Making Sense of the General Data Protection Regulation—Four Categories of Personal Data Access Challenges

Casandra Grundstrom
University of Oulu
casandra.grundstrom@oulu.fi

Karin Väyrynen
University of Oulu
karin.vayrynen@oulu.fi

Netta Iivari
University of Oulu
netta.iivari@oulu.fi

Minna Isomursu
IT University of Copenhagen
miis@itu.dk

Abstract

The General Data Protection Regulation (GDPR) was enforced in the pan-European area on May 25th, 2018. From the perspective of data access research, among others, this introduces significant changes into organizations and their practices. However, so far, there is limited research offering insights into such a new policy phenomenon for organizations from the perspective of access to personal data. This paper is based on an ethnographic study of a 2-day workshop in which five European insurance organizations came together to share the results of sensemaking in their organizations and knowledge around the GDPR. We examined how the participants interpreted the GDPR and the compliance challenges they faced. These challenges are categorized into four dimensions of personal data access, as follows: Procedure, Protection, Privacy, and Proliferation. These challenges are significant for any organization that acts as a processor and/or controller to consider.

1. Introduction

On May 25th, 2018 (and in the days and weeks that followed), users of online services received numerous emails asking if they wanted to stay subscribed to mailing lists, as well as requests to accept new cookies on websites and consent for mobile phone applications. This barrage of requests occurred because the General Data Protection Regulation (GDPR) replaced the existing Data Protection Directive 95/46/EC (now referred to as the DIR95) [10, 40]. This reform aims to update data protection and data privacy for empowering individuals concerning their personal data, as well as harmonizing data protection across Europe [8, 47].

The GDPR brings change, and now, any organization that collects, manages, or uses personal data of data subjects in any of the European Union (EU) member states is required to comply. Failure to comply results in hefty penalties of 4% of the worldwide turnover or up to €20,000,000 in fines [7, 40, 47]. One of the motivating factors for replacing the DIR95 was our society's evolution into a technologically distinct era. The DIR95 was generated at a time when internet access was not widespread, social media was still unheard of, and data were not produced by different smart devices [45]. Individuals, customers, patients, students, and so forth are now the 'data subjects' of the GDPR [7, 40].

Data protection is strongly related to questions of data access [42]. Yu et al. [52] stated that, "as a significant research area for system protection, data access control has been evolving in the past thirty years." In addition, when considering the different pieces of the GDPR, a fundamental constituent of personal data is data accessibility. Accountability [31] requires justifying the access an organization has to existing personal data through transparent actions. Portability [48] is for facilitating access and control to data subjects in organizations and across regions, including outside of the EU. The right to be forgotten (RTBF) [44] is for deleting any and all access to data. Protection necessitates ensuring privacy and that no unauthorized access to personal data occurs. This is strongly relevant in the GDPR in the concept of "privacy by design" [9, 35], where filtering for authorized access is pivotal when designing services.

There is some conceptual or theoretical research available on the GDPR, with a heavy emphasis on the legal schools of thought (e.g., [31, 47]). As the GDPR only recently came into effect, there is not yet much empirical research on organizations' GDPR compliance. One of the notable exceptions is Andreou et al. [2], who examined Facebook's response to the GDPR's transparency requirements and how to improve social media advertising. The regulations throughout the GDPR do not provide implementation rules, and they are subject to open interpretation [47].

URI: https://hdl.handle.net/10125/59941
ISBN: 978-0-9981331-2-6

This means that different organizations can take different approaches to ensuring compliance with the GDPR. Grundstrom et al. [15] called for research that helps understand the organizational challenges when dealing with policy (such as the GDPR). In addition, Belanger and Xu [3] suggested shifting the focus of privacy research in information systems (IS) away from the saturated user role to an organizational perspective, emphasizing qualitative interpretive studies. Against this backdrop, we ask the following research question:

"*What data access challenges are imposed by the GDPR for personal data in organizations in Europe?"* We examine data access challenges in five European mutual insurance companies that sought to make sense of how to comply with the GDPR.

2. Related Research

In this section, we provide some definitions to elucidate the fundamentals of the GDPR context (Section 2.1). We then define what data access means in this paper and briefly summarize relevant research on challenges (Section 2.2). Finally, we describe the theoretical lens on sensemaking and interpretation (Section 2.3).

2.1. The GDPR

The fundamental structure of the GDPR breaks down several important topics for consideration when dealing with personal data. Tikkinen-Piri et al. [47] identified 12 practical requirements for implementation as a result of comparing and contrasting the DIR95 against the GDPR, illustrating the changes taking place and how they implicate personal data processors and controllers. They argued that processors and controllers must also demonstrate their compliance via actions of accountability and transparency. Similarly, Khajuria et al. [24] offered a 12-point checklist to prepare for GDPR compliance.

For companies that process and control personal data, there are certain quintessential terms that must be defined, as follows: personal data, processors and controllers. Personal data are "any information related to an identified or identifiable natural person ('data subject')," a controller is "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," and a processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" [40]. A company acting as a controller—determining the purpose and means of processing of personal data—may use external companies that process data on its behalf. Moreover, if a processor uses personal data for its own purposes or does not follow the controller's instructions, it can become a controller [31]. Thus, a company can intentionally or unintentionally shift between being a controller, processor, or both. However, the burden of responsibility does not wane when this shift occurs and still requires strict compliance.

2.2. Personal Data Access Challenges

The concept of access is employed in a variety of contexts [30]. Accessibility is already an established research stream in Human Computer Interaction (HCI), addressing the needs of persons with disabilities, and it is classified in the ACM Digital Library under Human-centered computing [28]. The concept of access to healthcare in the literal sense refers to a person being able to receive health services in a clinic or online, where their ability to access health services may be limited because of demographic characteristics like age or ethnicity [33]. The importance of access to data is demonstrated through the purposeful actions of stakeholders. For any organization, "[a]ccess to data is obviously a fundamental business benefit for many companies and business ecosystems" [18]. Access to personal data is also a means of competitive advantage, involving such digital services as personalization [37].

In contrast to the previous examples, and for this paper, we consider access to be both an abstruse and intrinsic property of data that is enacted in various contexts by different stakeholders. These contexts, involving varying levels of complexity, emerge through stakeholder and technical interactions [32]. For instance, residents in Denmark have access to their health data through a central platform called Sundhed.dk. The act of a data subject (e.g. the resident) using this platform to find personal data is described as 'access', but a clinician may 'access' the same health data to make a diagnosis. These data can also be anonymized and 'accessed' by researchers for use in a clinical study. In this example, there are three different stakeholders and three different reasons for access. Considering the GDPR, the undertones of access to personal data are ubiquitous. The data subject is empowered by the GDPR to play a more distinct ownership role. This empowerment is found in the form of actions subjects can take and rights that protect them. The most apparent instance of access from the data subject perspective is the right to access personal data [40]. The data subject can take actions like asking for confirmation that their data is with a processor and/or controller, asking who has used the data, verifying their accuracy, or requesting clarification for

storage or use purposes (accountability) [31]. The data subject can have the data transferred to another organization or request them in a machine-readable format (portability) [48] or even demand erasure of personal data (RTBF) [44]. In addition, data subjects are empowered by the fundamental right for privacy and procedure of protection [9, 35, 38], to provide or revoke consent [35], and to be notified of failures to facilitate protection and privacy (e.g., data breaches) [42]. Data subjects also have the right to report actions not in accordance with the GDPR [47].

Considering all these actions and rights from another perspective, organizations are required to be compliant with the GDPR to support the empowerment of the data subjects. Koops [27] highlighted the fallacy challenges for data protection, which will continue to hinder data subjects' empowerment unless the GDPR can be interpreted in a fresh, innovative way. On top of this pressure, organizations must reckon with the severe punishments associated with noncompliance [7, 31, 40, 47]. Coupled with the regulation being purposefully left open for interpretation for ease of adoption into contexts and limited precedent to follow [31], organizations face many different challenges in facilitating access. For example, portability demands that an organization provides digital access to personal data in a machine-readable format on request by the data subject. However, this was challenging even before the GDPR was enforced due to difficulties around the process of ensuring data subjects know how to ask for access and the lack of digital standards for formats [16]. Another challenge for organizations is the idea of consent or anonymity. Organizations initially need to ask for informed consent from data subjects to access, use, or store personal data by providing digital or written consent for organizational access. The challenge of informing personal data subjects of what they are providing consent to access has long been a digital challenge [14]. The process of anonymization is especially important in medical research for primary or secondary reuse [34]. Alternatively, personal identifiers within data can be removed to provide anonymity.

2.3. Theoretical Lens

This study emphasizes that when new things are introduced into organizations, such as novel technologies, practices, strategies, or policies, sensemaking and sense giving are required, and these measures occur among organizational members. Organizations have now encountered the need to manage and respond to the changes caused by wide adoption of digital technologies and related regulatory developments. In IS and organizational research, there is a long tradition of studying how people make sense of and interpret technologies, different kinds of change efforts, and strategies in organizations [13, 20–22, 29, 36, 46, 50]. Such studies have shown that a multiplicity of meanings can be attached to a specific technology, change effort, strategy, or policy in an emergent and continuous process of sensemaking. Unexpected, paradoxical, or ironic interpretations and consequences may emerge, as Leonardi and Barley [29] or Robey and Boudreau [41] demonstrated.

This study continues along the lines of looking into sensemaking and interpretation in organizations around the GDPR, more specifically, around organizational compliance. Especially, the study considers sensemaking around the challenges in this endeavor by examining participants' views on what challenges emerge along the way. Overall, the study is inspired by social constructionism [4, 51], which is popular in IS and in organizational studies [23, 29, 36]. We use the social constructionist approach for identifying interpretations attached to the GDPR, and especially to the changes and challenges necessitated by it.

3. Methodology

This study was conducted as a qualitative descriptive study. A qualitative research approach [11, 26, 49] helps us understand how organizations make sense of the challenges related to personal data access that the GDPR brings about for these companies. Organizations' GDPR compliance is a recent development that is recondite. Eisenhardt [11] argued that a case study is suitable if "little is known about a phenomenon, current perspectives seem inadequate because they have little empirical substantiation, or they conflict with each other or common sense." Therefore, a case study is a suitable approach for the present research. We examine the process initiated and facilitated by the GDPR by studying the actors' sensemaking on how to accommodate the new regulation, how they plan to adapt it to their specific context for managing personal data and the related service offerings, and how their unique situational factors shape these processes. We identify the challenges these companies articulate.

3.1. Research Setting

The research setting was a 2-day workshop conducted at the end of 2017 on GDPR compliance challenges. The workshop was planned by an organization through which several European mutual insurance organizations partner. These insurance companies meet frequently to overcome challenges

that the continuously changing environment poses to them. Five mutual insurance companies from different European countries participated in this workshop, with the goal of discussing the challenges when planning for compliance of the GDPR, to brainstorm and hear from experts in the field.

Insurance organizations provide an especially fruitful ground for this research due to their existing role as an administrator of large amounts of sensitive and confidential personal data [1]. Insurance sector analytics see the biggest challenges and changes coming from digitalization, which is expected to thoroughly change insurance consumer behavior and business models [18]. Insurance companies are facilitated user networks, which can benefit from digital innovations through the more effective operation of the network [19]. Many organizations may not have intended to be in the business of personal data processing, but many have been drawn in by the dawn of the Internet of Things (IoT) [5].

Table 1. Participant information

Country Region	Role (Participant Identifier)
Western Europe 1	Consultant (*P1*)
Northern Europe 1	Compliance Officer (P2, P3) Lawyer (P4, P5), Program Manager (P6), Project Manager (P7)
Southern Europe	Project Manager (P8)
Western Europe 2	Consultant (*P9*), Department Head (P10), Project Manager (P11)
Northern Europe 2	Lawyer (P12, *P13, P14*), Product Manager (P15), Project Manager (P16, P17, P18, P19)
Central Europe	Compliance Officer (P20)

Twenty representatives from six European countries participated in the workshop (Table 1). Only region information is given here to protect the identity of the participants. Of the 20 representatives, four were guest speakers invited as external experts to offer their expertise in the workshop (participant identifier in italics in Table 1). Two of the external experts were lawyers and two were consultants on policy, but all worked in the context of privacy and data protection in the EU. All presentations by the external experts acted as a reflection on the GDPR policy, which set the stage for the workshop. Table 1 summarizes the workshop participants' roles in their respective mutual insurance companies. Six participants' positions intersected with technology roles, such as information architect, managing information and communications technology (ICT) projects, or data security. They represented the experts from the participating companies in what it means for the organization to comply with the GDPR.

3.2. Ethnographic Data Collection

In qualitative studies, data are collected to discover the "*who*, *what* and *where* of events or experiences, or their basic nature and shape" [43], and they are supported by the gathering of other data types for triangulation and to support a rich description of the GDPR sensemaking phenomenon [25, 43]. The result is "a generation of a theory, a description of the meaning or essence of people's lived experience, and an in-depth, narrative description about certain culture, respectively, through researchers' intensive/ deep interpretations, reflections, and/or transformation of data" [25]. The first author participated in the workshop in the role of "a fly on the wall," focusing on challenges related to personal data accessibility. The primary data that was analyzed for this study were 34 pages of field notes that the first author took when participating in the presentations by organizations and external experts, writing down what was said and who said it using color codes for countries and speakers' initials. These notes are short summaries taken during presentations, and direct quotations of participants are denoted with quotation marks ("") and presented in the results as such.

The secondary data used in this study to contextualize the primary data were the presentation slides shown during the workshop and notes about interactions during dinner, at coffee breaks, in the hotel lobby, and during taxi rides when talking with the organizations' representatives. These secondary data were used for data triangulation [43]. Specifically, important for sensemaking of the data was the first author's extensive preunderstanding of the GDPR that she had gained during the previous 2 years by studying the GDPR and conducting 30 interviews in one of the insurance organizations that participated in the workshop (conducted between August 2017 and January 2018, including three persons from the organization's GDPR project and the Data Protection Officer).

3.3. Data Analysis

The data analysis comprised of four phases. In the *first analysis phase*, two of the authors familiarized themselves with the data (presentation slides and workshop notes). All field notes were transferred to Excel sheets, where each note/comment made by the different actors represented one line. Each note/comment was related to data access in the context of the GDPR in some way. In the *second analysis phase*, we conducted a qualitative content analysis (see [43]) to identify how the participants had made sense of and interpreted the GDPR. Especially, we wished to

gain an in-depth understanding of the organizations' interpretations of the challenges arising through changes in their external environment (the GDPR) from a data access point of view by using the social constructionist lens of sensemaking. According to Choo [6], "The immediate goal of sensemaking is for an organization's members to share a common understanding of what the organization is and what it is doing." The views the workshop participants expressed were the outcome of sensemaking that had taken place in these organizations both *before* and *during* the workshop. Sensemaking *before* the workshop was found in the primary form of verbal presentations and the secondary form of the presentation slides. These represented the sensemaking that took place in the scope of the participants' specific organizations. Sensemaking *during* the workshop unfolded among the participants in the primary form of discussions, which depicted the participants' collective sensemaking as an entity. Thus, sensemaking is intertwined across both the singular participant and collective group. In the *third analysis phase*, we grouped the challenges arising from the content analysis into 13 cohesive challenge types. These reflected the participants' sensemaking, but at the same time, represented our sensemaking of the data. In the *final analysis phase*, meaning-making took place to give meaning to the identified challenges. Meaning-making is not automatic in the way that sensemaking is, and it can only take place after sensemaking occurs [17]. By categorizing, re-categorizing and re-structuring the 13 data challenges, we identified four main categories for access. The challenge categories regarding data access around which the actors' sensemaking revolved are as follows: 1) the procedure of access, 2) protection of access, 3) privacy of access, and 4) proliferation of access.

4. Results

4.1 The Procedure of Access

The procedure of access category includes the challenges discussed by the participants in terms of processes that must be enacted for organizational practice, including managing external partner relationships. This was so they could maintain and conduct themselves as responsible controllers and/or processors.

4.1.1. The challenge of managing processor relationships: External partnerships are challenging to navigate because insurance companies must ensure that the access they give vendors, suppliers, or other partners when sharing personal data is processed in compliance with the GDPR. Although the data are processed separately from the insurance company, the GDPR still imposes liability on controllers to prevent "outsourcing" that would circumvent the regulation. This would seem to be manageable at a one-on-one level. However, the insurance organizations highlighted that they have many partners across various sectors, including health care, in different parts of the world. According to P16, *The current challenges also include the contracts with processors because we have thousands of processors and need a new contract template for business use, and it is difficult to reach an agreement.* These partnerships need negotiating to ensure that personal data processing follows the regulations, which is a frustrating process.

4.1.2. The challenge of being accountable: Like most organizations, insurance companies are personal data processors; thus, they need to provide evidence for accountability. This is difficult because there is no precedent with established protocol to follow. As P1 stated, *It's challenging to define key rules and provide evidence for accountability.* Using the carrot and stick metaphor, they also questioned why the GDPR chose to incentivize compliance with a punishment (stick) instead of a reward (carrot). P11 commented, *There is almost never a carrot…* The participants also perceived the compliance process negatively due to its cost. Northern Europe 2 and Western Europe 2 shared an approximate investment budget of €10 million. However, this is only half the cost of failing to meet the GDPR demands, as detailed by the external expert P1: *Supervisory authorities have extensive and investigative powers to impose high fines, up to 4% of annual turnover or €20 million.*

4.1.3. The challenge of data properties: The participants reported several different challenges, which culminated in personal data properties. When it comes to personal data for the processors and controllers, both the speed at which personal data are created and the sheer volume of the data were identified as challenging: "*The biggest challenge is to manage the data in a quick way and everyday more and more data comes in. We don't have time to control the data like a conductor*" (P8). Furthermore, the unstructured nature of data creates problems due to format expectations for facilitating portability, especially without a clear standard of format output. P10 stated, *Everyone expects a format, but there are no standards.* Along the same lines, the quality of personal data lacks clear expectations related to the condition controllers and processers must maintain for portability: *There is no obligation for the data controllers to check and verify the quality of the data* (P1).

4.2 The Protection of Access

This category includes key views of the actors around challenges of planning the protection-oriented actions for personal data. Protection of personal data is about securing against unauthorized access.

4.2.1. The challenge of the underlying assumption of protection: Protection applies to all data subjects, even if they have nothing to hide, and these ideas of protection are nothing new. The notion that everyone has something to hide was best articulated by P11: "*At home you close the bathroom door*." A purely mitigating approach to protection is using anonymity for personal data as a possible tactic to prevent violations. Anonymous data are no longer under the purview of personal data, and this circumvents GDPR applications. This approach was highlighted by P8: *Consent is too risky, we should anonymize everything.* If personal data are not anonymized, then one of the alternative approaches is managing data breaches to facilitate protection. The participants discussed this approach in terms of the practical approach for classification and context. The challenge here is in deciding when anonymizing is suitable and when taking a more risk-based approach is appropriate.

4.2.2. The challenge of ICT: The actors discussed ICT for protection as important, but the challenges of needing better contextualization drove the role of ICT into the spotlight. Northern Europe 2 is relying heavily on ICT to facilitate a protection solution. P16 stated, *We are in the middle of implementing the GDPR project phases which are very ICT heavy.* However, it was mentioned that ICT does not provide a blanket solution for protecting personal data from access. Instead, the participants suggested it is only one part of a holistic solution. As P8 commented, the *Southern European area is too concentrated on technical aspects, we first have to deal with the problem through technical solutions.* Other approaches for protection voiced included encryption or information governance.

4.3 The Privacy of Access

This category comprises how organizations can design for privacy and the challenges for ensuring that authorized person(s) have the correct type of access to personal data. As a reminder, privacy grants access to personal data but requires security measures in the form of authorization.

4.3.1. The challenge of continued justification: The GDPR enforces the need for personal data processors or controllers to have a continued justification for having, storing, and using personal data. This means that it is necessary for any organization to delete information it should no longer have is necessitated, since it can no longer justify continued access to it. The deletion of personal data is problematic in itself because some personal data are in legacy systems or from the year 1893 for example. Questions of ownership are partly unclear in these cases. Furthermore, certain laws allow insurance companies to maintain access to data related to a claim or requiring a minimum storage period.

4.3.2. The challenge of enforcing privacy: Access rights to personal data is a question of whether one has valid authorization. This should be filtered through accountability by controlling who is able to access personal data and ensuring that unauthorized access has consequences. P8 stated, *We wrote it into our privacy policy that you can't access personal data that you aren't authorized to.* The challenge of being able to provide access to authorized persons must be balanced between the protection of the data subjects and privacy actions. According to P4, *You should prevent the worker from accessing certain data.* Proving that access is authorized is tied to the GDPR concept of accountability; where it is necessary to document access.

4.3.3. The challenge of the proactive design of privacy: How to prevent unauthorized access through design actions was discussed by the participants from both the opportunity and challenge perspectives. The participants understood that privacy is crucial when handling personal data, and because of the new regulations, they see the pressure for change as an opportunity, such as with P4: "*It's better to build a new house instead of renovating an old one.*" However, the challenge was outlined for both the cost allocation of privacy and the boundaries of understanding the customer. As reported by the external expert from Western Europe 1, P1, *The budget for privacy is 0.0004% of global turnover.* As the GDPR's enforcement is extremely new, the understanding of the owner of the personal data, or data subject, has privacy implications.

4.3.4. The challenge of changing organizational culture: Finally, the participants recognized the importance of privacy and a privacy-oriented mindset for the culture of an organization. P1 commented, *The GDPR requires creating a new culture in organizations because it is not just about compliance any more.* This mindset must be reflected in an organization's practices and culture, and herein is the challenge. As P4 remarked, *We need to teach our*

organization what privacy really means. The notion of needing to foster cultural change was echoed across all the countries. P8 especially emphasized the importance of having a privacy culture over anything else.

4.4 The Proliferation of Access

This category illustrates the participants' considerations of GDPR challenges for data subjects' access rights. The challenges for organizations are building requirements for accessibility functionality to empower the data subjects.

4.4.1. The challenge of facilitating portability: The participants identified interoperability functionality or portability across different organizations and countries as being difficult to facilitate. P8 stated, *It's a challenge for data destinations*. However, the portability of personal data empowers the data subjects with choice. Nonetheless, the expectations around data portability are restrictive in terms of time and cost. According to P1, *Customers expect data portability without delay and at no charge*.

4.4.2. The challenge of facilitating accessibility: Data subjects, including customers, have the right to access all their data. However, the challenge for the organization is that it requires a lot of effort to enable this access. P16 stated, *Complying with the right of access by the data subject requires a lot of manual work*. The participants also shared a negative perception of the implications of access, such as being unable to ensure that data subjects are personally storing their data securely so as to be protected. Another concern exists if the personal data is accessed for legal purposes, such as using them to fight a claim in court. According to P8, *People who don't get paid from a claim want to have access to the data for court*. Showing trust between insurance organizations and customers seemed to be a point of contention.

4.4.3. The challenge of the RTBF: Individuals are empowered to request that their personal data be fully removed (RTBF), and the participants honored this in how they discussed the process related to erasing. However, there are difficulties for insurance companies because certain national laws require storage of and continued access to personal data. P20 stated, *Insurance companies are bound by different laws, such as retention periods*. This conflicts with the RTBF when related to a claim like a car accident. P11 commented, *You can't have your data deleted if you have a claim that must be kept*.

4.4.4. The challenge of informed consent: To ensure data subjects have ownership over their personal data to make choices about who uses their data, when, and for what, is an act of empowerment. Through informed consent, individuals can choose how to navigate in the digital data world. As most organizations now process data in one form or another, giving the customers choice sanctions their 'shopping' capabilities. The challenge, however, is conveying actual, meaningful informed consent. P1 stated, *The action of just ticking boxes should be shifting toward the general interest of actual consent.*

5. Discussion

In this study, we set out to identify data access challenges that organizations face in GDPR compliance. We identified 13 challenges related to data access. We grouped these challenges into the four following categories of personal data access: Procedure, Protection, Privacy, and Proliferation. Our study contributes to research and practice in two ways. First, it is among the first empirical studies on organizations' GDPR compliance efforts and contributes to the stream of privacy research, specifically to research on data access. Second, our study makes a practical contribution by providing a framework (or checklist) that helps increase organizations' awareness of the different types of challenges that they will have to address and overcome in their effort to comply with the GDPR.

Our first contribution is researching data access in the field of privacy and data protection. Through conceptual methods, previous research identified practical implications of the GDPR and requirements for implementation [47] and provided guidelines for organizations to achieve GDPR compliance [24]. We empirically corroborated this previous conceptual research, finding that the organizations we studied are aware of these requirements for implementation, as the challenges that we identified match these GDPR implications and guidelines. However, our study extends previous research by providing deeper insights into the specifics of how organizations make sense of these requirements (see Section 4). For example, the organizations were aware of the RTBF but compliance with this requirement was contradicted by laws requiring insurance companies to keep certain data for a predefined period.

We also found that, for organizations, there is a challenge related to data properties (Section 4.1.3). All the property challenges reported by the participants aligned remarkably with the 4 'V' dimensions of big data – Volume (size of personal data), Velocity (speed at which personal data are created), Variety (structure

of personal data), and Veracity (quality of personal data) [39]. This implies that personal data can and should be thought of as big data. For organizations looking to manage the property challenges of personal data, inspiration from the well-established research schools of big data affords the opportunity to consider validated methods, tools, or approaches in the light of the GDPR. For instance, as 95% of big data is unstructured, companies could use more sophisticated tools such as statistical techniques when linked to predictive modelling [12]. This is especially important for organizations aiming to prevent or predict accidents, injuries, or illnesses.

Another interesting finding concerns changing organizational culture to better support or align with the GDPR. We see this as an important but challenging endeavor. Existing culture studies indicate that, in different cultural contexts, diverse types of interpretations and meanings may be attached to GDPR or privacy, and there may be a reciprocal relationship between culture and GDPR: They may shape each other, but this tends to be an emergent process that cannot be directly managed or directed by managers [20, 21]. Managers may aim at creating a GDPR-compliant or privacy-oriented culture in their organization, but they should be prepared for a long-term, emergent process with potentially unexpected and surprising consequences. Hence, future work is needed on this evolving phenomenon.

This study highlights that, when encountering this type of regulation, people have to make sense of it: They must connect it to their practical realities and contexts and interpret its implications. Technologies, practices, strategies, and policies are not static, coherent, self-evident things in the world; rather, they are interpreted and appropriated by people, who may attach various meanings to them. The literature indicates that there may be a multiplicity of meanings attached to the GDPR, as well as unexpected, paradoxical, or ironic interpretations and consequences [13, 22, 29, 36, 41, 46, 50]. This study sheds some light on this complex, dynamic process of sensemaking around the GDPR and its challenges.

Our study also provides practical implications for organizations seeking GDPR compliance. We think that the challenges we identified are relevant to organizations large and small that process personal data. However, due to resource constraints, smaller organizations especially may not have considered all the challenges that GDPR compliance can imply, and they can learn from the experience of the organizations we studied. As “a crucial task of management is to discern the most significant changes, interpret their meaning, and develop appropriate responses” [6], organizations need to make sense of the changes brought on by the GDPR and give meaning to them by bringing the challenges into their contexts before developing an appropriate response, such as designing new products and services. Our findings provide a basis for discussion to help them tackle all four categories of personal data access challenges. For mutual insurance companies, the GDPR can strengthen the strategic goal for better facilitation of the user-network business [19], as the insurance business is owned and used by the same people. In user-network business, increasing the role and responsibility of the customers in insurance service delivery can support the strategy and business model for providing benefits for the customers instead of creating external value.

6. Conclusion

In this study, we asked what data access challenges are imposed by the GDPR for personal data in organizations in Europe. Through a qualitative case study of five European mutual insurance companies, we identified 13 challenges of GDPR compliance that can be sorted into four categories of personal data access, namely Procedure, Protection, Privacy, and Proliferation. We discussed the theoretical and practical implications in the previous section. Here, we should mention that our study has certain *limitations*. First, it was conducted 6 months before the GDPR came into effect, which may have influenced the results. In addition, the study focused on organizations in a specific industry, and thus, some of our findings may be industry specific. We still consider that, due to being administrators for large amounts of personal and sensitive data, insurance companies are especially prone to try to ensure compliance with the GDPR and therefore, they are instrumental in showing the extreme side of GDPR compliance. *Future research* should involve empirical studies on whether the challenges we identified represent bigger practical challenges for compliance than others and study the concrete approaches that organizations take to overcoming the challenges of GDPR compliance regarding personal data access.

7. Acknowledgements

Author C.G. has received funding from the European Union's Horizon 2020 research and innovation programme - Marie Sklodowska-Curie Actions grant agreement no. 676201. CHESS - Connected Health Early Stage Researcher Support System.

8. References

[1] Abiteboul, S., B. André, and D. Kaplan, "Managing your digital life with a Personal information management system", *Communications of the ACM 58*(5), 2015, pp. 32–35.

[2] Andreou, A., G. Venkatadri, O. Goga, K.P. Gummadi, and P. Loiseau, "Investigating ad transparency mechanisms in social media: A case study of Facebook's explanations", *Network and Distributed Systems Security Symposium (NDSS)*(February), 2018.

[3] Belanger, F., and H. Xu, "The role of information systems research in shaping the future of information privacy", *Information Systems Journal 25*(6), 2015, pp. 573–578.

[4] Bijker, W.E., T.J. Pinch, and T.P. Hughes, *The social construction of technological systems: New directions in the sociology and history of technology*, MIT Press, Cambridge, 1987.

[5] Burkitt, F., "The digital interconnection of billions of devices is today's most dynamic business opportunity", *Strategy+Business*(77), 2014, pp. 2–12.

[6] Choo, C.W., "The Knowing Organization: How Organizations Use Information to Construct Meaning, Create Knowledge, and Make Decisions", *International Journal of Information Management 16*(5), 1996, pp. 329–340.

[7] Cooper, D.P., H. Milner-Smith, M. Young, and A. Moss, "Are You Ready for the European General Data Protection Regulation? A Practical Checklist for Employers.", *Employee Relations Law Journal 43*(3), 2017, pp. 60–65.

[8] Custers, B., F. Dechesne, A.M. Sears, T. Tani, and S. van der Hof, "A comparison of data protection legislation and policies across the EU", *Computer Law and Security Review 34*(2), 2018, pp. 234–243.

[9] Dickie, N., and A. Yule, "Privacy by design prevents data headaches later", *Strategic HR Review 16*(2), 2017, pp. 100–101.

[10] Directive, E.U., "95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", *Official Journal of the EC 23*(6), 1995.

[11] Eisenhardt, K.M., "Building Theories from Case Study Research.", *Academy of Management Review 14*(4), 1989, pp. 532–550.

[12] Gandomi, A., and M. Haider, "Beyond the hype: Big data concepts, methods, and analytics", *International Journal of Information Management 35*(2), 2015, pp. 137–144.

[13] Gioia, D.A., and K. Chittipeddi, "Sensemaking and sensegiving in strategic change initiation", *Strategic management journal 12*(6), 1991, pp. 433–448.

[14] Grady, C., "Enduring and Emerging Challenges of Informed Consent", *New England Journal of Medicine 372*(9), 2015, pp. 855–862.

[15] Grundstrom, C., K. Väyrynen, and M. Isomursu, "Dimensions of Accessibility and Interoperability for Electronic Health Records in the Nordic Countries : A Qualitative Evidence Synthesis of Facilitators and Barriers", *(In Print), Pacific Asia Conference on Information Systems (PACIS)*, 2018.

[16] Harjumaa, M., S. Saraniemi, S. Pekkarinen, M. Lappi, H. Similä, and M. Isomursu, "Feasibility of digital footprint data for health analytics and services: an explorative pilot study", *BMC Medical Informatics and Decision Making 16*(1), 2016, pp. 139.

[17] Van Den Heuvel, M., E. Demerouti, B.H. j. Schreurs, A.B. Bakker, and W.B. Schaufeli, "Does meaning-making help during organizational change? Development and validation of a new scale", *Career Development International 14*(6), 2009, pp. 508–533.

[18] Huhtala, T., M. Pikkarainen, and S. Saraniemi, "Transformation of the Business Model in an Occupational Health Care Company Embedded in an Emerging Personal Data Ecosystem: A Case Study in Finland", *International Journal of Economics and Management Engineering 9*(10), 2015.

[19] Hwang, J., and C.M. Christensen, "Disruptive innovation in health care delivery: a framework for business-model innovation", *Health Affairs 27*(5), 2008, pp. 1329–1335.

[20] Iivari, N., "'Representing the User'in software development—a cultural analysis of usability work in the product development context", *Interacting with Computers 18*(4), 2006, pp. 635–664.

[21] Iivari, N., "Culturally compatible usability work: An interpretive case study on the relationship between usability work and its cultural context in software product development organizations", *Journal of Organizational and End User Computing (JOEUC) 22*(3), 2010, pp. 40–65.

[22] Jarzabkowski, P., J.A.A. Sillince, and D. Shaw, "Strategic ambiguity as a rhetorical resource for enabling multiple interests", *Human relations 63*(2), 2010, pp. 219–248.

[23] Kallinikos, J., "Reopening the Black Box of Technology Artifacts and Human Agency", *International Conference on Information Systems*, 2002, pp. 287–294.

[24] Khajuria, S., L.T. Sørensen, and K.E. Skouby, "Implementation of General Data Protection Regulation (GDPR) in Enterprises", *Wireless World Research Forum 38*, 2017.

[25] Kim, H., J.S. Sefcik, and C. Bradway, "Characteristics of Qualitative Descriptive Studies: A Systematic Review", *Research in Nursing & Health 40*(1), 2017, pp. 23–42.

[26] Klein, H.K., and M.D. Myers, "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in

Information Systems", *MIS Q 23*(1), 1999, pp. 67–94.

[27] Koops, B.-J., "The trouble with European data protection law", *International Data Privacy Law 4*(4), 2014, pp. 250–261.

[28] Ladner, R.E., "Design for user empowerment", *Interactions 22*(2), 2015, pp. 24–29.

[29] Leonardi, P.M., and S.R. Barley, "What's under construction here? Social action, materiality, and power in constructivist studies of technology and organizing", *Academy of Management Annals 4*(1), 2010, pp. 1–51.

[30] Levesque, J.F., M.F. Harris, and G. Russell, "Patient-centred access to health care: Conceptualising access at the interface of health systems and populations", *International Journal for Equity in Health 12*(18), 2013.

[31] Lindqvist, J., "New challenges to personal data processing agreements: Is the GDPR fit to deal with contract, accountability and liability in a world of the internet of things?", *International Journal of Law and Information Technology 26*(1), 2018, pp. 45–63.

[32] Lupton, D., *Personal data practices in the age of lively data*, Policy Press Bristol, England, 2016.

[33] Manos, M.M., W.A. Leyden, C.I. Resendez, E.G. Klein, T.L. Wilson, and H.M. Bauer, "A Community-Based Collaboration to Assess and Improve Medical Insurance Status and Access to Health Care of Latino Children", *Public Health Reports 116*, 2001.

[34] Mostert, M., A.L. Bredenoord, M.C.I.H. Biesaart, and J.J.M. van Delden, "Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach", *Eur J Hum Genet 24*(7), 2015, pp. 956–960.

[35] O'Connor, Y., W. Rowan, L. Lynch, and C. Heavin, "Privacy by Design: Informed Consent and Internet of Things for Smart Health", *Procedia Computer Science 113*, 2017, pp. 653–658.

[36] Orlikowski, W.J., and D.C. Gash, "Technological frames: making sense of information technology in organizations", *ACM Transactions on Information Systems 12*(2), 1994, pp. 174–207.

[37] Pikkarainen, M.A., S. Pekkarinen, T. Koivumaki, and T.T. Huhtala, "Data as a driver for shaping the practices of a preventive healthcare service delivery network", *Journal of Innovation Management 6*(1), 2018, pp. 55–79.

[38] Politou, E., E. Alepis, and C. Patsakis, "Forgetting personal data and revoking consent under the GDPR: Challenges and Proposed Solutions", *Journal of Cybersecurity*(April), 2018, pp. 1–20.

[39] Raghupathi, W., and V. Raghupathi, "Big data analytics in healthcare: promise and potential", *Health Information Science and Systems 2*(1), 2014, pp. 3.

[40] Regulation, E.U., "2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", *Official Journal of the European Union L119*, 2016, pp. 1–88.

[41] Robey, D., and M.-C. Boudreau, "Accounting for the contradictory organizational consequences of information technology: Theoretical directions and methodological implications", *Information systems research 10*(2), 1999, pp. 167–185.

[42] Samarati, P., and S. Di Vimercati, "Data protection in outsourcing scenarios: Issues and directions", *ACM Symposium on Information, Computer and Communications Security*, 2010, pp. 1–14.

[43] Sandelowski, M., "Focus on Research Methods Whatever Happened to Qualitative Description?", *Research in Nursing & Health 23*, 2000, pp. 334–340.

[44] Steinbart, P., M. Keith, and J. Babb, "Measuring Privacy Concern and the Right to Be Forgotten", *Hawaii International Conference on System Sciences*, (2017).

[45] Tankard, C., "What the GDPR means for businesses", *Network Security 2016*(6), 2016, pp. 5–8.

[46] Taylor, S., "Critical policy analysis: Exploring contexts, texts and consequences", *Discourse: Studies in the cultural politics of education 18*(1), 1997, pp. 23–35.

[47] Tikkinen-Piri, C., A. Rohunen, and J. Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", *Computer Law & Security Review 34*(1), 2018, pp. 175–179.

[48] Vanberg, A.D., and M.B. Ünver, "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?", *European Journal of Law and Technology 8*(1), 2017, pp. 1–22.

[49] Walsham, G., "Interpretive case studies in IS research: nature and method", *European Journal of information systems 4*(2), 1995, pp. 74–81.

[50] Weick, K.E., K.M. Sutcliffe, and D. Obstfeld, "Organizing and the process of sensemaking", *Organization science 16*(4), 2005, pp. 409–421.

[51] Winner, L., "Upon Opening the Black Box and Finding It Empty: Social Constructivism and the Philosophy of Technology", *Science, Technology & Human Values 18*(3), 1993, pp. 362–378.

[52] Yu, S., C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", *IEEE Xplore*, (2010), 534–542.