consent). The GDPR obligations related to personal data processing may induce restrictions on companies' business operations. The companies may want to assess the impacts of these restrictions, for example, on their service production and the possibilities to offer different service types. The effects may be significant, specifically when producing services targeting children and in the healthcare sector, whose services require the collection of sensitive data types. A company may want to *profile* its customers for direct marketing purposes, for instance. Along with the new obligations, the reasons for profiling have to be given, and the need for it should be justified. Moreover, information about the logic involved in the profiling and its expected consequences on the data subjects must be presented. Companies that carry out profiling should check that this information is communicated to the data subjects and correspondingly, possibly update the content of their information provision. To ensure fair and transparent profiling, as GDPR Recital 71 advises, companies should use appropriate mathematical or statistical procedures for the profiling, implement measures to correct personal data inaccuracies and minimise the risk of errors, and secure personal data in a way that takes account of the risks to the data subjects and prevents discriminatory effects. Companies that carry out large-scale data analysis activities also need to consider whether they are required to obtain the data subjects' consent for these activities and how to implement appropriate consent mechanisms (cf. Hogan Lovells, 2015). If the data processing is performed by a processor, companies need to review their data processing contracts and ensure that these will include all the provisions required by the GDPR.

5.2 Considering conditions for data processing in international context

As the GDPR introduces some new conditions for personal *data transfers* to third countries or international organisations, companies that transfer these data should review their current grounds for transfers and find out whether they need to put into practice new safeguards. Companies also have to make decisions about what data will be transferred and how it will be processed. It should be borne in mind that the controller is responsible for the processor's processing operations; therefore, these operations may have to be audited before the transfer is made. If new safeguards are needed, companies have to choose and implement the suitable ones based on the setting in which the transfer takes place (e.g., BCRs may be used in multinational companies). If the European Commission has not made an adequacy decision about the data protection level of a third country, data transfers require appropriate safeguards in a legally binding instrument and in some cases, prior authorisation by the supervisory authority. For example, the GDPR endorses *BCRs* as new appropriate safeguards and defines the minimum requirements for their content. The commission may specify the format and the procedures for the information exchange that takes place based on the *BCRs*. When planning data transfers, it should also be considered that the Safe Harbor program for EU-US transfers is not valid anymore. Instead, the EU-US Privacy Shield (European Commission, 2016a) serves as a new framework for personal data exchanges for commercial purposes.

The GDPR extends its territorial scope to cover all companies that offer goods or services to the data subjects or monitor their behaviour within the EU. Non-EU companies, international companies and companies involving data processing in an international setting are now possibly obliged to comply with the GDPR, in addition to their national legislation. In case the GDPR provisions apply to a non-EU established controller, it has a new obligation to designate a representative in the EU (occasional and unlikely risky processing as exceptions) (Recital 80). The representative will act on the controller's behalf and may be addressed by a supervisory authority. Non-EU established companies may find this obligation challenging as parties interested in taking the required responsibilities may be scarce. However, it is not always clear whether a non-EU established company's goods or services can be regarded as being offered in the EU. To determine this matter, it should be ascertained whether it is apparent that offering the services is envisaged in one or more EU member states (Recital 23). For example, the use of a language or a currency that is used in one or more EU member states, with the possibility to order goods and services in the language in question, may indicate that the company envisages offering goods or services to data subjects in the EU. Furthermore, the following factors strongly indicate offering goods or services of this kind: a website with a top domain name of a member state, delivery of physical goods to the EU, referring to EU citizens to promote goods or services, a large customer base in the EU and advertising that targets individuals in the EU (Linklaters, 2016). Instead, the mere accessibility of the website in the EU, an email address or other contact details, or the use of a language that is also generally used in the controller's country is insufficient to ascertain the intention to offer goods or services to data subjects in the EU. As for monitoring data subjects' behaviour in the EU, to determine whether a processing activity can be considered as such, it should be ascertained whether the data subjects are being tracked on the Internet and possibly subsequently profiled (Recital 24).

5.3 Building privacy through data protection by design and default

Data protection by design and by default is one of the new principles of the GDPR. It has to be taken into account when determining the means for personal data processing and during the processing itself. To comply with the *data protection by design and by default* principle, companies should ensure that they have policies that support the proactive implementation of technical and organisational privacy protection measures and procedures with the effects required by the GDPR. Specifically, companies need to pay attention to the implementation of data-minimising mechanisms that ensure that any personal data are not collected, processed or retained beyond the minimum necessary, also regarding data storage time and accessibility. Appropriate privacy protection measures have to be implemented, considering their state of the art and the implementation cost. Companies should review their current protection measures, assess such measures' appropriateness to meet the *data protection by design and by default* principle and possibly implement new measures. It should be noted that under the GDPR, the obligation to implement security measures has been extended to cover companies carrying out processing on behalf of the controller. Therefore, the processors need to be aware of their new obligations and to consider whether they need a *data protection by design and by default* policy. It should also be taken into account that the GDPR does not provide any specific instructions for security mechanisms (if certificate practices for secure and trusted data exchanges are excluded). Instead, companies have to determine the actual solutions by themselves.

5.4 Demonstrating compliance with GDPR requirements

The GDPR promotes sector-specific *codes of conduct* to demonstrate compliance and the implementation of appropriate data protection measures. These codes can be used as means to respond to the GDPR requirements and put into practice their implementation. Adherence to approved *codes of conduct* can also be reasonable as it may be considered a mitigating factor

regarding sanctions for infringements of the GDPR (Article 83, 2(j)). The GDPR introduces simplifications relative to the approval of the *codes of conduct* by accepting national-level codes to be directly approved by the supervisory authority. Due to the new GDPR principle of accountability, companies may find it useful to participate in the preparation of these codes, as well as extend the existing ones, through the associations in their respective fields. *Codes of conduct* can be prepared for specific issues, such as implementation of technical and organisational measures, information provision to data subjects, protection of children or data transfers to third countries. Relevant stakeholders, such as third parties processing the data, or data subjects should be consulted when preparing the codes (cf. Recital 99). The GDPR introduces *data protection certification mechanisms, seals and marks* as new, voluntary means to demonstrate compliance. It is advisable for companies to start to follow the development of these means if this has not yet been done before. In addition to seeking certifications for themselves, the companies can take advantage of these when choosing a processor for their processing activities.

5.5 Developing processes to deal with data breaches

The GDPR introduces new notification obligations to companies regarding personal data breaches. Under the GDPR, both data protection authorities and data subjects must be notified of serious *data breaches* without undue delay, or if this is not possible, the corresponding information has to be conveyed through public communication. To meet these new requirements, companies need to plan and establish clear processes that enable reacting quickly to possible breaches and dealing with them. Specifically, companies should consider how to notify the data subjects as reaching them quickly may be challenging. Internal reporting processes should also be ensured for supporting communication to the authorities and the data subjects. These include processes that enable processors to notify the controller. The requirements related to the notification's content have to be taken into account, such as the nature of the breach and the description of its likely consequences. The controllers should also consider how to implement personal data security because the notification obligation to the data subjects will not be in effect in case appropriate protection measures have been put into practice (e.g., encryption). Implementing these measures possibly demands changes in the companies' current information systems.

5.6 Reckoning with sanctions for non-compliance

The GDPR specifies the member states' obligations to adopt measures for implementing its provisions. As the GDPR now entitles supervisory authorities to impose *sanctions* on companies for non-compliance, companies need to review their processes and privacy protection measures to ensure their compliance and avoid sanctions. Correspondingly, they need to reckon with the sanctions when planning new processes. For example, infringement of the basic principles for processing could cost a company €20 million or 4% of the total turnover worldwide. Regarding the damage caused to a data subject as a result of an infringement, it should be noted that under the GDPR, not only controllers but also processors are liable for the damage.

5.7 Designating a DPO

The GDPR introduces the new obligation to designate a DPO for companies whose processing operations demand regular and systematic monitoring of data subjects or use of special categories of data. If companies of this kind have no DPOs yet, they each have to designate one to act as the contact point for all data protection activities. This may be challenging since companies may lack the expertise needed, and there are not necessarily enough qualified DPOs currently in the market. One possibility to manage the DPO requirement is to draw up a service

contract, possibly together with a group of companies, with a DPO who is not employed by any company. Even if a company is not obligated to designate a DPO for now (for example, some SMEs), it might be beneficial to nominate a staff member internally, as this would help to focus on the GDPR implementation and drive accountability (cf. Bird & Bird, 2016a). This is the case specifically when a company is aiming for growth or more intensive personal data utilisation in the future. Building up competencies internally may be an effective strategy compared to hiring a new DPO, as a hands-on employee who knows the business is needed (cf. Bird & Bird, 2016a).

5.8 Providing information to data subjects

The GDPR adds new specified requirements regarding the content, intelligibility and accessibility of the information on personal data processing, as well as its provision mechanisms. To meet these new requirements, companies first have to check whether they provide the data subjects with all the required information when they collect the data from these individuals or process their data obtained from other sources. Companies also need to check whether they are able to provide all the required information to respond to the data subjects' requests. As the GDPR now clearly obliges companies to provide transparent, easily accessible and understandable information on their processing operations, security measures, the legal basis for the processing, data subjects' rights and the company's legitimate interests, their privacy policies might need to be re-written in plain language. Along with the new requirements, special attention has to be paid to planning this communication when the data subject is a child. Under the GDPR, companies are also obliged to put into practice the means for responding to data subjects' information requests within the defined deadline (one month). Companies need to consider how to ensure this matter if they have no suitable means in use yet. Concrete means of information provision that match the GDPR requirements have been suggested. For example, the Information Commissioner's Office (2016) recommends the following means: Websites can be revised by using layered privacy notices (i.e., key information is provided immediately, and more detailed information is available as needed), information policies can be founded on multiple information channels, and technological solutions, such as dashboards that enable access to a copy of personal data, can be designed. Furthermore, active privacy information provision (instead of just making information available for the data subjects) and user testing may be worth considering when planning information provision approaches. To address the requirements related to the data subjects' requests for access (as well as for deletion, restriction and porting of their personal data), companies' information systems should be designed so that these requests and the corresponding information provision can also be made electronically. Information systems of this kind may be beneficial specifically to SMEs because their usage can decrease the administrative costs associated with providing access to personal data.

5.9 Obtaining consent on personal data usage

The GDPR specifies the conditions for personal data processing consent and introduces the new requirement of the *burden of proof of the consent*. The specified conditions require obtaining *clearly distinguishable consent* from the data subject. Companies now have to make sure that the consent is separable from other information presented to the data subject and include detailed information on personal data usage by the controller and any third party processing the data. The requirement of a clearly distinguishable consent may demand additional resources and result in extra costs for companies through a separate consent management system implementation. For example, for websites that use cookies, the cookie approval consent need to be implemented. Based on the consent, the companies possess knowledge of their data subjects, that is, they know whose personal data are being processed. Correspondingly, under the new GDPR requirement of the *burden of proof*, they must be able

to demonstrate that the data subjects have consented to the processing. For this reason, companies need to ensure that they have procedures and systems for recording consent. New processes possibly have to be planned and established also for obtaining consent, as well as for its withdrawal. If companies carry out consent-based personal data processing that is not necessary to perform a contract, then in the process of obtaining consent, it is advisable to clearly inform data subjects about the voluntariness of giving their consent. The GDPR's specified conditions for consent also require the means to be put into practice for verifying the data subjects' ages and obtaining consent from the parents or the custodians if children's data are to be processed. This matter may pose challenges specifically for online companies. Companies have to take into account the age limits for lawful processing provided by the member states (13 years old at the minimum). Considering this point, companies need to implement appropriate parental consent mechanisms with verification processes (cf. Advertising Education forum, 2013).

5.10 Ensuring individuals' right to be forgotten

The GDPR specifies the conditions for the data subjects' right to obtain erasure of their personal data (i.e., the *right to be forgotten*). Companies are now obliged to delete personal data on the data subjects' request without any specific grounds, such as data incompleteness or inaccuracy. To comply with this obligation, companies need to check whether they have appropriate processes and technical means in place to deal with the data subjects and their data deletion requests within a given time frame (correspondingly, the *right to restriction of processing* necessitates processes and means for personal data blocking). Companies also have to ensure that ways are established for informing third parties that process the personal data about the deletion requests. Ensuring the *right to be forgotten* demands documentation of the data and how it is stored, as well as what parties it is shared with.

5.11 Ensuring individuals' right to data portability

The GDPR introduces the *right to data portability*. This new right requires the companies' capability to provide data subjects with their personal data in an electronic format that facilitates its further use. Specifically, the data subjects now have the right to receive their personal data for transmission to other systems. Due to these new requirements, companies need to ascertain that they have processes for personal data provision when requested by the data subjects. They should consider the type of format for exporting the data, as well as the possibilities to transmit it directly to other systems. This may be challenging due to the absence of uniform standards for ensuring transmission. For this reason, controllers are encouraged to develop interoperable data formats (cf. Recital 68). When the data are to be transmitted, it should be kept in mind that it may also concern other data subjects; hence, its porting can risk their privacy as well. Companies should consider how to mitigate these risks and possibly incorporate the issue into their awareness raising and employees' training programmes.

5.12 Maintaining documentation

The GDPR's accountability principle and documentation requirements demand the establishment, maintenance and availability of new documentation. Companies are now obliged to create two main parts of the documentation – a *record* of personal data *processing activities* and a *data protection impact assessment*. A *record of processing activities* describes those under the controller's charge or carried out by a processor on behalf of the controller, and it is also required of processors. Companies are obliged to make this record available to the supervisory authority on request. If the documentation is not maintained, fines will be imposed on the controller or the processor, according to the supervisory authority's rules. A *data protection impact assessment* has to be conducted prior to the processing operations that will

likely present high risks to the data subjects' rights and freedoms. Similar to the *record of processing activities*, *the data protection impact assessment* has to be available to the supervisory authority. In personal data intensive companies, the assessment also possibly indicates the need for *prior consultation* with the supervisory authority due to their processing operations' nature and scope. The existing guides on *privacy impact assessments* (PIA) can be used as starting points for the assessment required by the GDPR (e.g., Information Commissioner's Office, 2014; Oetzel and Spiekermann, 2014; Information and Privacy Commissioner of Ontario, 2015). However, companies may also want to develop their own assessment processes. The PIA process typically consists of the following stages: identification of the need for and scope of the assessment, identification of the risks related to the processing, and identification and reporting of data protection solutions. Different templates and tools are available to assist companies in performing PIAs. For example, screening questions (cf. Information Commissioner's Office, 2014) can be used by data protection non-experts to identify the need for a PIA as part of an organisation's project management procedures. Furthermore, a PIA template (cf. Information Commissioner's Office, 2016) can be used to record the results of different stages of a PIA (e.g., information flows, privacy risks and privacy solutions). Some PIA systems (e.g., AvePoint, 2016) have also been developed to help companies with their PIAs through an automated process and possibilities to create their own PIA templates. When conducting a *data protection impact assessment*, it is important to pay attention to the risks specific to the business sector and the company. Data subjects can also be consulted to seek their views on the intended processing as part of the assessment. The GDPR's documentation requirements may be challenging to put into practice, specifically for personal data intensive companies that operate according to agile and lean principles, with little documentation. These companies should pay specific attention to these requirements' implementation and may have to consider how to change their current ways of working.

6. Conclusion

The objective of this study was to identify the upcoming GDPR requirements' practical implications for personal data intensive companies' organisational and technical privacy protection measures, as well as business strategy and policy development. Understanding these implications has high practical relevance to such companies, as substantial amounts of time, strategic planning, employee training and financial and human resources are typically needed to implement the requirements. In this paper, we presented a systematic review, analysis and synthesis of the differences between DIR95 and the GDPR to identify the GDPR changes with the most practical relevance to personal data intensive companies. The key implications of these changes for the GDPR implementation were compiled into a framework with 12 aspects to be considered by companies to proactively prepare for and comply with the upcoming requirements and to avoid sanctions for non-compliance. Based on the framework, each aspect's implications were elaborated, and approaches to their implementation were outlined. Considering the 12 aspects, companies can plan their personal data protection improvement actions to implement adequate policies, procedures and processes and to take advantage of the adoption of the new requirements in their service and system design activities.

The GDPR brings considerable changes to personal data intensive companies' privacy protection implementation. Due to these changes, companies need to review their strategies, information systems and documentation to ensure their alignment with the GDPR provisions. Companies should first acquire sufficient knowledge of the GDPR requirements before conducting their reviews, paying attention to the aspects identified in this study. Their reviews' results may indicate the need for considerable changes and thorough planning of future privacy policies, procedures and documentation of their processing operations. Implementing these changes may prove challenging because no clear, ready-to-use solutions necessarily exist. For

compliance with the GDPR, some of its requirements have to be taken into account in the companies' *policy planning*. Their policies should support the *data protection by design and by default* principles through a proactive implementation of technical and organisational privacy protection measures and procedures, including *data-minimising mechanisms*. Specifically, strategic-level decisions have to be made about personal data collection and processing. The GDPR also states specified, detailed requirements for *information provision* to data subjects. Companies have to consider these requirements when collecting and processing personal data and obtaining the data subjects' consent. If the data are to be collected from children, a major question is how to implement the GDPR's requirements of information provision, age verification and parental consent. The GDPR introduces many new principles, obligations and data subjects' rights that require companies to *review and revise their organisational processes*. In this regard, one of the most substantial GDPR requirements is that processes dealing with possible data breaches and the associated notification obligations have to be put into practice. Correspondingly, organisations need to *define and assign new, clear roles and responsibilities* to their employees, as well as develop or acquire the necessary expertise. Specifically, a DPO is typically required to act as the contact point for a company's data protection activities. Many of the new processes call for *supporting information systems* with the capability to deal with data subjects' requests, as well as obtain their consent and allow its withdrawal. Information systems of this kind may specifically benefit SMEs through decreased administrative costs. Overall, when planning new procedures and revising existing ones, companies should also focus on sanctions for non-compliance with the GDPR to avoid the administrative fines for different infringements. The GDPR requires transparency, demonstrating compliance with its obligations, and establishing, maintaining and making available extensive new documentation, such as a record of processing activities and a data protection impact assessment. To comply with these requirements, possibly causing considerable additional costs, companies should allocate appropriate resources. *Systems for recording documentation* should be considered as well. Particularly, companies that operate according to agile and lean principles, with little documentation, may find the GDPR documentation requirements heavy and challenging to implement. Companies of this kind may need to plan and adopt new ways of working to ensure compliance.

This study aimed to provide information on the practical-level actions that companies should take to comply with the upcoming GDPR requirements. For this reason, the GDPR changes were reviewed, analysed and synthesised systematically. This process offered a comprehensive view of the new requirements and identified the 12 aspects to be considered in the GDPR implementation. The GDPR does not directly provide specific guidelines for its provisions' implementation. Although the GDPR introduces many clarified rules and instructions on the implementation, actual solutions for putting the provisions into practice have to be determined by companies themselves. For this reason, the 12 aspects identified in this study should be supplemented by practical guidance in finding suitable solutions. Companies are advised to use some of the existing guidelines, applicable to their operations and the country in question, to support their preparation for the GDPR's imposed changes (e.g., A&L Goodbody, 2016; Bird & Bird, 2016b; bitkom, 2016; Linklaters, 2016).

As we found in the data protection history (Section 2 of this paper), privacy legislation has evolved along with technological development, the increasing use of personal data intensive systems and services, and companies' growing interest in personal data usage in their business operations over the last decades. The GDPR will ensure the harmonisation and the data subjects' rights to personal data protection in the evolving data processing contexts. However, personal data collection technologies and the ways to utilise the data can be expected to further develop in the future. For this reason, companies should follow the data protection requirements' changes over time and find ways to do so. It is important to continuously review the need for developing current personal data management and usage practices, as well as for

drawing up new ones. Through active monitoring of the situation, companies can proactively adapt to the changes and possibly gain competitive advantage in their respective fields. One way to gain insights into developmental needs is to find out the data subjects' views on data collection and processing. Therefore, it could be fruitful to develop methods for this undertaking. Overall, raising awareness, training employees and obtaining new knowledge related to future changes are the keys to cope with them.

To understand how companies are adapting to changes in legislation, implementing its new requirements and addressing related challenges, future empirical studies should be conducted among personal data intensive companies. It is also crucial to investigate the GDPR implementation in companies of different sizes to find out how the implementation is carried out and how the challenges are addressed, for example, in the SME context. Through empirical research of this kind, the means for implementing the changes and the appropriate concrete solutions can be followed and analysed, along with how field-specific data usage and management practices are formulated in companies.

Acknowledgements

This research was financially supported by the Tauno Tönning Foundation and the Finnish Foundation for Technology Promotion.

References

Advertising Education forum (2013) *Children's data protection and parental consent. A best practice analysis to inform the EU data protection reform.* Available from: http://www.aeforum.org/gallery/5248813.pdf [Accessed 4 January 2017].

A&L Goodbody (2016) *THE GDPR: A guide for businesses.* Available from: https://www.algoodbody.com/media/The_GDPR-AGuideforBusinesses1.pdf [Accessed 7 February 2017].

Article 29 Data Protection Working Party (2003) *Working document: Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*. WP 74. Article 29 Data Protection Working Party.

AvePoint (2016) *AvePoint Privacy Impact Assessment System.* Available from: http://www.avepoint.com/assets/pdf/Fast_Facts_AvePoint_Privacy_Impact_Assessment.pdf [Accessed 22 December 2016].

Bird & Bird (2016a) *What should SMEs do to prepare for the upcoming General Data Protection Regulation?* Available from: https://www.twobirds.com/en/news/articles/2016/global/what-should-smes-do-to-prepare-for-the-upcoming-gdpr [Accessed 16 January 2017].

Bird & Bird (2016b) *Guide to the General Data Protection Regulation.* Available from: http://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en [Accessed 15 August 2016].

bitkom (2016) *What to know about the General Data Protection Regulation (GDPR)?* Available from: https://www.privacy-conference.com/sites/default/files/160916_EU-DS-GVO_FAQ_EN_02.pdf [Accessed 3 January 2017].

Cavoukian, A. (2009) *Privacy by Design: The 7 foundational principles*. Ontario: Information and Privacy Commissioner of Ontario, Canada. (Revised version published in 2013) Available from: https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf [Accessed 10 January 2017].

Commonwealth of Massachusetts (2010) *The Massachusetts General Law Chapter 93H,* regulations *201 CMR 17.00.*

Council of Europe (1950) *European Convention for the Protection of Human Rights and Fundamental Freedoms.* Strasbourg: European Court of Human Rights.

Council of Europe (1981) *Convention for Protection of Individuals with regard to Automatic Processing of Personal Data.* Strasbourg: European Court of Human Rights.

Council of Europe (2017) *Convention 108 and Protocol: Background*. Available from: http://www.coe.int/en/web/data-protection/background [Accessed 7 April 2017].

Court of Justice of the European Union (2015) *The Court of Justice declares that the Commission's US Safe Harbour decision is invalid.* Press Release No. 117/15. Luxembourg.

Dix, A. (2013) The Commission's data protection reform after Snowden's summer. *Intereconomics* 48 (5), 268–271.

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.* Official Journal L 281, 23/11/1995, 0031–0050.

European Commission (2000) *Commission decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*. Official Journal L 215, 25/08/2000, 0007–0047.

European Commission (2002) *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications)*. Official Journal L 201, 31/07/2002, 0037–0047.

European Commission (2012a) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions – Safeguarding privacy in a connected world. A European data protection framework for the 21st century.* COM (2012) 09 final.

European Commission (2012b) *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* COM (2012) 11 final.

European Commission (2016a) *Commission implementing decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*. C (2016) 4176 final.

European Commission (2016b) *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 the Directive 95/46/EC (General Data Protection Regulation)*. Official Journal L119, 04/05/2016.

European Data Protection Supervisor (2005) *Public access to documents and data protection.* Background document. Available from: https://edps.europa.eu/sites/edp/files/publication/05-07_bp_accesstodocuments_en.pdf [Accessed 7 April 2017].

European Data Protection Supervisor (2017) *Glossary*. Available from: https://edps.europa.eu/node/3098#convention108 [Accessed 7 April 2017].

European Union Agency for Fundamental Rights & Council of Europe (2014) *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union.

Federal Trade Commission (1998) *Privacy online: A report to Congress*. Washington, DC: Federal Trade Commission.

Gellman, R. (2015) *Fair information practices: A basic history.* Version 2.13. Available from: http://bobgellman.com/rg-docs/rg-FIPShistory.pdf [Accessed 8 July 2015].

de Hert, P. and Papakonstantinou, V. (2016) The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review* 32 (2), 179–194.

Hogan Lovells (2015) *Future-proofing privacy: A guide to preparing for the EU Data Protection Regulation.* Available from: http://www.hlmediacomms.com/files/2016/05/here.pdf [Accessed 3 January 2017].

Information and Privacy Commissioner of Ontario (2015) *Planning for success: Privacy Impact Assessment Guide*. Available from: https://www.ipc.on.ca/wp-content/uploads/2015/05/Planning-for-Success-PIA-Guide.pdf [Accessed 30 December 2016].

Information Commissioner's Office (2014) *Conducting privacy impact assessments code of practice*. Available from: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf [Accessed 7 January 2017].

Information Commissioner's Office (2016) *Privacy notices, transparency and control: A code of practice on communicating privacy information to individuals*. Available from: https://ico.org.uk/media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf [Accessed 7 January 2017].

Linklaters (2016) *The General Data Protection Regulation: A survival guide*. Available from: http://www.linklaters.com/Insights/Pages/General-Data-Protection-Regulation-survival-guide.aspx [Accessed 7 January 2017].

London Economics (2013) *Implications of the European Commission's proposal for a General Data Protection Regulation for business.* London Economics, final report to the Information Commissioner's Office. Available from: https://ico.org.uk/media/about-the-ico/documents/1042341/implications-european-commissions-proposal-general-data-

protection-regulation-for-business.pdf [Accessed 23 October 2015].

Mantelero, A. (2013) The EU proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security* 29 (3), 229–235.

Mikkonen, T. (2014) Perceptions of controllers on EU data protection reform: A Finnish perspective. *Computer Law & Security* 30 (2), 190–195.

Oetzel, M. C. and Spiekermann, S. (2014) A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems* 23, 126–150.

Organisation for Economic Co-operation and Development (2011) *The evolving privacy landscape: 30 years after the OECD privacy guidelines.* OECD Publishing, OECD Digital Economy Papers, No. 176. Available from: http://www.oecd-ilibrary.org/docserver/download/5kgf09z90c31-en.pdf?expires=1491498483&id=id&accname=guest&checksum=A453990EDCF2BC2A6799C14A112DA7C7 [Accessed 10 July 2015].

Reding, V. (2010). The upcoming data protection reform for the European Union. *International Data Privacy Law* 1 (1), 3–5.

Schwartz, P. M. (2013) The EU-U.S. privacy collision: A turn to institutions and procedures. *Harvard Law Review* 126 (7), 1966–2009.

Spiekermann, S. (2012) The challenges of Privacy by Design. *Communications of the ACM* 55 (7), 38–40.

Thüsing, G. and Traut, J. (2013) The reform of European data protection law: Harmonisation at last? *Intereconomics* 48 (5), 271–276.

Tracol, X. (2016) EU-U.S. Privacy Shield: The saga continues. *Computer Law & Security Review* 32 (5), 775–777.

TRUSTe (2015) *Preparing for the EU General Data Protection Regulation. Assessing awareness, readiness & impact of the proposed changes in US, UK, France & Germany.* TRUSTe Inc. Research Report. Available from: https://iapp.org/media/pdf/resource_center/TRUSTe_GDPR_Report_FINAL.pdf [Accessed 15 August 2016].

United Nations (1948) *The Universal Declaration of Human Rights.*

United States of America. *Fair Credit Reporting Act 1970* (15 U.S.C. § 1681).

United States of America. *Health Insurance Portability and Accountability Act 1996* (43 U.S.C. § 1320d-9).

United States of America. *Privacy Act 1974* (5 U.S.C. § 552a).

US Department of Commerce's International Trade Administration (2015). *U.S.-EU Safe Harbor Overview.* Available from: http://www.export.gov/safeharbor/eu/eg_main_018476.asp [Accessed 9 July 2015].

US Department of Health, Education, and Welfare (1973) *Records, computers and the rights*

of citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Chapter IV: Recommended Safeguards for Administrative Personal Data Systems.

Westin, A. (1967) *Privacy and freedom.* New York: McClelland & Stewart Ltd.