Towards an Understanding of Stakeholders and Dependencies in the EU GDPR

Dominik Huth[1], Anne Faber[1], and Florian Matthes[1]

[1] Technical University of Munich, Department of Informatics,
Garching bei München, Germany
{dominik.huth,anne.faber,matthes}@tum.de

Abstract. Personal data has evolved into an essential element of current business models, which pose new challenges to legislation and organizations. To address these challenges at a European level, the European Commission has passed the General Data Protection Regulation (GDPR). Using a data-driven approach, we identify the key stakeholders that are described in the GDPR, which are the data subject, the controller, the processor, the data protection officer and the supervisory authority. We provide a visual representation of how these entities are interrelated according to the corresponding GDPR articles and determine that companies acting as controllers have the largest need for future actions to achieve compliance with the GDPR.

Keywords: General Data Protection Regulation, GDPR compliance, stakeholders, dependencies, data privacy

1 Introduction

Personal data is the fuel for innovation. Recent technology advances have enabled a range of applications that were previously impossible to conduct. Sensor data from smartphones can be collected at virtually no cost, it can be transmitted via mobile networks, and stored and processed at volumes that were unattainable in prior times.

Since technological innovation is closely related to Business Models [1], the rapid technological developments have motivated substantial changes in Business Models as well. It has enabled a shift from product development towards information aggregation: Facebook creates no own content, Uber does not employ any drivers, German long distance bus company Flixbus does not own any buses, Airbnb does not own any real estate [2].

Some sources suggest that the extensive collection of personal data leads to an Orwellian society, where individuals lose their freedom through surveillance mechanisms [3]. [4], however, argues that not all collection activities interfere with such high values as freedom, but that the problem lies rather within the processing of information, because it changes the balance of power between individuals and institutions.

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Since *free of charge* is an appealing concept to consumers, the market for personal data has failed, just as economic markets can fail [5]. The European Union has recognized the need for unified regulation in this particular market and has passed the General Data Protection Regulation (EU GDPR) to address the challenges of privacy protection for its citizens that are induced by digitization [6]. The GDPR is a regulation that is released at the European Union level and, due to the special instrument as a regulation, is effective May 25, 2018 without further action from members of the Union [7].

The GDPR lays out an extensive set of rules to be followed and can be considered a goal definition in the state and abilities of an institution. We consider it our task in the Information Systems discipline to investigate the "appropriate technical and organizational measures" ([6], Art. 24, 28) to achieve compliance with the GDPR.

As an initial contribution, we regard it as essential to analyze who is involved and affected by the regulation. Thus, we define the research question *"Which are the major stakeholders mentioned in the GDPR and how are they related to each other?"*

The contributions of this paper are:

- A short survey of related work on the GDPR from the Information Systems discipline and in practice in section 2
- An analysis of the key stakeholders in the GDPR and a visualization of their interdependence in section 3

2 Related Work on GDPR Compliance

As the GDPR Regulation was initiated in 2012 and passed in 2016, related work on GDPR compliance is limited to this short timeframe. Work on the topic is investigated from either the perspective of jurisdiction, from information systems or from computer science. For practical advice, we identified guidelines by national supervisory authorities and whitepapers from commercial companies.

This discussion exclusively deals with work that specifically targets the GDPR. Results on compliance with prior regulation (e.g. Directive 95/46/EC, which will be repealed by the GDPR, [6]) will have to be subject of a detailed literature analysis. For the purposes of this work, we performed a literature analysis based on [8]. We searched for the term "EU GDPR" using the academic search engine Scopus in September 2017. The search resulted in 42 papers, with 38 being published in the year 2016 and after. In an analysis of the paper title, the results were reduced to 29, of which 18 were categorized as relevant after reading the abstracts. The available six works are presented in this section.

2.1 Academia

In [7], the implications of the GDPR from a legal perspective are discussed. While the underlying principles for the lawful processing are similar in prior legislation, penalties are increased dramatically with the GDPR. New rules include the transmission to third

countries, the accountability of the data controller, and the extended role of supervisory authorities. For organizations, the author derives a need for a data privacy management system, which supports the identification of relevant processes, provides guidelines, and enables control of compliance and discovery of deficits.

[9] points out the importance of personal data for medical research. The accountability principle and data protection by design pose new challenges to medical researchers. Especially the secondary use of research data has to be restricted to usages that are compatible with the initial reasons for collection. Communication of data breaches to data subjects and the supervisory authority requires the establishment of new processes.

[10] discusses the impact of the GDPR on the design and development of smart factories. The authors propose explicit guidelines for technical implementation of consent, the representation of data flows and data expiry as embodiment of the principles of data minimization.

A detailed two-step questionnaire for a data privacy impact assessment is given in [11]. The authors propose to use this artifact to identify risks in projects using cloud technologies. Unfortunately, the presented work lacks an evaluation.

Data compliance and data privacy is stated as one of the key requirements in data management in [12]. A reference model to guide practitioners in designing a data strategy is presented, considering processes & methods, roles & responsibilities, performance management, data architecture, data applications and the data lifecycle. The model addresses the recent developments in the Digital Economy.

[13] presents the architecture of a tool that focuses on the goal of data traceability. It incorporates the definition of customer records as XML files for data portability, central collection and distribution modules and a traceability module that implements an algorithm to discover all entities who received a copy of an individual's data.

The alignment of customer's privacy and security preferences with a service provider's system design is analyzed in [14]. They formalize Privacy Level Agreements (PLA) and develop an extensive metamodel to guide this analysis.

2.2 Practice

The United Kingdom's Information Commissioner's Office (ICO) represents the supervisory authority of the UK. [15] provides 12 steps for companies to take, such as assessing current processing and establishing processes for answering data subject requests or communicating data breaches. Due to the nature of the GDPR, the target state for implementation concurs in all EU countries, but the gap from previous national legislation differs.

The European Union Agency for Network and Information Security (ENISA) published guidelines for SMEs to achieve compliance with the GDPR [16]. The document gives detailed questionnaires for assessing risks and identifying need for action. Related topics of ISO 27001:2013 are given with the assessment questions.

Other practical advice is published by commercial organizations, usually with references to offerings related to achieving compliance with the GDPR. IBM [17] presents five key GDPR duties (rights of EU data subjects, security personal data,

lawfulness and consent, accountability of compliance, and data protection by design and by default) and proposes to start with pragmatic steps. Symantec [18] presents survey data that reinforces the need to act and provides four areas of action and corresponding products and implementation partners. Oracle [19] identifies nine core actors and four main areas of work: assess security risks, prevent attacks, monitor and detect breaches, and ensure the quality of protection. These areas are analyzed in the context of database technology.

3 Key Stakeholders in the EU GDPR

3.1 Research Approach

We adopted a two-step research approach analyzing the GDPR documents. First, we coded all stakeholders and relationships. Second, we consolidated the findings and visualized the key stakeholders to be considered for further evaluation in future work.

Following a sequence for a *structuring content analysis* [20], we defined the direction of analysis as the entities or authorities that are mentioned within the 99 GDPR articles [6], as well as statements or prescriptions on interactions between two such entities. We did not cover the means to fulfil these rules yet, because we regard it as essential to establish an understanding of the involved parties first before any other analysis can be conducted. It has to be clear who reports to whom before we can address technical or organizational measures. We defined the coding rule as unambiguous sentences with the structure *subject – predicate – object*, where we applied tags to both entities and the connecting relationship in the full regulation document. This data was extracted and collected in a relational table. We identified 17 unique entities and 64 bilateral relationships, each with their corresponding reference to an Article in the GDPR.

In the second step, we reduced the set of relationships from 64 specific relationships, such as *requests data from* or *consents to collection by* to 33 simple relationships of type *interacts with*. As criteria for a key stakeholder in the GDPR, we defined those entities that have at least three relationships with other entities (active or passive). We graphed these key entities as nodes and relationships as edges and specified the articles that define the corresponding connection.

3.2 Results

Out of the 17 entities we encountered in the document, 12 have a relationship with at most two other entities. The following five entities are involved in at least three relationships:

- *Data subject*: “an identifiable natural person (data subject) is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more

factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;" (Art. 4 (1))

- "*Controller* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (Art. 4 (7))
- "*Processor* means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;" (Art. 4 (8))
- *Data Protection Officer* (Art. 37-39) is designated by the controller or processor and has the tasks to advise and monitor the controller or processor and serve as a contact point for the supervisory authority
- *Supervisory Authority* (Art. 51): an independent public authority that is responsible for monitoring the application of the GDPR

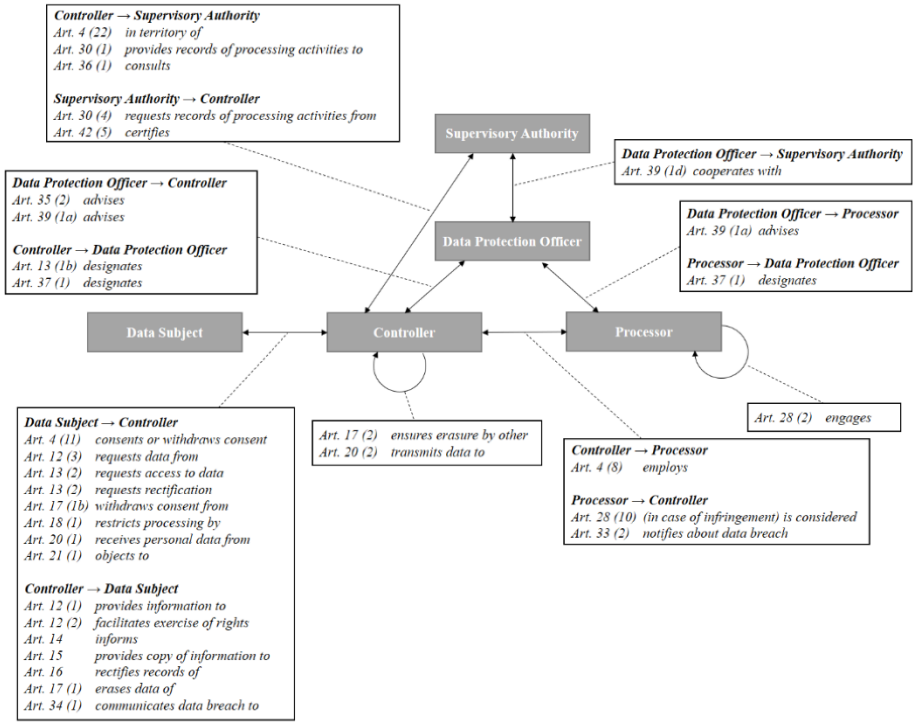

Figure 1: Network of most important stakeholders and their relationships within the GDPR

This list differs from the 9 core actors described by [19], who additionally mention personal data, recipient, enterprise and third party. We do not regard personal data itself as an actor, but rather the subject matter. Recipient, enterprise and third party do refer to entities, but not to a specific role described in the GDPR, i.e. a recipient could be both a controller and a processor.

Figure **1** shows a network of these most relevant stakeholders and their relationships. It becomes evident that the center of activity in this regulation revolves around the data subject and the controller with 15 explicit relationships, as well as

between the controller and the supervisory authority with 5 explicit relationships. Thus, we derive that the main actor in the GDPR is the data controller.

This implies a large set of necessary actions. From a technical perspective, systems need to be able to provide options for storing and revoking consent, as well as to restrict processing on a fine-grained level (Art. 4 (1), Art. 21(1)), Art. 18 (1)). The ability to deliver complete and coherent data to data subjects or transfer it to competitors has to be implemented (Art. 20 (2), Art. 20 (1)). The right to data rectification or deletion (Art. 16, Art. 17 (2), and Art. 17 (1)) pose further challenges, especially for tamper-proof systems.

From an organizational perspective, controllers must define processes for the timely communication of data breaches to data subjects and the supervisory authority (Art. 34 (1)). The role of the data protection officer, who reports directly to top management, has to be established (Art. 13 (1b), Art. 37 (1)).

4 Conclusion and Outlook

We have used a structured, data-driven approach to extract the most relevant stakeholders in the GDPR regulation: the data subject, whose personal data is collected and whose rights are reinforced by the GDPR; the controller, who is the single entity that is accountable for lawful data processing; the processor, who is not involved in direct communication with the data subject; the data protection officer as an entity within any processing or controlling entity; and the national supervisory authority. The majority of the articles refer to the interaction between the controller and the data subject and the controller and the supervisory authority.

An understanding of the stakeholders is one element in a complete picture of the GDPR, its implications and possible ways to act upon them. In future work, we will analyze the literature more thoroughly, especially with respect to analogous problems of achieving compliance with prior privacy regulation. Further, we plan to analyze industry efforts of becoming compliant before and after the GDPR enters into force on 25 May 2018. The goal is to identify patterns of dealing with single aspects of the regulation, e.g. the right to transparency, and investigate the effectiveness of the employed methods.

5 Acknowledgements

This work is part of the TUM Living Lab Connected Mobility (TUM LLCM) project and has been funded by the Bavarian Ministry of Economic Affairs and Media, Energy and Technology (StMWi) through the Center Digitisation.Bavaria, an initiative of the Bavarian State Government.

References

1. Baden-Fuller, C., Haefliger, S.: Business Models and Technological Innovation. Long Range

Plann. 46, 419–426 (2013)
2. Goodwin, T.: The Battle Is For The Customer Interface, https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/ (Accessed: 29.09.2017)
3. Schneier, B.: Data and Goliath: The hidden battles to collect your data and control your world. WW Norton & Company (2015)
4. Solove, D.J.: I've got nothing to hide and other misunderstandings of privacy. San Diego l. Rev. 44, 745 (2007)
5. Stiglitz, J.E.: The price of inequality: How today's divided society endangers our future. WW Norton & Company (2012)
6. European Union: Regulation 2016/679 of the European parliament and the Council of the European Union (2016)
7. Hamann, C.: Europäische Datenschutz-Grundverordnung - neue Organisationspflichten für Unternehmen. Betriebs-Berater. 1090–1097 (2017)
8. Kitchenham, B.: Procedures for performing systematic reviews. Keele, UK, Keele Univ. 33, 1–26 (2004)
9. Chassang, G.: The impact of the EU general data protection regulation on scientific research. Ecancermedicalscience. 11, 1–12 (2017)
10. Preuveneers, D., Joosen, W., Ilie-Zudor, E.: Data protection compliance regulations and implications for smart factories of the future. Proc. - 12th Int. Conf. Intell. Environ. IE 2016. 40–47 (2016)
11. Alnemr, R., Cayirci, E., Dalla Corte, L., Garaga, A., Leenes, R., Mhungu, R., Pearson, S., Reed, C., de Oliveira, A.S., Stefanatou, D.: A data protection impact assessment methodology for cloud. In: Annual Privacy Forum. pp. 60–92. Springer (2015)
12. Pentek, T., Legner, C., Otto, B.: Towards a Reference Model for Data Management in the Digital Economy. Des. Digit. Transform. DESRIST 2017 Res. Prog. Proc. 12th Int. Conf. Des. Sci. Res. Inf. Syst. Technol. 51–66 (2017)
13. Gjermundrød, H., Dionysiou, I., Costa, K.: privacyTracker: A Privacy-by-Design GDPR-Compliant Framework with Verifiable Data Traceability Controls BT - Current Trends in Web Engineering: ICWE 2016 International Workshops, DUI, TELERISE, SoWeMine, and Liquid Web, Lugano, Switzerland, June 6-9, 201 (2016)
14. Ahmadian, A.S., Jurjens, J.: Supporting model-based privacy analysis by exploiting privacy level agreements. Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom. 360–365 (2017)
15. Information Commissioner's Office: Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now. 11 (2016)
16. ENISA: Guidelines for SMEs on the security of personal data processing. (2016)
17. IBM: Planning for the General Data Protection Regulation
18. Symantec: Compliance, the " Privacy By Design " Approach To Protect. (2017)
19. Rajasekharan, D.: Accelerate Your Response to the EU General Data Protection Regulation (GDPR). (2017)
20. Mayring, P., Brunner, E.: Qualitative Inhaltsanalyse. (2009)