Exercising the right of access: a benchmark for future GDPR evaluations

AUTHORS DETAILS:

1. Glen Joris (corresponding author)

Affiliation(s): [a]imec-mict-UGent, Department of Communication Sciences, Ghent University, Ghent, Belgium; [b]Center for Journalism Studies (CJS), Department of Communication Sciences, Ghent University, Ghent, Belgium.

E-mail: glen.joris@ugent.be

Twitter: https://twitter.com/JorisGlen

ORCID: 0000-0002-4202-2641

3. Peter Mechant

Affiliation(s): [a]imec-mict-UGent, Department of Communication Sciences, Ghent University, Ghent, Belgium.

E-mail: peter.mechant@ugent.be

ORCID: 0000-0002-5283-5806

4. Lieven De Marez

Affiliation(s): [a]imec-mict-UGent, Department of Communication Sciences, Ghent University, Ghent, Belgium.

E-mail: lieven.demarez@ugent.be

Twitter: https://twitter.com/LievenDeMarez

ORCID: 0000-0001-7716-4079

Exercising the right of access: a benchmark for future GDPR evaluations

ABSTRACT: Despite the importance of the right of access in scholarly and judicial debates, empirical research on how this right is exercised in practice is very limited, especially in terms of studies, sample size and sample diversity. This might hinder a thorough evaluation of the EU's General Data Protection Regulation (GDPR) that recently reinforced the right of access. This article describes the results of a large-scale investigation (n = 220) on how data organizations handled the right of access under the former EU Data Protection Directive and 1992 Belgian Privacy Act. As such, it aims to establish a more reliable benchmark for future GDPR evaluations. Our results show how data controllers fall short in complying with their specific obligations stemming from the right of access vis-à-vis data subjects. While this result has important societal implications, it should nonetheless be seen against a broader context in which citizens – at least until recently – rarely make use of their right of access. The latter is demonstrated with empirical data, which was exclusively gathered using a formal written parliamentary question.

KEY WORDS: Data Protection, Data request, Directive 95/46/EC, General Data Protection Regulation (GDPR), Personal Data, Right of access

Word count: 6581

Introduction

"Everyone has the right of access to data which has been collected concerning him or her"; the EU Charter of Fundamental Rights (2000) is quite explicit concerning personal data access rights in the European Union. In practice, this means that each individual should always be able to obtain a copy of his or her personal data from data processing organizations, as well as other supplementary information describing the purposes for which the data is collected and processed (Article 15 in GDPR, 2016). Such a right helps people to understand how and why organizations are using their information. Moreover, it gives them the opportunity to verify whether organizations are processing their personal data lawfully.

Despite the growing importance of personal data in today's data and internet economy, the right of access is argued to be generally "ignored, inefficient, underused and obsolete in practice" (Ausloos & Dewitte, 2018, p. 1). Previous studies such as Norris, De Hert, L'Hoiry, and Galetta (2017) or Mahieu, Asghari, & van Eeten (2018) confirm that getting access to personal data is indeed harder than legal theory would suggest. In practice, access rights have been oftentimes denied on the basis of several grounds; ranging from a lack of support and assistance for data controllers, a lack of expertise in handling data requests, to difficulties in locating data controllers details (Galetta, Fonio, & Ceresa, 2016).

This inconsistency between theory and practice might be explained by the fact that previous legal instruments, and most importantly the 1995 EU Data Protection Directive, have always omitted flexible and strong mechanisms to enforce compliance (Hoofnagle, van der Sloot, & Borgesius, 2019). As a consequence, little incentives existed for data controllers to grant data subject rights in general. The application of the EU's General Data Protection Regulation (GDPR) on the 25th of May 2019 is, however, assumed to change this situation drastically as infringements by data controllers can now be administratively fined by the member states' supervisory authorities up to 20 million EUR, or up to 4% of the total worldwide annual turnover (Article 83 in GDPR, 2016). When also taking into account the potential damages in offenders' reputation (e.g., Cambridge Analytica), the GDPR is assumed to have a significant effect on how data controllers implement and execute the various data protection principles (Hoofnagle et al., 2019).

In order to assess a possible "GDPR-effect", it is essential to have a solid benchmark of how organizations complied with data protection legislation before the GDPR was enforced. Previous studies on the right of access, however, fail to sufficiently provide these benchmarks on a country-specific level. For Belgium, for instance, samples from previous research are limited in terms of sample size, ranging from 19 to 60 data requests, and in terms of diversity in the domains researched, which concerned internet service providers (e.g., Ausloos & Dewitte, 2018; Galetta et al., 2016) and public authorities (e.g., Galetta et al., 2016). As a consequence, current knowledge on the right of access in Belgium is strongly focused on data-sensitive areas, even though data protection is clearly pertinent to all organizations working with personal data. This might eventually lead to bias in policy evaluation and making.

It is this study's ambition to minimize this bias by conducting a large-scale empirical investigation (n = 220) on the right of access in one specific country, namely Belgium. As such, our study can take into account the legal context in which the right of access is exercised which may significantly differ from

other European countries in a pre-GDPR context (Galetta et al., 2016). This ensures a more reliable benchmark on which future policy evaluations can build.

To this end, our research consisted of two complementary studies conducted in Belgium. In the first study, we exercised our right of access to our personal data stored by several Belgian public and private organizations by asking them how and why personal data is processed. Then, we conducted a quantitative content analysis of all stages required to exercise the right of access, including locating contact information on websites, reading privacy policies, submitting data requests and interpreting the data access output. In a subsequent study, we focused on how Belgian public authorities handle data requests. By means of a formal written parliamentary question, posed by [name deleted to maintain the integrity of the review process], we gathered data on the prevalence of the right of access requests towards public authorities in Flanders. This data provides important contextual information on how citizens use their right of access. It is the first time that such empirical evidence on the prevalence of exercising the right of access is provided.

Literature review

We start our review with a historical overview of the empirical work in this field. We thereby focus on previous studies on Europa in general, or more specifically Belgium. We outline their sampling strategies and results. Next, we reflect on these strategies from a communication science perspective.

Historical overview on the right of access research

The first examination of the right of access, to the best of our knowledge, can be traced back to 2012 when an EU-funded project, called 'Increasing Resilience in Surveillance Societies' (IRISS), was launched. In this project, researchers from ten different European countries submitted a data request to several public and private organizations who collected and stored the subject's personal data on a systematic and habitual basis (L'Hoiry & Norris, 2015). For Belgium, 19 organizations were empirically examined including public authorities with surveillance instruments such as CCTV cameras and large private companies such as Google, Microsoft and Facebook (Galetta et al., 2016).

In general, results of the cross-country study showed relatively poor practices regarding the practical aspects of exercising the right of access (L'Hoiry & Norris, 2015). This study found several difficulties to locate a data controller in order to proceed with a data request. Even more, for around a fifth of the data request, it was simply not possible to identify the organization that was in possession of the personal data. When data controllers' identity could be indeed found online, researchers from the IRISS project observed that some data controllers actively try to hide content related to privacy and data protection; for a quarter of the instances, the 'three click-rule' (Zeldman, 2001), which is required to successfully locate the desired information, was transgressed. Consequently, in 37% of the cases, the visibility of the privacy links on websites was rated as poor by individual researchers.

Galetta and colleagues (2017; 2016) elaborated further on these results by discussing their personal experiences of attempting to exercise one's right of access in Belgium and Italy. Based on ethnographic observations, they distinguished several strategies of avoidance and denial data controllers undertake to prevent and dissuade data requests. These included comprehensible strategies such as creating or sustaining a lack of information, a lack of clarity, a lack of support and assistance and a lack of knowledge about legislation (Galetta et al., 2016).

A year before the GDPR came into force, an increasing number of privacy and data protection breaches entered the public debate (e.g., Cambridge Analytica, fitness tracking app Polar). Against the backdrop of these events, Ausloos and Dewitte (2018) identified a growing number of tools and platforms facilitating the drafting, follow-up and assessment of access requests such as 'My Data Done Right'. 'My Data Done Right' (see https://www.mydatadoneright.eu/) is an online tool developed by Bits Of Freedom, an independent Dutch digital rights foundation, that helps data subjects to prepare, send and keep track of requests to access one's personal data or to correct, delete or request one's personal data. In order to nurture the discussion of these legal applications and increase the awareness of them, Ausloos & Dewitte conducted a study focusing on the practical issues relating to exercising the right of access. However, in contrast to Galetta et al. (2016) who predominantly sampled public authorities, Ausloos and Dewitte (2018) focused on 66 commonly used online service providers (i.e., organizations whose economic activity is taking place online). As one of the main aims of their study was to define and test an effective methodology for gathering evidence on compliance with data subject rights in general, they put considerable effort into the development of a formalized questionnaire in which the different steps, interactions and overall findings could be gathered. This questionnaire creates opportunities for future researchers to gather insights on the process of other informational rights such as the right of erasure, data portability and explanation.

In general, and similar to the results of the cross-country study, Ausloos and Dewitte (2018) encountered a significant amount of issues when locating and reading data controllers' privacy policies. In particular, they rated this first, essential step in exercising the right of access as 'difficult' to 'very difficult' in 31% of the cases. The most important reason for this result is the poor navigation quality of websites (such as not placing a hyperlink to the privacy section at the bottom of every webpage). Examining the privacy policies in detail, Ausloos and Dewitte (2018) also found that only 66 % of the cases provided concrete information (and instructions) on the right of access.

When data requests were actually sent, Ausloos and Dewitte (2018) had to undertake extra steps before obtaining a reaction from data controllers. In particular, in 87% of the cases, they had to send reminders or provide further authentication details. During these conversations, the authors encountered several obstacles, ranging from organizational obstacles such as an IT ticketing system or interpersonal obstacles such as suspicion, irritation, and bad faith. As Ausloos and Dewitte explain, these obstacles led to lengthy and frustrated conversations. After five months, they recorded a response rate of 74%. 36% of these responses were registered too late (> 30 days after the initial request). No less than 67% of the responses were considered to be incomplete and several attachments were perceived as non-human- or -machine-readable (e.g., Excel documents, PDFs).

On the 25th of May 2018, the GDPR's entry came into force. From then on, the right of access became enforceable and thus, data controllers were assumed to have implemented the necessary procedures to handle data requests efficiently and securely. From this point of view, Di Martino et al. (2019) assessed how secure these data controllers handle data requests. To do so, they investigated which procedures data controllers use to verify the identity of the applicant and which techniques are effective methods to steal personal data from others. Although the focus of this study was primarily on identity verification and authentication mechanisms, the authors have indeed examined their right of access to 55 organizations from several domains such as finances, entertainment, retail and others.

Results of this study show that a significant number of organizations are vulnerable to personal data leakage. Out of 55 examined organizations, 15 have leaked personal information without any permission of the person whose personal data was leaked. This personal information also included sensitive information such as financial transactions, website visit histories and timestamped locations. The study also showed that four organizations had not responded to the data request, even after repeated attempts of Di Martino et al. (2019). This is, both in absolute and relative numbers, significantly lower than the results of other studies conducted in Belgium such as Galetta et al. (2016) and Ausloos and Dewitte (2018) whose data requests remained respectively 8 (42%) and 17 (26%) times unanswered.

Sampling strategies

As we have discussed in the previous section, studies on the right of access are characterized by several sampling strategies. Although most of these sampling strategies are formulated on an individual basis, depending on the scope of a particular study, we identified several overlaps in how these sampling strategies are formed, indicating a relatively dominant way of reasoning in this particular type of research.[1] In this section, we discuss these strategies from a communication-science perspective.

A first sampling strategy concerns the choice to exclusively select data controllers that are in possession of the data subject's personal data, even though this is not a prerequisite to exercise the right of access. Data subjects are legally allowed to exercise their right of access to any data controller even when they are not sure that they are in possession of their personal data. The rationale underlying this strategy, however, may lie in that scholars regularly focus on the output of their research in that a significant amount of empirical data should be collected and analyzed to make interesting statements about the topic in question. When, for instance, most of the data requests lead to short, negative answers, few results may be presented by the researcher. It is therefore common to purposively focus on organizations data subjects are familiar with (i.e., purposive sampling).

Despite the rationale underlying this strategic choice, there are some important implications regarding the ecological validity that should be taken into account. In particular, the question arises whether the research findings of the discussed studies are applicable to people's everyday lives. Although data subjects actually submit their data requests themselves in this type of research, they do not send any data requests to data controllers that are not in possession of personal data. Subsequently, there is currently no empirical evidence on how data controllers handle such data requests. This, however, might also happen in people's everyday lives. Individuals who deliberately stay away from online service providers such as Facebook and Google might, for instance, have the spontaneous inclination to send a data request to these type of organizations. In the same vein, individuals who recently asked a data controller to delete all personal data related to him/her might want to check, by means of a data request, whether this deletion actually took place.

[1] As a side-note to this discussion, we would like to emphasize that we are aware that, due to practical considerations (e.g. time, budget), some choices with regard to sampling strategies are inevitable. In fact, this study is also subjective to some choices that may hinder us to foster the ideal. However, despite these limitations, it is of particular importance to constructively communicate of what these choices are and which implications they have on the presented results. By doing this, we hope that future research on informational rights in general and the right of access in specific profoundly consider their choices regarding sampling strategies.

A second sampling strategy concerns the choice to exclusively select data controllers who operate in data-sensitive areas such as online service providers, or data controllers who collect and store personal data on a systematic and habitual basis such as operators of CCTV cameras. The rationale underlying these choices can be found in the researchers' knowledge and/or professional judgment on data protection. As they know the ins and outs of the legal context in which these type of organizations store and collect personal data, they are also familiar with the potential impact (and risks) of these processing activities on human rights such as privacy (Edwards, 2005). Subsequently, they may deliberately seek for data-sensitive areas, as they may provide the most relevance to their field of study.

However, by focusing on such specific areas, the question arises whether the results of these studies may be generalized beyond the specific research context. This is often not the case, as the characteristics of these organizations differ significantly from other organizations such as small and medium-sized enterprises (SMEs). The technological infrastructure of large companies like Google and Facebook, for instance, is assumed to be far more advanced to capture and store personal data in terms of volume or velocity (Chen et al., 2013). Consequently, it may be more complicated to handle data requests efficiently, even though they have more means to employ legal and technical experts.

A third sampling strategy concerns the choice to sample beyond the national (and legal) borders of the right of access. The rationale underlying this choice lies in the opportunities that cross-country studies entail. In particular, by comparing two or more cases or nations, scholars may have a better understanding of the (legal) context in which social phenomena are taking place. This may eventually result in deeper theoretical insights on the right of access.

However, the potential risk of cross-country studies is the insensitivity to the legal context in which private and public organizations operate. This is especially true in a pre-GDPR era that is characterized by a lack of harmonization within the European Union (Blume, 2012; Norris et al., 2017). This was also confirmed by Galetta et al. (2016) who concluded that significant differences can be found between the legal framework of Italy and Belgium under the directive 95/46/EC. Consequently, there is a risk to make statements about and comparisons between different countries, while not taking into account the legal differences that underlie these results.

Conclusion

Our literature review shows that the right of access is in general not properly accommodated by data controllers, even though they are legally assumed to do so. Based on the insights of several empirical studies (e.g., Ausloos & Dewitte, 2018; Di Martino et al., 2019; L'Hoiry & Norris, 2015), we demonstrated, both quantitatively and qualitatively, how apparent this issue is and which obstacles might be encountered during a data request. Furthermore, in order to establish a more reliable benchmark for future policy evaluations, our literature review also examined which methodological implications underlie the sampling strategies used by these studies. This discussion led to some important insights for future studies, including this study, on informational rights in general and the right of access in specific.

Methodology

Study one

In order to conduct a large-scale investigation on exercising the right of access, we adopted a multi-method approach based on (i) the analysis of textual documents such as privacy policies and data request results, also known as *content analysis*, and (ii) the principles of *action research*, indicating an active role of the researcher during several stages of the research process. This role concerns the submission of a formal data request, for instance, in which the researcher significantly participates in how data is requested.

In order to maximize the potential of both methodologies, we invited six students of [name deleted to maintain the integrity of the review process], to participate in this study. We asked them to exercise their right of access as realistically as possible. This included a five-step procedure consisting of (1) locating data controllers' details, (2) reading and coding privacy policies, (3) submitting formal data requests, (4) following up data request and (5) interpreting and coding the data requests results. As this approach confronted us with some methodological challenges regarding the reliability of the research process, we formulated a clear procedure for each stage of the research process, briefly discussed below.

In the first phase of the research process, we formulated a sampling strategy in which the students were asked to select organizations in their environment for which they thought that they were in possession of their personal data. Doing so, we used a bottom-up approach in which the students had the ability to select data controllers themselves. This approach enabled us to balance between several methodological criteria, as we presented in the previous section, such as ecological validity and sample diversity as well as the need to collect a significant amount of empirical data. A first iteration resulted in a sample list of 300 organizations. Then, we checked in a second iteration whether the sampling groups of all students were mutually homogeneous, in order to prevent double requests. This round excluded more than 80 organizations, resulting in a total sample group of 220 organizations (see Appendix 1 for a full list). We also classified each organization into a category based on its economic activities. These categories were created by means of a manual cluster analysis.

The second research phase was concerned with how data controllers publicly disclose the right of access. This is usually reflected in a privacy policy in which the data controller explains how they protect the data subject's privacy. The privacy policies of the 220 companies were coded using a coding manual (see Appendix 2). The main dimensions in this manual include: (1) whether privacy policies were easy to find and read (i.e., degree of difficulty), (2) whether privacy policies explicitly mentioned the right of access and (3) whether any legal requirements regarding the submission of the right of access were disclosed such as identity verification. The first criterion, the degree of difficulty, was based on four variables, including (1) the number of clicks one needed for going from the homepage to the privacy policy webpage, (2) the presence of a referral link to the privacy policy webpage on the homepage, (3) the word count of the privacy policy web page and (4) the name of the web page describing the privacy policy.

The third phase focused on the most important part of exercising the right of access: submitting a data request. In this phase the performance of the students was of particular importance. In order to

standardize this process, we provided them with a model letter (see Appendix 3) and general request guidelines. Many of these guidelines were already formulated by the national Data Protection Authority of Belgium (DPA). The data subject, for instance, was required to prove his or her identity by attaching a copy of his/her identity card to the request. Moreover, the data request has to be signed and dated and has to be sent by a means of telecommunication (e.g., a fax or an e-mail with an electronic signature) or delivered personally. Although we respected most of these imposed requirements, we decided to omit one them: we left the identity card purposely behind to elicit safety issues regarding the right of access. All data requests were sent in November 2017.

The fourth phase in the research process involved following up the data requests. When data organizations had any questions, for instance, the students had to be able to respond appropriately and, importantly, similar to their fellow students. We therefore also formulated general follow-up guidelines which the students had to adhere to. These were instructed through a training program of 2 x 2 hours in which they learned how to use these guidelines. An online collaboration platform was also launched to inform each other and discuss experiences or unexpected events.

The last research phase involved the interpreting and coding of the responses of the data controllers. Similar to phase two, we constructed a coding manual (see Appendix 2). The main questions used to structure this manual were: (1) whether data controllers responded within the statutory period of 45 days, (2) whether data controllers transferred all information required, (3) whether barriers or security issues were identified and (4) whether the attachments were human- and/or machine-readable.

Study two

In order to examine the prevalence of the right of access, we analyzed the data that was collected by [name deleted to maintain the integrity of the review process] as a result of a written parliamentary question. This question was posed shortly after the publication of the results of study one in a press release.

By posing a formal written parliamentary question, all organizations that receive funding from the Flemish government, by means of structural subsidies, were obliged to give answers to the questions. As a result, the second study contains a representative sample of 131 Flemish-funded organizations, ranging from Flemish departments and agencies to independent entities such as 'VRT', the public broadcaster of Belgium. The response rate was 100%. The number of variables that could be requested was limited to four, including (1) the number of data requests received during 2014-2017, (2) the average number of days needed to respond, (3) the availability of a uniform protocol to guarantee a response and (4) the presence of a uniform protocol concerning the verification of the respondents' identity.

Results

Study 1

Reading privacy policies

Our analysis shows that 51 of the 220 data controllers (23,18%) do not mention the right of access on their website. Most of the websites of data controllers that mention the right of access do so on their

home or start page by means of a hyperlink to their privacy policy (148/169 = 87,57%). Subsequently most mentions of the right of access can be navigated to in one mouse click, while 45 websites require visitors to click twice or more before reaching a web page that outlines the right of access.

We discovered that web pages describing the right to access are named in more than 29 different ways. The most popular names to describe this document are 'privacy policy' (92 times), 'privacy' (18 times), 'disclaimer' (9 times) and 'privacybeleid' (i.e., Dutch for 'privacy policy') (8 times). These pages have an average word count of 2690 words but differ widely in length; the shortest text mentioning the right of access counted 67 words, the longest no less than 30780 words.

Further analysis of these texts shows that data controllers mentioning the right of access, often do not provide a contact person or contact address to submit such requests to. This was the case for more than 57 (33,73%) data controllers. Also, data controllers mentioning right of access on their website, more often than not, did not mention that a data subject should provide a verifiable credential of his or her identity in order to request access to his or her data stored by the data controller. Of the 169 data controllers mentioning the right of access on their website only 21,30% (36/169) explicitly mention this condition.

Requesting and receiving data access

Most notably, our data requests to 220 data controllers showed that fewer than half (49,09%) responded to this request by giving an answer to one of the five questions we posed. This means that 108 organizations granted individuals the right of access and 112 refused to do so. Of those 108 data controllers who granted the right to have access, 100 did so within the statutory period of 45 days. In other words, 8 requests were handled too late. On average, organizations took 18 days to process a data request.

When we breaking this result down according to the their economic activities, we found that the majority of requests are granted in: 'local libraries' (100,00%), 'food retail' (80,00%), 'games' (75,00%), 'smartphone' (75,00%) and 'health' (71,43%). In contrast, organizations in which the majority did not grant the request for access belonged to the categories 'events and ticketing' (20,00%), 'UGC platforms' (4,29%), 'sport devices' (0,00%) and 'driving schools' (0,00%) (see Table 1).

Table 1. Percentage granted request for access for data controllers clustered on economic activity

Category	Frequency	% Request granted	Category	Frequency	% Requests granted
Local libraries	5 out of 5	100,00%	Newspapers & magazines	5 out of 10	50,00%
Food retail	4 out of 5	80,00%	NGO	1 out of 2	50,00%
Games	3 out of 4	75,00%	Schools	5 out of 10	50,00%
Smartphone	3 out of 4	75,00%	Sport organizations	5 out of 10	50,00%
Health	5 out of 7	71,43%	Temporary agency work	6 out of 12	50,00%
Other	7 out of 10	70,00%	Clothes	10 out of 22	45,45%
Retail	7 out of 10	70,00%	Traveling	6 out of 16	37,50%
Local Economy	4 out of 6	67,67%	Social network platforms	2 out of 7	28,57%
Public service	2 out of 3	67,67%	E-commerce	4 out of 16	25,00%
Telecommunication	2 out of 3	67,67%	Television	2 out of 9	22,22%
Finances	5 out of 8	62,50%	Events & ticketing	1 out of 5	20,00%
Hobbies	4 out of 7	57,14%	UGC platforms	1 out of 7	4,29%
Online sharing & storage	4 out of 7	57,14%	Driving schools	0 out of 2	0,00%
Cities and villages	3 out of 6	50,00%	Sport devices	0 out of 3	0,00%
Music	2 out of 4	50,00%			

As explained in the methodology section, we deliberately omitted several requirements such as identity verification, signature or date when exercising right to access, in order to investigate whether organizations would impose these requirements before giving the applicant access to his or her personal data. Results show that, out of 108 organizations who granted the right of access, disturbingly only 59 (54,63%) verified the identity of the applicant in some kind of way. Put differently, in more than 4 out of 10 granted requests (45,39%) someone else could have been the applicant and would still have received all personal data of someone else. Signature and date were respectively 6 and 4 times asked.

When identity verification was requested, various forms of identity verification emerged (see Table 2). While the majority (18/59 = 30,51%) asked the applicant to send a copy of his or her identity card or identity card information such as national registration number or birth day, other data controllers asked the applicant to re-sent the request from an email address known to them (11/59 = 18,64%) or at least to verify that the known email address actually belonged to them (6/59 = 10,17%). Other data controllers (7/59 = 12,28%) even requested a physical visit to their premises, asked to contact them by telephone (3/59 = 5,84%) or asked to provide them with some customer information such as client number (3/59 = 5,84%). Only a few (11/108 = 10,19%) applied a combination of different forms of identity verification such as identity card and verification via known email address (7/59 =11,86%), identity card and submission via known email address (3/59 =5,84%) or identity card and contact in person (1/59 = 1,69%).

Table 2. The number of times data controllers imposed a particular type of identity verification

Types of encountered identity verification	Frequency
ID card (information)	18
Submission via known email address	11
Verification via known email address	6
Contact in person	7
Customer information	3
Contact by telephone	3
Combination: ID card and submission via known email address	3
Combination: ID card and contact in person	1
Combination: ID card and verification via known email address	7

Evaluating correspondence and data request results

Format - When students received their personal data as an attachment, they had to open and interpret the results of their data requests. Although they were generally surprised by the amount of personal data some organizations process, they predominantly experienced serious difficulties with opening and interpreting the data documents properly. First, they noted that data controllers use a wide range of file formats (e.g., .csv, .png, .json, .pdf). In particular, some file formats caused problems in terms of machine- (e.g., .png) or human-readability (e.g., .json). Second, and linked with the previous human readability-problem, several variables within the data file were difficult to interpret or, in some cases, completely not understandable. For instance, variables with names such as 'WPComEnabledToggleDate' or 'ClientFriendlyName' and cells with unknown answer categories did not have any significant meaning.

Language - Although the right to access was exercised in Dutch and most data controllers were located in Belgium and used Dutch as the language to communicate with us (93), some organizations that granted the right of access and communicated with us, used a different language. In particular, 12 organizations used English and 1 organizations used French as the main language to communicate. For some students who were not very familiar with foreign languages, this was perceived as a possible hindrance to correspond effectively.

Emails – On average, data subjects were required to send (or answer) 3 emails, excluding the submission itself, before receiving access. In 15 cases, five or more emails had to be sent. Most notably, we found that in a few cases submitting a data request also automatically activated an opt in-mechanism for irrelevant and unsolicited e-mail messages. As such, exercising the right of access ironically led to the processing of personal data to which the right of access appeals.

Study 2

This study focused on the analysis of data that was collected as a result of a formal written parliamentary question. Although this question was answered by all public authorities in Flanders, a number of organizations were not able to provide insights into the number of data requests they received during the time period 2014 - 2017. This can be explained by the fact that public authorities were not obliged to hold a register of these parameters under the Directive. Despite this, most public authorities responded to the parliamentary question with concrete figures on the number of data requests they had each received during the time period 2014 - 2017.

Analysis of these responses shows how few organizations receive data requests (see Table 3). Except for the year 2017, only one organization had to grant the right of access to individuals during the time period 2014 - 2017. In 2017, a small increase is noticeable in that 7 organizations were asked by individuals to grant the right of access. However, this number still remains marginal in comparison to the number of organizations that did not receive any data request. Moreover, it is important to note that this increase can be partly explained by our first study in which we submitted a data request to three public service authorities.

Table 3. The number of public authorities that received data requests during 2014 – 2017.

	2014	**2015**	**2016**	**2017**
Public authorities that received data requests (number of cases)	1 (6)	1 (5)	1 (10)	7 (15)
Public authorities that did not receive data requests	112	112	112	107
Public authorities that did not register data requests	18	18	18	17
Total	131	131	131	131

For each year, we wrote the number of requests received by public authorities in brackets. These numbers show that the number of individuals exercising their right of access also remains very low during this time period. However, there is a small increase visible in the last (couple of) year(s), even though this can also be interpreted as marginal.

Despite a low number of access requests and public authorities, most organizations succeed in handling the access requests within 45 days. Only in 2017, one public authority needed more time to grant the right of access. More specifically, 82 days were needed to respond.

Discussion

In this article, we investigated how organizations deal with the right of access in practice. Although previous studies on the right of access have shown that this right is not adequately accommodated in data-sensitive areas such as public authorities or internet service providers, it was the article's aim to broaden the sample scope and involve a large number of different sectors. Moreover, by focusing on one specific country (i.e., Belgium), we were able to pay attention to the legal context in which organizations operate. We believe that this might enable a more reliable benchmark on which future GDPR evaluations can build.

In a first study, we exercised our access rights by addressing 220 organizations. We identified a relatively low response rate (49,09%) as well as several difficulties in the process leading up to receiving access to the data. These results confirm previous studies (e.g., Ausloos & Dewitte, 2018; Di Martino et al., 2019; Galetta et al., 2016) in which low response rates were registered and in which a lack of awareness, organization and motivation was shown to be the main hurdle obstructing effectively exercising the right of access. Most notably, we found severe privacy and security issues in identity verification. In more than 4 out of 10 granted requests (45,39%) no verification of the applicant's identity was conducted. This means that someone else could have been the applicant and would still have received personal information. A similar result on identity verification has been noted by Di Martino et al. (2019) who were able to impersonate 15 data subjects and obtain full access to sensitive data, including financial transactions, website visits and physical location history.

Moreover, we noticed that most data controllers who verified identity fall back on analogue techniques, most often requesting the data subjects to transfer a copy of their physical ID. There are, however, more recent frameworks and technologies such as eIDAS, a regulatory framework that wants to enable EU citizens to do cross-border interaction with their own national eID and that targets making electronic identities comparable and interoperable (European Commission, 2018) or 'self-sovereign identity systems' (Dunphy & Petitcolas, 2018) that are becoming increasingly available to mediate identity verification and identification of individuals (Sullivan, 2018). Such technologies could enable data controllers to remediate and ease identification processes in the future. However, as Di Martino et al. (2019) mentioned, organizational measures such as the creation of formal procedures and training might be at least as important to prevent privacy and security issues regarding identity verification.

In the second study we registered very low scores on (1) the number of public authorities receiving access request and (2) the number of access requests received by public authorities. This means that, in practice, citizens rarely exercise their right of access to public authorities. Despite the marginality of these results, it is important to note that these scores do not indicate low levels of citizen's interest in (1) the right of access in general or (2) governmental processing activities. On the contrary, in line with previous studies (e.g., European Commission, 2019; Hallinan, Friedewald, & McCarthy, 2012; Niemann & Schwaiger, 2016), we argue that a large group of citizens have a desire to understand how public authorities process personal data. However, to this end, exercising their rights should be easier and more user-friendly, as psychological barriers may lie too high to efficiently execute their right of access.

For instance, in our first study, we found several psychological barriers, both in terms of time and cognitive loading, that prevent individuals to exercise the right of access. In particular, several access requests required far-stretched efforts to submit and/or to follow-up. As such, we had to explain several times to organizations (1) what they are obliged to do when receiving an access request and (2) what we, as a citizen, expected from them when sending an access request. This amount of effort is also reflected in the average number of emails (3) we had to send or the average number of days (18) we had to wait before receiving the definite answer. A recent study on the awareness of the rights guaranteed by the General Data Protection Regulation confirm this idea by showing that that a large group of individuals in Belgium (43%) have heard of the right of access, but have not exercised it yet (European Commission, 2019). Therefore, we recommend policy makers to stimulate the development of legal applications such as 'My Data Done Right' that could ease the process of requesting right of access considerably.

Furthermore, for multiple reasons, we strongly encourage scholars to replicate this study in a GDPR context. First of all, because we believe that the true value of this study will only emerge when similar studies on the right of access are conducted and a reference point is required against which results may be compared. Second, because we believe that the mechanisms underlying the GDPR should be sufficient enough to enforce compliance. This assumption can only be assessed by empirical research in which informational rights such as the right of access are examined. Third, because we believe that this type of research exclusively provides transparency and insights into how organizations are processing personal data. This argument also corresponds with how Ausloos (2019) positions this type of research: "as a complementary method for data-driven research (…) that may provide high-quality data" (p. 5). In order to support our call, we included all information and material (e.g. sample list, manual coding book) required to conduct a similar study in (the appendices of) this study.

Limitations

An important limitation of our research is that the first study's sampling strategy does not give all data controllers in the population equal chances of being selected (i.e., probability sampling). In fact, and similar to previous studies, our sampling strategy was limited to organizations who were in possession of personal data. As we discussed in our literature review, this can be explained by the fact that a significant amount of empirical data must be collected to make statements about the topic in question. When, for instance, all data requests are submitted to organizations that do not process personal data, few results may be presented. We therefore argue that non-probability sampling is an inherent characteristic of this type of research.

Still, this does not mean that sampling strategies should be predominantly focused on data-sensitive areas such as online service providers or public authorities. In this research, we did not impose any inclusion criteria to our sample; students were able to create their own sample and select organizations active in their personal environments and contexts. As such, we aimed to heighten the diversity in our sample, while maintaining the ecological validity of this study. We recommend future studies to adopt a similar approach and seek a balance between these two important methodological criteria.

Acknowledgments

We would like to sincerely thank [name deleted to maintain the integrity of the review process], who took part in the data collection process and exercised their right of access for research purposes. In addition, we would also like to express appreciation to [name deleted to maintain the integrity of the review process] who acted upon this research and submitted a formal parliamentary question to [name deleted to maintain the integrity of the review process] to give explanation on their policies regarding data protection and the right of access.

Disclosure statement

No potential conflict of interest was reported by the authors.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available in order to conceal information that could compromise the privacy of research participants.

Bibliography

Ausloos, J. (2019). *GDPR Transparency as a Research Method*. Manuscript sumbitted for publication. doi: 10.2139/ssrn.3465680

Ausloos, J., & Dewitte, P. (2018). Shattering One-Way Mirrors. Data Subject Access Rights in Practice. *Data Subject Access Rights in Practice. International Data Privacy Law, 8*(1), 4-28. doi: 10.1093/idpl/ipy001

Blume, P. (2012). Will it be a better world? The proposed EU Data Protection Regulation. *International Data Privacy Law, 2*(3), 130-136. doi:10.1093/idpl/ips007

Charter of fundamental rights of the European Union (2012/C 326/02). (2012). *Official Journal of the European Union, 55*, 391-407. doi:10.3000/1977091X.C_2012.326.eng

Chen, J., Chen, Y., Du, X., Li, C., Lu, J., Zhao, S., & Zhou, X. (2013). Big data challenge: a data management perspective. Frontiers of Computer Science, 7(2), 157-164. doi:10.1007/s11704-013-3903-7

Di Martino, M., Robyns, P., Weyts, W., Quax, P., Lamotte, W., & Andries, K. (2019). *Personal Information Leakage by Abusing the GDPR 'Right of Access'.* Paper presented at the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019).

Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. *IEEE Security & Privacy, 16*(4), 20-29. doi: 10.1109/MSP.2018.3111247

Edwards, L. (2005). Switching off the surveillance society? Legal regulation of CCTV in the UK. In *Information Technology and Law Series* (pp. 91–114). doi: 10.1007/978-90-6704-589-6_5

European Commission. (2018). Digital Single Market. Trust Services and Electronic Identification (eIDAS). Retrieved from https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

European Commission. (2019). *487a. General Data Protection Regulation - 487b. Charter of Fundamental Rights*. Retrieved from https://ec.europa.eu/commfrontoffice/publicopinionmobile/index.cfm/Survey/getSurveyDetail/surveyKy/2222

Galetta, A., & de Hert, P. (2017). Exercising access rights in Belgium. In *The Unaccountable State of Surveillance* (pp. 77-108): Springer. doi: 10.1007/978-3-319-47573-8_5

Galetta, A., Fonio, C., & Ceresa, A. (2016). Nothing is as it seems. The exercise of access rights in Italy and Belgium: dispelling fallacies in the legal reasoning from the'law in theory'to the'law in practice'. *International Data Privacy Law, 6*(1), 16. doi: 10.1093/idpl/ipv026

Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer law & security review, 28*(3), 263-272. doi: 10.1016/j.clsr.2012.03.005

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. Information & Communications Technology Law, 28(1), 65-98. doi:10.1080/13600834.2019.1573501

L'Hoiry, X. D., & Norris, C. (2015). The honest data protection officer's guide to enable citizens to exercise their subject access rights: lessons from a ten-country European study. *International Data Privacy Law, 5*(3), 190-204. doi: 10.1093/idpl/ipv009

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). DOI: 10.14763/2018.3.927

Nicolaidou, I. L., & Georgiades, C. (2017). The GDPR: New Horizons. In *EU Internet Law: Regulation and Enforcement* (pp. 3-18). Cham: Springer International Publishing. doi: 10.1007/978-3-319-64955-9_1

Niemann, A., & Schwaiger, M. (2016). *Consumers' Expectations of Fair Data Collection and Usage--A Mixed Method Analysis.* Paper presented at the 2016 49th Hawaii International Conference on System Sciences (HICSS).

Norris, C., de Hert, P., L'Hoiry, X., & Galetta, A. (Eds.). (2017). The Unaccountable State of Surveillance. Law, Governance and Technology Series. doi:10.1007/978-3-319-47573-8

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. (2016). *Official Journal of the European Union, 59*.

Sullivan, C. (2018). Digital identity–From emergent legal concept to new reality. *Computer law & security review, 34*(4), 723-731. doi: 10.1016/j.clsr.2018.05.015

Zeldman, J. (2001). *Taking your talent to the web: A guide for the transitioning designer*: New Riders Publishing.

Appendices

Appendix 1. Sample list.

Category	Name
Schools	Bernardus Scholen
Schools	SJKS
Schools	Howest Kortrijk
Schools	Sint-Rembert Instituut Torhout
Schools	De Negensprong Koekelare
Schools	Sint-Martinus Instituut Koekelare
Schools	Hult
Schools	International Business School
Schools	Universiteit Gent
Schools	KU Leuven
Local libraries	Bib Sint-Niklaas
Local libraries	Bib Koekelare
Local libraries	Bib Gent
Local libraries	Bib Sint-Amands
Local libraries	Bib Bornem
Driving schools	Rijschool Vlaamse Ardennen
Driving schools	Rijschool VAB Torhout
Cities and villages	Wortegem-Petegem
Cities and villages	Tielt
Cities and villages	Ruiselede
Cities and villages	Gent
Cities and villages	Koekelare
Cities and villages	Bornem
Sport organisations	Basic fit
Sport organisations	LRV
Sport organisations	Tennis Vlaanderen
Sport organisations	KNWU
Sport organisations	Wielerbond Vlaanderen
Sport organisations	Voetbalbond
Sport organisations	Voetbal Red Star Waasland
Sport organisations	Real Madrid
Sport organisations	Jims
Sport organisations	Wima bowling
Traveling	Trivago
Traveling	Trip Advisor
Traveling	Cheap Tickets
Traveling	AirBnb
Traveling	Route du Soleil
Traveling	Delta
Traveling	Kilroy
Traveling	TourRadar

Traveling	Paperflies
Traveling	Uber
Traveling	Wizz Air
Traveling	Aeroflot
Traveling	Tui Fly
Traveling	Air France
Traveling	Ryanair
Traveling	Voyages SNCF
Social network platform	WhatsApp
Social network platform	Swarm by foursquare
Social network platform	Facebook
Social network platform	Twitter
Social network platform	LinkedIn
Social network platform	Happening
Social network platform	Snapchat
User-generated content platform	9gag
User-generated content platform	VSCO
User-generated content platform	Pinterest
User-generated content platform	Fancy
User-generated content platform	Tumblr
User-generated content platform	Youtube
User-generated content platform	Strava
Sport devices	Polar
Sport devices	Nike+run club
Sport devices	Garmin
Online sharing and storage	Outlook
Online sharing and storage	Studoc
Online sharing and storage	Wezoozacademy
Online sharing and storage	Dropbox
Online sharing and storage	Prezi
Online sharing and storage	Knooppunt
Online sharing and storage	Lees ID
Smartphone	Microsoft
Smartphone	Apple
Smartphone	Google
Smartphone	Samsung
Telecommunication	Orange
Telecommunication	Mobile Vikings
Telecommunication	Proximus
Newspapers and magazines	De Standaard
Newspapers and magazines	VRT.Nu
Newspapers and magazines	Humo
Newspapers and magazines	HLN
Newspapers and magazines	Nieuwsblad
Newspapers and magazines	Running.Be

Newspapers and magazines	Roularta
Newspapers and magazines	Krant van West-Vlaanderen
Newspapers and magazines	De Morgen
Newspapers and magazines	Blendle
Games	Candycrush
Games	Playstation
Games	EA sports
Games	Switch (VRT)
Public services	Bpost
Public services	NMBS
Public services	De lijn
Retail	I.Ma.Gi.N Jewels
Retail	Ace & Tate
Retail	Hema
Retail	The Phone House
Retail	Mediamarkt
Retail	Vandenborre
Retail	Rituals
Retail	Kruidvat
Retail	Horta
Retail	Aveve
Clothes	Sissy Boy
Clothes	Zara
Clothes	& Other stories
Clothes	Woman Secret
Clothes	Cos
Clothes	Massimo Dutti
Clothes	Hünkemuller
Clothes	Inno
Clothes	Timmermans
Clothes	Pepe Jeans
Clothes	Springfield
Clothes	Jules
Clothes	Hollister
Clothes	Zumo
Clothes	Ici Paris XL
Clothes	Castaner schoenen
Clothes	ASOS marketplace
Clothes	Urban Outfitters
Clothes	Paprika
Clothes	AS Adventure
Clothes	Modemakers
Clothes	Esprit
Food retail	Colruyt
Food retail	Smatch

Food retail	Dominos
Food retail	Delhaize
Food retail	Bioshop
E-commerce	Smartphoto.be
E-commerce	Superga.nl
E-commerce	About you
E-commerce	Amazon
E-commerce	Immoweb
E-commerce	Kapaza
E-commerce	Smartphonehoesjes
E-commerce	Ebay
E-commerce	2dehands.be
E-commerce	Photobox
E-commerce	Casecompany
E-commerce	4ucampus
E-commerce	Aliexpress
E-commerce	Asos
E-commerce	Xumexoffice
E-commerce	Zalando
Work	Man Power Oudenaarde
Work	Sodexo Card
Work	Expenza
Work	Adecco
Work	T-interim
Work	Konvert Interim
Work	Indeed
Work	Startpeople
Work	ISS
Work	Delhaize Jobs
Work	Ago Jobs & HR
Work	My Edenred
Hobbies	Politeia
Hobbies	Kinepolis
Hobbies	Universal studios Hollywood
Hobbies	Jumpsky
Hobbies	Sphinx cinema
Hobbies	Chiro
Hobbies	Academie muziek, woord en dans Bornem
Television	VTM
Television	Netflix
Television	Één
Television	Stievie
Television	Ketnet
Television	Eleven sports
Television	Sporza

Television	Q2
Television	Vier/SBS Belgium
Events and tickets	Tomorrowland
Events and tickets	Teleticketservice
Events and tickets	Pukkelpop
Events and tickets	Ticketmaster
Events and tickets	Rock Werchter
Finances	BNP Paribas Fortis
Finances	ING
Finances	Bankcontact
Finances	Argenta
Finances	Belfius bank
Finances	Payconic
Finances	Paypal
Finances	Kbc
Music	Shazam
Music	Deezer
Music	Spotify
Music	Soundcloud
Local economy	De Kreke
Local economy	Apotheek Ter Platen
Local economy	Zorgpunt koekelare
Local economy	Tandarts koekelare
Local economy	Brilart Torhout
Local economy	Deswarte Kappers Torhout
Health	AZ Ronse
Health	AZ Roeselare
Health	Ziekenhuis Torhout
Health	Ziekenhuis Dendermonde
Health	Ziekenhuis Bornem
Health	Ziekenhuis Oudenaarde
Health	Algemeen Medisch Laboratorium
NGO	Amnesty International
NGO	Rode kruis
Other	Luminus
Other	GoPro
Other	Scorito
Other	Pinnacle
Other	Funbal
Other	Team Tile
Other	Studentenmobiliteit
Other	Studenteninternet
Other	Energy lab
Other	Laperre

Appendix 2. Coding manual.

Dimension	Description	Categories
Cluster	To which cluster does the organization belong? (in Dutch: tot welke cluster behoort de organisatie?)	A. Local libraries B. Food retail C. Games D. Smartphone E. Health F. Retail G. Local economy H. Public services I. Telecommunication J. Finances K. Hobbies L. Online sharing and storage M. Cities and villages N. Music O. Newspapers and magazines P. NGO Q. Schools R. Sport organizations S. Temporary agency work T. Clothes U. Traveling V. Social network platform W. E-commerce X. Television Y. Events and tickets Z. USG platform AA. Driving schools BB. Sport devices CC. Other
Website	Does the organization have a website? (in Dutch: heeft de organisatie een website?)	A. Yes B. No
Privacy policy: right of accesss	Is there a page or document on the website in which the right of access is mentioned? (In Dutch: staat er ergens op de website het inzage-recht vermeld?)	A. Yes B. No
Privacy policy: clicks	How many clicks is required to navigate from the start page to the page in which the right of access is mentioned? (in Dutch: hoeveel clicks heb je nodig om van de startpagina van de website naar de pagina of het document te gaan waarin het inzagerecht staat vermeld?)	A. [open text field]
Privacy policy: visibility	Is the page or document in which the right of access is mentioned, visible on the start page of the website?	A. Yes B. No

	(in Dutch: is de pagina of het document waarin het inzagerecht staat vermeld zichtbaar op de startpagina van de website?)	
Privacy policy: word count	What is the word count of the page or document in which the right of access is mentioned? (in Dutch: kopieer het hele document waarin het inzagerecht staat vermeld naar word; hoeveel woorden telt het document?)	A. [open text field]
Privacy policy: description	What is the title of the page or document in which the right of access is mentioned? (in Dutch: Hoe heet de pagina of het document waarin het inzagerecht staat vermeld?)	A. [open text field]
Privacy policy: recipient	If the right of access is mentioned, is a recipient mentioned to whom you can send your data request? (in Dutch: indien het inzagerecht is vermeld; is er een specifieke ontvanger vermeld?)	A. Yes B. No
Privacy policy: legal requirement	If the right of access is mentioned, are there any requirements imposed by the organization? (in Dutch: indien het inzagerecht is vermeld; zijn er specifieke vereisten die zij vooropstellen (bv. identiteitsbewijs)?	A. Identity verification B. Dated C. Signed D. Charges E. Other: [open text field]
Output: time duration	How many working days they needed to answer your request? (in Dutch: hoeveel dagen duurde het om de data te ontvangen? - werkdagen, te starten vanaf 'startdatum: verwerking aanvraag', exclusief dag van verzending, inclusief dag van ontvangst)	A. [Open text field]
Output: response	Does the organization fulfilled one of the five right mentioned in the right of access? (in Dutch: heeft de organisatie voldaan aan één van de inzagerechten?)	A. Yes B. No
Output: emails	How many emails have you send? (In Dutch: hoeveel mails zijn er verstuurd - excl. aanvraag?)	A. [Open text field]
Output: language	In which language did the organization respond?	B. English C. French D. Dutch E. Other language

Output: requirements	Does the organization impose a requirement before answering the data request? (in Dutch: stelde de organisatie een bepaalde vereiste voorop nadat de aanvraag is gebeurd?)	A. Identity verifictation B. Dated C. Signed D. Vergoeding E. Verification via known email address F. Submission via known email address G. Contact in person H. Contact by telephone I. No requirements
Output: identity verification	If identity verification was a requirement, how was it verified? (in Dutch: indien identificatie een vereiste is: op welke manier?)	A. Contact in person B. ID card (information) C. Customer information D. Verification via known email address E. Submission via known email address F. Contact by telephone
Output: human and machine readability	If a file was attached to the response of the data controller, what is the file extension? (in Dutch: indien je een bestand hebt ontvangen, wat is de bestandsextensie?)	A. .zip B. .docx C. .pdf D. .rtf E. .csv F. .xlsx G. .png H. .jpg I. Other: [open text field]

Appendix 3. Right of access request letter (in Dutch).

(verantwoordelijke voor de verwerking)

Naam

Adres

Mijn voornaam en naam

Mijn adres

Mijn e-mailadres (Protonmail)

Betreft: recht van toegang tot mijn persoonsgegevens

Geachte mevrouw

Geachte heer

Hierbij stuur ik u een verzoek om toegang tot de persoonsgegevens die u mogelijk over mij bezit.

Volgens artikel 10 van de Privacywet[2] bent u verplicht mij op de hoogte brengen of u al dan niet mijn gegevens verwerkt. Indien dat het geval is, gelieve mij bijkomend de volgende informatie te bezorgen:

- ✓ de aard van de gegevens die u over mij verwerkt;
- ✓ het doel waarvoor u de gegevens gebruikt;
- ✓ de oorsprong van de gegevens (waar en hoe u ze hebt verkregen);
- ✓ de categorieën ontvangers van de gegevens: aan wie hebt u de gegevens meegedeeld, of aan wie u ze (mogelijk) zult meedelen;
- ✓ de gegevens zelf die u over mij verwerkt.

De Privacywet bepaalt verder dat u mij de gevraagde informatie binnen 45 dagen na ontvangst van het verzoek moet verstrekken. Als ik van u geen reactie ontvang, als u mij geen toereikend antwoord stuurt of als u weigert mij de gevraagde informatie te verstrekken, dan zal ik contact opnemen met de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL).

Ik dank u bij voorbaat voor de inlichtingen.

Hoogachtend

Mijn voornaam en naam

[2] De Wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*. Zowel de gecoördineerde versie van de Privacywet als de tekst van het KB van 13 februari 2001 dat de Privacywet uitvoert, zijn beschikbaar op de website van de CBPL: www.privacycommission.be.

List of tables