

# GDPR Reality Check – Claiming and Investigating Personally Identifiable Data from Companies

Fatemeh Alizadeh  
Information systems and new media  
University of Siegen  
Siegen, Germany  
Fatemeh.alizadeh@student.uni-siegen.de

Timo Jakobi  
Information systems and new media  
University of Siegen  
Siegen, Germany  
Timo.jakobi@uni-siegen.de

Alexander Boden  
User-centered design computing  
Fraunhofer institute for applied  
information technology  
Bonn, Germany  
Alexander.boden@fit.fraunhofer.de

Gunnar Stevens  
Information systems and new media  
University of Siegen  
Siegen, Germany  
Gunnar.stevens@uni-siegen.de

Jens Boldt  
Information systems and new media  
University of Siegen  
Siegen, Germany  
Jens.boldt@student.uni-siegen.de

**Abstract**—Today, more personal data than ever before is being collected and stored by companies of all types for a wide variety of purposes. The General Data Protection Regulation (GDPR) aims to strengthen the rights of consumers by providing them with tools for controlling data collection and processing. While companies are now subject to legal obligations, precedent cases are still missing. At the same time, it remains unclear how the right to access data can be concretely implemented in practical and technical terms. Our study intends to address this problem by investigating the case of loyalty card providers—an established branch that collects the purchase data of users in exchange for discounts. For our study, we asked 13 households to request their personal data from their respective loyalty program providers. Based on interviews, we investigate the expectations of these users of the GDPR and the right to access data. Furthermore, we analyze the currently implemented process of claiming and receiving data as well as the sense-making of said data by the users. Based on our analysis, we make the following contributions: We shed light on what users know about and expect from the GDPR, particularly concerning the right to access, we report user expectations regarding the process to claim access to data and the data archives provided, and finally, we also show why also companies could benefit from actively designing the data takeout to demonstrate their data collection practices.

**Keywords**—GDPR, Usable Privacy, Data takeout, Claim personal data

## I. INTRODUCTION

The collection and processing of personal data for commercial purposes is an increasingly widespread phenomenon gaining importance for companies associated with both digital and non-digital products across all sectors. New, connected, “smart” products collecting and exchanging detailed personal data, such as smart fitness trackers, smart home systems, or connected cars, contribute to this trend [19]. Loyalty programs are quasi-archetypical and very widespread examples of companies commercially collecting and processing personal data. In Germany, loyalty programs such as Payback (> 29 million active cards) or Deutschlandcard (> 20 million cards) enjoy great popularity [10, 11]. Bonus programs offer customers rewards and discounts for shopping and also serve commercial partners by increasing the loyalty of their customers. Additionally, these loyalty programs can profile users for targeted advertisements based on the data generated with each purchase at partnering companies.

For companies, however, this new framework raises uncertainty regarding requirements for compliance with the

regulation: For the case of the right to access data, companies need to provide a way for users to claim their data, but it is yet unclear how this “takeout” should be designed and how the data archives should be provided, presented, and explained to customers in a compliant manner. The GDPR itself formulates only vague principles but leaves an ambiguous manner, in which companies must implement them concretely. At the same time, preceding jurisdiction is largely missing [17].

Human-computer interaction research on usable privacy can play a major role in informing both practical solutions and case law based on a user-oriented view. This would not only help companies implement the GDPR in a manner that is faithful to the idea of strengthening user’s rights and data literacy, but also increase the trust of the customers and alleviate fears of data scandals. To contribute to this aim, we investigated user demands regarding the data claiming process and the provision of the data collected with 13 customers of a German loyalty program. Our findings include results of

1. interview studies on expectations regarding the GDPR in general and the right to access data in particular,
2. an observation and thinking aloud of the process of claiming access to data from the loyalty program, and
3. a collaborative exploration of data provided by loyalty programs and connected user demands to make sense of data.

Against the backdrop of these experiences, we discuss potential improvements and guidelines for designing a takeout in terms of the process. In particular, we shed light on the role that the right to access has for privacy control as perceived by users, report user expectations regarding the design of a usable process to claim access to data, and explore potentials for supporting intelligible and transparent design of the data archives provided.

## II. RESEARCH BACKGROUND AND RELATED WORK

For our study, it is first important to understand the regulative framework of the GDPR. We first outline a set of related terms and regulations, focusing on the rights of the data subject (the person who disclosed data), particularly the right to access data through the controller (the entity that collected the data; Article 15). To show the research gap that we want to address, we then move on to outline research from HCI on usable privacy and on making data accountable and transparent.

## A. General Data Privacy Regulation

Article 4 No. 1 of the GDPR defines “personal data” as any information relating to an identified or identifiable natural person (here: “data subject”) [28]. Identifiability refers to the potential of identifying a natural person by association with an identifier. These could be a name, an identification number, location data, an online identifier, or one or more specific characteristics that are expressions of the physical, physiological, genetic, psychological, economic, cultural, or social identity of that natural person. Following this definition, for example, an IP address is to be regarded as personally identifiable information. All these kinds of information are subject of the GDPR and its new rules for handling and protecting personal data, with which data processors must comply.

On the consumer end, the GDPR introduces new rights, too: For example, Art. 20 of the GDPR introduces a new right to request data for transfer to other companies. This right is intended to increase data protection competition among companies. It obliges data controllers to make personally identifiable information available to the new service provider in a structured, common, machine-readable format as far as this is feasible [26].

Chapter 3 of the GDPR introduces four rights for data subjects:

1) The right for transparent information provides the data subjects with a concise, transparent, intelligible, and easily accessible form of any communication and information related to processing their personal data using clear and plain language.

2) The right to correction and deletion enables the data subjects to have their incomplete or unwanted personal data completed or erased without undue delay.

3) The right to object to automated decision making allows the data subjects to object at any time to the processing of personal data concerning him or her, especially where personal data are processed for direct marketing purposes, including profiling.

4) The right to access personal data grants data subjects the right to claim personally identifiable information collected by a company in a precise, transparent, understandable and easily accessible form in clear and simple language.

For each case, the fuzziness of terms poses major challenges in practice: It is highly unclear, what measures will be perceived as sufficient to comply with concepts such as “understandable,” “transparent,” and “accessible” in court, even more so because these partly overlap depending on the content [26].

While legislation now is in place and enacted, it remains unclear how to design a data takeout processes that complies with both the GDPR and users’ demand for privacy.

## B. Institutional Goals and Mandate for Transparency

According to the Article 12 of the GDPR, the controller shall provide information on the action taken at the request of the data subject without undue delay and in within one month of receipt of the request. Moreover, Article 15 of the GDPR requires the process of claiming data to result in information provision “in a concise, transparent, intelligible and easily accessible form” [9].

Criteria for easy access could largely be subsumed under usability criteria and the way to design the process of claiming data. Previous studies show that consumers often have no idea what data is collected about them, and the lack of transparency may lead to anxiety and concern [18]. Instead, companies should design products and services with transparency in mind to increase consumer trust [18]. Granting transparency and intelligibility, however, impose rather complex and abstract requirements [5, 11], especially given that non-programming users often struggle to understand information flow on the internet in general [14].

The usable privacy community from HCI has a longstanding history of investigating how to design for these factors, often taking a user-centered perspective to design usable solutions in this regard [13, 24].

Besides seeking to improve privacy policies [21, 22] and password usability [3], usable privacy studies also target supporting and fostering the understanding of data by means of adequate and flexible visualizations [20]. For example, Angulo et al. built a data tracking tool that displayed an overview of a user’s data disclosures to different online service providers and provided them with the collected data about them [4]. Bentzing et al. also conducted an online user study with two different application designs to investigate how increasing transparency can influence users’ privacy-related behavior on mobile phones [6]. Similar studies targeting the support of data and privacy awareness have been conducted in the area of smart home data [11, 25] and smart metering [12].

A few studies have also explicitly targeted the implementation of rights provided by the GDPR. For example, the right to data portability has been investigated [8, 27]. In addition, closely related to the right to access data, transparency-enhancing tools – mostly following a dashboard approach – have been proposed. For example, Raschke et al. designed a usable privacy dashboard to simplify data access and interpretation for the data subjects [20]. Similarly, Olausson developed a dashboard specifically targeting nurses’ work [19]. Still, while these studies evaluate their concepts with users, a consideration of users during the development and discussion of features is largely missing, disregarding the socio-technological nature of the concept of transparency [23].

Following Spagnuolo et al. [23], our study informs jurisdiction-holders and designers of systems by providing a dedicated user perspective. In doing so, our study provides new insights into a usable design of the right to access data in three ways:

1. We shed light what users know about and expect from the GDPR and especially the right to access.
2. We report user expectations regarding the process to claim access to data and the data archives provided.
3. Finally, we also show why companies could benefit from actively designing the data takeout process to demonstrate their data collection practices.

## III. METHODOLOGY

In this chapter, we explain the methods used to conduct this study, as well as the context of the case study.

### A. Interviews and Data Takeout

Following a user-centered design approach [1], our empirical explorative study consists of three parts.

1. First, we conducted semi-structured interviews with 13 users (see below for details) about the usage of loyalty cards, customer data collection by companies, and how data information practices according to Articles 12 and 15 of GDPR can be applied to serve them best. During this stage, we asked participants some demographic questions (e.g., about their age and level of their gross income) to gain background information on our sample. Moreover, the respondents were asked to evaluate their tech-affinity as well as attitude and experience regarding data protection (see the detailed interview protocol in appendix A).
2. Second, after the interview, we asked the participants to request their data from their loyalty program. Using thinking aloud [7], we observed the process and conducted a brief 5–10-minute post-interview for clarification. We did not explicitly refer to any medium and focused on letting the participants go through the process on their own, so that the complexity of the process would be evaluated more realistically through first-hand experiences.
3. Due to personal pre-tests, we knew that the data takeouts would not be provided instantaneously by the companies. Instead, the GDPR grants them 30 days to fulfill the data access requests of the data subjects. We therefore stayed in touch with the households and regularly checked whether they had received any information from the companies. Once the data takeouts were provided, we made a second onsite visit and had the participants examine and reflect on their data and its presentation in a collaborative session, which resembled the idea of data work introduced by Tolmie et al. [25]. During these collaborative sessions, after the participants explored their data freely themselves, the researcher engaged in the process by asking them to evaluate their experience (see Appendix A).

### B. User Sample and Data Collection

Our participant pool consisted of 13 participants (9 f, 4 m) with an average age of 35 years. We also took care to collect a sample with a mixed technological background (see Table 1).

As our sampling method, we used convenience sampling [2] combined with the snowball method. We paid no compensation, but the participants had an intrinsic interest in the topic. The interviews were conducted onsite. The only restrictions we took into consideration were having a shopping loyalty card and being willing to participate in our study. An overview of the participants can be found in Table 1.

Three of our participants also had an app installed by their loyalty card provider, two of whom actively used it. None of the participants, however, had the location-tracking, which provides information on the closest partnering shops, activated. One of the participants also used a browser extension on his computer to be notified when the loyalty system provider offered rewards or discounts on the partners' sites.

After obtaining participants' consent for data collection, usage, and recording, interviews and the feedback sessions were audio-taped, transcribed, and translated (from German to English). We then applied the deductive coding based on Mayrings qualitative content analysis [16] to analyze and categorize the interview transcriptions.

Table 1 Participants' information

#	Sex	Tech Experience	Age	Education	Gross Income
P1	M	High	31	M.Sc.	5000
P2	F	Low	67	Commercial training	4000
P3	F	Mid	38	Diploma of Law	6000
P4	M	Mid	33	Commercial training	3500
P5	M	Mid	35	High School	5000
P6	F	High	24	B.Sc.	700
P7	F	Mid	35	High School, training	4500
P8	M	High	35	B.Sc. of Law	4500
P9	F	Low	29	Secondary School	3500
P10	F	Mid	34	High School	4000
P11	F	Low	31	High School	4000
P12	F	High	23	High School	600
P13	F	High	35	-	-

## IV. FINDINGS

In this section, we discuss the results of our empirical study.

### A. Pre-Interviews

In this section, we categorize the feedback gained from the interviews based on the questions we asked. These covered the users' perception and motivation to use shopping loyalty cards and their existing perception of the role of privacy in their life in general as well as towards their loyalty program.

#### 1) Impact on shopping and life.

To gain a deeper understanding of why and how participants were using their loyalty cards, we started with an open introduction. Unsurprisingly, saving money was the major trigger for signing up:

*“Collect points and save money while shopping. Actually, I never wanted to have a [name of provider] card, because I am aware that my shopping behavior is tracked. However, I was infected with it through my friends. Especially as a student, it is simply a factor to save money or to finance a purchase by collecting points.” (P6)*

The positive experiences of others – especially partners – saving money were also found to be a trigger.

*“My wife put the card in my wallet.” (P8)*

The small but constant rewarding system provided positive experiences, motivating users to use the card continuously.

*"I don't how much you save. I don't think much. But you really get money. You get a reward each time you go shopping and can spend it to get some money." (P10)*

Three participants explained the continuous motivation to use the card in terms of the innate urge to collect:

*"My motivation was only to collect the points, only collecting them and nothing more." (P4)*

*"It has a slightly motivating character to collect anything." (P1)*

The low effort and convenience of using the card while standing at the checkout counter was also noted. Interestingly, P5 highlighted the role of cashiers as a social factor, as they often actively ask customers if they have a loyalty card.

*"Every time you go shopping, you're asked if you have a card. A card seems to be a nicer answer than a 'No.'" (P5)*

In two cases, the "desired" – from the perspective of partnering companies – result of changing shopping behavior was self-reflected by participants:

*"So, I'd rather go to business A instead of business B, because I'm getting points. And if the prices are the same, I'd also rather to gas station C than other to ones." (P12)*

Special offers for collecting multiple points on certain occasions increased this motivation even further.

## 2) Perception of Data Sensitivity

The sensitivity of data was valued differently, although most participants were rather uncritical, especially regarding their shopping data. P2 reflects this wide-spread position:

*"I would say, everybody can know how old I am, where I live, and what I buy, anyway." (P2)*

P10 and P2 found their personal data not that critical, so they saw no need for data protection regulations:

*"I don't have any security precautions on my PC, nor am I stressing myself. If people tell me my mobile phone could be hacked... Well, what are they going to find? So, I don't care." (P10)*

Despite varying privacy attitudes and awareness regarding data collection, all participants felt rather helpless and not in control of data disclosure. This helplessness typically manifested in frustration over being forced to either agree to the data collection policies of the service provider or stop using the service altogether. The participants also did not expect the GDPR to change much in this regard:

*"I assume that, despite the new data protection regulation, companies will get access to all my data and process it." (P11)*

Although P7 valued privacy, she thought that the GDPR would take things too far. Referring to media coverage, she talks about what she heard about how kindergarten staff handled the need for compliance:

*"Privacy is important to me. But sometimes I find the GDPR a bit exaggerated. The kindergarten photographers don't work in kindergarten anymore because of the new data protection regulations, I think this is too extreme. Of course, I think it is right if you have to be asked, if they post a picture from you or if your data is passed on and processed, but I think we should say, at some certain point, it is enough." (P7)*

Beyond general knowledge from media, the respondents generally had already had experience with GDPR, especially in their work environment:

*"Of course, I have heard about the general data protection regulation in my private life. But as a working student, I was also increasingly confronted with this topic in business as well. The point is to protect individual personal data from third-party access. Companies must be able to prove how and where they have stored their customer data. The customers have the right to request their stored personal data from companies, and the company must provide them with the relevant information. This may be an advantage for the consumer. This way, one has a certain control and transparency over which data is stored by enterprises. You and can also retrieve these data, and you have the right to ask the enterprise to delete these data from their system." (P6)*

P1 had a different opinion on the GDPR, discussing the matter from the two different perspectives of customers and companies.

*"Basically, I think the idea behind the GDPR makes sense. That is, of course, a question of perspective. It is good for users, but on the provider side, we naturally have an extreme diversity of good and bad players. Companies which actually do nothing wrong with the data are imposed with additional bureaucracy and suddenly have to deal with these IT issues about how they have to store things, so that they are GDPR-compliant. So, I think there is a lot of chaos and many problems in the companies, which have to be solved now, and would have been better solved earlier." (P1)*

While he sees positive outcomes for citizens, he feels that many honest companies are imposed with bureaucratic and infrastructural burdens due to the misbehavior of others. Regarding the right to access data, we also received negative feedback. P6 stated that when the user has no options other than using the service, having this much awareness will lead to fear and anxiety. As the users grow aware of the actual "costs" of using services:

*"Now I have the right to ask, and they are legally obliged to tell me what they do with my data, why they store it, and to whom they pass it. Sounds good to me at first, but then you might get really scared from this much control. Now you want to know which data they exactly have and what they do with it, but you basically have to continue using their service, because you don't have any other choice. I don't think I want this right at all." (P6)*

P6 reflects upon her own use of services and the disclosure of data and points out that an aware user has no choice other than using certain services. In light of this intractability, she prefers not to know about what is being done with her data, rather than being informed.

P4 and P7 were critical about the GDPR, believing that the regulation will be neglected by companies, which might, for example, collect data only temporarily or provide information that cannot be understood by the customer. As a result, the regulation would not be able to actually provide transparency about data collection practices, but only provide users with snapshots:

*"If they collect data about me and I have knowledge about that, then this knowledge should mean that I should understand the data, which I don't think is the case" (P4)*

*“Data access would be transparent if users would get some information about the data collected at regular intervals, not only on their active demand. But I don't think the GDPR can ensure that or that there is some transparency in your account, regarding what was collected by a company at some specific point in time. I'm not sure whether they do it that way, or whether the GDPR asks them to do so.” (P7)*

P7 here refers to a more sophisticated way of informing data subjects than only when users pull data. Instead, he wants information to be provided to him with a push mechanism, with data collectors regularly informing data subjects about their data collection.

Respondents also expressed their expectations regarding the right to gain access to their data from Art. 15 of the GDPR. P3 in particular had a detailed expectation of her rights, which are also reflected in the GDPR.

*“I expect that if I notice someone is collecting data from me or has data about me, then I have the right to ask what kind of data they have, why they have it, and how the data can be used. I expect from the law that if they do not use the data themselves, so for self-purposes, they can't just pass it to a third party and sell it. (P3)*

Throughout our study, the right to gain insight into the collected data, information about processing purposes, and limitations to sharing personally identifiable data further were the key protective measures mentioned.

With regard to the one-month deadline as the maximum response time for the data takeout applications, users were largely satisfied and found it reasonable:

*“I can imagine that they need some time to provide the data. So, I find one month as a fixed deadline appropriate.” (P5)*

Although the participants were familiar with Art. 15 and their right to claim their personal data, our findings showed that only one of them (P3) mentioned the necessity of Art. 12, pointing out the users' need to understand and be able to interpret the collected data. Thus, she expects the law to support her to ask not only why the data was collected, but also how it can be used. P3 also mentioned another important expectation:

*“I expect from the law that there is an institution somewhere that can check that there will be a penalty if they don't obey the regulations. (P3)*

Except for P6, none of the participants stated a desire for constant access for increasing transparency.

### *3) Customer perspective on data collection by loyalty programs*

We also looked into the participants' awareness of the data stored about them and their potential use. Except for P7, all participants believed that every purchased item and where it was purchased would be stored.

*“They collect data about what I buy, where I buy it, how much, and when. They can also trace me. Because if I use my card at 12:00 every day at [store's name], then they know that I work nearby” (P2)*

*“They probably save what I buy, where I buy it, how often, and how much money I spend. They also save my name, my*

*address, and my age, because I needed to give them this personal information.” (P9)*

Although P7 claimed that she had not thought about the information they collect about her, she showed some interest in the issue in terms of articulating vague privacy demands:

*“I haven't thought about [what is collected about me], yet. I hope they don't collect everything.” (P7)*

Marketing, advertisement, and market research to design new products were mentioned as potential motivations for data collection by companies. Still, the participants were very unsure about the extent of the collection.

*“They probably use the data for advertising purposes. I don't know if they sell [the data] – I cannot imagine that would be legal – but the data will definitely be used for personalized advertising.” (P12)*

Much like the amount and types of data collected, representative of our sample, P12 remained unsure about whether and to what extent data is used for profiling or classification. Generally, participants felt left without a clear view on how their data is used beyond a basic idea of personalized advertising taking place.

#### *4) Expectations of data takeout*

No participant had tried to exercise the right to access data before. In addition to their shopping loyalty card provider, participants specifically mentioned Google, their internet service provider, their smartphone operating system provider, their smartphone vendor, a supermarket chain, and a drugstore chain (both partners in the loyalty program) to be relevant enterprises from which to claim personal data. We also asked the respondents what they expected from the data takeouts, more specifically:

*“I would imagine that somewhere on [company's] website there is a contact person whom I would contact and request to access the data gathered about me, and I would probably have to verify myself first. Then they will send me all the information by mail or email.” (P1)*

For almost all participants felt that email would be the most natural way to claim their data. Only two participants stated a preference for telephone:

*“I would write them an email, and the data I would like most of all is electronic data.” (P2)*

Participants who had not been concerned about the collection of personal data before preferred a simpler process, while those who had already experienced some concerns in this area were interested in having more levels of control and continuous access:

*“Customer-friendly for me would be: You have this [company] customer login, where you can log in and data takeouts and simply all information is displayed, basically integrated in the system, not received via email or mail, but in the customer center or in the customer portal, where I can simply access the data whenever I wish.” (P1)*

Although we chose participants with a wide range of technical affinity, in terms of envisioned and preferred data-format of the takeout, all of them mentioned only standard data formats for the data takeout, such as word or pdf files and spreadsheets. Four participants, especially the ones demanding permanent access to data, also referred to a web-

based solution, which would in turn also allow for more flexible visualizations and exploration of data:

*“The format of the data should be well-structured, possibly chronologically sorted, in tabular form, when and where I shopped, how many points I received. Let’s say a pdf or simply a table in a web frontend [ . . . ]. I would probably prefer the web frontend to a pdf because I can work better with it.” (P10)*

P10 here mentioned the potential to further “work” with the data, pointing towards the idea to further explore data according to individual demands. Often, we found that by asking the participants to express their expectations and preferences about the data takeout and process to retrieve their data, they started considering the comprehensibility and its understandability of the data provided as a factor. We also found that having access to data independent of needing to contact the service provider, for example, via an automated process, was perceived more positively by participants.

### B. The process of claiming data and post-interviews

As part of the case study, we asked all participants to submit a request for their data to their loyalty card provider, to find out, how the implementation of the “right to access” would meet their expectations. Since participants were asked to submit the request on their own without any trainings or instructions, we were able to both observe the process of claiming data and compare the results with the participants’ expectations (which they had mentioned in pre-interviews). During the observation, we avoided any interaction with the participants, so that they could evaluate and reflect on their experiences more accurately afterwards

In our examples, the members were able to request and obtain their data. All participants used the website as the first point of contact, and then used different means to get in touch with the company, looking for a call center, using a general contact form on the website, or contacting the data protection officer via email. The way in which data takeouts were supposed to be provided (either via email or by post) could be chosen by the data subjects during the process. Among our participants, only P11 chose to receive her data via post. For authorization, participants had to provide their customer number and other identifying features such as name, address, and date of birth.

Tables 2 and 3 show the second and the first file provided by the loyalty card company, respectively. The first file (which is dementated in Table 3) contained information about the card number, transaction date, processing date, points, scoreable amount, amount, partner, promotion, receipt, blocked until, branch, street, postal code, and city. Although the lines of the table reflected each individual purchase of the customer in total, they did not transfer a list of the purchased items. If the card was used at a partner company, this company had reported the customer number and the discount data (i.e., goods/services, price, discount amount, location, and time of the transaction). The complete original file can be seen in Appendix B.

The second file (see Table 2) contained personal data of the customers including name, address, card number, and email address. It also contained various additional consents that the customer had provided. The original table can be seen in Appendix B.

Table 2: The data from the second data takeout file

<b>Personal data on the main collector</b>	
Number of the main card	-
Status of the PAYBACK account	-
Status of the card	-
Card issuing partner	-
Member status	-
Date of application	-
Registration channel	-
Mr./Mrs.	-
First name	-
Last name	-
Gender	-
Date of birth	-
<b>Address</b>	
Address valid since 13.07.2018	-
<b>Contact data</b>	
email valid since 13.07.2018	-

### 1) Post-Interviews

After emailing, it took approximately one month until participants received their data takeouts, either by post or by email with a link to download the files. The link had a limited validity of 14 days.

Once the participants received their data takeouts, we conducted semi-structured post-interviews in which the participants evaluated the process of claiming their data retrospectively and compared the data takeouts they received with the expectations they had (the interview protocol can be found in Appendix A). All participants evaluated the requesting process as straightforward and suitable. P13 and P11 mentioned that they even expected a more complicated process:

*“I requested my data easily and it did not take that much time from me. To be honest, it was easier than what I expected.” (P13)*

*“The process was unexpectedly straight forward and uncomplicated; I could request my data without much effort.” (P11)*

However, data takeouts did not meet participants’ requirements with regard to the content. The customer data directory did not indicate the individual items that had been purchased, which strongly irritated participants. Therefore, six participants expressed their dissatisfaction with the data takeouts:

*“I don’t think [company] hasn’t saved every purchased item. When you ask for your data, everything [they have collected about you] should be made available.” (P11)*

Noticeably, although the loyalty company has implemented a takeout mechanism, which overall allowed participants to easily request the takeout, and the data provided was readable, six users did not believe the data to be complete. Participants told us they expected their shopping items to be listed in detail. Therefore, being more privacy-friendly towards customers by providing data takeouts raised customers’ mistrust.

Table 3: The data from the first data takeout file

Card number	Date of transaction	Date of processing	Points	Scoreable amount	Amount	Partner	Promotion	Receipt	Locked until	Branch	Street	Postal code, Place
-	20.04.2019 19:43	20.04.2019 19:43	8.0	17.57 €	17.57 €	PETZ REWE	Collect points	43344592013576201 9042019432701		-	-	-
-	11.04.2019 19:39	12.04.2019 21:02	8.0	8.49 €	8.49 €	Burger King	Collect points	17478		-	-	-
-	11.04.2019 19:39	13.04.2019 03:04	40.0	8.49 €	0.0 €	Burger King	6FACHP	17478	02.05.2019 00:00	-	-	-
-	28.03.2019 18:40	23.03.2019 20:02	8.0	8.29 €	8.29 €	Burger King	Collect points	27423		-	-	-
-	12.03.2019 14:25	13.03.2019 18:32	8.0	8.29 €	8.29 €	Burger King	Collect points	8694		-	-	-

*“I thought my purchased items are collected, because I collect different points for different items. The system should somehow recognize how many points I collect.” (P9)*

The issue of demanding web-based continuous access was not mentioned in the data work phase. This likely was connected to the very low amount of data received.

## V. DISCUSSION

In this section, we discuss the essence of our findings with regard to their potential to inform more usable implementations of the right to access data as provided by the GDPR. To this end, we outline user expectations and perception of the GDPR, and, more specifically, the right to access data. Based on our case study, we identify a set of user demands regarding the design of both the process of claiming data and the data archive itself, which may help users exercise their right to access data in the future.

### A. Folk understanding of GDPR and the right to access data

The GDPR today appears to be quite well-known in general. All participants knew that there was a “something new” in data protection regulation in the EU, although not all were able to name the GDPR. Regarding privacy in data-based services or online in general, participants felt like defending privacy was fighting a losing (if not lost) battle and that they did not have strong hopes that the GDPR would change this in any fundamental ways.

Knowledge about and perception of the new regulation, however, was largely based on the public and media discourse. Our interviews show that there are some infamous stories, such as the kindergarten photographer, that frequently popped up as examples of the GDPR being misguided.

In a similar vein, first-hand experience was largely limited to professional life. In this context, participants typically did not exercise their rights granted by the GDPR, but had to handle its new obligations and restrictions, for the respective company to comply with the GDPR and to avoid fines. In view of the participants, applying the GDPR to their small businesses and employers does not make sense. It should rather distinguish between different enterprises and their intentions of data collection and use.

As opposed to knowing stories or having experience with the bureaucratic burden of GDPR, the rights introduced by the GDPR, and more specifically the existence of a right to access data held by companies, was unknown to four

participants. Moreover, none of the participants previously ever tried to exercise this right.

As a result, the GDPR – one year after it was put into effect – is largely negatively connoted. Currently, from our users’ perspective, the GDPR is making life unnecessarily difficult, especially for smaller companies, while there are no tangible benefits.

Despite the fact that the first fines have been issued, participants do not see how the GDPR affects their life positively. In this regard, the GDPR has an image problem. Arguably, it might take more time for success stories of this new regulation to arrive on a broader scale and for the GDPR to make its mark and change the culture of data collection and processing.

With regard to new rights, however, we argue for making the exercise more visible in public and for providing support for the easy accessibility of these rights. Promoting these rights and making them part of everyday life is a task of science transfer, but also of vendors themselves, consumer protection agencies, educational establishments, and the media in general.

### B. User demands for gaining, exploring, and understanding data

The GDPR requires a transparent and machine-readable data format and data access processes from enterprises, but it does not provide users with any information on the possible use of the data. From the user’s point of view, an insight into the data is not that interesting, as most participants were largely aware of the data that their loyalty card provider would receive and collect: For the most part, the data takeout only delivers what users know anyway.

It was much more interesting for the participants to know how data could be used for specific purposes. This strategy may also contribute to reducing the mistrust we witnessed: If expectations are violated, higher procedural transparency could help counteract mistrust [15], for example, by showing how a loyalty program can work effectively, even though its calculations relate only to the total value of the goods purchased – thus, being more privacy-friendly than users expected. This lack of information is similar to recent findings in privacy research, suggesting that the resulting information for third parties is more relevant to users than unprocessed raw data [12]. In this regard, one challenge for HCI will be to inform jurisdiction with insights on consumer demands and expectations and weigh them with potentially

conflicting interests [13, 24]. On the other hand, demands will have to be discussed against the backdrop of companies potentially seeking to reveal business secrets.

### C. Designing the right to access: Why companies should care

Our findings show that the data takeouts from the loyalty cards do not confirm cardholders' expectations of transparency, especially because the data directory does not indicate the individual items that were purchased. This mismatch between customers' expectations and data takeouts created irritation, thus countering one primary goal of transparency, that is, seeking to increase trust in data collectors and processors. In this regard, our findings confirm the previous study on the effects of transparency [15], which revealed an increase in mistrust due to violated expectations. The participants simply did not believe that the companies' data takeout painted a complete picture, since they expected to see individual purchased items.

Apparently, however, the loyalty card provider does not collect this data, or else, it is not in their interest to be more transparent. Still, the non-provision of data in the takeout only increased the participants' mistrust in their business operations. Likewise, the loyalty program does not provide any information regarding profiling or classification itself. However, from a consumer perspective, since its business model basically relies on personalized advertising, profiling seems to be a natural thing to do and at the heart of the business.

Our findings, therefore, show that the right to access is not only a mere obligation for companies to comply with regulation. The data takeout we found, and the process provided, seemed very much in line with the GDPR. Whereas it is understandable that the first and most important goal is compliance, we argue that the right to access data should be taken seriously. Our user study shows that beyond legal compliance, this new right also introduces:

1. The necessity to make data practices accountable to consumers. From the user's point of view, this is necessary to make sure the company is not flouting the law and disguising the amount of data stored about its customers.
2. The chance to demonstrate an appreciative handling of private data. From the point of view of data-processing companies, this is desirable in order to reduce the reservations and mistrust of customers who wonder why so little data is stored about them.

Given that the right to access exists, our study shows that it should be used as an asset by companies to engage with users and demonstrate why and how data is collected and processed. Data controllers should therefore extend their understanding of the necessity to comply and use it as a chance to develop a more trustful relationship towards their customers.

### D. Future Work

As is typical for empirical studies, this work was influenced by several restrictions, which can be examined in future works. One aspect such avenue for future research

would be including a larger sample group and considering other loyalty card providers. Applying more objective sampling methods to reduce the possibility of self-selection bias and considering compensation to engage a wider range of users (as well as those with no general interest on the topic) are among other aspects that can be addressed in future to evaluate and improve our implications and findings.

Moreover, our study calls for researching more customer-friendly implementations of the right to access data collected about data subjects than mere "data" takeout. In particular, the socio-technical concepts embedded in the GDPR, such as "understandable" means to increase "transparency," require user-centered design and appropriation studies. To this end, the GDPR lacks concepts, enterprises, and experts that could support companies in dealing with personal data. For example, the GDPR could also provide a recommended structure for a platform in which users can be informed about data takeouts. In this vein, since provided takeouts suffered from a lack of users' understanding of data, a challenge for HCI is to develop new concepts for usable and informational data takeout that adheres to user demands.

## VI. CONCLUSION

In this paper, we delivered a user perspective on expectations and requirements regarding GDPR and its implementation in the data protection policy of the loyalty card providers. For this purpose, we conducted an empirical study, consisting of interviewing 13 loyalty cardholders and evaluating the data access process provided by their card issuer. By analyzing the data takeout policy and considering data subjects' right according to the GDPR, we conclude that data takeouts should deliver more detailed information and inform data subjects of the purpose of data collection to prevent mistrust. Moreover, further compliance checking by an independent organization seems to be necessary for enterprises. In addition, users must be informed about their rights and the meaning of transparency to be able to judge whether the GDPR is a successful approach to gaining more data protection.

## REFERENCES

- [1] Abras, C. et al. 2004. 1. Introduction and History. (2004), 14.
- [2] Acharya, A.S. et al. 2013. Sampling: why and how of it? *Indian Journal of Medical Specialities*. 4, 2 (Jul. 2013). DOI:<https://doi.org/10.7713/ijms.2013.0032>.
- [3] Adams, A. et al. 1997. Making Passwords Secure and Usable. *People and Computers XII* (London, 1997), 1–19.
- [4] Angulo, J. et al. 2015. Usable Transparency with the Data Track: A Tool for Visualizing Data Disclosures. *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems* (New York, NY, USA, 2015), 1803–1808.
- [5] Bellotti, V. and Edwards, K. 2001. Intelligibility and Accountability: Human Considerations in Context-Aware Systems. *Human-Computer Interaction*. 16, 2–4 (Dec. 2001), 193–212. DOI:[https://doi.org/10.1207/S15327051HCI16234\\_05](https://doi.org/10.1207/S15327051HCI16234_05).
- [6] Betzing, J.H. et al. 2019. The impact of transparency on mobile privacy decision making. *Electronic Markets*. (Feb. 2019). DOI:<https://doi.org/10.1007/s12525-019-00332-3>.
- [7] Boren, T. and Ramey, J. 2000. Thinking aloud: reconciling theory and practice. *IEEE Transactions on Professional Communication*. 43, 3 (Sep. 2000), 261–278. DOI:<https://doi.org/10.1109/47.867942>.
- [8] De Hert, P. et al. 2018. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*. 34, 2 (Apr. 2018), 193–203. DOI:<https://doi.org/10.1016/j.clsr.2017.10.003>.



- [9] EUR-Lex - 32016R0679 - EN - EUR-Lex: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Accessed: 2020-03-15.
- [10] Fischer, B. Bonuskarten: Das System Payback.
- [11] Jakobi, T. et al. 2018. Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 2, (Dec. 2018), 1–28. DOI:<https://doi.org/10.1145/3287049>.
- [12] Jakobi, T. et al. 2019. It Is About What They Could Do with the Data: A User Perspective on Privacy in Smart Metering. *ACM Transactions on Computer-Human Interaction*. 26, 1 (Jan. 2019), 2:1–2:44. DOI:<https://doi.org/10.1145/3281444>.
- [13] Jakobi, T. et al. 2018. Privacy-By-Design für das Connected Car: Architekturen aus Verbrauchersicht: Eine nutzerorientierte Diskussion. *Datenschutz und Datensicherheit - DuD*. 42, (Nov. 2018), 704–707. DOI:<https://doi.org/10.1007/s11623-018-1029-7>.
- [14] Kang, R. et al. 2015. “My data just goes everywhere”: user mental models of the internet and implications for privacy and security. *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (Ottawa, Canada, Jul. 2015), 39–52.
- [15] Kizilcec, Rene. F. 2016. “How much information?”: Effects of transparency on trust in an algorithmic interface. *CHI 2016, May 7–12, 2016, San Jose, CA, USA*, 39–52. ACM 978-1-4503-3362-7/16/05...\$15.00
- [16] Mayring, P. 2010. Qualitative Inhaltsanalyse. *Handbuch Qualitative Forschung in der Psychologie*. G. Mey and K. Mruck, eds. VS Verlag für Sozialwissenschaften. 601–613.
- [17] Medien zur DSGVO: Die Berichterstattung vor und seit dem Stichtag im Vergleich: <https://www.springerprofessional.de/en/medien-zur-dsgvo-die-berichterstattung-vor-und-seit-dem-stichtag/16515496>. Accessed: 2020-03-15.
- [18] Morey, T. et al. 2015. Customer Data: Designing for Transparency and Trust. *Harvard Business Review*.
- [19] Olausson, M. 2018. User control of personal data : A study of personal data management in a GDPR-compliant graphical user interface. (2018).
- [20] Raschke, P. et al. 2018. Designing a GDPR-Compliant and Usable Privacy Dashboard. *Privacy and Identity Management. The Smart Revolution: 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Ispra, Italy, September 4-8, 2017, Revised Selected Papers*. M. Hansen et al., eds. Springer International Publishing. 221–236.
- [21] Reidenberg, J.R. et al. 2015. Disagreeable Privacy Policies: Mismatches between Meaning and Users’ Understanding. *Berkeley Technology Law Journal*. 30, (2015), 39.
- [22] Schaub, F. et al. 2018. A Design Space for Effective Privacy Notices\*. *The Cambridge Handbook of Consumer Privacy*. E. Selinger et al., eds. Cambridge University Press. 365–393.
- [23] Spagnuolo, D. et al. 2019. Accomplishing Transparency within the General Data Protection Regulation: *Proceedings of the 5th International Conference on Information Systems Security and Privacy* (Prague, Czech Republic, 2019), 114–125.
- [24] Stevens, G. et al. 2014. Mehrseitige, barrierefreie Sicherheit intelligenter Messsysteme. *Datenschutz und Datensicherheit - DuD*. 38, 8 (Aug. 2014), 536–544. DOI:<https://doi.org/10.1007/s11623-014-0180-z>.
- [25] Tolmie, P. et al. 2016. “This has to be the cats”: Personal Data Legibility in Networked Sensing Systems. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (San Francisco, California, USA, Feb. 2016), 491–502.
- [26] Voigt, P. and Bussche, A. von dem 2018. *EU-Datenschutz-Grundverordnung (DSGVO): Praktikerhandbuch*. Springer-Verlag.
- [27] Wong, J. and Henderson, T. 2018. How Portable is Portable?: Exercising the GDPR’s Right to Data Portability. *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers - UbiComp ’18* (Singapore, Singapore, 2018), 911–920.
- [28] 1995. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*.

## VII. APPENDIX

### A. Interview Protocol

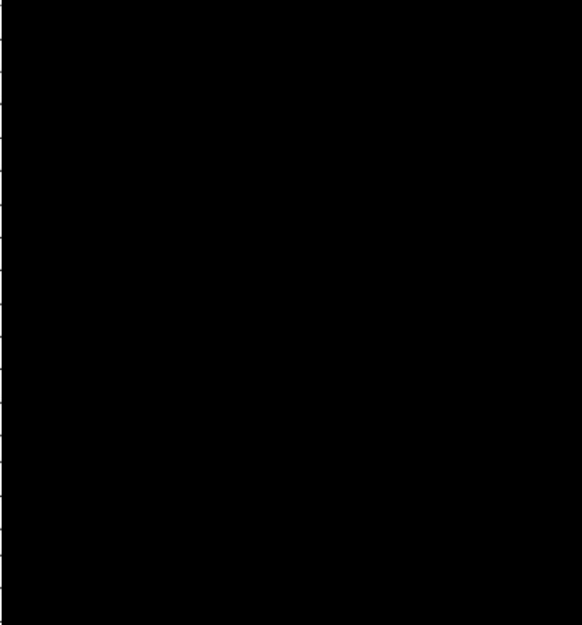
#### 1) Pre-Interview

- Introduction, explaining the goals and process of the research project
- Demographic information
  - Age
  - Educational background
  - Gross income
  - Tech affinity (low, medium, high)
- Motivation to use shopping loyalty cards
  - What was your motivation?
  - How do you use your card?
  - How large are the possible savings?
  - Do you go to [*company*] more to shop and collect points?
- Perception and role of privacy
  - Describe your attitude towards data protection
  - Have you already heard of the GDPR?
  - What do you think about Article 12 of the GDPR?
  - What do you expect from Article 15 of the GDPR?
  - Where do you think Article 15 of the GDPR matters?
    - In which situations?
    - For which data?
- Data collection of loyalty programs and expectations of data takeouts
  - What do you think [*company*] collects about you?
  - How do you think this data is being used?
  - What would you like to know about your shopping attitude personally?
  - What might the data takeout look like?
  - What should the data takeouts look like?

#### 2) Post-Interview

- Data access process
  - How would you describe the process?
    - Complexity
    - Speed
- Data takeout
  - What do you think about your data takeout?
  - Does it fulfill your expectations?

B. Original data takeout files

<b>Persönliche Daten zum Hauptsammler</b>	
Nummer der Hauptkarte	
Status des PAYBACK Kontos	
Status der Karte	
Kartenausgebender Partner	
Mitgliedsstatus	
Anmeldedatum	
Anmeldekanal	
Herr/Frau	
Vorname	
Nachname	
Geschlecht	
Geburtsdatum	
<b>Adresse(n)</b>	
Adresse gültig seit 13.07.2018	
<b>Kontaktdaten</b>	
E-Mail gültig seit 13.07.2018	

---

# Einzeltransaktionsliste für Konto-Nr.

Kartenummer	Transaktionsdatum	Verarbeitungsdatum	Punkte	Punkte/fähiger Betrag	Partner	Aktion	Kassenbon	Gesperrt bis	Filiale	Strasse	PLZ Ort
	20.04.2019 19:43	20.04.2019 19:43	8,0	17,57 €	PETZ REWE GmbH	Punkte sammeln	433445920135762019042019432701				
	11.04.2019 19:39	12.04.2019 21:02	8,0	8,49 €	Burger King	Punkte sammeln	17478				
	11.04.2019 19:39	13.04.2019 03:04	40,0	8,49 €	Burger King	6FACH *P	17478				
	28.03.2019 18:40	29.03.2019 20:02	8,0	8,29 €	Burger King	Punkte sammeln	27423				
	12.03.2019 14:25	13.03.2019 18:32	8,0	8,29 €	Burger King	Punkte sammeln	8694				
	12.03.2019 14:25	14.03.2019 03:04	72,0	8,29 €	Burger King	10FACH *P	8694				
	17.02.2019 08:25	17.02.2019 08:25	1699,0	0,0 €	PAYBACK Prämienshop	Punkte eingelöst	590022388				
	11.02.2019 15:44	14.02.2019 10:23	333,0	0,0 €	PAYBACK Aktionen	Gut gemischt - 333 *P EINGELÜTET!					
	02.02.2019 13:12	02.02.2019 13:13	13,0	35,92 €	Aral Tankstelle Stefan Noidartl	Punkte sammeln	190202131511406570687643				
	02.02.2019 13:12	02.02.2019 13:13	52,0	0,0 €	Aral Tankstelle Stefan Noidartl	5-fach Punkte Coupon Kraftstoffe	190202131511406570687643				
	21.01.2019 19:30	22.01.2019 17:31	8,0	8,49 €	Burger King	Punkte sammeln	40212				
	21.01.2019 19:30	23.01.2019 03:09	32,0	8,49 €	Burger King	5FACH *P - Vielen Dank für Deinen Einkauf!	40212				
	18.01.2019 17:45	18.01.2019 17:46	15,0	15,35 €	dm drogerie markt GmbH + Co. KG	Punkte sammeln	201901181937014026				
	18.01.2019 17:45	18.01.2019 17:46	60,0	0,0 €	dm drogerie markt GmbH + Co. KG	5FACH *P	201901181937014026				
	12.01.2019 18:23	12.01.2019 18:23	6,0	13,59 €	PETZ REWE GmbH	Punkte sammeln	433445920274882019011218235801				
	12.01.2019 18:23	13.01.2019 16:02	6,0	13,59 €	PETZ REWE GmbH	Mobil bezahlt, doppelt gepunktet bei REWE	00000005601590074581901121823				
	11.01.2019 18:58	12.01.2019 17:32	8,0	8,99 €	Burger King	Punkte sammeln	32877				
	11.01.2019 18:58	13.01.2019 03:04	56,0	8,99 €	Burger King	8FACH *P	32877				
	11.01.2019 18:58	13.01.2019 03:04	100,0	8,99 €	Burger King	100 EXTRA *P	32877				
	11.01.2019 13:10	11.01.2019 16:01	200,0	0,0 €	Loyalty Partner GmbH	200 EXTRA *P für Ihren PIA Login					
	08.01.2019 14:50	08.01.2019 14:50	20,0	0,0 €	PETZ REWE GmbH	Jan-Special: 5-fach *P bei REWE	433445920370862019010814503901				
	08.01.2019 14:50	08.01.2019 14:50	5,0	11,36 €	PETZ REWE GmbH	Punkte sammeln	433445920370862019010814503901				
	08.01.2019 14:50	09.01.2019 16:02	5,0	11,36 €	PETZ REWE GmbH	Mobil bezahlt, doppelt gepunktet bei REWE	00000005601599170861901081450				
	07.01.2019 09:39	07.01.2019 20:13	0,0	0,0 €	PAYBACK Aktionen	Los geht's - 333 *P EINTUTEN!	914652556d0-4f08-ae53-146e39ed7601				
	05.01.2019 09:12	07.01.2019 05:09	11,0	22,37 €	eBay	Punkte sammeln	782694ae54b72d076c94b829ddc8				
	03.01.2019 16:03	04.01.2019 10:32	17,0	29,38 €	Otto	Punkte sammeln bei OTTO					
	03.01.2019 16:03	10.01.2019 10:04	34,0	29,38 €	Otto	3FACH *P bei Otto					
	31.12.2018 15:46	31.12.2018 15:46	10,0	21,93 €	REWE Supermarkt, Schneider GmbH	Punkte sammeln	436533010327592018123115461801				
	31.12.2018 15:46	01.01.2019 15:31	20,0	21,93 €	REWE Supermarkt, Schneider GmbH	Mobil bezahlt, 3-fach gepunktet	0000000560209827591812311544				
	30.12.2018 19:00	31.12.2018 20:31	8,0	8,49 €	Burger King	Punkte sammeln	24198				
	26.12.2018 09:01	26.12.2018 09:04	30,0	60,98 €	Alternat.de	Punkte sammeln	453918604				
	26.12.2018 09:01	26.12.2018 09:04	120,0	60,98 €	Alternat.de	5FACH *P bei Alternate	453918604				
	18.12.2018 18:28	21.12.2018 02:01	500,0	0,0 €	CHECK24 Energievergleich	Extra-Punkte aus Glasvertrag	78918388-95f7-4416-974f-7695fac22872				
	13.12.2018 08:51	15.12.2018 04:08	81,0	17,98 €	eBay	10FACH *P bei ebay	78918388-95f7-4416-974f-7695fac22872				
	13.12.2018 08:51	15.12.2018 04:08	9,0	17,98 €	eBay	Punkte sammeln	78918388-95f7-4416-974f-7695fac22872				
	11.12.2018 16:35	14.12.2018 02:01	500,0	0,0 €	CHECK24 Energievergleich	Extra-Punkte aus Stromvertrag					
	11.12.2018 16:35	15.12.2018 03:06	2018,0	0,0 €	CHECK24 Energievergleich	2.018 EXTRA *P bei Check24					
	11.12.2018 16:35	21.12.2018 14:33	200,0	0,0 €	Online Shop Aktionen	200 EXTRA *P für Ihren ersten Online Einkauf					
	11.12.2018 12:54	11.12.2018 12:54	4,0	9,0 €	REWE Supermarkt, Schneider GmbH	Punkte sammeln	45655301020727018121112550301				