Eduard Rupp, Emmanuel Syrmoudis*, and Jens Grossklags

Leave No Data Behind – Empirical Insights into Data Erasure from Online Services

Abstract: Privacy regulations such as the General Data Protection Regulation (GDPR) of the European Union promise to empower users of online services and to strengthen competition in online markets. Its Article 17, the Right to Erasure (Right to be Forgotten), is part of a set of user rights that aim to give users more control over their data by allowing them to switch between services more easily and to delete their data from the old service. In our study, we investigated the data deletion practices of a sample of 90 online services. In a two-stage process, we first request the erasure of our data and analyze to what extent public data (e.g., posts on a social network) remains accessible in a non-anonymized format. More than six months later, we request information on our data using Right of Access requests under Art. 15 GDPR to find out if and what data remains. Our results show that a majority of services perform data erasures without observable breaches of the provisions of Art. 17 GDPR. At 27%, the share of non-compliant services is not negligible; in particular, we observe differences between requests submitted using a dedicated button and formal requests under Art. 17 GDPR.

Keywords: Right to Erasure, GDPR, Privacy Regulation, Right of Access, Right to be Forgotten, Data Erasure

DOI 10.56553/popets-2022-0080
Received 2021-11-30; revised 2022-03-15; accepted 2022-03-16.

1 Introduction

Today, individuals are confronted with countless situations in which data (about them) is created, transferred, and stored by online services. At the same time, the rapidly increasing technological complexities have made gaining control over one's own data increasingly harder over recent years; partly because by its very nature, personal data is intangible and therefore its duplication is relatively easy [1]. Thus, data privacy has become increasingly important.

Politou et al. [2] argue that users primarily want more control and transparency on the way data is used and reused, rather than privacy in the sense of concealment. However, eight out of ten EU citizens state that they feel as if they do not have complete control over their data and of these, two thirds are concerned about it [3]. Changing the default settings on online platforms can help to increase privacy [4]. However, in Germany, only 54% of users tried to change the default privacy options on social networks [5]. Research on the privacy paradox phenomenon indicates that the behavior of users does not reflect their concerns about privacy [6, 7]. Privacy regulation can help to close that gap, in particular, by empowering users in their relationships with online services.

One of the most prominent privacy regulations, which addresses the need of users to gain control over their data, is the General Data Protection Regulation (GDPR). It came into effect on May 25, 2018, and features the *Right to Erasure* (Article 17). This right allows data subjects (e.g., users), under certain circumstances, to have their personal data erased from data controllers (e.g., companies) without undue delay [8]. To reduce one's digital footprint it is certainly useful to have one's data deleted if the processing of the data by the data controller does not seem useful or beneficial to the user. There are many different reasons why a data subject would want to make use of the Right to Erasure:

- The data subject discovers that a certain service collects and processes too much data and therefore no longer wishes to use the service and wants their data deleted for privacy reasons.
- The data subject switched providers (e.g., using the GDPR's *Right to Data Portability* [9]) and wants their data to be erased from the previous provider.
- Having inactive accounts poses a security risk. For example, the more accounts a user has, the higher the chance of being involved in a data breach. In 2018, MyHeritage experienced a data breach in which more than 92 million email addresses and

Eduard Rupp: Technical University of Munich,
E-mail: eduard.rupp@tum.de
***Corresponding Author: Emmanuel Syrmoudis:**
Technical University of Munich,
E-mail: emmanuel.syrmoudis@tum.de
Jens Grossklags: Technical University of Munich,
E-mail: jens.grossklags@in.tum.de

hashed passwords were stolen [10]. The disclosure of email addresses alone can be sufficient to infer sensitive user information, in this case the request of a genetic test. Other data breaches have occurred, where even more sensitive data was leaked, such as credit card information [11].

However, for companies, data is a valuable resource in data-driven markets implying a desire to hold onto user data rather than deleting it. This leads to the following research question: **How do data controllers deal with data erasure in practice and what are the implications for data subjects?** To answer this, we examine the following aspects:

- What kind of data can users of websites easily delete in their accounts?
- Under what circumstances and how can data subjects exercise their Right to Erasure?
- Is requesting an account deletion within the account equivalent to a formal Right to Erasure request?
- How do data controllers respond to data deletion requests?
- What kind of data remains after a successful data deletion request?

For this purpose, we created accounts on 90 digital platforms and provide them with our data, which we then subsequently try to have deleted. First, we examine what kind of data a user can delete from within the account without terminating the account completely. Second, we try to delete all our data by deleting the account within the account settings and, wherever not possible, we formulate a proper Right to Erasure request to the data controller. After this process, we verify the completeness of the deletion by analyzing possibly remaining public data. Finally, we make *Right of Access by the Data Subject* (Art. 15 GDPR) requests after a waiting period of more than six months. To gain additional insights into the deletion processes, we also analyzed the privacy policies of all 90 services regarding the Right to Erasure, we sent out a set of questions concerning data deletion to the Data Protection Officers of the services, and, whenever the deletion process was not complete, we asked data controllers for an explanation. To the best of our knowledge, this study is the first to investigate data erasure under Art. 17 GDPR from an empirical perspective.

Within this study, we find evidence that 27% of services do not erase data in a way that is compliant with the provisions of the GDPR's Right to Erasure. We further find a compliance gap between data erasure requests submitted using dedicated erasure buttons and formal written requests under Art. 17 GDPR. This observation raises the regulatory question of whether these methods should lead to an equivalent scope of deletion. From our results, we can derive several recommendations which can serve as best practices for services. We especially see a need for reducing heterogeneity in the processing of erasure requests, for providing more information on the scope of deletion, and for a stricter authentication before requests are processed.

The remainder of the paper is structured as follows: In Section 2, we explain the Right to Erasure (Art. 17) and the role of the GDPR alongside the challenges the Right to Erasure might pose for companies. In Section 3, we describe our methodology and discuss ethical implications. The results are then presented in Section 4. We give specific insight on data erasure practices of services in Section 5. In Section 6, we discuss our findings and suggest best practices. We end with a brief summary and possible limitations in Section 7.

2 Background

The GDPR regulates the processing of personal data and aims to empower users by giving data subjects more control over their personal data that is stored by data controllers. Recital 7 of the GDPR states that "natural persons should have control of their own personal data" [8]. Notable user rights are formulated as the Right to Data Portability (Article 20), the Right of Access by the Data Subject (Article 15), the Right to Object (Article 21) and the Right to Erasure (Article 17), which is the main topic of this paper.

Article 6 ("Lawfulness of processing") states that "processing shall be lawful only if and to the extent that at least one of the following applies": when consent by the data subject is given, when processing is necessary for a contract that the data subject is part of, when processing is necessary for compliance with legal obligations, when processing is necessary for the performance of a task carried out in the public, and when processing is needed for legitimate interests of a data controller [8].

Article 7 ("Conditions for consent") explains that the consent "shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language" [8]. Thus, for example, a pre-ticked box during a sign up process violates the GDPR (e.g., when

signing up for a social media platform, a pre-ticked "make my profile public" checkbox does not comply with the GDPR; see [12] for the related decision of the Court of Justice of the European Union on cookie consent). Furthermore, the data subject has the right to withdraw from their consent and it should be "as easy to withdraw as to give consent" [8]. Generally, the approach the GDPR takes is to enable privacy by default and by design [1].

The GDPR intends to punish non-compliance with hefty fines of up to 20 million Euros or 4% of the total worldwide annual turnover of the preceding financial year, as stated in Article 83 [8]. Thus, it is in the best interest of data controllers to achieve compliance with the GDPR as the consequences are quite substantial.

2.1 Right to Erasure

In Article 17, the GDPR formulates the Right to Erasure which, in certain circumstances, enables data subjects to have their personal data deleted from data controllers, e.g., when:

- The controller does not need the data anymore.
- The controller is processing the data unlawfully.
- The data subject objects to the data processing.
- The data subject withdraws their consent and there is no legal ground for the data controller to keep processing the data.
- The data subject was a child at the time of the data collection.
- The data has to be erased because of a legal obligation.

The erasure of a data subject's data must be performed "without undue delay" [8]. Article 12(3) demands that controllers inform individuals on actions taken within one month with a possible extension by two further months. Furthermore, the controller must inform third parties, those that also process the data subject's data, of the Right to Erasure request.

Article 17(3) defines exceptions where the data controller is not obliged to always erase a data subject's personal data:

- The processing is needed for exercising the right of freedom of expression and information.
- The processing is needed for compliance with certain legal obligations.
- The processing is needed for reasons of public interest in the area of public health.
- The processing is needed for archiving purposes in the public interest, or for scientific or historical research purposes or statistical purposes.
- The processing is needed for the establishment, exercise or defense of legal claims.

2.2 Challenges for Companies

Just prior to the GDPR coming into effect in 2018, a survey on the challenges the GDPR created for companies found that the article of greatest concern was Article 17, which 42% of interviewed companies mentioned [13]. 46% of respondents noted that they had a limited understanding of the GDPR. 51% said that there was a way to clear old data, while 60% answered that this would "lead to changes in procedures and routines" [13].

In 2018, shortly after the GDPR came into effect, Wong and Henderson [14] made 230 Right to Data Portability requests (a right which allows users to export their data from services) and found that only 163 (70.9%) data controllers actually responded. Out of those responses, the data was not always in a compliant file format. In 2020, Syrmoudis et al. [15] found similar results: out of 182 data portability requests, only 135 (74.2%) were executed in some form within the legally required period. Within the legally specified timeframe, only 52 (28.6%) services provided a data export that was compliant with the provisions of Art. 20 GDPR (i.e., a complete export in a structured, commonly used, and machine-readable format).

Already in 2014, Herrmann and Lindemann [16] sent out deletion requests to vendors of smartphone apps and websites popular in Germany. Their findings show that, out of 56 apps that allowed creation of a user account, 54% fulfilled the request properly after one request. After a second request, this compliance rate increased to 57%. Out of 120 websites, 48% fulfilled the request properly after the first inquiry and 52% after the second inquiry.

The Right to Erasure poses some challenges for companies handling data. Not only the original data but also all replicas have to be erased [17]. Sarkar et al. [17] argue that identifying replicas, especially when data is stored over multiple servers and databases, can be difficult. Furthermore, they mention that designing algorithms for data erasure is not an easy task as they must ensure secure deletion and leave minimal room for retrieval of the deleted data. Additionally, Kelly et al. [18] state that companies only process a fraction of the stored

data and therefore do not understand the majority of the data they hold.

Depending on the kind of technologies a company uses to store personal data, compliance with the Right to Erasure might pose a serious challenge. This can be demonstrated by taking blockchains as an example. As the GDPR was drafted with centralized data storage in mind, the evolution of decentralized solutions raises new regulatory challenges [19]. Pagallo et al. [20] state that, when looking at the Right to Erasure and blockchains, a clash can be observed.

One of their proposed ways to combine the use of blockchains with the possibility of data erasure is the use of encryption methods. Then, upon receipt of a Right to Erasure request, the encryption key can be destroyed, thereby "erasing" the personal data. When using strong encryption, it is almost impossible to decrypt the encrypted data without having access to the key.

3 Methodology

To examine what kind of data can be deleted from data controllers and how they handle data deletion requests in the real world, several fresh accounts were created on various websites by one of the authors.

For this purpose, a fictional person was created by randomly generating a male first and last name from the top 500 German first and last names, respectively. [21, 22]. Additionally, date of birth, place of birth, occupation, address, phone number, credit card, and interests were assigned to this fictional person. For the date of birth, a random date was chosen. For the place of birth, the city of the author was chosen. As occupation, student was chosen. For the address, the author's address was chosen, excluding the apartment number. This was done to ensure that in the event of a data controller sending a letter, the author would be able to access it. A prepaid SIM card and a prepaid credit card were registered. Five separate email accounts at five different providers were created in order to register on the websites. The major reason for the use of multiple email addresses was to mitigate the risk of data loss if we were to be locked out of our email account for some reason. Lastly, a website, which uses AI to generate fake portrait pictures of humans, was used to create a profile picture [23].

The purpose of the process was to protect the author's own privacy where possible, even though not fully (an ID card was required for the registration of the prepaid SIM card, the author's real address had to be chosen, no methods were used to hide the real IP address). Furthermore, a fake name was used to mitigate the risk of a data controller deleting data from the author's private accounts.

The data collection for this study was divided into six steps:

1. Sign Up Process
2. Data Feeding Process
3. Manual Data Deletion Process (within the account)
4. Complete Deletion Process
5. Data Access Process
6. Follow-Up and Survey

We discuss the individual steps in the following subsections.

3.1 Sign Up Process

The SimilarWeb [24] ranking of top websites was used to choose 90 services. The accounts were created in December 2019. At that time, the ranking data from SimilarWeb was from November 1, 2019. Accounts for each of the top 50 websites worldwide and in Germany were created, respectively, excluding websites that:

- do not feature an account creation
- do not operate in the European Union
- do operate in the European Union, but the website's language is not English or German (e.g., Russian, Chinese)
- are already in the sample with an associate service (e.g., Google and Gmail, Bing and Microsoft; only one account was created and not two)
- come under the *adult* category

One website did not come under any of those five points but was excluded because it did not accept the last name of the created fictional person.

To ensure each category in the sample is represented by multiple services, we added more services to the sample. Therefore, we made sure that for each SimilarWeb category, which contains at least one service in the German top 50, its five most popular services in Germany are in the sample.

The registration process for the 90 accounts was evenly spread across four of the five previously created email accounts (one email address per 19–24 services). The fifth email account was used in one case to register on a website that we had not been able to register on with another email address. If the registration process

required the creation of an own email address on the website (e.g., if the website was a mail service provider), then this was performed instead.

During the registration process, the kind of data which was required to sign up was documented. Notably this included the full name, date of birth, address, phone number, email, interests or a description, username, and whether or not to receive emails (newsletters). This was done in order to know what kind of data, after the step described in Section 3.2, was actively entered on a website and to ultimately assess what kind of data could be deleted in the step described in Section 3.3.

3.2 Data Feeding Process

In this step, data was given to the websites. Therefore, in each account, the settings were examined and data was entered wherever possible. Data, which was entered in the settings (or anywhere else on the website), included the full name, gender, date of birth, address, phone number, interests or a description, credit card information, and a profile picture. Additionally, if a website offered the possibility of signing up for a newsletter (or to receive emails more generally), this setting was enabled as well.

If a website offered the possibility of creating public posts or comments, sending private messages or if the account featured a public profile, a second account for that website was created, private messages were exchanged between both accounts and public posts/comments were created on the first account. The reason for keeping track of this was to see whether such data could be deleted in the step described in Section 3.3 and what happens to public posts/comments, private messages and public profiles in the step described in Section 3.4. For the second account, we used a separate email address and separate information. Since that account was only used to exchange private messages and to verify the deletion of them (plus to verify the deletion of public posts and public profiles if they can only be seen when logged in), only the bare minimum of information needed to be entered during the registration process.

Furthermore, each website was periodically logged into and the website was used in order to create behavioral data. We tried to use the services as a normal user would, e.g., streaming music on streaming platforms, viewing items and creating wishlists on shopping websites, reading news articles on news websites, etc. This was performed manually to avoid the risk of being flagged as a bot and potentially losing access to the account. Furthermore, this process was aimed at simulating the reality in which a user might use an account over many weeks, months or even years. A data deletion request on a fresh account could skew the results because the data controller might see that the user does not have any meaningful data and therefore might complete the request more quickly.

Overall, the data feeding process took six weeks before the next step was initiated. Over the course of those six weeks the active time spent on each website was around 60 minutes, depending on the website. Using the site passively, e.g., streaming music, does not count towards this active time measure.

3.3 Manual Data Deletion Process (Within the Account)

The previous two steps documented what data was actively entered on various websites. In this step, it was examined whether a specific type of data could be deleted manually whilst logged into an account (without making a Right to Erasure request or terminating the whole account). It should be noted that, if the data could be deleted, the same data was immediately reentered, in order to have the highest possible amount of data prior to initiating the data erasure requests later on.

It was also checked whether the user was able to delete their profile photo, public posts/comments, and private messages. Private messages were only classified as being able to be deleted if the sender could delete them and they were also deleted for the receiving party silently, without any notification. Whether messages also get deleted from servers cannot be assessed. If the sender could delete a message but it was still visible in the receiving party's account, then this was classified as not being able to be deleted.

3.4 Complete Deletion Process

The fourth step consisted of initiating the actual data deletion requests. For this purpose, in each of the accounts, the settings were examined and checked to determine whether there was a dedicated option (e.g., a button) for initiating an erasure request. If no such button was found, the search engine Google was used to check online whether that specific website offers such a button. If that was not successful either, the corresponding privacy policy was inspected and the stated proce-

dure was executed (e.g., sending an email to the Data Protection Officer). This approach was chosen because this is how a regular user would most likely try to delete their account/data. For users, it is more convenient and faster to delete their account and data from within the account than having to write an email or fill out a designated form. For Right to Erasure requests processed by email, a self-created template was used, which is based on two templates that were available online [25, 26]. The email that was sent out to data controllers can be found in Appendix A.

The data deletion requests were initiated in March 2020. It was observed how the data deletion requests were handled, whether any challenges occurred when making those requests, whether any authentication of the user was necessary and what the response times were. When a service contacted us for authorization, we provided the necessary information.

Furthermore, after a completed request, the public posts/comments, private messages, and public profiles were checked as well. We categorized the results as *deleted*, *anonymized*, and *not deleted*.

If data is *deleted*, the data should be completely deleted from the data controller's servers. In our case, we classified data as deleted when there was no visible personal data to be found, e.g., when the public profile page no longer existed or when public posts and private messages were completely deleted, as if they had never existed.

When data is *anonymized*, it is altered in such a way that the data subject is no longer identifiable. We used this classification when any association between the user and their content was removed, e.g., the username was set to "deleted user" and the profile picture was removed but comments/posts and private messages remained and were then associated with the deleted user. It should be noted that a comment/post or private message may itself contain personal information if the user included such information themselves. In all our public posts or private messages we did not share any information that might identify the user. In cases where the user shared personal information, a dissociation between the content and the user would still leave the user identifiable.

Lastly, when data is *not deleted*, it is not erased from the data controller's servers. In our case, we found visible personal data, e.g., a comment/post remained and was still associated with the user's username/account.

3.5 Data Access Process

To further investigate if data has been properly erased, Right of Access by the Data Subject requests (Article 15) were sent out to all digital platforms. This was done in November 2020, more than six months after the complete deletion process was initiated. Privacy policies of the websites were checked for either a contact email address or a dedicated form. Again, a self-created template was used, based on two templates available online [27, 28]. The corresponding template can be found in Appendix A.

3.6 Follow-Up and Survey

In cases where a service sent us a non-empty response to the data access request, we wanted to know why there was personal data remaining at the service. We therefore sent an informal follow-up email to these services requesting an explanation for the incomplete deletion.

Additionally, and independent of the data erasure and data access requests, we sent out a voluntary questionnaire to all 90 Data Protection Officers. For sending out the questionnaire, a separate email address was used. The questionnaire consisted of nine questions regarding the data erasure practices of the service (see Appendix B for a list of questions) and was sent via email.

3.7 Research Ethics

Ethical considerations are necessary to minimize negative impacts on the studied companies and their employees.

The focus of the study lies on organizational practices rather than individual behavior. We therefore collected data through interaction with interfaces and through email contact with companies. We closely followed the methodology of recent related studies [14, 15, 29] to adhere to accepted data collection practices.

Less than one year after the GDPR became effective, a survey conducted by Kantar at the request of the European Commission [30] found that 57% of respondents have heard of the Right to Erasure and 13% have even exercised it. Our study was conducted two years after the GDPR became effective. We therefore assume that our data erasure requests did not cause significant harm (e.g., financial costs, employee time) to the stud-

ied firms, as they should already have established procedures to process requests.

29 of the studied services explicitly require the provision of truthful personal information during registration, especially the correct name. For these services, our methodology means a violation of their terms and conditions. In most cases, the intention behind this requirement is to get correct information for processing orders or to prevent hate speech from anonymous users. We neither ordered anything nor interacted with other users and therefore the violation of their terms and conditions did not harm the services. Our methodology does not violate other terms such as the prohibition of the use of automatic data processing or web crawling.

The survey was conducted independently of the data erasure and access requests. The contacted Data Protection Officers could answer the questions voluntarily and the focus of the questions was solely on the practices of the service rather than individual employees.

When collecting data and communicating with the services, we behaved like normal users and did not disclose the actual reason for our requests. This minor deception was necessary to ensure that we received unbiased answers.

In order to protect the investigated services and their employees from averse effects, we make sure that none of the practices described can be linked to single services. We further chose to follow the reasoning of [29] to not debrief the services. In cases in which the processing of GDPR requests is not fully automated, our requests might be linkable to single employees. We want to avoid any negative consequences for these employees in cases in which our requests have not been fulfilled in a GDPR-compliant way.

Apart from the impact on companies, the data feeding process could potentially adversely affect other users of the services. To minimize this risk, we did not post or spread any political content or hate speech in our public posts. There was no direct communication with other users (except our own second account) and edits on wikis and similar platforms were limited to the user namespace.

Causing the harm documented above cannot be avoided in order to effectively study the implementation of data erasure among online services. Nevertheless, it is necessary to evaluate the current state of data erasure to provide both lawmakers with evidence needed for possible adjustments of privacy legislation and services with insights on how to improve their processes. We believe that our methodology minimizes the harm caused for the services and employees involved and that this harm is outweighed by the societal benefits of our study.

4 Results

For users who want to delete personal data, both the deletion of specific data and the erasure of complete accounts are relevant scenarios. Our findings on manual deletion are presented in Section 4.1, Sections 4.2 – 4.4 focus on account erasure, and Section 4.5 compares data erasure practices by service popularity, request method, company domicile, and industry.

4.1 Manually Deleting Individual Data

Besides deleting their whole account, a user might also want to only delete specific parts of their personal data, e.g., public posts in social networks or their message history.

Table 1. Data that could be completely deleted, changed only, or neither deleted nor changed during the data deletion attempt within the account.

Data	Yes	Change Only	No
Full Name	23	38	10
Gender	20	31	2
Date of Birth	24	20	12
Address	32	25	0
Phone Number	40	13	2
Interests/Description	28	4	4
Credit Card	14	1	2
Profile Photo	35	7	0
Comments/Public Posts	13	0	11
Private Messages	2	0	17

Table 1 lists the number of services that allow deleting or changing of different data categories. We find that out of 83 services where data for at least one of these categories can be entered, a total of 76 services (92%) enable the deletion of data. Services which offer a (private) messaging functionality usually do not offer means of deleting the messages (11%). Public data such as social media posts or comments can be deleted in 54% of cases.

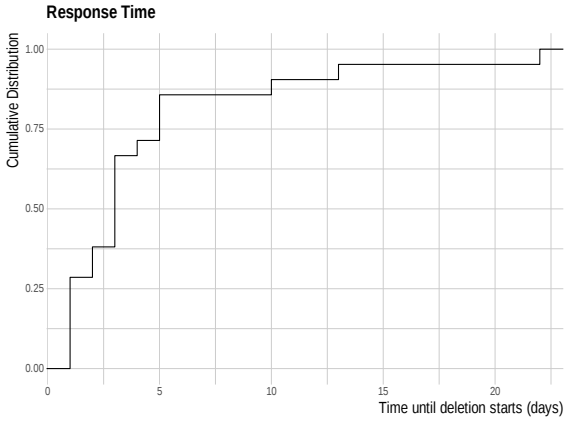

Fig. 1. Cumulative distribution of response times to requests sent via email.

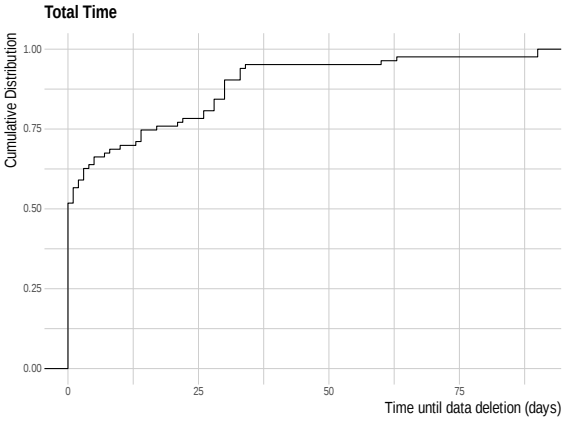

Fig. 2. Cumulative distribution of total deletion times.

4.2 Requesting the Data Erasure

In order to request the deletion of the complete account, we first searched for a way to trigger an account deletion from within the account settings. In our sample, 62 services (69%) offer a way of doing so.

The other 28 services were contacted via email or contact form. Figure 1 shows the cumulative distribution of response times to email requests, i.e., the time required before the services started the erasure procedure. The mean response time is 4.4 days with a median response time of 3 days. 3 services did not respond at all of which 2 deleted the account silently. That means, at some unknown point in time, the data controller deleted all user data without notifying the user of said action. 3 services responded, but did not process the erasure request. One service could not be contacted in the first place because they did not list any email address or contact form. Thus, 85 services processed the erasure request, 83 of them actively confirmed that the erasure has taken place.

37 services (41%) required at least one additional authentication step. 27 of them requested the user to reenter their password, 9 sent out an email where a confirmation link had to be clicked, an additional 4 required the user to specify their email address, and 5 required additional personal information (such as full name, address, date of birth, etc.) as a proof of identity. One of those 5 services asked for the address even though it had never previously been entered.

After starting the erasure procedure, either by clicking on a "delete account" button or by the service's Data Protection Officer or by customer support after being contacted, 54 of the 83 services (65%) deleted the data on the same day. For 25 services, there was a transition period between 7 and 90 days (median: 30 days). 19 services explicitly stated that during this period, the account erasure could be cancelled by the user, e.g., by logging into the account or by contacting customer support via email.

Figure 2 shows the cumulative distribution of total deletion times, consisting of both response time (if applicable) and transition period. We find that for more than 50% of services, the account can be deleted on the same day, the mean deletion time is 10.8 days.

For button requests, 30 out of 62 (48%) data controllers sent a confirmation email directly after the deletion process, stating that the account was either deleted (when the account was deleted immediately) or set to be deleted (when the response time was not 0). 15 out of 19 (79%) data controllers that did not delete the account immediately, did not send a reminder email when the account was deleted while 4 (21%) of them did once it had been deleted.

For all email requests that were successfully completed, except when done so silently, we received a notification when the erasure was completed.

4.3 Scope of Erasure

After the account erasure was completed, we checked for any remaining visible personal data from our deleted accounts.

We were able to check this for 33 services where the user has a public profile, can make public posts or comments, or send private messages to other users. As

Table 2. Distribution of public profiles, public comments/posts, and private messages which were deleted, anonymized or not deleted.

Data	Deleted	Anonymized	Not Deleted
Public Profile	22	1	4
Public Posts	12	6	6
Private Messages	8	7	4

shown in Table 2, we find that a majority of services deleted or anonymized this data. At 9 of the 33 services (27%), personal data was not properly deleted or anonymized.

Out of the 90 services, we could choose to receive recurring newsletters or promotional emails upon registration or within the user account in 67 cases. After the complete deletion process, 12 services (18%) still sent a newsletter.

4.4 Data Access

More than six months after the erasure requests, we contacted all 90 services again with a data access request under Art. 15 GDPR. 78 services replied to our request, 58 of them stated that there was no data stored for the given email address, and 6 could not process the request.

However, 14 replies contained actual personal data, like the user's email address, for example. Furthermore, these replies could also contain, but were not limited to, the full name, address, last used IP address(es), registration date, given consent to a newsletter subscription, and email conversations. One data controller replied with an extensive amount of data, including the user's search queries, wishlist, products and items the user has viewed, and a list of advertisers whose ads the user has clicked. Another data controller included sent and received private messages and the user's public comments.

The mean response time was 13.5 days with a median of 10 days. 5 services took more than 30 days to respond, one of them requested an extension of the processing period as required by the GDPR.

For 9 of the 14 services that replied with data, we already knew from Section 4.3 that they had not deleted all personal data or had continued to send newsletters. On the other hand, 2 of the services that had continued to send newsletters and were therefore still storing personal data (at least the user's email address), replied that there was no data stored for the given email address.

4.5 Analysis

Combining the results from Section 4.3 and Section 4.4, we find that 24 (27%) of the 90 services did not complete the data erasure request in a way which ensures that all personal data is deleted or anonymized (we henceforth call these services *non-compliant*).

Table 3 gives an overview on compliance rates by request method, country (company domicile), and popularity of service (measured by SimilarWeb rank). Note that for the newsletter column only the subset of services is considered where the possibility to register for a newsletter upon registration or within the user account exists. Similarly, for the public data column only those services are considered where public data such as posts or messages can be entered.

As noted in Section 4.2, 62 services offered means for deleting the account using a dedicated button while the other 28 had to be contacted with a formal request under Art. 17 GDPR via email or contact form. Comparing the compliance rates of these groups of services, we find that 82% of the email requests were completed in a compliant way. In contrast, the compliance rate for button requests is only 69%.

The majority of services in our sample have their company domicile either in Germany (56 services) or the United States (19 services). The compliance rates in these countries are 75% and 74%, respectively, and therefore not substantially different from each other.[1]

When comparing the services by popularity (using the SimilarWeb rank as a proxy for popularity), we did not find substantial differences either. As shown in Table 3, a share of 75% of the most popular services erased the data in a compliant way. For services with medium or lower popularity, the compliance rates are of comparable levels at 68% and 78%, respectively.

Finally, the comparison of services by SimilarWeb type (for types where the number of services in the sample is at least 6) yields a range of compliance rates between 50% (Food and Drink) and 100% (Travel and Tourism).

1 We do not provide compliance rates for EU or non-EU services, as these categories are dominated by German and US services in our sample.

Table 3. Data erasure compliance by request method, country, popularity, and type of service.

	Compliance	Newsletter still sent	Public data not deleted	Positive Art. 15 request
All services (n = 90)	73%	18%	27%	16%
Request method: button (n = 62)	69%	19%	24%	18%
Request method: email (n = 28)	82%	15%	50%	11%
Services from DE (n = 56)	75%	19%	31%	13%
Services from US (n = 19)	74%	9%	18%	21%
Rank < 500 (n = 32)	75%	9%	14%	19%
500 ≤ Rank < 3000 (n = 31)	68%	30%	36%	13%
3000 ≤ Rank (n = 27)	78%	14%	38%	15%
Type: Arts and Entertainment (n = 13)	54%	30%	44%	31%
Type: Business and Consumer Services (n = 7)	71%	17%	—	14%
Type: Computers Electronics and Technology (n = 18)	83%	8%	25%	11%
Type: E commerce and Shopping (n = 9)	67%	14%	33%	11%
Type: Food and Drink (n = 8)	50%	33%	50%	50%
Type: News and Media (n = 6)	67%	20%	33%	17%
Type: Travel and Tourism (n = 8)	100%	0%	0%	0%

5 Further Insights into Deletion Processes

As illustrated in Section 4, a significant proportion of online services do not delete all personal data when a user requests the deletion of their account. This is especially the case when the deletion is requested by clicking a "delete account" button in the service's account settings instead of requesting it via email and referencing GDPR Art. 17.

We, therefore, want to shed more light upon the data deletion processes of online services. To do so, we asked services, where the data erasure was incomplete, for an explanation (Section 5.1). We further analyzed the privacy policies of all services (Section 5.2) and sent out a questionnaire to the Data Protection Officers of the services (Section 5.3).

5.1 Follow-Up

From 14 services (those that did not anonymize and those where we managed to have the account deleted but surprisingly sent us personal data during the Art. 15 requests) we wanted to know why the data deletion was not fully completed.

Two of them stated that an account closure and a data removal request are not the same thing. Both offered to delete the remaining personal data afterwards. For one service, the remaining personal data only consisted of the username, while the other one held significantly more personal data.

For three services the reason for the incomplete deletion of data could potentially be attributed to technical errors. During the Art. 15 request process, one platform acknowledged themselves (without being asked) that personal data was left undeleted which should not have been the case because the account had previously been deleted. A previously associated email address still remained in the newsletter database even though it should have been deleted. Apparently, there was a data synchronization error between the main database and the newsletter database. A different service still held data because the account deletion was never initiated even though the user received an "account successfully deleted" prompt during the deletion process via a button click in the account settings. When asked, the platform did not rule out a technical error as account deletion does not happen very often and such an error could have gone unnoticed for an extended period of time. However, it was possible for the account to be properly deleted afterwards. The last data controller stated that the account was only deactivated (clears profile page and user-generated content) rather than deleted. In order to delete their account, users must go to the GDPR tab in the account settings and exercise their Right to Erasure from there. This tab was only visible in the account settings when the direct link sent by the support staff was clicked on but otherwise remained hidden. After pointing this out and providing evidence, the support staff stated that this should not have been the case and that the problem had been sent to the IT department for rectification.

For one data controller the answer as to whether an account closure and a data removal request were not

treated in the same way or whether it was attributable to a technical error was unclear. They stated that they did not hold any of our personal data but when asked why public comments were not anonymized (username and profile picture were still seen) they first only offered to anonymize it but never provided a reason as to why it was not deleted or anonymized in the first place. After asking why those comments were not deleted or anonymized after the account closure, we received the response that the technical implementation of the account closure button is not the same as a formal Art. 17 request. They furthermore stated, that it should be treated in the same way but was not working properly for a short period of time and that by now it should work as intended and the profile picture is deleted when the user initiates an account closure in the settings themselves. However, the username and the submitted comments are not deleted as those are not considered personal data and the data controller is not able to link them to a specific person after an account closure.

For one platform, the data deletion within the privacy portal only applies to certain services of the account but does not fully erase the account. For another platform, we received a similar response where the account was linked to a different service and, while the account and profile were deleted, data still remained at the other service.

One of two services that continued to send newsletters stated it was necessary to unsubscribe from the newsletters separately. The other one did not give an explanation, merely offering to cancel our newsletter subscription.

One platform was contacted twice but their mailbox was full on both occasions. On the third occasion, we merely received an answer that there was no account associated with the corresponding email address. When we mentioned that the response to our Art. 15 request was positive and included two email addresses, the platform replied that they only archive that data as evidence for having given consent to receive promotional mails. It was stated that the data was not being used for anything else other than archiving purposes.

Another platform was questioned as to why the username was not anonymized in private messages after the account deletion. The reply did not answer the question properly because it stated that after an account deletion the username is no longer visible on the website and that it is anonymized (e.g., in reviews).

Another data controller stated that they will respond to us about why they still held data but we received no further reply in the subsequent 8 months. One platform did not respond at all.

5.2 Privacy Policies

To gain further insights about how online services process data erasure requests, we analyzed the privacy policies of all 90 services to determine whether they provide information about the data deletion process.

We find that each service has a privacy policy and 85 (94%) of them inform the user that they have the right to delete their data. 59 (66%) of the services instruct the user on how to execute this right. 30 of them state that in order to execute one of the rights of the data subject, they need to contact customer support or the Data Protection Officer of the service. 9 services offer a dedicated web form that can be used to trigger a Right to Erasure request and 20 services state that a user can request the erasure of their data simply by clicking a "close account" button (or similar) in the account settings.

Interestingly, we can see a difference in compliance rates when comparing the overall sample to the services that explicitly state that the erasure can be requested by clicking a button. In the overall sample, 19 out of 62 services where the deletion was requested by clicking a button, did not erase or anonymize all personal data. However, only 3 out of the 20 services that state that the deletion can be requested by clicking a button were found to be non-compliant.

Regarding information on the actual deletion process, we find that almost all services do not provide information on the deletion process that goes beyond quoting Art. 17 GDPR. There are only 3 services that provide detailed information in their privacy policies on the deletion process on their platform. These services give an overview on the data that is erased and the data that is anonymized instead. Additionally, they point out the consequences that follow with a data erasure, e.g., losing access to the online account and user-generated content.

5.3 Questionnaire

We have seen that ensuring that personal data is properly deleted is not a trivial task and leaves a lot of questions unanswered. Frequently, privacy policies just inform the user of their rights and are not very transparent in regards to what happens to the user's data, e.g.,

after a Right to Erasure request. Some open questions include:

- What kind of data may be anonymized, rather than erased?
- Does the data controller just comply with the GDPR and therefore erases just personal data or does the data controller erase additional data as well?
- How is it ensured that data is deleted from third parties?
- Is a "delete account" button equivalent to a formal Right to Erasure request?

Therefore, in order to take a deeper look at the Right to Erasure – and how data controllers deal with data erasure in general – a compact questionnaire was sent out to the 90 digital platforms via email by one of the authors of this paper in July 2020. The questions, the categorized answers, and the number of observations for each category can be found in Appendix B.

We received a total of 56 replies of which 31 primarily directed us towards their privacy policy. Those replies were excluded in our results. The other 25 replies were from 14 data controllers who answered the questions individually and 11 data controllers who did not answer the questions individually but rather wrote a text that was somewhat related to the questions asked. It should be noted that these data controllers did not necessarily answer all or even most of our questions but were still included in the results when they did answer a specific question as the answer might contain useful information.

The data controllers' answers to each question were categorized by the author who sent out the set of questions. Then, a second author of this paper analyzed a subset of data controllers and assigned their answers to the same categories; in this way the inter-rater reliability could be determined. The percentage of agreement was 84.7%. For mismatches, the authors discussed the cases and made a joint decision on the categorization.

Implications of a Right to Erasure Request

11 data controllers (79%) stated that they only delete personal data, while 3 (21%) stated that they also delete other data, which can, for example, be other information entered in the account or usage data. With 13 (76%) responses, a majority stated that personal data is primarily deleted but some data might instead be anonymized. It was not always stated what kind of data is anonymized, but we frequently read that public posts or the username would be anonymized. Surprisingly, contrary to the findings in the results section, no data controller mentioned that they delete public posts. One data controller mentioned that, when they process a Right to Erasure request, they try to anonymize as much personal data as possible as far as permitted under law. The data controller mentioned that this enables them to maintain consistency in their handling of personal data. The argument was given that the principles of data protection under GDPR do not apply to anonymized data and therefore data anonymization has the same effect as an erasure.

Furthermore, data that data controllers are required to keep by law can remain. Point (c) of Art. 6(1) GDPR and point (b) of Art. 17(3) state that data controllers can process data that is necessary for compliance with a legal obligation and that this kind of data is exempt from erasure [8]. For example, we were informed that invoices must be kept by German companies for 10 years for tax purposes. A total of 13 data controllers mentioned that they have to keep data that is required by law.

Data Deletion from Third Parties

12 (67%) platforms told us that they inform third parties or other data processors of a user's Right to Erasure request, while 1 (6%) company stated that they do not directly inform third parties as deleted data is automatically cascaded for those. The way we understood this is that this data controller has a service, which third parties refer to, and when the data controller deletes certain data from it, the third party automatically loses access to this specific data. We got 3 (17%) replies where it is stated that data is not being shared with any third parties in the first place and 2 (11%) responses did not properly answer the question or missed the point.

"Delete Account" Button Equivalent to Formal Art. 17 Request?

Lastly, and probably most importantly, we wanted to know whether a dedicated "delete my account" button somewhere in the account settings of a platform is considered the same as a formal Art. 17 request. In total, we got 16 responses from platforms that featured such a button. In 1 (6%) of those responses the question was left unanswered. 3 (19%) told us that deleting

data through such a button is different from deleting data through a formal Right to Erasure request, while 12 (75%) stated that these methods are equivalent. Two of the 12 data controllers even mentioned that deleting the account via a dedicated setting in the account is the preferred way, one of them stating that the user should only send them a Right to Erasure request via email if they were in contact with the data controller in some other way in addition to just using the website, e.g., via postal mail. A different data controller stated that the implementation of such a button within the account fulfills the privacy by default (Art. 25 GDPR) principle. Out of the 3 data controllers who mentioned that the button is not equivalent to a Right to Erasure request, two stated that, while the account and its associated personal data will be deleted, some personal data may remain at third parties or in other databases, e.g., the newsletter database. The third data controller informed us that the information is deleted from their database but the username will not be anonymized. In order to have the username anonymized, users should contact them via the support center form or email.

6 Discussion

As our analyses show, data erasure practices vary substantially across services. We therefore examine reasons for these differences, further implications and conflicts, and possible ways to harmonize the services' erasure practices.

6.1 Lack of Information and Differences in Processing of Requests

For a majority of services, no non-compliant data erasure processes can be observed given the information that we have available. The compliance rate with GDPR Art. 17 is, therefore, higher than the compliance rates found in comparable studies on Art. 15 or Art. 20 (see, e.g., [15, 29, 31]). However, these differences might also stem from the nature of data erasure, i.e., the unobservability of the actual erasure, as a user cannot verify that data really has been deleted from the internal systems of a service. Furthermore, we have observed that services are in general reluctant to provide information on what happens when a data erasure request is received and on whether this request is forwarded to third parties the data has been shared with. With a small number of exceptions, neither privacy policies nor additional communication via email provide information on the scope of the erasure. Therefore, a user who requests an erasure of their data does not precisely know what data might remain. Refined regulation is needed that obliges services to provide more information on their erasure processes, e.g., in the respective privacy policies. To verify that data erasure is actually carried out, Data Protection Authorities could order services to provide information on their data erasures (see [32] for a similar process) or conduct random on-site inspections.

In addition to missing information, we find that the experience of requesting a data erasure varies widely between services. There is no one clear way with which data erasure can be requested. We see differences in the method of the initial request (request buttons, web forms, sending an email to the Data Protection Officer), as well as the duration, the existence of transition periods where the erasure can (unintentionally) be cancelled, and the scope of the erasure. These findings are consistent with those of Habib et al. who report inconsistent locations of privacy choices across services and a difficulty in executing them from a user's perspective [33, 34].

In particular, the request method is subject to further research and possibly further regulation. Our findings suggest that some services treat requests received via the click of an erasure button in a different way to formal requests under Art. 17 GDPR sent via email. Here, more insight is needed about whether these requests are equivalent from a legal perspective.

We have also seen inconsistencies in the scope of the data erasure, especially in respect of newsletter subscriptions. As all our subscriptions were started from within the user account, we hold the view that an erasure of user data also includes data on newsletter subscriptions. However, as seen in Section 5, some data controllers explicitly separate account data from newsletter data and therefore require an additional erasure of newsletter subscriptions – especially when the original data erasure was requested via a button click. This example emphasizes a need to provide more precise regulations or guidelines on the scope of data erasure.

6.2 Data Erasure in Conflict with Legitimate Interests and Other Rights

A Right to Erasure request can conflict with a service's legitimate data processing interests on the one hand and

fundamental rights, such as freedom of expression, on the other hand.

A data erasure request does not necessarily cause the termination of a contract. In cases where a contract is not terminated, it can be in the legitimate interest of a company to keep user data, e.g., for billing purposes. While there was no service in our sample that required payment, even a free registration implies the formation of a contract. Therefore, services could have argued that they were not able to delete user data as we had not explicitly terminated the contract. Nevertheless, all services in our sample where the data erasure was successful treated the erasure request as an implicit contract termination and none of the services where the erasure was not successful stated a missing contract termination as a reason.

Regarding possible conflicts of data erasure with fundamental rights, the Wikimedia Foundation reportedly receives several Right to Erasure requests per year, but granted none of them in 2020 as "[e]veryone should have free access to relevant and neutral information of public concern; delisting and removing such content from the internet harms our collective ability to remember history and understand the world" [35].

On social networks or services such as Wikipedia, personal data is often shared or entered by third parties, resulting in interdependent privacy problems [36]. In contrast, in our study, all personal data was entered by the first party only, i.e., by the (fictional) person themself. Nevertheless, for public data such as blog posts or posts on social networks, a service might use similar arguments to avoid data erasure.

Surprisingly, only one service in our sample directly informed us that it could not execute the data erasure for one of these reasons. Indeed, public data was typically either deleted or anonymized to ensure compliance with GDPR Art. 17. This finding indicates that services weigh the Right to Erasure higher than possibly conflicting other rights, possibly in order to avoid any fines for non-compliance. Further research is needed to determine whether this practice also exists when a user requests the deletion of personal data concerning them, which was entered by another user.

6.3 Best Practices

From a user's perspective, there is a high level of heterogeneity in the processing of data erasure requests. This makes it difficult to keep track of the state of each erasure request and the actual scope of erasure. We therefore suggest that the processes from making the request until erasure should be harmonized.

A majority of services already offer a dedicated account erasure button. The availability of this request method increases accessibility for users and can reduce the workload for services in processing written requests. Services should indicate in their privacy policies whether they handle erasure requests via button in an equivalent way to formal requests under Art. 17.

Most of the services do not inform the user about the scope of data erasure. Here, in particular, we found a discrepancy in the erasure of newsletter registration data. When a data erasure is requested, the default behavior should be to delete all personal data where possible or to give users choice on what data to delete. If data remains, users should be informed what data remains and why it cannot be deleted.

Online services' authentication processes can be vulnerable to data breaches as has been shown for the GDPR's Right of Access [37, 38]. For data erasure, unauthorized requests can cause users to suffer a loss of data. Services therefore need to make sure that only authorized users can request an erasure of their data. It should be best practice to require at least one additional authentication step before executing an erasure request. In our sample, we found that only 41% of services require such an additional authentication step (e.g., an email confirmation in addition to being logged in).

The time until deletion and the existence of a transition period differs between services. A transition period can be an additional protection against unauthorized erasure, as the process can be stopped within the given period. To achieve a reasonable compromise between speed of execution and protection of data, an appropriate transition period could have a length of 30 days. The information on this transition period should be formulated in a neutral way and not used for pressuring users into cancelling their requests.

Apart from these procedural issues, services need to consider which data they can delete upon receiving a data erasure request. The GDPR only mandates an erasure where technically feasible, so personal data stored in log files or backups may be exempt from immediate erasure. However, if personal data were kept in backups, services would need to keep track of erasure requests for execution when restoring a backup [39]. As suggested by Politou et al. [40], cryptographic erasure can be an alternative to deleting data from backups [41].

7 Conclusion

In a digital world where services collect an increasing amount of data with data-driven business models playing an ever more import role, it becomes crucial to empower users in their relationship with online services. Privacy regulation such as the EU's General Data Protection Regulation [8] aims to achieve that by granting users certain rights for gaining control over their data.

The most basic scenario for controlling data is to demand the erasure of it from an online service. For this data erasure scenario, the GDPR's Article 17 ("Right to Erasure"), which gives the user an explicit right to delete their data, and Article 6 ("Lawfulness of processing"), which restricts the grounds on which a service is allowed to process data, are of particular relevance.

Therefore, we studied how data can be deleted from services by a user. As in general, typical users would rather use integrated erasure functionalities than formally request an erasure under Article 17 GDPR, we used the most accessible approach wherever possible. We then verified if publicly visible personal data remained and also used requests under Article 15 GDPR ("Right of Access by the Data Subject") to check if services answer with data that should already have been deleted.

We find that when data erasure is requested at the click of a button, personal data are substantially more often not completely deleted compared to formal data erasure requests under Article 17. This raises the legal question of whether the provisions of the GDPR's Right to Erasure do only apply when formally referenced or in all cases in which a user requests the erasure of their account. Further investigations based on the privacy policies of the services and a questionnaire sent to the Data Protection Officers yield mixed results. Both services which explicitly treat "button clicks" and formal requests in an equivalent way, and services which highlight differences between the two approaches, exist.

The sample in our study consists of 90 services of which 56 are based in Germany and 63 are amongst the most popular ones with a SimilarWeb rank better than 3000. Therefore, the results should not be generalized until they are replicated with different samples, covering the groups of services that are under-represented in our study. As we requested data erasure just once from each service, we either requested it at the click of a button or by using a formal request under Art. 17 GDPR. While this procedure allowed us to analyze a higher number of services, it comes with the risk of a potential bias when comparing button clicks to formal requests. Therefore, both legal and more empirical research is needed to analyze the equivalence of user-friendly and more formal ways of deleting data.

Our study does not explicitly focus on data collected by third parties. While there was no indication of uncompliant behavior of third parties, further research with an adapted methodology is needed.

Acknowledgments

We would like to thank the anonymous reviewers as well as Katharina Hartinger, Moritz Hennemann, Kai von Lewinski, Carmen Loefflad, Stefan Mager, and Frederike Zufall for helpful feedback. We further are grateful for funding support from the Bavarian Research Institute for Digital Transformation (bidt). Responsibility for the contents of this publication rests with the authors.

References

[1] Iris van Ooijen and Helena U. Vrabec. Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of Consumer Policy*, 42(1):91–107, 2019.

[2] Eugenia Politou, Efthimios Alepis, and Constantinos Patsakis. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, 4(1), 2018.

[3] European Commission. Special Eurobarometer 431, 2015. Available at: http://data.europa.eu/88u/dataset/s2075_83_1_431_eng.

[4] Eric J. Johnson, Steven Bellman, and Gerald L. Lohse. Defaults, Framing and Privacy: Why Opting In-Opting Out1. *Marketing Letters*, 13(1):5–15, 2002. ISSN 1573-059X.

[5] Maciej Sobolewski, Joanna Mazur, and Michał Paliński. GDPR: A step towards a user-centric internet? *Intereconomics*, 52(4):207–213, 2017.

[6] Spyros Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64:122–134, 2017. ISSN 0167-4048.

[7] Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM Conference on Electronic Commerce*, page 38–47. Association for Computing Machinery, 2001.

[8] European Parliament and Council. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

(General Data Protection Regulation), 2016. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04, last accessed: February 14th, 2022.

[9] Sophie Kuebler-Wachendorff, Robert Luzsa, Johann Kranz, Stefan Mager, Emmanuel Syrmoudis, Susanne Mayr, and Jens Grossklags. The Right to Data Portability: Conception, status quo, and future directions. *Informatik Spektrum*, 44 (4):264–272, 2021.

[10] MyHeritage. Myheritage statement about a cybersecurity incident, 2018. Available at: https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/, last accessed: February 14th, 2022.

[11] Lucas Ropek. 70,000 SSNs, 600,000 credit card records leaked after stolen-data hub gets hacked, 2021. Available at: https://gizmodo.com/70-000-ssns-600-000-credit-card-records-leaked-after-s-1846638234, last accessed: February 14th, 2022.

[12] Court of Justice of the European Union. Judgment in Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH, 2019. Available at: https://curia.europa.eu/juris/documents.jsf?num=C-673/17, last accessed: February 14th, 2022.

[13] Wanda Presthus, Hanne Sørum, and Linda Renate Andersen. GDPR compliance in Norwegian companies. *Norsk Konferanse for Organisasjoners Bruk at IT*, 26(1), 2018.

[14] Janis Wong and Tristan Henderson. The right to data portability in practice: Exploring the implications of the technologically neutral GDPR. *International Data Privacy Law*, 9 (3):173–191, 2019.

[15] Emmanuel Syrmoudis, Stefan Mager, Sophie Kuebler-Wachendorff, Paul Pizzinini, Jens Grossklags, and Johann Kranz. Data portability between online services: An empirical analysis on the effectiveness of GDPR Art. 20. *Proceedings on Privacy Enhancing Technologies*, 2021(3):351–372, 2021.

[16] Dominik Herrmann and Jens Lindemann. Obtaining personal data and asking for erasure: Do app vendors and website owners honour your privacy rights? In Michael Meier, Delphine Reinhardt, and Steffen Wendzel, editors, *Sicherheit 2016 - Sicherheit, Schutz und Zuverlässigkeit*, pages 149–160. Gesellschaft für Informatik e.V., 2016.

[17] Subhadeep Sarkar, Jean-Pierre Banâtre, Louis Rilling, and Christine Morin. Towards enforcement of the EU GDPR: Enabling data erasure. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 222–229. IEEE, 2018.

[18] Miriam Kelly, Eoghan Furey, and Juanita Blue. GDPR Article 17: Eradicating personal identifiable information & achieving compliance in a hybrid cloud. In *2019 30th Irish Signals and Systems Conference (ISSC)*, pages 1–6. IEEE, 2019.

[19] Michele Finck. Blockchains and Data Protection in the European Union. *European Data Protection Law Review (EDPL)*, 4(1):17–35, 2018.

[20] Ugo Pagallo, Eleonora Bassi, Marco Crepaldi, and Massimo Durante. Chronicle of a clash foretold: Blockchains and the GDPR's right to erasure. In *JURIX*, pages 81–90, 2018.

[21] Knud Bielefeld. Top 500 der beliebtesten Vornamen des Jahres 2018, 2019. Available at: https://www.beliebte-vornamen.de/jahrgang/j2018/top-500-2018, last accessed: February 14th, 2022.

[22] Verein für Computergenealogie (CompGen) e. V. Die 1000 häufigsten Familiennamen in Deutschland, 2019. Available at: http://wiki-de.genealogy.net/Die_1000_h%C3%A4ufigsten_Familiennamen_in_Deutschland, last accessed: February 14th, 2022.

[23] This person does not exist, 2019. Available at: https://thispersondoesnotexist.com/, last accessed: February 14th, 2022.

[24] SimilarWeb LTD. Top websites ranking, 2019. Available at: https://www.similarweb.com/top-websites/, last accessed: February 14th, 2022.

[25] Datenanfragen.de e. V. Musterbrief für Anträge auf Löschung nach Art. 17 DSGVO („Recht auf Vergessenwerden"), 2018. Available at: https://www.datenanfragen.de/blog/musterbrief-dsgvo-anfrage-loeschung, last accessed: February 14th, 2022.

[26] Verbraucherzentrale NRW e.V. Musterbrief: Löschung personenbezogener Daten, 2019. Available at: https://www.verbraucherzentrale.de/sites/default/files/2019-10/Loeschung_nach_Art._17_DSGVO.pdf, last accessed: February 14th, 2022.

[27] Information Commissioner's Office. Preparing and submitting your subject access request, 2020. Available at: https://ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data/preparing-and-submitting-your-subject-access-request/, last accessed: February 14th, 2022.

[28] Verbraucherzentrale NRW e.V. Musterbrief: Auskunft und Kopie der personenbezogenen Daten, 2019. Available at: https://www.verbraucherzentrale.de/sites/default/files/2019-10/Auskunft_nach_Art._15_DSGVO.pdf, last accessed: February 14th, 2022.

[29] Jacob Leon Kröger, Jens Lindemann, and Dominik Herrmann. How do app vendors respond to subject access requests? A longitudinal privacy study on iOS and Android Apps. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ARES '20, pages 1–10. Association for Computing Machinery, 2020.

[30] European Commission. Special Eurobarometer 487a, 2019. Available at: http://dx.doi.org/10.2838/579882.

[31] Tobias Urban, Dennis Tatang, Martin Degeling, Thorsten Holz, and Norbert Pohlmann. A study on subject data access in online advertising after the GDPR. In Cristina Pérez-Solà, Guillermo Navarro-Arribas, Alex Biryukov, and Joaquin Garcia-Alfaro, editors, *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, Lecture Notes in Computer Science, pages 61–79. Springer International Publishing, 2019.

[32] Mobile security updates: Understanding the issues, February 2018. Available at: https://www.ftc.gov/reports/mobile-security-updates-understanding-issues, last accessed: February 14th, 2022.

[33] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. An empirical analysis of data deletion and Opt-Out choices on 150 websites. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*,

pages 387–406. USENIX Association, 2019.

[34] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–12. Association for Computing Machinery, 2020.

[35] Requests for content alteration and takedown, April 2021. Available at: https://wikimediafoundation.org/about/transparency/2020-2/requests-for-content-alteration-and-takedown/, last accessed: February 14th, 2022.

[36] Yu Pu and Jens Grossklags. Towards a Model on the Factors Influencing Social App Users' Valuation of Interdependent Privacy. *Proceedings on Privacy Enhancing Technologies*, 2016(2):61–81, 2016.

[37] Mariano Di Martino, Pieter Robyns, Winnie Weyts, Peter Quax, Wim Lamotte, and Ken Andries. Personal information leakage by abusing the GDPR 'right of access'. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 371–385. USENIX Association, 2019.

[38] Mariano Di Martino, Isaac Meers, Peter Quax, Ken Andries, and Wim Lamotte. Revisiting Identification Issues in GDPR 'Right Of Access' Policies: A Technical and Longitudinal Analysis. *Proceedings on Privacy Enhancing Technologies*, 2022(2):95–113, 2022.

[39] Vincenzo Mangini, Irina Tal, and Arghir-Nicolae Moldovan. An empirical study on the impact of GDPR and Right to be Forgotten - Organisations and users perspective. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ARES '20. Association for Computing Machinery, 2020.

[40] Eugenia Politou, Alexandra Michota, Efthimios Alepis, Matthias Pocs, and Constantinos Patsakis. Backups and the Right to be Forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, 34(6):1247–1257, December 2018.

[41] Dan Boneh and Richard J. Lipton. A Revocable Backup System. In *Proceedings of the 6th USENIX Security Symposium (USENIX Security)*. USENIX Association, July 1996.

A Default Request Emails

For the Art. 15 and 17 requests, based on examples from established online sources [25–28] separate templates were created. For the follow-up emails, no specific templates were created because the responses were individualized. Therefore, two examples of follow-up emails (i.e., one for non-anonymization and one for when data remained after an Art. 15 request) are provided below.

A.1 Template: Article 17

Erasure of personal data as stated in Art. 17 General Data Protection Regulation (GDPR)

Hereby I make a request for the erasure of my personal data without undue delay as stated in Art. 17(1) GDPR. Without undue delay, I request the erasure of all my personal data which is stored by you.

If I have given my consent to the processing of my personal data (e.g. according to point (a) of Art. 6(1) or point (a) of Art. 9(2)), I hereby object to the processing of my personal data.

Furthermore, I object to the processing of my personal data as stated in Art. 21 GDPR. This also applies for profiling.

If you have disclosed my personal data to others, I demand that you inform controllers, that are processing my personal data, of the request for the erasure of all my personal data without undue delay.

I request confirmation without undue delay that all my personal data has been erased from you and that you have informed other controllers by sending them a copy of my request for the erasure of all my personal data without undue delay.

A.2 Template: Article 15

Right of access by the data subject request (Art. 15 GDPR)

Hereby I request whether personal data concerning me are being processed. If this is the case, I request access to the following information:

a) the purposes of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the personal data are not collected from the data subject, any available information as to their source;

h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject as stated in Art. 15(1) GDPR.
If personal data is transferred to a third country or to an international organisation, I want to be informed of the appropriate safeguards pursuant to Art. 46 GDPR relating to the transfer.
Please provide me with a copy of the personal data undergoing processing without undue delay and within one month the latest as stated in Art. 12(3) GDPR.
Contact me should you need further information from me to process this request.

A.3 Examples for Follow-Up Messages

For Non-Anonymization

I would like to ask why there are still visible public posts after the account has been deleted? My username and profile picture are still shown. This counts as personal data.

For When Data Remained

I used to have an account on your website but I requested a full erasure earlier this year. I got a confirmation that my account was deleted. Therefore, I would like to ask why personal data remained?

B Questionnaire

A questionnaire on data erasure practices was sent to 90 Data Protection Officers via email. The questions and categorized answers are listed below.

1. If I delete certain data in my account on your website (e.g. my name), will that data be permanently deleted from your database or does it remain?
Data gets deleted: 10
User cannot delete data within account because it is essential to provide services: 3
Question was not properly answered: 2

2. If I request an erasure of my data as stated in Art. 17 GDPR, what kind of data will be deleted? Only personal data or further data as well? What kind of data is that?
Personal data only: 11
Personal data and further data as well: 3

3. Is certain data going to be anonymized instead of deleted? If yes, what kind of data?
Deletion only, no anonymization: 3
Primarily deletion, some anonymization: 13
Primarily anonymization: 1

4. What kind of data remains?
Certain anonymized data: 5
Data required by law: 13
Public posts: 6
Log files: 3
No data remains: 2

5. What happens with usage and behavioral data?
It gets deleted: 5
Partially deleted, partially anonymized: 1
It gets anonymized: 4
No profiling or usage data in the first place: 3
Question was not properly answered: 3

6. If your website offers the creation of a public profile, public posts/comments and private messages, what happens with that data when I request an erasure of my data?
Anonymized: 8
May remain (not specified whether it gets anonymized or not): 3
No public profiles, public posts/comments or private messages on website: 7

7. Is there a way in which I, as a user, can make sure that my data was deleted properly?
User gets confirmation of successful deletion: 5
Login does not work anymore: 8
Article 15 request would be negative: 4
Public user profile page is not accessible anymore: 1
User does not get any more newsletters: 1
Only Data Protection Authority can check: 1
No: 1

8. If you transmit my data to third parties, how is it ensured that those delete my data as well?
Third parties and other data processors are informed: 12
Data is being cascaded for third parties: 1
Data is not being shared with third parties: 3
Question was not properly answered: 2

9. In the account settings on your website you offer a way to delete the account. Does that comply with Art. 17 GDPR or do you have to submit such a request by other means, e.g. via email?
Data deletion button within account is equivalent to a formal Right to Erasure request: 12
Data deletion button within account is not equivalent to a formal Right to Erasure request: 3
Was asked but question was not answered: 1
Was not asked because there is no data deletion button within account: 9