Data Protection Officers' Perspectives on Privacy Challenges in Digital Ecosystems

Stephan Wiefling[1], Jan Tolsdorf[2], and Luigi Lo Iacono[2]

[1] Ruhr University Bochum, Bochum, Germany
stephan.wiefling@rub.de
[2] H-BRS University of Applied Sciences, Sankt Augustin, Germany
{jan.tolsdorf,luigi.lo_iacono}@h-brs.de

Abstract. Digital ecosystems are driving the digital transformation of business models. Meanwhile, the associated processing of personal data within these complex systems poses challenges to the protection of individual privacy. In this paper, we explore these challenges from the perspective of digital ecosystems' platform providers. To this end, we present the results of an interview study with seven data protection officers representing a total of 12 digital ecosystems in Germany. We identified current and future challenges for the implementation of data protection requirements, covering issues on legal obligations and data subject rights. Our results support stakeholders involved in the implementation of privacy protection measures in digital ecosystems, and form the foundation for future privacy-related studies tailored to the specifics of digital ecosystems.

Keywords: GDPR · Digital Ecosystem · Data Protection Officer · Expert Interviews

1 Introduction

Digital ecosystems [14] are ubiquitous, and both end users and businesses use them to exchange services and digital or analog goods: be it customer-to-customer (C2C) as with Airbnb, business-to-customer (B2C) as with Amazon Marketplace, or business-to-business (B2B) as with Google AdSense. As part of this, in many cases digital ecosystems require the processing of personal data, i.e., data relating to an identified or identifiable natural person [10] – either because individuals disclose personal data in order to participate in the digital ecosystem or because the services and goods exchanged themselves require or constitute personal data. In the process, many different actors gain access to this data. Next to platform operators and providers of services or goods, these include, e.g., providers of IT infrastructure, payment services, and logistics. The resulting complex flows of personal data and the increasing proliferation of digital ecosystems undoubtedly pose a challenge to the protection of this data - and thus to the protection of the privacy of millions, if not billions, of people worldwide. The General Data Protection Regulation (GDPR) [10] addresses this issue by defining the responsibilities and obligations of the various actors involved in the

Paper accepted at SPOSE '22, co-located with ESORICS '22.

processing of personal data and by requiring the implementation of appropriate technical and organizational measures (TOMs) to protect such data. However, there is currently a lack of insight on how digital ecosystems are mastering the challenge of putting GDPR requirements into practice.

Research question. In this paper, we address this lack of insight from the perspective of the *service asset broker*, i.e., the entity who owns and operates a digital ecosystem's underlying digital platform. As they are at the center of digital ecosystems, insights from this stakeholder can contribute to a better understanding of the overall challenges for implementing data protection in digital ecosystems. To this end, we formulate the following research question:

RQ1: What challenges are met in practice when implementing data protection requirements in digital ecosystems from the perspective of *service asset brokers*?

Answering this research question is of high practical relevance, because practical insights and a thorough understanding of the field allow researchers and other stakeholders involved in privacy engineering and enforcement to support digital ecosystems in translating the often abstract data protection requirements into actual TOMs.

Contributions. We conducted four semi-structured interviews with seven data protection officers (DPOs) appointed by 12 digital ecosystems in Germany. On this basis, we report on the challenges that the DPOs identified in implementing data protection in digital ecosystems, who they think is responsible, and what they would like to see happen in the future to achieve more effective data protection in practice. In general, we find that DPOs demanded for action by the regulatory and supervisory bodies to increase harmonization of laws, and to provide more consistent and more accurate guidance and examples of TOMs. We further find that the implementation of data subjects' rights remains in a state of non-digitalization. In addition, DPOs considered the implementation of transparency in the processing of personal data in digital ecosystems to be a major future challenge – both for data subjects to become informed and privacy aware, and for themselves to keep track of personal data flows.

To our knowledge, our work offers the first insight into how DPOs perceive digital ecosystems putting data protection requirements into practice. We expect this focus to provide insights of high practical relevance, as DPOs guide and evaluate the privacy practices of potentially multiple digital ecosystems, making them proven experts on the data protection challenges in this subject. Our contributions support digital ecosystems and privacy engineers to implement privacy regulations more effectively. Regulators get insights into DPOs' thoughts on their privacy regulations, and the challenges they face when putting the regulations into practice. Researchers get insights from a hard-to-reach population, and directions for further research in the domain of digital ecosystems.

2 Privacy in Digital Ecosystems

Below, we provide an overview of digital ecosystems and a working definition, review relevant data protection requirements, and discuss related work.

2.1 Digital Ecosystems

The subject area of digital ecosystems is extremely heterogeneous and is essentially influenced by social, economic, computer, and natural sciences, all of which define digital ecosystems, their components, and parties differently [14]. Following recent efforts for a unified understanding, we adopt the definition that *"[a] digital ecosystem is a socio-technical system connecting multiple, typically independent providers and consumers of assets for their mutual benefit."* [14] Accordingly, a digital ecosystem is founded on the provision of at least one *ecosystem service* (e.g., software distribution) by a *service asset broker* (e.g., Google) via a digital platform (e.g., Play Store). The *ecosystem service* brokers *service assets* (e.g., apps) between *service asset providers* (e.g., app manufacturer) and *service asset consumers* (e.g., app users). Both are considered consumers of the *ecosystem service*. If required, *support providers* (e.g., PayPal) can assist *service asset brokers* in providing the *ecosystem service*. Due to the heterogeneous nature of digital ecosystems, some digital platforms cannot be clearly classified as such [14]. Additionally, the idea of digital ecosystems in practice is strongly bound to economic aspects, i.e., using advances in information and communication technology to drive business by digitalization [17].

2.2 Data Protection Requirements

The brokerage of *service assets* in digital ecosystems typically involves the processing of personal data; this is the case, e.g., when (i) personal data themselves represent *service assets* (e.g., behavioral data), (ii) personal data underlay *service assets* (e.g., user-targeted advertisements), (iii) consumers of *ecosystem services* disclose personal data to the *service asset broker* for participation, or (iv) *service asset consumers* disclose personal data to *service asset providers* in the course of the *service asset* exchange. To the extent that individuals whose personal data are processed or other actors in a digital ecosystem are located in the European Union (EU), the processing of personal data is subject to the rules of the GDPR (Art. 3)[3]. Actors who determine the purposes and means of the processing of personal data in a digital ecosystem acquire the role of a (data) controller (Art. 4). From the above definition it follows that at least *service asset brokers* (e.g., Google), but often also *service asset providers* (e.g., app manufacturer) and *support providers* (e.g., PayPal) have this role. Controllers are responsible for and must demonstrate compliance with the following fundamental principles (Art. 5): (i) *Lawfulness* denotes that personal data processing must be based on a valid legal basis prior to processing. Likely legal bases in

[3] Unless otherwise stated, all articles mentioned refer to the GDPR [10].

digital ecosystems include consent, the necessity of the processing for the performance of a contract, or the legitimate interests of the controller (Art. 6). (ii) *Fairness* means that personal data are not processed in a manner that is unjustifiably harmful, unlawfully discriminatory, unexpected, or deceptive to data subjects [8]. (iii) *Transparency* means that personal data processing is transparent, open, and clear to data subjects. This entails informing data subjects about the nature and scope of the processing, as well as enabling them to understand and exercise their rights (Arts. 12 - 14, 34). (iv) *Purpose limitation* means that personal data must only be obtained for specific, explicit, and legitimate purposes. The data must also not be processed in a manner incompatible with the purposes for which they were obtained. (v) *Data minimization* refers to only processing personal data that are adequate, relevant, and limited to what is necessary in relation to a purpose. (vi) *Accuracy* implies that personal data processed are accurate and up to date, and that reasonable efforts are made to delete or rectify inaccurate data in relation to a specific purpose. (vii) *Storage limitation* means that the processing of personal data does not allow the identification of data subjects for longer than is necessary for the original purpose or to comply with legal requirements. (viii) *Integrity and confidentiality* require the implementation of appropriate TOMs to ensure personal data security, including safeguards against unauthorized or unlawful processing, accidental loss, destruction, or damage. (ix) *Accountability* denotes that controllers ensure and are able to demonstrate compliance with the aforementioned principles.

To enforce these principles, the GDPR obligates controllers and entities processing personal data on the controller's behalf (i.e., processors) to implement TOMs (Art. 24) as well as to provide and implement several data subject rights. Among other things, individuals have the right to be informed about data processing and get access to their personal data (Arts. 12 - 15, 20), the rights to rectification and erasure (Arts. 16, 17), the rights to restriction and objection of processing (Arts. 18, 21), and the right to be protected against solely automated decisions with legal or similar effect (Art. 22). For infringements of the principles or the data subject rights by controllers or processors, the GDPR provides for penalties in the tens of millions of Euros or up to 4% of annual global turnover.

2.3 Related Work

Previous work on implementing the GDPR from the perspective of organizations has largely focused on identifying universal success factors, barriers, challenges, benefits, and consequences [1,21,27,28]. Specific insights on these aspects have been provided for public administrations [15], financial services industries [12], education institutions [11], and SMEs [6,25]. Few of these studies included DPOs [11,28]. In contrast, work specifically addressing digital ecosystems is thus far limited. Anwar et al. [2] conducted a review of international laws, regulations, and standards to identify and sort aspects related to (1) the protection of individuals' privacy, (2) guarantees to be made about the processing, (3) measures to be taken for the handling of information, and (4) consequences for technical implementation. Kira et al. [13] address the problem that digital ecosystems

must comply with both competition policy and privacy law. They propose an integrated approach in which privacy considerations are incorporated into competition decisions to improve enforcement of both. Furthermore, some studies have touched aspects of privacy engineering when evaluating privacy issues in digital ecosystems and similar platforms. Park et al. [19] provide a conceptual model to uncover potential threats to the privacy of users of digital ecosystems due to algorithmic decisions. They argue that individuals' privacy concerns should be taken into account in the design, and that effective protection against, e.g., discrimination requires effective data minimization and processing restrictions. In addition, Van Landuyt et al. [30] describe pros and cons of using centralized versus federated approaches for both the documentation of data processing and the enforcement of data protection in digital ecosystems with inter-organizational personal data flow. Additional work remains largely focused on human factors and user studies [31]. For example, this includes studies on online social networks [5,18], mobile ecosystems [22], and sharing economies [23,29]. To the best of our knowledge, our study is the first to provide insights on the challenges of implementing data protection in digital ecosystems with the help of a very important but so far overlooked stakeholder: the DPO.

3 Methodology

We conducted a semi-structured interview study with seven DPOs representing a total of 12 digital ecosystems in Germany between December 2021 and January 2022. The following subsections provide details on the interview guideline design and study procedure, participant recruitment and background, data collection and analysis, and how we addressed ethical concerns.

3.1 Interview Guidelines Design and Study Procedure

We designed a questionnaire with an estimated interview length of 45 minutes, which focused on challenges in implementing data protection requirements in digital ecosystems. The interview length was chosen to accommodate the expected busy schedules of DPOs, and to obtain as much information as possible, while avoiding fatigue on the participants' side.

To ensure that our interview guidelines cover the main points of interest, we collected topics of interest using expert group discussions and literature review. The experts came from the fields of psychology, ergonomics, information security, and usable security & privacy. They were researchers, software and architecture engineers working on digital ecosystems, as well as DPOs not working for digital ecosystems. We also conducted a one-hour background interview with a digital ecosystem expert to go over the identified topic areas in greater depth. The insights gained from all these activities were used as the basis for deriving our interview guidelines. We then revised our interview guidelines by discussing them with researchers experienced in conducting interviews. Our final interview guidelines are available in Appendix A.

All interviews were conducted using remote conferencing software. Before starting the actual interview, we welcomed our participants and briefed them about the study procedure and conditions. We asked for informed consent to record the audio and video streams. We ensured anonymity and communicated our anonymization measures to the participants to counteract a social desirability bias that can occur in privacy topics [26]. Furthermore, we made it clear to the participants that there are no "right" or "wrong" answers.

The interview consisted of two parts. In the first part, we asked our study participants to give an introduction to their digital ecosystems. This served the purpose of allowing our participants to recapitulate the ecosystem and the interviewer to gain knowledge and understand the digital ecosystem. This involved questions about the actors involved, the personal data processed, the purposes for which the data are used, as well as the data flow and its depth. The second part regarded the challenges in implementing data protection requirements in digital ecosystems. We asked our participants what major challenges they have faced in the past and expect to face in the future. We also asked specifically about challenges related to the implementation of data subjects' rights and what responsibility the operator has for implementing data protection requirements in digital ecosystems. We concluded this section by asking what would be useful or helpful to make data protection more effective in the future. After that, the audio and video recording was stopped, the study participants were thanked for their time, and farewells were said. Excluding briefing and debriefing, the interviews lasted between 30 and 45 minutes.

3.2 Participant Recruitment, Enrollment, and Background

To recruit participants for our study, we contacted the DPOs of 24 *service asset brokers* of digital ecosystems in Germany via email. We identified these ecosystems based on Internet research using the definition in Section 2.1. The email included an invitation to a background discussion on data protection challenges in digital ecosystems. The email also mentioned that the contents of the conversation would be treated anonymously and stored in anonymized form.

In the end, we were able to recruit a total of seven DPOs. As is common with DPOs in Germany, six participants had a legal background. Moreover, three participants stated that they performed the function of an internal DPO, and one participant each stated that they acted as an external DPO, data protection engineer, data protection coordinator, or project manager for data protection.

3.3 Data Collection and Analysis

After the interviews were completed, we extracted the audio streams from the recordings and stored them separately. We then sent the audio recordings to an external transcription service so that the answers could be pseudonymized and coded afterwards. In the transcripts, any names of companies and persons were replaced by a generic name (e.g., "[name]" instead of "Jane Doe").

For the analysis of our interview material, we used inductive coding because the topics emerge from the content itself. In total, three coders (A, B, and C) were involved in the coding process. Coder A, the principal investigator [4], carried out the initial coding and created the code book based on the responses given in the interview material. After that, coder B also coded the full interview transcripts, using the code book created by coder A. The inter-rater agreement was 82.49% with $\kappa = 0.82$, which deemed strong consistency [16]. Coder C resolved any coding conflicts for the final analysis.

3.4 Ethical Considerations

Although our institution does not have a formal institutional review board (IRB) process, we made sure to minimize potential harm by complying with the ethics code of the German Sociological Association as well as the standards of good scientific practice of the German Research Foundation. Our study follows national and EU privacy laws, and was approved by our institution's DPO. We pseudonymized or anonymized the data after the interview. In particular, we eliminated all direct identifiers from the audio recordings before sending them to the transcription service. We further ensured that the service provider was located in Germany, complied with the GDPR, and deleted the submitted audio data after transcription and transmission to us. Any contact information was kept separate from the responses and was not linked to it.

4 Digital Ecosystems Overview

Based on the first part of our interview, this section provides an overview of the digital ecosystems covered. Overall, our study covers the perspective of four companies in Germany who act as *service asset brokers* for analog or digital goods. Two companies were market leaders (listed corporations), one company was an SME, and another company was a startup with its own newly created market segment. Depending on the company, the DPOs oversee multiple digital ecosystems simultaneously, so our results capture insights for a total of 12 digital ecosystems. The market segments include transport and travel, online social network, and online marketplaces. Three digital ecosystems focus on the B2B segment and nine on the B2C and C2C segments. In the following, we outline the stakeholders considered by digital ecosystems, the data processed within them, the purposes of the processing, and provide insights into the data flows. Detailed information on all these aspects based on our coding is available in Table 1.

Involved stakeholders. Our participants reported a mixture of individual persons and companies that participate in the respective digital ecosystems. When asked about stakeholders' main motivations for participation, our participants cited financial benefits, added value, and workflow optimization (3/4), as well as gaining market advantage and marketing (2/4) as the primary reasons.

Data and intended use. Our participants explained that different types of personal data are processed in digital ecosystems. In the case of online dating,

Table 1. Overview personal data processing in digital ecosystems covered.

Stake-holders	End customer (4), ecosystem operator (2), product manufacturer (2), business intelligence (1), cloud service provider (1), development partner (1), infrastructure partner (1), employees (1), online marketing (1), carriers (1)
Personal data	Name (3), address (3), email address (2), comments/messages (2), user account (2), user activities (2), payment data (2), age (1), operating system (1), consent (1), product identification number (1), pictures (1), gender (1), sexual orientation (1), VAT number (1), behavioral data (1), log data (1)
Purposes	Enabling use (4), authorization checks (2), payment processing (2), error analysis (1), fraud protection (1), traceability (1)
Recipients	Processor (3), employees (2), customer service (2), partners (2), users (1)

Note. Values in parentheses indicate the number of interviews in which we identified the topic. Baseline is four interviews.

this also includes special categories of personal data (Art. 9). Identified purposes generally concern the provision and maintenance of the platform and services.

Data flow and control. For the ecosystems surveyed, personal data also flows to external partners or processors (3/4), such as financial systems, cloud computing providers, insurance companies, and car workshops. Our participants explained that audits of external recipients (2/4) and the requirement to sign a data processing agreement (2/4) are used to ensure that personal data is processed for the intended purposes. To further protect personal data within the company, employees are instructed to limit data use to a specific purpose (3/4) and to follow strict instructions, particularly in customer service (1/4).

5 Data Protection Challenges

This section deals with the second part of our interview that directly addresses our research question. We translated relevant statements of our participants from German into English. We indicate the number of interviews in which we identified specific themes. These counts are intended to provide an indication and not a basis for quantitative analysis.

5.1 Implementing Legal Requirements

After our participants finished describing the digital ecosystems, we asked them what the biggest challenges were in implementing data protection requirements. Below, we report on the various challenges identified based on our analysis.

Accountability obligations and keeping track. First, one participant explained the challenges arising from the controller's accountability obligation:

> *"For one thing, the legal basis, ensuring the legal basis and the accountability. The purpose-related access [of the data], so that we are in a position to say: Okay, we now have no access that has no legitimate purpose [...] Then the topic of secure storage and transmission. [...] And the issue of proof of consent [...] and thus also the implementation of the right to object, which goes hand in hand with this [...]."* (I1)

In this regard, some participants also found it challenging to keep track of a constantly growing digital ecosystem with many actors involved (2/4):

> *"I think that the biggest challenge for an extremely fast-growing company [...] is to maintain an overview as a data protection officer and to weigh up the risks and opportunities."* (I3)

To streamline proof to supervisory authorities, one DPO proposed to introduce certifications for the data protection management systems used by controllers. However, they also expressed concerns that certifications can mislead supervisory authorities into drawing wrong conclusions:

> *"We have such a confusion of certifications. Everyone can come up with a certificate. We deliberately don't do it, [since controllers] [...] can pretend [...] [having] a certificate [...] that (in reality) is worth nothing"* (I1)

Contractual challenges. We further found that concluding contracts with processors can be challenging, in particular, when processors involve external partners in other legislation. In such a case, personal data processing could collide with the data protection requirements of *lawfulness* and *accountability*:

> *"[...] when it comes to [data] processing, it becomes difficult, because in the context of maintenance and support activities there is always the possibility that American or Canadian [...] companies also have other American employees as subcontractors in their context."* (I1)

To make it easier to conclude contracts with external partners, our participants highlighted the usefulness of standard contractual clauses provided by the EU. However, those were not seen as a one-size-fits-all solution in all use cases:

> *"[A large] company like ours [...] conclude[s] a lot of contracts [with processors]. [...] This means that we are, of course, very happy that there are standard contractual clauses at the EU level [...] Beyond that, however, there are other points here and there that simply have to be agreed upon. And since other companies have the same problem, it can be a bit difficult to reach a common consensus in individual cases. Because everyone would prefer to sign a standard document that everyone knows and has agreed on. And that can be a bit exhausting."* (I4)

Similarly, education about new data protection clauses can be an issue that delays contract negotiations, for instance with smaller companies (1/4):

> *"[...] it is sometimes the case [...] that you first have to explain them [(contractual partners)] where the new legal or regulatory challenges are. 'What does Schrems 2 actually mean, what does the conclusion of the standard contractual clauses mean?' And then to come to a reasonable result that meets the legal requirements."* (I2)

Beyond that, limited personnel capacities in the legal departments responsible for data protection issues pose an additional challenge for concluding contracts (1/4):

> *"Due to the mass [of requests], the challenge is also often to check all measures in the desired period of time. For example, if the specific departments want to conclude contracts in a quick period of time."* (I2)

Diverse legislation. Our participants further explained that different legislation in different countries poses a challenge to operating digital ecosystems in a legally compliant manner, since it increases the required efforts (2/4):

> *"So I think, not only in this case, but in all cases [are] the biggest problems [...] when we have processors involved and especially when they are not located in Europe. [...] Then we have to meet extremely high requirements [...]. Then we [...] still have to send out questionnaires and evaluate them, make a risk assessment. So that, in my opinion, was the greatest challenge, at least the greatest effort."* (I4)

> *"The legal situation in the U.S. and thus also the inadmissible, or unsatisfactory, legal situation that we have with regard to data exchange or the use of U.S. service providers [...] are the biggest pitfalls we have here. We are talking about the global economy on the one hand and data protection measures on the other."* (I1)

Inferior power to Big Tech. DPOs in our study also stated that enforcing legal requirements is difficult, even in relatively large digital ecosystems, when Big Tech companies are involved (1/4):

> *"Of course you often have the problem of power balance when you look at large players, such as, [...] Google, Facebook, or Amazon. Then, even if [our company] is not a small corporation, it is of course a smaller corporation compared to these large corporations. There is the particular hurdle of enforcing [...] the legal requirements on these contractual partners, who are superior in terms of power balance [...]."* (I2)

Uncertainty in interpretation of law. New laws that impose novel and additional requirements on existing processing of personal data (e.g., cookies) often pose a challenge to DPOs in terms of their interpretation (2/4). They also criticized the lack of recommendations from the relevant supervisory authorities, making the process a huge drain on resources (1/4).

> *"Now [...] we all have the new TTDSG*[4] *and the cookie web tracking issue on the table, which [...] keeps us busy [...] as a large digital corporation [...]. The challenge is always the time and the legal requirements that you are [...] exposed to [...] in the legal team. And [...] you also try to catch up [with the legal requirements] as quickly as possible, and then actually implement them in practice as soon as possible."* (I2)

> *"When a law such as the TTDSG comes into force, but there are not yet sufficient or only limited recommendations from the regulatory authorities, then [it is difficult] to conclude which legal requirements should now actually be implemented in practice."* (I2)

Barriers to transparency. DPOs expressed their concern that the obligations put forward by the GDPR essentially undermine the principle of *transparency*:

> *"It is precisely this balancing act [...] between the legal requirements, which of course must be implemented [...]. But also to provide users with data protection in a friendly, transparent manner and with an eye to keeping them informed, and to find a healthy balance."* (I2)

> *"[T]he biggest problem [...] is that the GDPR intends well in principle [...] but in part has the wrong focus. [...] [W]ith all the transparency that we have to demonstrate, we are actually completely non-transparent [...]. If you look at prominent websites on the Internet and open the data privacy policies, there are usually 30, 40, 50 pages full of [...] policies. And the purpose of these is actually to make it clear to the user [...] where their data is now located and what is being collected. And [in] my opinion [...] this is actually completely non-transparent [...]."* (I3)

5.2 Implementing Data Subject Rights

We explained to our participants that one of our research goals is to help digital ecosystems implement data subject rights. To this end, we asked them what major challenges digital ecosystems face in this regard. In the following, we present the different answers, grouped into themes according to our coding.

Privacy policies. Our participants explained that setting up a company privacy policy for handling data subject rights can be challenging, because it must document necessary processes in a way comprehensible to non-legal staff who have to respond to data subject requests (3/4):

> *"If you look at the various departments, who, for example, handle such data subject rights in the first place and respond to inquiries. Then, of*

[4] The Telecommunication Telemedia Data Protection Act (TTDSG) is the national adoption of the EU ePrivacy Directive in Germany. It further replaces previous regulations on data protection and secrecy for telecommunications services in Germany.

course, it must always comply with the legal requirements. This means that there is a need for comprehensive documentation or legal requirements that are also prepared for the relevant departments, which of course also have to be educated on a regular basis." (I2)

Requests for erasure. Our participants expressed particular concern regarding data subjects' right to erasure (2/4). One DPO explained that requests for erasure are submitted in written form, but without a standardized format. This often leads to difficulties of interpretation in practice. Another DPO pointed out that actual erasure is difficult in practice, but too often confirmed by controllers or processors without the data actually being deleted:

"In particular, we must also pay attention to the interpretation of the wording used by the parties concerned, because when a party concerned asserts its request for deletion, 'deletion' is not always expressly mentioned, so that problems also arise here in the interpretation." (I2)

"A lot of companies have [...] many IT systems and scattered data from their respective users. And I think that many companies, simply also because of the speed that they are up against [to process deletion lawfully], have difficulties there in creating a proper deletion request." (I3)

Strict deadlines. We further found that strict deadlines given by the law to handle data subject requests can be challenging in (complex) digital ecosystems:

"If, for example, a request under the right to access is to be processed, there is a time limit of one month [...], within which the request [...] must be answered. And depending on how the [digital] ecosystem is set up, there is the problem of time [...]." (I2)

5.3 Responsibility of Operators for the Entire Digital Ecosystem

We further asked our participants what responsibility a *service asset broker* has to ensure data protection throughout the entire ecosystem.

Data protection mechanisms. To protect data misuse by external partners, the ecosystems rely on contractual assurances (1/4), minimization of the amount of data stored (2/4), and a kind of social control by only working with reputable companies that would have a reputation to lose if they did not comply with data protection regulations (1/4):

"When we work with external partners, I would say they are usually larger, well-known companies. I think it's fair to say that they also have something to lose if they don't meet their data protection requirements. So [...] we make sure that the partners we work with have the right standing in the market. That's how social control works." (I4)

Data protection as an ongoing process. Another responsibility mentioned to ensure data protection throughout the ecosystem was to make and see data protection as an ongoing process (1/4):

> *"I don't just do data protection and then put a check mark on it, but I have to establish structures that make it possible on a continuous basis and also make it possible to have an early warning system."* (I4)

Documentation of the digital ecosystem was also seen as a part to fulfill this responsibility (1/4):

> *"When I launch a new application, [...] you also look again: 'Are other services integrated here? Has the topic of data protection been sufficiently addressed?' And so on. Documentation, things like that, general things. But that's also quite a lot. (laughs) You're quite busy with that. "* (I4)

5.4 Helpful (Future) Steps for More Effective Data Protection

To address the challenges of implementing data protection, we asked our participants what would be helpful to make data protection more effective in digital ecosystems in the future. Below, we present the themes identified by our coding.

Harmonization. Our participants greatly appreciated the harmonization of privacy laws caused by the GDPR for the implementation of legal requirements in international markets. They would therefore appreciate the regulators taking further steps in this direction, both at the international and national level (2/4):

> *"It would help a lot if either the European data protection authorities were to scale down their demands a bit [...]. Or if the U.S. government, in particular, were to move a bit and keep its intelligence services under control for a while. Because that is exactly [...] why data transfer to the U.S. in particular has been made so difficult."* (I1)

> *"We have the problem of federalism here in Germany, so to speak. It always depends on which federal state you are located in, how strictly the data protection authorities interpret certain things. [...] [A] certain standardization would be helpful for all of us, first of all at the German level, but also with a view to the EU."* (I2)

Explicit requirements and guidelines. Following the idea of harmonization, our participants stated that regulators and supervisory authorities should focus on consistent and clear communication of data protection requirements (2/4). In addition, DPOs sought guidance and templates to avoid problems due to different interpretations from the outset:

> *"From my point of view, the legal requirements, or what is expected of us, should be communicated a bit more clearly by the regulatory authority. Because a lot of things need to be interpreted and a lot of things are actually implemented a bit differently in German law than the European legislator specifies."* (I2)

> *"And [...] the data protection conference, as the highest national data protection body, should provide guidance, perhaps even more practical recommendations and practical examples in the form of screenshots of cookie banners, [...] [and] I could certainly imagine open online consultation hours being helpful here. Perhaps the universities could also provide support in this context."* (I2)

In this regard, however, there was also a desire for supervisory bodies to have a better understanding of technology (1/4):

> *"We have few supervisory authorities, who are very tech-savvy. We have other supervisory authorities, who have less understanding there."* (I1)

Transparency. Our participants regarded measures for improved transparency as an essential step toward more effective implementation of data protection requirements in digital ecosystems. Different aspects were addressed here. One aspect related directly to the challenge of keeping track of a growing digital ecosystem by implementing *"central transparency"*, i.e., measures that facilitate DPOs to keep track centrally of all entities and personal data flows (2/4):

> *"[W]e have the requirement that we must document everything. There has to be central transparency somewhere. It's not enough for someone to have thought of something good on a decentralized basis [...] [W]e also have to keep an eye on the bigger picture and have an overview."* (I4)

Further aspects discussed by our participants relate to transparency and honesty about data processing towards data subjects. DPOs see a particular need to raise people's (limited) privacy awareness (3/4), believing that this would relieve data controllers from being blamed. However, DPOs also pointed out the problem that management might be concerned that transparency would reduce revenue:

> *"In my view, [a service asset broker is responsible for] making data protection simple and comprehensible. Especially with regard to the data subjects' rights and their exercise. 'Transparency', so to speak, and maybe also taking users by the hand a bit and showing them, 'okay, this is what we do with the data and this is what happens there. And that way, you can retain control over your data yourself', so to speak."* (I2)

> *"If the user doesn't know what they're handing over their data for, then I think it's always a bit easy to finger-point at the provider and say 'Watch out! You were obliged to do everything right with my personal data.'. But if you had communicated transparently with them in advance, I think that would have been different."* (I3)

> *"I believe that DPOs and customers are the ones who are easiest to deal with [...] by transparently, [...] openly and honestly explaining what is happening with the data. [...] But of course that goes hand in hand with the management perhaps not always being happy, because for platforms, personal data [...] are hard cash."* (I3)

6 Discussion and Implications

Digital ecosystem providers face the challenge of meeting the various data protection requirements imposed on them as data controllers. From our interviews with DPOs we revealed various challenges for the implementation of those requirements. For discussion, we cluster them into three broader topic areas.

Action by official authorities. Overall, we find that several data protection challenges mentioned by DPOs implicitly or explicitly demand for action by regulators and supervisory authorities. As such, DPOs seem to consider harmonization and establishment of standard solutions as the most and direct relief to current issues of (international) personal data transfer, contract conclusion, and accountability issues in digital ecosystems. Probably due to the many different actors in digital ecosystems with different power relationships and expertise in data protection, we found repeated calls for greater clarity and specification by official bodies. In practice, businesses appear to be hesitant to come up with innovative solutions on their own in order to avoid problems with supervisory authorities. However, concrete specifications issued by authorities for the implementation of, e.g., cookie banners, as some of our participants suggested, may reduce the incentive to develop innovative and creative solutions. Instead, consolidating publications and findings to provide a summary guide to digital ecosystem developers or auditors could be a first step toward greater legal certainty. In this regard, our findings encourage future research oriented to the efforts of the European Data Protection Board to provide practical recommendations on how to assess and avoid dark patterns in interfaces that infringe GDPR requirements [9]. Solutions provided by researchers and privacy engineers may also need to be accompanied by more precise linkage to the actual legal requirements they help to address. Inspiration may be taken from the privacy pattern community to sort catalogs according to ISO 29100 [7].

Transparency enhancements. Our findings indicate that challenges regarding transparency in digital ecosystems play a significant role. On the one hand, DPOs stated that they themselves have difficulties in maintaining an overview of data flows. At the same time, honesty and transparency toward data subjects is of particular importance. Here, DPOs considered the digital platform to have a duty to support data subjects in exercising their rights in the digital ecosystem. Our participants see a clear need for improvement in this regard, but at the same time explained that the GDPR's requirements are detrimental to comprehensible transparency. In addition, there is possible reluctance on the part of providers so as not to scare off potential customers with being 'too' honest.

Digitalization deficit in data protection. Our interviews showed that digitalization in digital ecosystems does not necessarily capture the implementation of data protection requirements. In particular, our participants reported error-prone and time-consuming workflows related to managing data subject rights, because they had to be handled and interpreted manually. Since the implementation of data subjects' rights is inextricably linked to the processing of personal data, it must certainly be understood as an integral business process of any

digital ecosystem provider. In this regard, our finding seems surprising, because the companies do not seem to take advantage of digitalization benefits for data protection the same way they do for their core business processes (cf. Section 4). Our work therefore suggests that efforts are needed to truly embed data subjects' rights in digital ecosystems in a digital-native way. For example, Big Techs like Microsoft, Meta, and Google have integrated self-service tools into their products for several years to efficiently address data subject rights, especially rights related to access requests under Arts. 15 and 20. These self-service tools have come to be known as "privacy dashboards" and are seen as promising in the research community for helping both data controllers fulfill their obligations and data subjects exercise their rights more easily [3,20,24]. However, when we specifically asked our participants about their experience with such tools, they stated that they were largely unfamiliar with these types of privacy-related self-services. Nevertheless, they expressed a general interest in such tools to achieve a more efficient implementation of data subjects' rights in the future (4/4):

> *"Of course, if you wanted to use something like this, you would have to make sure that you don't bypass the legally mandated right to access in Article 15 of the General Data Protection Regulation. If this is within the legal limits and within the legal permissibility, then I would definitely be very open to it, especially in terms of user transparency."* (I2)

In conclusion, our findings suggest that potential (off-the-shelf) solutions to strengthen data subjects' rights may be successful if they are easy to integrate for ecosystem operators and legal compatibility is made clear.

Limitations. Our results are certainly not representative of all digital ecosystems in Germany. Furthermore, recruitment bias and self-report bias are possible, as not all companies responded to our invitation and our respondents only disclosed the information they wanted to reveal. Nevertheless, our findings provide an initial overview of data protection challenges for digital ecosystems in Germany, which can serve as a basis for further studies.

7 Conclusion

Digital ecosystems are drivers of digital transformation. It is therefore important that data protection challenges are addressed in these complex systems. To better understand these challenges, we conducted interviews with seven DPOs responsible for a total of 12 digital ecosystems in Germany. Our results indicate that DPOs are aware of the *service asset brokers*' responsibility in digital ecosystems for data protection. Key challenges are accountability obligations and collaborations with processors, especially non-EU based processors. The implementation of data subject rights remains in a state of low digitalization. To strengthen data protection, DPOs expect clear, unambiguous instructions and implementation examples from official bodies. At the same time, they see transparency as a key challenge, both to maintain an overview themselves and

to demonstrate transparency and openness to their users. Our findings suggest that more concrete recommendations for solutions with legal categorization and solutions for privacy self-service tools could be helpful here.

Acknowledgments. We thank Marian Hönscheid and Benedikt Malchow for helping us code the interviews. This research was supported by the project D'accord funded by the German Federal Ministry of Education and Research (grant number: 16KIS1508).

References

1. Almeida, J., da Cunha, P.R., Pereira, A.D.: GDPR-Compliant Data Processing: Practical Considerations. In: Proceedings of the 18th European, Mediterranean, and Middle Eastern Conference (EMCIS). pp. 505–514 (2021)
2. Anwar, M.J., Gill, A.Q., Beydoun, G.: A review of information privacy laws and standards for secure digital ecosystems. In: Proceedings of the 29th Australasian Conference on Information Systems (ACIS). pp. 1–12 (2018)
3. Bier, C., Kühne, K., Beyerer, J.: PrivacyInsight: The Next Generation Privacy Dashboard. In: Proceedings of the 4th Annual Privacy Forum. pp. 135–152 (2016)
4. Campbell, J.L., Quincy, C.D., Osserman, J., Pedersen, O.K.: Coding in-depth semistructured interviews. Sociological Methods & Research **42**, 294 – 320 (2013)
5. Chen, Z.T., Cheung, M.: Privacy perception and protection on Chinese social media. Ethics and Information Technology **20**(4), 279–289 (2018)
6. da Conceição Freitas, M., da Silva, M.M.: GDPR Compliance in SMEs: There is much to be done. Journal of Information Systems Engineering and Management **3**(4), 30 (2018)
7. Drozd, O.: Privacy Pattern Catalogue: A Tool for Integrating Privacy Principles of ISO/IEC 29100 into the Software Development Process. In: Proceedings of the 10th IFIP International Summer School on Privacy and Identity Management. pp. 129–140 (2016)
8. EDPB: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (2020), Version 2.0
9. EDPB: Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognise and avoid them (2022), Version 1.0
10. European Union: GDPR (2016), Regulation (EU) 2016/679
11. Fernandes, J., Machado, C., Amaral, L.: Identifying critical success factors for the General Data Protection Regulation implementation in higher education institutions. Digital Policy, Regulation and Governance **24**(4), 355–379 (2022)
12. Holler, M., van Giffen, B., Benzell, S., Ehrat, M.: The General Data Protection Regulation in Financial Services Industries: How Do Companies Approach the Implementation of the GDPR and What Can We Learn From Their Approaches? In: Proceedings of the 82th Jahrestagung des Verbands der Hochschullehrer für Betriebswirtschaft (VHB). pp. 1–11 (2020)
13. Kira, B., Sinha, V., Srinivasan, S.: Regulating digital ecosystems. Industrial and Corporate Change **30**(5), 1337–1360 (2021)
14. Koch, M., Krohmer, D., Naab, M., Rost, D., Trapp, M.: A matter of definition: Criteria for digital ecosystems. Digital Business **2**(2), 100027 (2022)
15. Lisiak-Felicka, D., Szmit, M.: GDPR implementation in public administrationin Poland - 1.5 year after: An empirical analysis. Journal of Economics & Management **43**, 1–21 (2021)

16. McHugh, M.L.: Interrater reliability: The kappa statistic. Biochemia Medica **22**(3), 276–282 (2012)
17. Nachira, F., Nicolai, A., Dini, P.: Digital Business Ecosystems. European Commission (2007)
18. Namara, M., Sloan, H., Knijnenburg, B.P.: The Effectiveness of Adaptation Methods in Improving User Engagement and Privacy Protection on Social Network Sites. Proceedings on Privacy Enhancing Technologies **2022**(1), 629–648 (2022)
19. Park, Y.J., Chung, J.E., Shin, D.H.: The Structuration of Digital Ecosystem, Privacy, and Big Data Intelligence. American Behavioral Scientist **62**(10), 1319–1337 (2018)
20. Popescu, A., Hildebrandt, M., Breuer, J., Claeys, L., Papadopoulos, S., Petkos, G., Michalareas, T., Lund, D., Heyman, R., van der Graaf, S., Gadeski, E., Le Borgne, H., deVries, K., Kastrinogiannis, T., Kousaridas, A., Padyab, A.: Increasing Transparency and Privacy for Online Social Network Users – USEMP Value Model, Scoring Framework and Legal. In: Proceedings of the 4th Annual Privacy Forum (APF). pp. 38–59 (2016)
21. Poritskiy, N., Oliveira, F., Almeida, F.: The benefits and challenges of general data protection regulation for the information technology sector. Digital Policy, Regulation and Governance **21**(5), 510–524 (2019)
22. Qiu, Y., Gopal, A., Hann, I.H.: Logic Pluralism in Mobile Platform Ecosystems. Information Systems Research **28**(2), 225–249 (2017)
23. Ranzini, G., Etter, M., Lutz, C., Vermeulen, I.: Privacy in the Sharing Economy. Tech. rep., Ps2Share (2017)
24. Raschke, P., Küpper, A., Drozd, O., Kirrane, S.: Designing a GDPR-Compliant and Usable Privacy Dashboard. In: Proceedings of the 12th Annual IFIP Summer School on Privacy and Identity Management. pp. 221–236 (2017)
25. Sirur, S., Nurse, J.R., Webb, H.: Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). In: Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (MPS). pp. 88–95 (2018)
26. Spiekermann, S., Grossklags, J., Berendt, B.: E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In: Proceedings of the 3rd ACM Conference on Electronic Commerce (EC). p. 38–47 (2001)
27. Teixeira, G.A., da Silva, M.M., Pereira, R.: The critical success factors of GDPR implementation: A systematic literature review. Digital Policy, Regulation and Governance **21**(4), 402–418 (2019)
28. Teixeira, G.A., da Silva, M.M., Pereira, R.: The Critical Success Factors of GDPR Implementation: A Delphi Study. In: Proceedings of the 29th International Conference on Information Systems Development (ISD). pp. 1–12 (2021)
29. Teubner, T., Flath, C.: Privacy in the Sharing Economy. Journal of the Association for Information Systems **20**(3) (2019)
30. Van Landuyt, D., Sion, L., Dewitte, P., Joosen, W.: The Bigger Picture. In: Proceedings of the 2nd Workshop on Security, Privacy, Organizations, and Systems Engineering (SPOSE). pp. 283–293 (2020)
31. Yun, H., Lee, G., Kim, D.J.: A chronological review of empirical research on personal information privacy concerns. Information & Management **56**(4), 570–601 (2019)

A Appendix – Semi-structured Interview

We conducted the semi-structured interview using the main questions below. The interviews were held in German. To ease understanding, we translated the interview questions from German to English in this paper. We also included optional questions. We asked these questions only when we still had sufficient time to ask them, and when study participants had not implicitly answered these questions in the previous ones.

A.1 Introduction

- Please briefly introduce yourself, including your function in the company.
- Please briefly introduce the digital ecosystem for which you are here today.
- Please briefly describe your areas of responsibility in this digital ecosystem.

A.2 Detailed Description of the Ecosystem

- Stakeholder
  - Who is involved in the digital ecosystem and with what motivation?
  - Which actors and participants are involved?
- Data and purpose of use
  - What common personal data are processed in the digital ecosystem and for what purposes are they processed?
  - *Optional: Are there any particularly sensitive personal data that you work with?*
- Data flow
  - Who gets access to the personal data? So who are the recipients of the personal data?
  - *Optional: Where/how does which personal data flow to whom for which purpose?*
  - *Optional: To what extent does the broker influence data flows? Also on those of providers?*
- Data flow depth
  - Do you know what the recipients process the personal data for?
  - If external recipients: Do you know what external recipients process the personal data for?
  - How do you ensure that recipients use the data only for the intended purposes?

A.3 Privacy Challenges

- Based on your comments and descriptions: In your opinion, what are the biggest challenges and problems in implementing the legal requirements for data protection?
  - What have been the biggest challenges in the past?
  - What do you think will be challenges to deal with in the future?

- With our research, we want to strengthen the rights of data subjects and support digital ecosystems in their implementation. When you think about data subjects' rights, what challenges do you face in implementing them in particular?
- In your view, what responsibility does the provider of the digital ecosystem have to ensure data protection throughout the ecosystem and for all participants/actors?
  - How do you assess the responsibility for the various players in the digital Ecosystem for data protection?
  - *Optional: How is data protection ensured, e.g. at the recipients' side?*
- What do you think would be useful or helpful to make data protection in digital ecosystems more effective in the future?

A.4 Privacy Dashboards

- Do the terms "privacy cockpits" or "privacy dashboards" mean anything to you?
- Do you already use such tools or do you plan to use them in the future?