H. Roßnagel, C.H. Schunck, J. Günther (Hrsg): Open Identity Summit 2023,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023 135

Balancing Privacy and Value Creation in the Platform Economy: The Role of Transparency and Intervenability

Stefanie Astfalk, [1] and Christian H. Schunck [2]

Abstract: Data are essential in the platform economy to create value. Since the General Data Protection Regulation (GDPR) demands a high level of protection for personal data, it becomes challenging for small- and medium-sized businesses to provide both: data-based services and compliance to the GDPR. Therefore, the paper focuses on the privacy protection goals of transparency and intervenability to enable privacy friendly business models. To better understand how this approach supports the needs of small- and medium-sized platform providers, a qualitative interview study is conducted. Especially, the lack of legal certainty and the unclarity of how the GDPR can be implemented compliantly in practical terms is found to be a challenge. Based on the interviews, requirements are derived which a personal rights management tool enabling transparency and intervenability should fulfill such as supporting legal compliance or reducing operational complexity. In summary, small- and medium-sized platform providers see providing transparency and intervenability as a promising new approach which they are willing to deploy given the right personal rights management tool.

Keywords: Transparency, Intervenability, Small- and Medium-sized Platforms, GDPR, Qualitative Interview Study, Requirements, Personal Rights Management Tool

1 Introduction

The European General Data Protection Regulation (GDPR) is in force since May 2018 and strengthens the rights of EU citizens when companies such as platform providers are processing personal data. One way to comply with the GDPR is to focus on the privacy protection principle of unlinkability [HJR15] or anonymization and thus reducing the handling of personal data to an absolute minimum [Zi19], [Kn21], [Me17], [HSC08]. However, this approach is not compatible with many data driven business models and the provision of personalized services users expect and request. Alternatively, privacy friendliness can be enabled through other privacy protection principles such as transparency [Fi16], [FAP14] and intervenability [Zi19], [HSC08], [HJ16]. In PERISCOPE, a BMBF funded research project, for which this paper's study was conducted, these principles are utilized with the aim to enable privacy friendly business models in the platform economy. Ensuring the rights of data subjects in terms of transparency and the ability to intervene is an open challenge for today's complex

[1] University of Stuttgart, Institute of Human Factors and Technology Management IAT, Allmandring 35, 70569 Stuttgart, stefanie.astfalk@iat.uni-stuttgart.de, https://orcid.org/0000-0002-1926-639X
[2] Fraunhofer Institute for Industrial Engineering IAO, Nobelstraße 12, 70569 Stuttgart, Germany christian.schunck@iao.fraunhofer.de, https://orcid.org/0000-0002-7917-8180

cbe doi: 10.18420/OID2023_12

platforms: data subjects should receive an easy-to-digest overview on how their data are processed and on what legal basis with easy-to-use tools to exercise their data subject rights. Platform providers should be able to identify all data that refer to a data subject, record audit relevant information and have easy-to-use tools to respond efficiently, timely and appropriately to data subjects' rights requests. Therefore, qualitative interviews with small- and medium-sized platform providers (SMPs) were conducted to identify the status quo and the challenges they encounter. In addition, requirements for designing a personal rights management (PRM) tool that enhances transparency and intervenability for customers of SMPs is derived.

2 A Qualitative Interview Study

The qualitative semi-structured interviews were conducted with nine SMPs from various industries, such as fintech, medical, tourism or software development. The recording and transcription ensure the validity of the data material and a possible loss of information [GL10], [Ma13]. From all study participants informed consent was obtained.

General Questions	GDPR related Questions	PRM Tool related Questions.
• What data do is utilized? • Which business models are used or influence the data usage? • What data is shared with third-parties?	• What knowledge is available? • What obstacles are encountered? • What is the cost of implementation? • How are the different legal bases for data processing documented?	• Which components should a PRM tool have to generate added value? • Does the PRM tool enable new business models or a competitive advantage? • What is the willingness of usage?

Figure 1: Overview of the research questions investigated in the qualitative interview study.

The questionnaire was developed systematically and theory-based [Pr14] to test the research questions presented in Figure 1 and consists of three blocks. Firstly, there are general questions on the background and business model of the platform. Secondly, GDPR related questions cover the knowledge and implementation of the GDPR. Thirdly, there are questions focusing on transparency, intervenability, the design and added value of the required PRM tool to efficiently identify personal data and respond to requests from data subjects. The questions add up to a category system which is utilized for the evaluation. The qualitative content analysis according to ref. [Ma15] was used for data evaluation, which ensures a high level of comprehensibility. Core of this method is the category system which was developed deductive as well as inductive, [Ma15], [HSE13]. Subsequently, the extracted material was summarized, reduced to the relevant text passages, and interpreted in relation to the research questions [Ma15].

3 Interview Study: Qualitative Results

The interviewed platform providers offer heterogeneous business models and target different customer segments. Accordingly, different types of (personal) data are utilized. This shows that the business model of the platform influences the data utilization.

Mostly internal (personal) data is used and collected for registration purposes, customized services or the fulfillment of contracts or services relying on a legal basis according to Art. 6 GDPR. However, two of the interviewed platform providers do not assess personal data due to the GDPR restrictions and the fear of penalties for an incorrect implementation. Regarding the sharing of data with third-party providers, six out of nine of the interviewed platform providers regards data transfer to third parties not as the primary benefit for their platform. However, six platform providers transfer data to third parties for implementing their business model as well as for contract fulfilment. Hence, data sharing mainly takes place with contractual partners. The self-assessment of the knowledge regarding the GDPR is medium (mean = 3.05) on a 5-point Likert scale and is mostly acquired through the implementation and engagement with the GDPR and less by certification. Regarding the challenges SMPs encounter while implementing and maintaining the GDPR, the interview study confirms a high cost and time expenditure. The exact costs are difficult to quantify for the interviewees as these are not measured directly and are thus estimated to be between 3 % and 5 % of the platform's overall costs. In line with that, platform providers see two major challenges in addition to the economic ones: organizational and technical. The main organizational problem is a lack of structured processes for the implementation of the GDPR as [Br19] confirms. A high number of working hours is required to analyze which business processes are affected and to develop and adapt the platform accordingly. Still there remains doubt which changes are required, and which are sufficient. The main technical challenge is to develop a GDPR compliant architecture for data storage and processing without any redundancies. The prevailing different data formats and different data processing systems result in a massive effort. For example, just one out of nine platform providers was able to easily retrieve the legal basis for data processing on a case by case basis as it is used quite frequently in the fintech segment. Most interviewees have little knowledge on how to retrieve this information. Seven out of nine of the interviewed SMPs have a high readiness to utilize a PRM tool which supports transparency and intervenability. The main reasons are increased legal certainty and traceability as it supports the implementation of the GDPR and enables clarity through centralization of data privacy topics. In addition, a competitive advantage through time and cost benefits arises. Even though the PRM tool delivers an added value for the business model of most platforms, for some platforms an internal implementation is expected to be more promising. In line with that, six out of nine interviewees regard utilizing the tool as a competitive advantage. Overall, the most relevant components represent a transaction log, data subject rights management, automation of GDPR related topics and modular structure.

4 Interview Study: Requirements and Measures

Derived from the above-mentioned results, following requirements and measures for SMPs are identified and illustrated in Figure 2. Those requirements and measures apply for PRM tools which are going to be developed as part of the PERISCOPE project.

Legal Compliance	Compelxity Reduction	Integration	Business Case
• Must support a legally compliant implementation of the GDPR • Should be updatable in case of changes to legal frameworks	• Should be user-friendlyand usable with little time • Should centralize data protection-related topics • Must simplify GDPR-related processes • Should automate GDPR-related processes	• Must support various business models and data usage models • Should have a good technical documentation • Should be modular and integrable into various systems	• Should save more costs than it causes for platform providers • Should present a positive business case for the platfrom provider

Figure 2: Overview of the requirements and measures for SMPs derived out of the qualitative interviews.

Regarding legal compliance, the PRM tool must make it easier for SMPs to meet their accountability obligations, e.g., provide audit functionalities. Moreover, it must log GDPR-relevant processes for legal certainty and traceability, e.g., in a transaction log. In addition, the PRM tool must increase legal certainty for cooperations which involve the transfer of personal data to other companies, i.e., third parties, and must be able to document the legal basis for each type of data processing. Also, it must provide a reference system to the exact form of consent granted and should provide an overview regarding compliance with legal requirements. Additionally, the PRM tool should be updatable in case of changes in jurisdiction as well as be easily adaptable. Regarding complexity reduction, the PRM tool should be designed to be user-friendly and easy to use for SMPs with little GDPR knowledge and should centralize the SMPs' data protection-related topics and make them clearly arranged. Hence, the PRM tool must simplify GPDR-relevant processes and should also automate data protection relevant processes. For this, the PRM tool should support and log processes in which personal data is transferred to third parties, including the legal basis. Moreover, the PRM tool must facilitate or automate the process of handling a revocation of consent and should simplify GDPR provisions, such as data portability, and make compliance with GDPR rules verifiable. Additionally, it should simplify a timely response to the exercise of data subject rights and should be allowed to send automated warnings in case of expiring deadlines. Regarding integration, the PRM tool must support different business models as well as different data and data usage models. Moreover, it should be able to assign personal data to the respective data subject across systems and should have a good technical documentation. Furthermore, the PRM tool should be able to be integrated into various existing systems and thus be modular i.e., provide suitable interfaces, different combinable and flexibly selectable components as well as a guided setup process. Regarding the business case, the PRM tool should present a positive business case for the platform providers. Costs for its implementation and ongoing operation, license fees and further development must be compensated by process simplifications and automation, increased customer satisfaction and new business opportunities.

5 Discussion

The qualitative interviews illustrate the manifold GDPR related SMPs encounter. Those challenges mainly classify into organizational, technical as well as economic challenges

and indicate that the implementation and maintenance of the GDPR is resource intensive as other studies also confirm [CFP22], [DD18]. The main challenge represents the high resource consumption as well as the lack of certainty, regarding a legally compliant implementation of the GDPR. Therefore, there is a high readiness to utilize a PRM tool which supports platform providers in achieving increased transparency and respond to requests from data subjects. However, the modalities of the respective PRM tool are crucial for the readiness for use. Those requirements range from being applicable to different heterogeneous customer groups, different business models to the mapping and automation of the GDPR-related topics in a PRM platform with a modular system. The most relevant components represent the transaction log, the data subject rights management, the automation of GDPR-related topics and a modular structure. The main reasons for the utilization of such a PRM tool include increased legal certainty and auditability which the interviewed platforms aim to achieve as well as a competitive advantage through time and cost benefits. However, the platform providers' expectations of the respective PRM tool are very extensive, so that, for example, the automation of all GDPR-relevant processes cannot be realized by such a tool. In several instances case-by-case considerations that consider the specific situation of the platform provider as well as the data subject are required. These cannot be automated by the respective PRM tool. The willingness for use by the platform providers can therefore only be assessed when such a PRM tool is available in practice, and when it is clear whether the existing expectations are sufficiently addressed and solved by the tool.

6 Conclusion and Future Work

It has been seen that SMPs encounter significant challenges while implementing and maintaining GDPR compliant operations and the readiness to implement novel PRM tools that assist in addressing these issues and provide increased legal certainty is high. Therefore, requirements for a PRM tool that increases transparency and intervenability for SMPs in the data economy have been obtained. This qualitative interview study presents a first steps towards developing, testing, and adapting the PRM tool and the next steps are currently under way. The applied qualitative approach lies the foundations for this research and can be utilized to explore this new area to assess novel tendencies.

Supplementary information such as the interview guideline is available here.

Acknowledgements

This research is funded by the German Federal Ministry of Education and Research under grant agreement numbers 16KIS1479K and 16KIS1484 (PERISCOPE project).

Bibliography

[Br19] Brodin, M.: A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises. European Journal for Security Research 2/4, pp. 243–264, 2019.

[CFP22] Chen, C.; Frey, C. B.; Presidente, G.: Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally. The Oxford Martin Working Paper Series on Technological and Economic Change 1, 2022.

[DD18] Da Freitas, M. C.; Da Mira Silva, M.: GDPR Compliance in SMEs: There is much to be done. Journal of Information Systems Engineering & Management 4/3, 2018.

[FAP14] Fischer-Hübner, S.; Angulo, J.; Pulls, T.: How can Cloud Users be Supported in Deciding on, Tracking and Controlling How their Data are Used?. In Privacy and Identity Management for Emerging Services and Technologies: 8th IFIP WG, Springer, pp. 77–92, 2014.

[Fi16] Fischer-Hübner, S. et al.: Transparency, privacy and trust–Technology for tracking and controlling my data disclosures: Does this work?. In Trust Management X: 10th IFIP WG, Springer International Publishing, pp. 3–14, 2016.

[GL10] Gläser, J.; Laudel, G.: Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen. VS Verlag, Wiesbaden, 2010.

[HJ16] Hubaux, J.-P.; Juels, A.: Privacy is dead, long live privacy. Communications of the ACM 6/59, pp. 39–41, 2016.

[HJR15] Hansen, M.; Jensen, M.; Rost, M.: Protection Goals for Privacy Engineering. IEEE Security and Privacy Workshops, pp. 159–166, 2015.

[HSC08] Hansen, M.; Schwartz, A.; Cooper, A.: Privacy and Identity Management. IEEE Security and Privacy Magazine 2/6, pp. 38–45, 2008.

[HSE13] Hussy, W.; Schreier, M.; Echterhoff, G.: Forschungsmethoden in Psychologie und Sozialwissenschaften für Bachelor. Springer-Verlag, Berlin / Heidelberg, 2013.

[Kn21] Kneuper, R.: Allgemeine Grundlagen des Datenschutzes nach DSGVO: Datenschutz für Softwareentwicklung und IT. Springer Verlag, Berlin Heidelberg, pp. 19–62, 2021.

[Ma13] Mayer, H. O.: Interview und schriftliche Befragung: Grundlagen und Methoden empirischer Sozialforschung. 6th rev. ed., Oldenbourg Wissenschaftsverlag, München: Oldenbourg, 2013.

[Ma15] Mayring, P.: Qualitative Inhaltsanalyse. Grundlagen und Techniken. Beltz Verlag, Weinheim, 2015.

[Me17] Mester, B. A.: Auswirkungen der DSGVO auf die IT. Wirtschaftsinformatik & Management 4/9, pp. 12–15, 2017.

[Pr14] Porst, R.: Fragebogen: Ein Arbeitsbuch. 4th, ext. ed., VS Verlag, Wiesbaden, 2014.

[Zi19] Zibuschka, J. et al.: Anonymization Is Dead – Long Live Privacy: Open Identity Summit, pp. 71–82, 2019.