INTERNET POLICY REVIEW
Journal on internet regulation

Volume 7 | Issue 3

Collectively exercising the right of access: individual effort, societal effect

René L. P. Mahieu
Delft University of Technology, Netherlands, r.l.p.mahieu@tudelft.nl

Hadi Asghari
Delft University of Technology, Netherlands

Michel van Eeten
Delft University of Technology, Netherlands

Published on 13 Jul 2018 | DOI: 10.14763/2018.3.927

Abstract: The debate about how to govern personal data has intensified in recent years. The European Union's General Data Protection Regulation, which came into effect in May 2018, relies on transparency mechanisms codified through obligations for organisations and citizen rights. While some of these rights have existed for decades, their effectiveness is rarely tested in practice. This paper reports on the exercise of the so-called right of access, which gives citizens the right to get access to their personal data. We study this by working with participants—citizens for whom the law is written—who collectively sent over a hundred data access requests and shared the responses with us. We analyse the replies to the access requests, as well as the participant's evaluation of them. We find that non-compliance with the law's obligations is widespread. Participants were critical of many responses, though they also reported a large variation in quality. They did not find them effective for getting transparency into the processing of their own personal data. We did find a way forward emerging from their responses, namely by looking at the requests as a collective endeavour, rather than an individual one. Comparing the responses to similar access requests creates a context to judge the quality of a reply and the lawfulness of the data practices it reveals. Moreover, collective use of the right of access can help shift the power imbalance between individual citizens and organisations in favour of the citizen, which may incentivise organisations to deal with data in a more transparent way.

Keywords: Access rights, Privacy measurement, General Data Protection Regulation, Data governance

Article information

Received: 07 Feb 2018 **Reviewed:** 17 Apr 2018 **Published:** 13 Jul 2018

Funding: This work was supported by the Princeton University Center for Information Technology Policy (CITP) Interdisciplinary Seed Grant Program.
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/collectively-exercising-right-access-individual-effort-societal-effect

Citation: Mahieu, R. L. P. & Asghari, H. & van Eeten, M. (2018). Collectively exercising the right of access: individual effort, societal effect. *Internet Policy Review*, *7*(3). https://doi.org/10.14763/2018.3.927

1. INTRODUCTION

Personal data is one of the main assets in the new data economy. As a by-product of the growth of internet-enabled communication, computing power and storage capabilities, the amount of personal data that is being collected, processed and stored is growing fast. The increase in the use of personal data provides potential economic and academic benefits, but also entails risks with regards to power and privacy (Zuboff, 2015). This raises new questions as to how this new data economy should be governed (Bennett & Raab, 2017; Economist, 2017).

The European Union (EU) and the United States (US) have different approaches toward the question of how to govern personal data, though many elements seem similar and there is a partially shared genealogy (Hustinx, 2013; Schwartz, 2013). Recent events, such as the fall of the Safe Harbor agreement and the continued questioning of the EU-US Privacy Shield agreement, show that the differences are not just theoretical. While the US overall has a regime founded in consumer protection law starting from the principle that data practices are allowed as long as they have a legal ground, the EU is taking a more cautionary approach with more focus on protecting citizens rights, by approaching privacy and data protection as a fundamental right. As part of this fundamental rights approach, Europe is focusing more on safeguarding citizen rights through principles of transparency and individual control. According to Article 29 Data Protection Working Party (2018) - a cross European panel of data protection agencies - transparency is especially important, as it is one of the preconditions for the ability to exert control with respect to the processing of personal data.

The European Union has had a unified data protection framework since 1995. In light of the developments sketched above and with the aim of providing better protection of its citizens, a new data protection regulation is going into force in the EU in 2018. While there are some important additions to the data regulation framework, the central core of the framework remains essentially unchanged. This happens while we do not even know if the elements of this core function, and while some elements like informed consent, have been shown to be largely dysfunctional (e.g., Zuiderveen Borgesius, 2015). [1]

The right of access is one of the key legal provisions in this framework, which should provide transparency to citizens. It puts an obligation on organisations to, upon request, provide citizens with the personal data held on them, the source of this data, the purpose of this data, and who this data is shared with (we discuss these provisions in more detail in Section 2). The right of access intends to enable citizens to verify the lawfulness of the data practices of an organisation, after this processing has already started. So, in theory, this right should enable citizens to protect their rights related to the use of their personal data.

This paper addresses the following key questions: To what extent does the exercise of the right of access meet its objective in practice? Does it provide meaningful actual transparency to citizens?

We answer these questions by recruiting participants who send data access requests and share the replies with us. We then first analyse the replies to the access requests from the point of view of their compliance with the law. Next, we collect the views of the study participants, the citizens for whom the law is written, and ask them to rate the replies that they receive, what they expect from the law, and how they evaluate the right of access after having used it. Lastly, we reflect on these findings and explore under what conditions the right of access might contribute to transparency and ensuring the lawfulness of data processing. We conclude that a much deeper story emerges through perceiving the requests as a collective endeavour.

Our paper contributes to a considerable amount of scholarly work that deals with the different data protection regulations by legal scholars (e.g., Galetta & De Hert, 2015), and governance scholars (e.g., Bennett & Raab, 2017), by providing empirical evidence to analysis that often deals with abstract principles. There have been a few small-scale studies in the Netherlands of exercising access requests in practice, such as the studies by Van Breda and Kronenburg (2016) and Hoepman (2011). We extend these works by sending requests to a larger set of organisations, sending multiple requests to the same organisation, sending follow ups, and sending requests for specific types of data. The most similar study to ours has been performed by Norris, De Hert, L'Hoiry, and Galetta (2017) who have conducted the first major multi-country empirical study of the right of access, sending and monitoring 184 access requests. To some extent, our work corroborates their findings, albeit in another country, as their study did not include the Netherlands. Our main methodological contribution is the inclusion of non-researcher citizen-participants in gathering the data, as well as in the interpretation of and reflection on the replies.

2. RIGHT OF ACCESS

In order to empower its citizens, European lawmakers have created the so called right of access in the Data Protection Directive (DPD). This gives citizens the right to obtain information about personal data that is processed pertaining to them. In the Netherlands, the DPD has been codified into law via de "Wet Bescherming Persoonsgegevens" (Dutch Personal Data Protection Act). Article 35 of that act defines the right of access as follows:

> 1. The data subject may request the controller without constraint and at reasonable intervals to notify him about whether personal data relating to him are being processed. The controller will notify the data subject about whether or not his personal data are being processed in writing within four weeks.

> 2. Where such data are being processed, the notification will contain a full summary thereof in an intelligible form, a description of the purpose(s) of the processing, the categories of data concerned and the recipients or categories of recipients, as well as the available information on the source of the data.
>
> 3. Before a controller provides the notification referred to in subsection 1, against which a third party is likely to object, he will give that third party the opportunity to express his views where the notification contains data relating to him, unless this proves impossible or involves a disproportionate effort.
>
> 4. Upon request, the controller will provide knowledge of the logic involved in any automatic processing of data concerning him.

In this research, almost all data access requests fall under the scope of this Dutch law. If the organisation is located in another European country the national implementation of the DPD applies. In most important aspects, these implementations are very similar. Differences can be found in attributes like the maximum time allowed for the response (e.g., four weeks in the Dutch law and 40 days in the UK law). In May 2018, when the new General Data Protection Regulation (GDPR) came into effect, these differences became a thing of the past. [2]

The data protection regulation consists of a set of different obligations to data controllers and rights for data subjects. The goals of the different provisions overlap. With regards to transparency, there are rules that require *a priori* information provision directly to the data subject (art. 13 GDPR and art. 14 GDPR) and to the data protection authority (DPA) (art. 30 GDPR). There are also rules that require information provision *a posteriori* (art. 15 GDPR) via the right of access. A key difference between the two types of transparency is that *a priori* transparency can only describe data practices in abstract terms, it will describe the categories of data that are being processed more or less precisely. A statement may for example say that an organisation collects names but can only say that it recorded the name Adam after processing started. Therefore, *a posteriori* transparency can be used to check the accuracy of the processing while *a priori* information provision cannot. We think that this specificity is also needed to verify the lawfulness of the processing. People have a better understanding of processes when they are observable in concrete terms.

The text of the law is rather unclear in this respect saying that "a full summary of the data" and "the recipients *or* categories of recipients" have to be provided. [3] This seems to leave room for an interpretation that allows forstating categories as an acceptable reply (Van Breda & Kronenburg, 2016). However, the Dutch DPA (2007) has taken the position that the reply should include a full reproduction of the data, and this position has been accepted by the courts. [4]

The transparency related rights and obligations should help the data subject, the right of access enables data subjects to check the quality of their personal data and the lawfulness of the processing. Recital 41 of the DPD defines it as follows*: "... any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing"*[5]. De Hert and Gutwirth (2006) explain that the rationale for the data protection regulation is "*to promote meaningful public accountability, and provide data subjects with an opportunity to contest inaccurate or abusive record holding practices*".

Notwithstanding these legal provisions, recent surveys show that European citizens, as elsewhere, do not feel that they have transparency and control over the use of their personal

data. And while the regulatory framework for dealing with the rapid increase of the collection and use of personal data relies heavily on citizen empowerment, very little is known about the practical effectiveness of the legal provisions, such as the right of access, that should guarantee this empowerment (OECD, 2013, p. 34).

3. RESEARCH METHOD

To find out how the right of access functions in practice, we need to observe how organisations answer data access requests in practice, compared to the criteria formulated in the law, and furthermore evaluate the experience of citizens making use of the right. In order to do so, we recruited participants to send data access requests, and interviewed them about their experience during the process, as we will explain in this section.

3.1. DATA COLLECTION

The data used in this study all derive from actual replies from organisations to right of access request letters sent by seven individuals—two of the authors and five participants. Initially, to gain a basic understanding of the process involved, the authors sent approximately 35 access requests. At a later stage, eight participants connected to the authors but not data governance researchers were invited to participate in the study, five of which completed it. [6]

Potential participants received documentation explaining the basics of the legal right under investigation, the purpose of the study, a template of the access request letter, a list for choosing the organisations to send a data access request to, and a consent form. Participants took part in a semi-structured intake interview, and were asked about their expectations of access requests, their attitudes towards the use of personal data in society, and their motivation for participation. These interviews served as a reference for the subjective judgment of the effectiveness of the access requests later on.

Participants were next tasked to choose at least ten organisations to send data access requests to—with a suggestion of five that deliver public services (e.g., public transport and education), three dominantly online companies (e.g., online shops and internet service providers), and two miscellaneous. The suggestions were to ensure we collect multiple data points on similar organisations, while giving participants the freedom to engage actively and with personal interest.

Subsequently, we helped the participants draft the data access requests, based on a fixed template. The standard template was a slightly adapted version of the template that the Dutch Data Protection Authority (DPA) offers on its website. [7] One participant used the standard letters provided by the Dutch digital rights organisation Bits of Freedom, which while worded slightly differently, contains the same elements. This includes a request for (i) an overview of the data being processed, if any, (ii) an explanation of the purposes of collection, (iii) with whom data has been shared, and (iv) the origin of the data. In 14 cases an English letter was sent, based on a similar template provided by the British DPA, the Information Commissioner's Office (ICO). In 16 cases the letter was thereafter individualised, requesting specific types of data a participant wished to receive (e.g., internet traffic, or data related to a specific flight). The postal address of the target organisation was also added to the template. This address was found by looking for it in the organisation's privacy policy, and if it was not provided, the address provided in Bits of Freedom's online database, or the general address of the organisation was used. As a means of identification by the receiving organisation, a copy of an ID document was

added.

Overall, the seven individuals sent a total of 106 access requests to organisations in different sectors, as shown in Table 1. Of these, 65 requests were sent to public organisations and 41 to private organisations. Most requests were sent by letter (85), but e-mail (15) and web forms (6) were also used. The majority of the target organisations (92) were located in the Netherlands.

In order to check the progress on the data access requests, and to find out if there were any problems, we had regular (often weekly) contact with the participants. If after four weeks—the maximum time allowed by the law—a reply was not received, participants were asked to send reminders to the organisation, indicating they expected a swift answer and referring to the legal deadline. And again, two weeks later, a second reminder suggesting the possibility to seek recourse via the DPA if a reply was not received. With regards to reminders, 47 first reminders and 21 second reminders were sent, while none of the participants filed a complaint with the DPA for non-response.

When participants received a reply, they were asked to share it with us. From these responses we recorded basic process information, such as response time, numbers of reminders sent, and how the response was received (regular post, registered post or e-mail). We noted if the responses contained answers to the different sub-questions asked—where the data comes from, with whom it is shared, and why it has been collected—and if these answers were generic or specific. We also asked the participants to evaluate the responses on completeness, communication style, and accuracy of the data received (to the extent that it was provided). They could also write down general remarks.

Finally, after all data access requests were processed, participants were interviewed again, and asked to reflect on the effectiveness of the right of access and their participation in the research.

Table 1: Number of data access requests sent to different sectors

Sector	Example organisations	Access requests sent	Target organisations
Education	Delft University of Technology, Design Academy Eindhoven, Gymnasium Haganum (high school).	7	5
Finance	ABN, Mastercard, OHRA	6	5
Government	Tax authority, municipalities, UWV	30	19
Platforms	Mi, Skype, Spotify	10	9
Retail	Happy Socks, Ikea, Bol.com	8	6
Telecom	KPN, T-Mobile, Ziggo	8	6
Transport	Car2Go, NS, Amsterdam Airport Schiphol	20	7
Utilities	Eneco, Energiedirect, PostNL	7	7
Other	NGOs, art institutions, general practitioners	10	10

3.2. DATA ANALYSIS

As we have discussed, the right of access aims to bring transparency to citizens about the way in which organisations use their personal data. The transparency to be achieved is, however, not defined precisely or uniformly in the law, case law, or scientific literature.

We operationalised transparency in two ways. The first way was to compare the access responses to the formal legal criteria. The law and related case law specify several mandatory elements in response to an access request (see section 2 "Right of access"). There needs to be a reply to an access request within a number of weeks (four in Dutch law), and the reply needs to include the categories of data that an organisation processes, the actual data that is processed, an explanation of the reasons for which it is processed and an explanation of how the organisation received the data, and if, and with whom, the data was shared. We checked the replies for these elements, and whether they were given in general or specific form.

Our second way is to let citizens, for whom the law is intended, judge whether the responses gave sufficient insight into the lawfulness and accuracy of the data processing, as the law intends. This, as was described in Section 3.1, was done by asking the participants to grade each access request and response, plus the intake and final interviews.

3.3. ETHICAL CONSIDERATIONS

Before involving participants, we sought and received approval from the Delft University of Technology's Human Research Ethics Committee.

Our research requires the participants to share replies to their access requests with us, which by their nature might contain highly sensitive personal information. One principle of ethical data sharing is informed consent. We thus informed participants in detail about the setup of the experimental design, and strived for open communications and an atmosphere that makes it easy for participants to decide to share or not share their data, to share only part of their data or to revert any previously taken decision on this matter. Participants can at any point and for any reason pull back from the research. Moreover, keeping the data safe is a key concern. The original response letters were held by the participants themselves, and we stored a digital copy on an encrypted university server, accessible to two of the researchers, and the individual participants only.

Another consideration is that replying to a data access request, if taken seriously, may take much time for an organisation. Some organisations we talked to have reported that they have been previously targeted by public data access request campaigns and have experienced this almost as a 'distributed denial of service attack'. While acknowledging this concern, given that organisations have a legal obligation to reply to access requests, and given the importance of investigating access rights by the actual application of the right (versus investigation by proxy), we deem our method acceptable. For larger size research with participants, however, some form of load balancing with regards to the queried organisations in the research design is needed. Finally, since our research is not intended as an attack on any organisation, and especially not on any individual within an organisation, we protect the privacy of individuals responding to access requests within organisations and never mention their names.

4. LEGAL COMPLIANCE

We will now present our findings of the extent in which the replies to the access requests complied with the law. In 4.1 we look at the most basic questions: was there a reply at all, and how long did it take for organisations to reply. In 4.2 and 4.3, we describe the extent to which the replies were complete. In 4.4 we discuss how responses to specific requests and follow up questions were handled, and patterns that can be observed by matching replies to similar requests.

4.1. IS ANYBODY LISTENING?

Approximately 80 percent of the data access requests where eventually answered. [8] About half were answered within the four weeks stipulated under the Dutch law and, as the response time histogram in Figure 1 shows, a relatively large proportion of the replies return in the fourth and fifth week after the request, around the legal deadline. Coolblue, a web shop, responded to a request by letter in two days with data. A small proportion (7) of organisations replied within a week, but most of these responses did not contain the requested data. [9] At the other end of the spectrum, 34 organisations answered late, 21 answered after one reminder, and 9 after two reminders were sent.

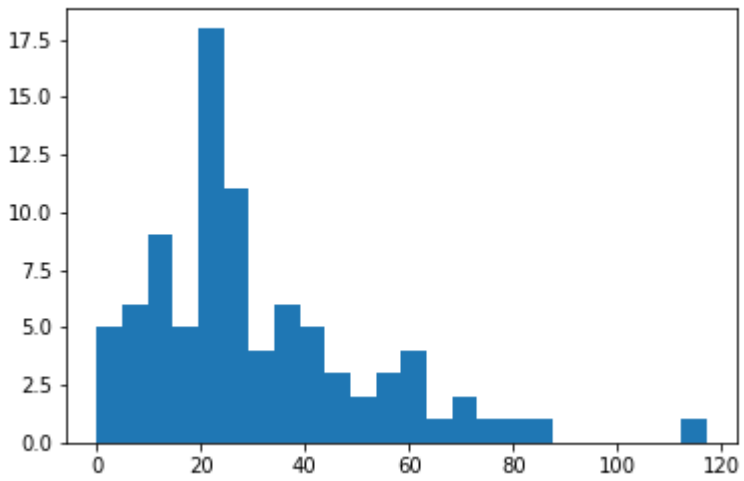

Figure 1: Histogram of response time (in days)

Figure 2 provides an overview of the replies received, and the department that has sent the reply. Approximately 33% of the responses included user data and an additional 15% included categories of data but not the data itself, while 26% stated they did not have any data, and 5% of responses referred the participant to another organisation. Most replies were signed by the customer service department (25%), followed by privacy (13%), legal (12%), and others.

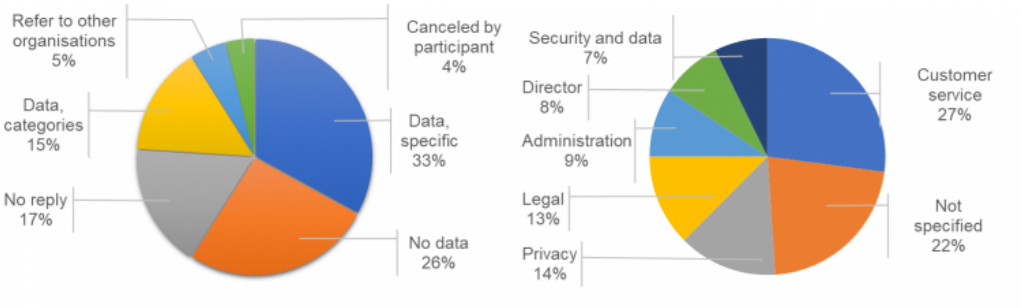

Figure 2: Response classification (left) & responding department (right) for total sample

Finally, Table 2 shows the response classification and time *by sector*. We can see quite some diversity across sectors. For instance, all educational organisations in our sample offered replies, while 35% of the requests to companies in the transport sector remained unanswered.

Table 2: Access request response classification and time (by sector)

Sector	N	Data (specific or categories)	No data or Referral	No reply (excluding cancelled)	Response time (mean number of days)
Education	7	57%	43%	0%	29.3
Finance	6	67%	33%	0%	40.8
Government	30	40%	43%	10%	34.2
Platforms	10	60%	10%	20%	33.1
Retail	8	50%	25%	25%	30.8
Telecom	8	38%	38%	25%	21.8
Transport	20	30%	35%	35%	26.5
Utilities	7	57%	29%	14%	20.7
Other	10	80%	0%	10%	28.8
Total	*106*	*48%*	*31%*	*17%*	*30.5*

4.2. DIVERSITY OF RESPONSES

In order to give a feel of the diversity among the replies, which exists in many different regards, we will start with providing a detailed description of two answers, one compliant and one non-compliant.

Stroom

A data request was sent by letter to *Stroom The Hague*, a publicly funded art centre in The Hague, by a participant who collaborates with them. Nineteen days after the request was sent, a response was received in the form of a letter from the director of the organisation.

In the two-page reply, seven categories of data, including name and contact details, artist details, nationality, and correspondence, are discussed. For each category, the letter describes how the organisation has received the data (for example, if it was given to them by the participant). The data is either provided in the letter, or a reference is given to an online platform where the participant can access the data, and they briefly explain why the data has

been (or is) processed. Furthermore, the letter indicates which of these data are publicly available, and even includes a section about data they do not currently have, but might have under different conditions, for instance, if the participant would have had a financial relationship with this organisation.

Ziggo

A data access request was sent to Ziggo—a large Dutch cable company owned 50% by Vodafone and 50% by Liberty Global—by a participant. A customer service representative called within two days asking if the participant is facing any problems, for example with their password, and expressing that they do not really know what to do with this request. The participant explains that she would like to know how Ziggo deals with personal data, and if, for example, they record what television programmes have been watched or which internet pages have been visited. The customer service representative responds that they will figure this out and get back to the participant in writing.

Four days later, the participant is called again, this time by a representative of complaints management, who again expresses that it is not "really clear" to them what they have to do with the letter. The participant explains the same story again, and requests access to her data. The complaints manager suggests the participant read the information on the website, with no additional information. The same day the participant receives Ziggo's privacy policy by email, which in layman terms explains the right of access: "You have the right to know which of your personal data we store. We can request a small fee for the administrative costs that are connected to offering this type of data". But still no data is offered, nor are the specific questions regarding specific types of data answered.

A few weeks later, the participant sends a more specific data access request, and specifically asks for an overview of all the data related to her internet use in the past three months, and refers to the fact that, in her mind, the previous data access request was not sufficiently addressed. Nine months, and a reminder letter later, no response has been received.

4.3. HOW COMPLETE ARE THE REPLIES?

The data protection law stipulates that organisations should, upon request, provide a full overview of the personal data held, plus the purpose and method of collection, and who the data was shared with. Just like the diversity in response time, there is quite some diversity in the content of replies across sectors, as the breakdown by sector in Table 3 shows.

Table 3: Completeness of access responses, based on the elements specified in the law and reiterated in the requests, grouped by sector

Sector	N	Contains data (specific or general)		Purpose of collection	Method of collection	Data sharing (specific or general)	
Education	7	14%	43%	57%	43%	29%	29%
Finance	6	50%	17%	67%	50%	17%	67%
Government	25	24%	24%	36%	24%	24%	20%
Platforms	7	71%	12%	43%	29%	0%	71%
Retail	6	50%	17%	33%	33%	33%	17%
Telecom	6	50%	7%	33%	0%	0%	33%

Sector	N	Contains data (specific or general)		Purpose of collection	Method of collection	Data sharing (specific or general)	
Transport	13	46%	0%	54%	15%	8%	46%
Utilities	6	50%	17%	50%	67%	0%	50%
Other	8	62%	38%	50%	62%	62%	12%
Total	*84*	*61%* [10]		*45%*	*32%*	*55%*	

Overall, even among the organisations that did respond to the data access request, it only very rarely seemed to be with a complete overview. Many organisations reply with lists of labels of data or categories of data, instead of sharing the specific data. As an example, Happy Socks sent a participant an email in which they said that they have data like his name and home address, but they did not give the actual name and address that they have on file. [11] OHRA, a health insurance company, after 69 days and two reminders, sent a letter containing a list of categories of data they collect, containing, amongst other things "medical data" and a list of the categories of potential recipients of the personal data containing, amongst others "healthcare providers".

When data is given, it can be challenging for the data subject to know if it is complete. For example, The Hague Library sent a reply that contained a *print-screen* from what seems to be their Customer Relationship Management (CRM) system. This print-screen shows a tab called "borrower registration" which includes fields like the name, date of birth, home address, contact details, and bank account number. Is this all the information the library system holds? Or are there other tabs in the system—with for instance payment history, a history of the books that have been borrowed, or a profile of the borrower's interests —which are not included because of a narrow interpretation of "personal data"? [12]

Access requests sent to several municipalities—who all received the same request, and probably hold similar personal data—shed light on another aspect. Large organisations often find it hard to give a complete overview of all the personal data they have, and choose different ways to handle this complexity. The Municipality of The Hague sent a 16-page list of labels of data they share with other organisations on two databases, "BRP Verstrekkingsvoorziening" (Personal Records Database Distribution Facility) and "Beheervoorziening BSN" (Social Security Number Distribution Facility), but didn't offer any further explanation (see Appendix 1 for the first page of the reply). The Municipality of Amsterdam on the other hand responded with a letter explaining that they have a multitude of public tasks and responsibilities, and are therefore registering personal data in multiple systems. They invited the participant to visit in person to see if the access request could be more narrowly specified. The Municipality of Amstelveen took the middle ground: they sent an overview of some registrations, and invited the participant to visit in person to learn about the ways that the municipality deals with personal data.

Indeed, the text of the law is rather unclear, stating that "a full summary of the data" and "the recipients *or* categories of recipients" have to be provided. This seems to leave room for various interpretations, for instance that stating categories only is an acceptable reply (Van Breda & Kronenburg, 2016). However, as previously mentioned, the Dutch DPA (2007) has taken the position that the reply should include a full reproduction of the data if the data subject asks for it, not just the categories, and this position has been accepted by the courts. [13] The GDPR addresses the ambiguity with regards to returning the actual data. [14]

Another aspect of incompleteness is that many organisations do not answer the sub questions about purpose of processing and data sharing (Table 3). In fact, while 83% organisations answered to the access requests, only 22% answered to all the sub questions asked, and only 10% organisations were specific in both the aspect of the data collected and the aspect of which organisations data was shared with. Bol.com, a large Dutch online web shop, was unique in the sample for sharing the specific third-party partners that receive data for processing payments and product delivery.

4.4. DO MORE SPECIFIC REQUESTS AND FOLLOW-UPS HELP?

One might expect that the likelihood of receiving the full and specific data increases when a more specific request is sent. The empirical data shows a mixed picture in this respect. Participants sent 16 modified access requests asking for specific forms of data. Out of these 16 cases only three received a response that directly addressed the specific question posed. Participants also sent 13 follow-up requests. These requests were almost invariably responded to with an individualised response directly addressing the question posed.

For example, participants sent five access requests to Amsterdam Airport Schiphol, two of which were modified. Schiphol replied to four participants, all with the same answer: that the airport does not have any personal data relating to them in their databases. [15] This was while one participant requested all personal data related to one specific recent flight and another requested data related to the Wi-Fi-tracking system while including the MAC address of the phone carried. These specific elements were simply ignored. We also sent one follow up letter to Schiphol, asking how it is possible that the airport has no personal data, while handling luggage and boarding passes, and engaging in Wi-Fi-tracking. Schiphol answered that they indeed keep luggage and boarding pass data, but delete these a few days after a flight, and the Wi-Fi-tracking data they hold cannot be traced back to an individual. [16]

This example follows a pattern we regularly observed. In most cases a request for information about specific data in an initial data request is ignored, while follow up requests get an individualised reply more often.

Sometimes a follow up request does receive an answer with data that was previously withheld. The UWV (Employee Insurance Agency), which is the autonomous administrative authority commissioned by the Ministry of social affairs and employment to implement employee insurances and provide labour market and data services, is an example of this. In first instance, a participant sent a standard access request to the agency, to which they replied that they did not use any of the participants' personal data. [17] Then the participant sent a follow-up letter, in which she pointed out that according to information on their own website, UWV processes data about work and income history of all employees in the Netherlands, and that she therefore does not understand how it is possible that UWV does not process any of her personal data. In response to this letter, UWV sent a reply including many pages from a system in which various personal details, including detailed income data, were recorded.

Through the examples Schiphol, UWV, and the Dutch municipalities (section 4.3), we can learn that *matching* responses from the same (or related) organisation increases the ability to judge the quality, completeness, and veracity of an access response. To demonstrate this point, consider how Van Breda and Kronenburg (2016) judged Schiphol's access response, in isolation, to be of rather high quality. They find the response, despite providing no data, to be transparent and helpful as it provides information on other organisations that may process information about the data subject in the airport, and they commend the fact that the response was sent by

registered post. But by sending five requests and comparing the answers we found that Schiphol sends *exactly* the same letter, irrespective of the precise question posed in the request. In other words, matching responses allows for a better judgement of the completeness of the individual answers.

5. PARTICIPANT PERCEPTIONS

Our overall analysis so far suggests a rather mixed conclusion with regards to compliance. There clearly are organisations that are putting an effort to be transparent about the way they process personal data, while others, whether out of inability or unwillingness, are non-compliant with the basics of the law. More importantly however, the right of access is a data subject right intended to empower the citizen. Thus, we have to go beyond a formal legal judgment, and take into account the citizens' perspective, to assess the extent to which the right of access functions. We shall do that in this section.

5.1. BEST AND WORST RESPONSES

When participants were asked which of the responses they thought were best in the interview, two criteria emerged throughout: the completeness of the data, and in different forms, the feeling of *being taken seriously*. The completeness was appreciated, in terms of sheer quantity, the coverage in time, and the precision in describing the origin of the data. But the much more striking aspect that participants judged was the *tone and the implied willingness to provide transparency* of the interactions: "Amstelveen Municipality did best because they invited me and were clearly putting an effort to get you the insight you wanted, even though you did not even know exactly what you wanted", or "TU Delft explained a lot and although I did not get the data I felt that I could have gotten it".

When asked which were the worst responses, the mirror image emerges. While participants disliked responses without data, they are more vehemently critical of responses that do not treat them respectfully. Participants made remarks such as: *"You get the feeling that they try to keep you at a distance and make it complicated"*, *"The way they are responding is almost like I am an idiot and they are making stuff up"*, *"the way in which they address you is kind of aggressive to start with",* or *"Their answer seems like a Jedi/Sith mind trick"*.

5.2. COMPLETENESS AND COMMUNICATION STYLE

We asked participants to grade all individual access request replies on a Likert scale (very bad – bad – neutral – good – very good) on the aspects of *perceived completeness* and *communication style satisfaction*. If we map these grades to numbers (very bad = 1, very good = 5), the average grade participants gave for perceived completeness was 2.1 (bad), and for communication satisfaction 2.6 (midway between neutral and bad).

While the number of requests is too low to make statistically significant claims about sectors as a whole, there seems to be quite a marked difference between different sectors in the sample, as shown in the Figure 3 boxplots. The high grades for the educational organisations and low grades for the telecommunications sector in particular stand out.

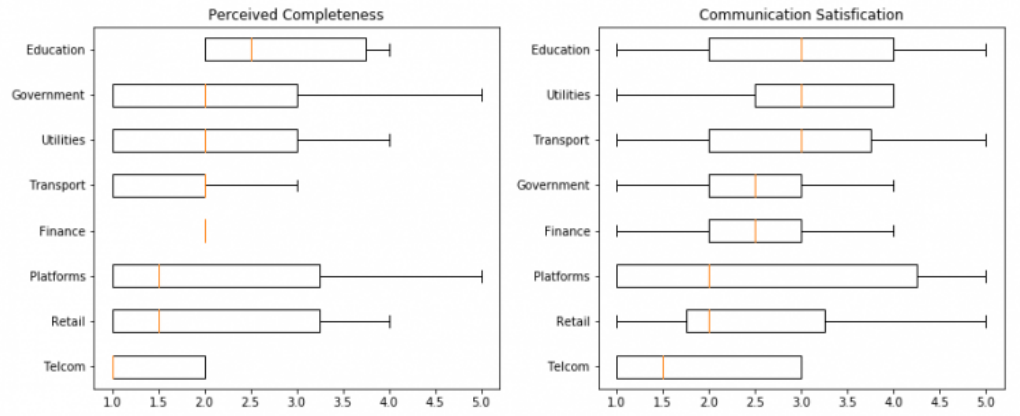

Figure 3: Perceived completeness (left) & Communication satisfaction (right) grades given by participants to access responses (Boxplots are ordered by the median grade per sector, indicated by the orange line in the rectangles. The rectangles show the 25 and 75 percentiles of grades, which are on a Likert scale)

Low grades in the telecommunications sector (which includes mobile operators and ISPs) can be traced to a number of specific behaviours. For example, three out of four organisations (Car2go, Tele2, Telfort, Ziggo) that told participants to check out their privacy policy were in the telecommunications sector. This made participants feel *"[they] let you walk in circles, [and] you get nowhere"*, as their privacy policies explicitly mention the right of access that the participant is trying to make use of. With regards to completeness, none of companies in the telecom sector provided internet traffic or location data (gathered through connections with cell-phone towers), even when specifically requested. Participants felt very uncomfortable about this, because they believed that these companies have much more data than they are sharing through the access response. Additionally, participants expect more from technologically capable companies: "*I tend to be a bit more lenient with companies or organisations that are not really IT based. [But] for example if a whole business is set up around databases and providing a website and giving you services, I would expect that they also have the expertise to very easily create a database dump and just give it to me*". Our finding about the negative perception on the telecommunication sector is in line with findings from Norris et al. (2017) who find that seven out of ten organisations in the mobile telephony branch apply restrictive practices when answering to data access requests.

5.3. WHAT DO CITIZENS EXPECT FROM THE RIGHT OF ACCESS?

Before sending the data access requests, we interviewed participants and asked them what they expected from exercising the right of access, and why they were participating in our research. After having sent data access requests and receiving the replies, we interviewed participants again and asked them to reflect on the right of access based on their experience within this research.

Most participants expressed before sending access requests that they did not expect to get access to their data through using the right. Instead, participants expressed that exercising the right of access could still be good for other reasons. They expressed that when confronted with an access request, an organisation might start to critically assess its data practices, or as one participant put it, "*I want to participate in this research because I want it to initiate a discussion. This to me is even more important than getting to see my own data. These two things are not even comparable. It is extremely important that we will make sure that in society, in politics and within organisations, the awareness is built*".

Most participants reported that the replies were, by and large, in line with their expectations, i.e., the right does not work that well with respect to getting the data that they expected organisations to have: "*No, it is not effective*", " *In reality it is worse than I expected*", and "*It feels you are still ending up in some kind of black box*". However, they also expressed that the right works with respect to getting a deeper understanding of data practices: " *It has made me more aware*" and "*The experience of sending out these access requests was really eye opening"*

Most importantly, a feeling of gaining strength through collectivisation was expressed. Participants said things such as "*I think it has contributed to organisations building some kind of process for dealing with access requests, especially because I know we were in a group*" and "*it gives me a feeling of the potentiality of this [right] helping society in order to be more in control of our data or to be at least informed [...] about our data being hosted by third parties.*"

6. DISCUSSION

6.1. A FAILING INSTRUMENT

The goal of the right of access as a juridical tool is to enable citizens to verify the lawfulness of the processing. [18] In these goals, it mostly fails. A substantial proportion of the queried organisations, whether out of inability or out of unwillingness, are non-compliant with the law. And while many replies are quite elaborate, even these replies frequently provide inadequate information to the individual for making an informed judgment about the lawfulness of the processing. Most participants reported the process to be a poor experience in terms of transparency and empowerment.

We also found that, even after over fifteen years since this law is in place, certain organisations reported that they never received an access request, indicating that the right of access is rarely exercised by citizens. This is especially intriguing in the case of large organisations that process personal data, such as Delft University of Technology with over 20,000 students, or Stedin, an electricity and gas network company with around 2,000,000 clients. Participants did not ask the organisation to report if their request was the first they ever received, but this is probably true for other cases as well. This is quite remarkable especially when taking into account that the right of access is already present in Dutch law since 2001.

That the right of access has so far not been used very often is another sign that the right of access does not function well now. Of our participants, only one had ever used the right of access. If we ask why this may be the case, a possible answer is that people just do not care so much about the particular data practices of individual organisations. But given the reflections by the participants in the interviews (section 5.3), an alternative cause maybe that the expectation of success is very low.

6.2. A WAY TO SALVAGE IT

Based on our experience, we see some ways forward. First, the exercise of the right of access can be part of an effort to create awareness and spark dialogue among citizens as well as organisations. And second, it could be used collectively as a way to increase empowerment.

The underlying problem that could be addressed through collectivisation is two-folded. In the relationship between the citizen and the data controller, the starting point is one of a deficit of both power and knowledge on the part of the citizen (as argued by De Hert and Gutwirth, 2006).

With regards to the question of knowledge there are a few connected issues. Once a reply to an access request is received, it is very hard to know to what extent the reply is complete, or to judge the quality of the reply and the lawfulness of the data practices it reveals. To be able to judge the completeness, one needs to exactly have the knowledge that one does not have and is trying to receive through the access request. This judgement therefore can only take place in a context of a *network of knowledge*. This contextual knowledge needed to judge the quality of a reply can come from matching replies from other access requests, and from others with specialised knowledge.

That matching can help was demonstrated in the cases of Amsterdam Schiphol Airport (Section 4.4) and the Dutch municipalities (Section 4.2). We were only able to see that Schiphol was always sending the same answer, because we had different answers to compare with each other. And by comparing the reply of one municipality which only sent information regarding one database to those of other municipalities who showed they had personal data in a variety of databases, it appears likely that this municipality processes more data than what they sent to some participants.

The ability to judge the quality of a reply is also dependent on specialised knowledge coming from the legal and technical realms. Such is the case for example when the question is concerned whether a Media Access Control (MAC) address, a unique identifier for a communication device that is collected during Wi-Fi tracking, should be considered personal data or not. According to the Dutch DPA (2015), a MAC address is personal data, even when hashed by the organisation. A citizen that does not have the technical knowledge to understand how this works, or the legal knowledge that the DPA has voiced in this opinion, stands very weak against an organisation that takes an opposing position. Similarly, when the Dutch unemployment agency UWV, one of the largest governmental institutions of the Netherlands, claims not to process any personal data, a citizen needs to (1) know that this cannot be true, and (2) have the audacity to oppose the claim of a large government organisation. In such situations, doing access requests in a community of people, some of whom possess specialised knowledge, empowers the position of citizens.

Viewing the right of access as a legal tool to empower citizens *vis-à-vis* more powerful and knowledgeable organisations has parallels with *freedom of information act* (FOIA) rights. The ideal behind FOIA rights is that the citizenry has the right to gain knowledge about the functioning and decision making of governmental bodies (Kreimer, 2008). And similar arguments have been made with regards to private companies (Pasquale, 2015). Only an informed citizenry can make informed political judgments with regards to a government that in a democratic society should be under its control. The rationale for having the right of access is very similar. Moreover, similar to the right of access, FOIA rights are individual rights, while the benefit is meant to be for the society as a whole.

Similarly, the difficult conditions of unequal information and power experienced by citizens that exercise their right of access, resemble the conditions experienced with FOIA rights. Kreimer (2008) notes for example that "*to press a recalcitrant administration for disclosure under FOIA requires time, money and expertise*". And while the right of access has been codified in such a way that it ought to be relatively easy for the citizen to execute, for example by having a low level of formal requirements to the request or capping the cost that organisations can charge for fulfilling a request, getting a clear picture of data practices through the exercise of the right of access is still very difficult, as organisations limit accessibility to the information in many different ways. Given the parallels, the conditions under which the right of access bears full

fruition will also be very similar to FOIA rights. As Kreimer (2008) phrases it, FOIA regulation is effective when part of a broader "ecology of transparency" that includes "tenacious requesters" like well-financed NGOs and an active media.

6.3. THE ECOLOGY OF ACCESS REQUESTS AND FUTURE WORK

If indeed, as we argue, the access right works best when used collectively and is aimed at empowerment and transparency at a societal level, the next question is what are the best fitting forms of collective organisation for this right?

Several forms have been tested so far. A number of online projects, including Bits of Freedom's *Privacy Inzage Machine* and Citizen Lab and Open Effect's *Access My Info* (see Hilts & Parsons, 2015) help citizens generate access request letters. These projects create awareness for citizens about the right, and lower the boundary of exercising the right by simplifying the process. They may also encourage organisations to be better stewards of personal information, as receiving access requests in high numbers signals to an organisation that citizens are concerned about how their personal data is used, and can "spur institutions to improve their privacy practices"[19]. Activists, such as Rejo Zenger (in the Netherlands) and Max Schrems (in Austria and Ireland) have exercised their right of access, used blogs and websites to share findings about the results with a broader public, and entered into litigation in order to force organisations into increased transparency about their personal data practices (e.g., Zenger, 2011). Others like Dehaye (2017) have combined the creation of an online access request tool with academic work and investigative journalism.

We plan to extend the current research in two ways. First, we are currently building a digital platform to recruit a larger group of participants in various EU countries, to send and track access requests in line with the method explored in this paper (see Asghari et al., 2017). This allows a more elaborate empirical assessment of the right of access in action, and in particular, to compare sectoral and country level differences. Second, we plan to include the point of view of the target organisations, by interviewing their DPOs in the future.

7. CONCLUSION

Just as the proverbial proof of the pudding is in the eating, rather than in a careful assessment of its recipe, the right of access should be assessed by how effective it is in practice. And since the right is meant to empower citizens, citizens should be the ones to judge if it empowers them. In our study, we asked participants to send access requests, and collected responses to their requests, and interviewed them along the way. The resulting picture is not pretty: while there are some positive exceptions, overall the compliance with the right of access is a mess. Non-compliance with the formal requirements of the law is widespread, with some organisations failing to answer at all, and others obstructing transparency in their answers. This mess did not surprise our participants though.

This sobering picture, however, does not mean that the right is useless. When the right is used in a collective manner, it creates a context to judge the quality of replies and the lawfulness of the data practices by comparing replies to similar access requests. Participants also perceived a societal much more than an individual value in exercising this right, not the least because through collective use, the power imbalance between individual citizens and organisations shifts in favour of the citizen.

ACKNOWLEDGEMENTS

We thank the participants for their effort in sending all the access requests, thinking through the replies they received and positive support of this research endeavour. We thank Nele Brökelmann, Kathalijne Eendhuizen, Stefanie Hänold, Joris van Hoboken and Mirna Sodré de Oliveira, as well as the reviewers, for their constructive critical comments on the text. This work was supported by the Princeton University Center for Information Technology Policy (CITP) Interdisciplinary Seed Grant Program.

REFERENCES

Article 29 Data Protection Working Party. (2018). *Guidelines on transparency under Regulation 2016/679* (No. WP260 rev.01). Brussels: European Union. Retrieved from http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Asghari, H., Greenstadt, R., Mahieu, R. L. P., & Mittal, P. (2017). The Right of Access as a tool for Privacy Governance. Presented at HotPETs during *The 17th Privacy Enhancing Technologies Symposium*. Retrieved from https://petsymposium.org/2017/papers/hotpets/rights-of-access.pdf

Bennett, C., & Raab, C. D. (2017). *Revisiting the Governance of Privacy*. (SSRN Scholarly Paper No. ID 2972086). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2972086

Bruening, P. J., & Culnan, M. J. (2015). Through a Glass Darkly: From Privacy Notices to Effective Transparency. *North Carolina Journal of Law & Technology*, *17*(4), 515-579. Retrieved from http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ncjl17&section=20

Dehaye, P.-O. (2017). Cambridge Analytica and Facebook data. *Medium*. Retrieved May 23, 2017, from https://medium.com/personaldata-io/cambridge-analytica-and-facebook-data-299c54cb23fa

De Hert, P., & Gutwirth, S. (2006). Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In E. Claes, A. Duff, & S. Gutwirth (Eds.), *Privacy and the criminal law* (pp. 61–104). Antwerp/Oxford: Intersentia.

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, *32*(2), 179–194. doi:10.1016/j.clsr.2016.02.006

Dutch DPA. (2015). *Wifi-tracking rond winkels in strijd met de wet*. Retrieved from https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-wifi-tracking-rond-winkels-strijd-met-de-wet

Dutch DPA. (2007). *Publication of personal data on the internet*. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_20071108_richtsnoeren_internet.pdf

Economist. (2017). Regulating the internet giants: The world's most valuable resource is no longer oil, but data. *The Economist*. Retrieved from http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

Galetta, A., & De Hert, P. (2015). The proceduralisation of data protection remedies under EU data protection law: towards a more effective and data subject-oriented remedial system? *Review of European Administrative Law*, *8*(1), 125–151. Retrieved from https://www.researchgate.net/publication/280034195_The_Proceduralisation_of_Data_Protection_Remedies_under_EU_Data_Protection_Law_Towards_a_More_Effective_and_Data_Subject-oriented_Remedial_System

Hilts, A., & Parsons, C. (2015). Access My Info: An application that helps people create legal requests for their personal information. In *The 15th Privacy Enhancing Technologies Symposium, Philadelphia, PA*. Retrieved from https://www.petsymposium.org/2015/papers/hilts-ami-hotpets2015.pdf

Hoepman, J. H. (2011). Het recht op inzage is een wassen neus. Wat nu? *Informatiebeveiliging*, *2011*(6), 16–17. Retrieved from https://repository.tudelft.nl/view/tno/uuid:6be95e4c-a836-4d64-8ad2-eeb1b987bfa7/

Hustinx, P. (2013). EU data protection law: The review of directive 95/46/EC and the proposed general data protection regulation. *Collected Courses of the European University Institute's Academy of European Law, 24th Session on European Union Law*, 1–12. Retrieved from https://pdfs.semanticscholar.org/f1e3/333fcc1344d28134e0ab418817d5f7aa270d.pdf

Kreimer, S. F. (2008). The freedom of information act and the ecology of transparency. *University of Pennsylvania Journal of Constitutional Law*, *10*(5), 1011-1080. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1088413

Norris, C., De Hert, P., L'Hoiry, X., & Galetta, A. (Eds.). (2017). *The Unaccountable State of Surveillance - Exercising Access Rights in Europe*. Cham: Springer International Publishing. Retrieved from http://www.springer.com/us/book/9783319475714

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms that Control Money and Information*. Harvard University Press.

The Organisation for Economic Co-operation and Development (OECD). (2013). *The OECD Privacy Framework*. OECD Publishing. Retrieved from: https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

Schnackenberg, A. K., & Tomlinson, E. C. (2016). Organizational transparency: A new perspective on managing trust in organization-stakeholder relationships. *Journal of Management*, *42*(7), 1784–1810. doi:10.1177/0149206314525202

Schwartz, P. M. (2013). The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. *Harvard Law Review*, *126*(7), 1966–2009. Retrieved from http://papers.ssrn.com/abstract=2290261

Van Breda, B. C., & Kronenburg, C. C. M. (2016). Inzage in de praktijk van het inzageverzoek. *Privacy & Informatie*, *2016*(50), 60–65. Retrieved from http://old.ivir.nl/syscontent/pdfs/232.pdf

Zenger, R. (2011). *Winst bij de rechter, Telfort geeft inzage in álle persoonsgegevens*. Retrieved November 17, 2017, https://rejo.zenger.nl/focus/winst-bij-de-rechter-telfort-geeft-inzage-alle-persoonsgegevens/

Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, *2015*(30), 75–89. doi:10.1057/jit.2015.5 Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754

Zuiderveen Borgesius, F. (2015). "Informed Consent. We Can Do Better to Defend Privacy." *IEEE Security & Privacy*, *13*(2), 103–107. doi:10.1109/MSP.2015.34 Retrieved from http://papers.ssrn.com/abstract=2793769

APPENDIX

Below is the first page of a reply to an access request to the Municipality of The Hague. It contains a list of labels of data they share with other organisations through two databases "BRP Verstrekkingsvoorziening" (Personal Records Database distribution facility) and "Beheervoorziening BSN" (Social Security Number distribution facility). No further information, background or invitation for further questions is given.

Den Haag

DPZ/ 2014.362

2

Retouradres: Postbus 12 600, 2500 DJ Den Haag

Aan :
<Name Participant>
<Address participant>

Uw brief van
11 augustus 2017
Uw kenmerk
inzage Brp
Ons kenmerk
<reference nr organization>
Doorkiesnummer
070 -3533192
E-mailadres

Aantal bijlagen

Datum
18 september 2017

Onderwerp
Inzage BRP 2016-2017

Geachte <Name participant>

In antwoord op uw hierboven vermelde brief deel ik u mede dat er geen informatie over u verstrekt is vanaf 11 augustus 2016 t/m 3 augustus 2017.

Voor wat de verstrekkingen uit de BRP Verstrekkingsvoorziening en Beheervoorziening BSN in dezelfde periode vermeld ik deze hieronder, t.w.:

Verstrekkingen: Ad Hoc

Afnemer	606501 Universitair Medisch Centrum St. Radboud
Verstrekkingsdatum	27-01-2017
Verstrekte rubrieken	01.01.10 ANr
	01.01.20 Bsn
	01.02.10 VoorNaam
	01.02.20 TitelPredikaat
	01.02.30 GeslachtsNaamVoorvoegsel
	0 1.02.40 GeslachtsNaam
	01.03.10 GeboorteDatum
	01.03.20 GeboortePlaats
	01.03.30 GeboortelandCode
	01.04.10 GeslachtsAand
	01.01.10 NaamGebruikAand
	05.01.10 ANr
	05.02.30 GeslachtsNaamVoorvoegsel
	05.02.40 GeslachtsNaam
	05.03.10 GeboorteDatum
	05.06.10 RelatieStartDatum
	05.07.10 RelatieEjndDatum
	06.08.10 OverlijdenDatum
	06.08.20 OverlijdenPlaats
	08.09.10 InschrijvingGemeenteCode
	08.10 .20 GemeenteDeel
	08.10.30 AdreshoudingStartDatum
	08.11.10 StraatNaam
	08.11.20 HuisNr
	08.11.30 Huisletter
	08.11.40 HuisNrToevoeging

1

Reply to an access request to the Municipality of The Hague

FOOTNOTES

1. For a critical analysis on the functioning of notice regulation in the US, see Bruening and Culnan, 2015.

2. The DPD was replaced by the GDPR effective May 2018. According to De Hert and Papakonstantinou (2016) the GDPR is not substantially different than past law with regards to the right of access. Two major motivations for the introduction of the GDPR were harmonisation and increased protection for citizens in an environment of intense technological change. Harmonisation is achieved by the fact that the regulation will be directly applicable in all member states, whereas the DPD applied only through its implementations into respective national laws. Stronger data protection for citizens is pursued by, among other things, increased fines, which may increase the relevance of our work.

3. In the GDPR the first ambiguity seems to be solved as the law says: "The data subject shall have.... access to the personal data.... *and* the following information: .... (b) the categories of personal data concerned. The ambiguity with regards to the recipients however remains as the law still states ... (c) The recipients or categories of recipient ..."

4. Dutch DPA (2007) p. 39 "Pursuant to Article 35 of the Wbp, a report must be a complete and clear overview of the data that are being processed in relation to a data subject. This must not be a description or summary of the data, but a complete reproduction. If the report were incomplete, the data subject would of course be insufficiently able to exercise his or her rights under the terms of the Wbp. This interpretation was confirmed in mid-2007 by the Supreme Court in the judgments on the Dexia case, Supreme Court, 29 June 2007, LJN: AZ4663 and Supreme Court, 29 June 2007, LJN: AZ4664."

5. Similarly, recital 63 of the GDPR does the same. It reads: "A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing."

6. The small number of participants and selection method impose limitations on the generalisability of our findings, for instance about how citizens as a whole perceive access rights, or how all organisations handle access requests. Our design, however, offers insights into sentiments and data practices that are present in society.

7. We add a subject line, a paragraph explaining why the citizen requested the data, and a paragraph explaining that we add a copy of a passport in order for the organisation to be able to verify the identity.

8. We only count a request as unanswered after at least 60 days have passed. It is of course possible that some organisations will still reply at some later point.

9. In two of these cases the replies referred back to the privacy policy of the organisation, and in two cases they referred to another organisation.

10. Participants agreed with seven of the responses without data. If we count the lack of data in these replies as the correct data, the percentage within this cell increases to 69%.

11. This only happened after the participant first sent a reminder, then received a copy of the privacy policy, and then again asked Happy Socks to act upon the access request as detailed in

their own privacy policy.

12. We in fact had a follow up conversation with The Hague Library, and they stated that the former is true; in particular they stated that they do not keep borrowing history nor any borrower profile.

13. Dutch DPA (2007) p.39 "Pursuant to Article 35 of the Wbp, a report must be a complete and clear overview of the data that are being processed in relation to a data subject. This must not be a description or summary of the data, but a complete reproduction. If the report were incomplete, the data subject would of course be insufficiently able to exercise his or her rights under the terms of the Wbp. This interpretation was confirmed in mid-2007 by the Supreme Court in the judgments on the Dexia case, Supreme Court, 29 June 2007, LJN: AZ4663 and Supreme Court, 29 June 2007, LJN: AZ4664"

14. The GDPR states *"the data subject shall have…. access to the personal data…. and the following information: …. (b) the categories of personal data concerned."* The ambiguity with regards to the recipients however remains as the law still states *"… (c) The recipients or categories of recipient …"*

15. The fifth participant received a confirmation one month after their request, stating Schiphol expects to answer with a delay because of the holiday period.

16. To clarify, we are not proposing that organisations should retain the data longer in order to respond to an access request; rather that the initial response could have pointed out the collection-deletion practice to improve transparency.

17. Of the five others who sent data access requests to two different branches of UWV, three never received a reply, even after sending reminders, and two received a reply that UWV did not process their personal data.

18. As both the explanatory memorandum of the Dutch Personal Data Protection Act as well as recitals of the GDPR state, as discussed in Section 2.

19. See https://accessmyinfo.org/