# Feedbacks on Guidelines 01/2022 on data subject rights -Right of access

Cédric Lauradoux, Cristiana Santos

# Feedbacks on Guidelines 01/2022 on data subject rights - Right of access

Cédric Lauradoux*,
Cristiana Santos†

March 11, 2022

## Introduction

Since the application of the GDPR, legal scholars and computer scientists have identified several issues with the right of access:

1. Organizations are not prepared to answer subject access requests (see [AD18]).
2. Organizations are using weak methods to verify subject access requests (see [BMMS20, DMQ+]).
3. European Data Protection Authorities (DPAs) are providing different recommendations (see [BFB+19]) and they request non proportional or unnecessary documents to verify the identity of the requester [ALS22].

We note that the EDPB guidelines [Eur22] address the first two issues. We hope that these Guidelines will shape and homogenize the recommendations published by all European DPAs in their websites and help in the complaining process. Whereas the present guidelines consist of a significant step to the exercise of the right of access, they need to clarify several important elements discussed in the following sections.

## Contents



*Univ. Grenoble Alpes, Inria, France, cedric.lauradoux@inria.fr
†School of Law, Utrecht University, The Netherlands, c.teixeirasantos@uu.nl

# 1 On GDPR-compliant processing of subject access requests

The processing of subject access requests is critical for data controllers as they need to comply with the GDPR. Data controllers need confirm in their privacy impact assessment (PIA) that they are handling securely subject access requests, and that they consider the main risks of these access requests. Boniface et al. [BFB+19] have considered the three main risks associated with the processing of subject access requests. Data controllers need to address them explicitly in their PIA.

- *Privacy invasion* occurs when a data controller is perceived as *malicious* and aims to exploit the authentication as a method to obtain more information from the data subject, incurring into *abusive identity checks*.
- *Denial of access* occurs when the data controller refuses to allow a legitimate data subject to access her data. Denial of access is often reported in the works of [AMMG17, AFC17, AD18] testing the access right.
- *Data breach* occurs when a data controller discloses information of a data subject to someone else (a third party) than the concerned subject. Unauthorized disclosure is qualified as a data breach, under Article 4(12) of the GDPR. A concrete instance of a data breach is named *impersonation*. *Impersonation* occurs when a malicious individual is able to impersonate a data subject by forging the identity verification enforced by the data controller.

A data controller can indicate that the processing of subject access requests is not *privacy invasive* by demonstrating that all the elements required to verify the request are *relevant* and *proportional*. Similarly, a data controller can demonstrate that it has minimized the risks of data breach by using state-of-art authentication schemes, to avoid *impersonation* attacks, and secure communications channel (to avoid eavesdropping attacks). However, currently, many data controllers process subject access requests carelessly, as demonstrated in several studies [DRW+19, Pav19, CHP19].

Several studies identified techniques that bypass existing SAR verification practices through *impersonation*. In [Pav19], the authors lure data controllers to use weak identifying documents or authentication procedures. To bypass SAR verification, they created and sent a vague SAR letter to organizations. Out of 150 organizations, 24% disclosed personal data. Cagnazzo et al. [CHP19] found that a third party adversary can abuse the functionality provided by a company to update a subject's address (both email and residential addresses). Subsequently, this adversary could then request access to the data from this new address. Out of 14 organizations tested, 10 shared personal information and 7 of these contained sensitive data. Di Martino et al. [DRW+19] demonstrated that by using publicly available information, such as the email address, date of birth and profile pictures, controllers can be persuaded to disclose sensitive personal data of the data subject to a malicious third-party. Out of the 55 tested organizations, 15 thereof were leaking personal data to an unauthenticated third-party consisting, among others, of financial institutes such as banks. The researchers persuaded the controllers using the following techniques:

- Photoshopping an ID card by replacing the date of birth, name and profile picture of the subject, while censoring the National Register Number.
- Spoofing an email address by exploiting weak email encryption measures, making an email address look exactly the same as if they are sent from the legitimate data subject.
- Performing social engineering methods to make the controller believe that their account is 'hacked' and they need 'quick access to help them fix the problem'.

In this study, each vulnerable data controller was contacted with advice on how to improve their process to reduce the risk of data breaches through the 'Right of Access'.

In 2021, Di Martino et al. [DMQ+] showed that most organizations did not improve their policies, as around 50% of the previously vulnerable organizations still leaked personal data from other subjects. In several interviews conducted with these organizations, they referred to the advice given by their national DPAs and sometimes exhibited signs of security misconceptions – which was also confirmed by prior work [UTD+19]. Other works [BMMS20, KLH20, CHP19] also confirmed that these potential threats are practical to conduct in real-life cases.

**Recommendation 1.** *The guidelines could recommend data controllers to demonstrate in their PIA that their processing of subject access requests addresses the main risks. It will significantly help data controllers to implement robust and secure procedures to deal with subject access requests. It will also help Data Protection Authorities' auditing.*

## 2 On the eligibility of subject access request

The territorial scope of the GDPR (Article 3) has implications for the right of access and requires some clarifications from these guidelines. Article 3.2 explains how the GDPR applies outside of the EU:

> 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) the monitoring of their behavior as far as their behavior takes place within the Union.

A data controller established in the EU can process the data of subjects who are in the Union, which are either European residents or non European residents. Data subjects which are European residents can submit SARs to this data controller. When the data controller receives an access request based on Article 15, it needs to check if the data subject is a European resident or not. This scenario has been encountered in the work of Boniface et al. [BFB+19].

**It is important to clarify in the guidelines what are the elements that can be requested by a controller to verify whether the data subject is a European resident to prevent abusive identity check attacks**. Moreover, this step needs to be included on the flowchart provided in the Annex.

**Recommendation 2.** *The guidelines need to specify how data controllers outside the European Union verify that a request has been sent by an European resident. This is particularly important because the guidelines need to address the issues that controllers may encounter.*

## 3 On Requesting ID document for identity verification

Many researchers [AD18, BFB+19, DRW+19, DMQ+] observed that data controllers often asked for the copy of an identification document like an ID card or a passport. This practice is criticized in the guidelines at several paragraphs. **Identity proofing** based on identification documents is a technique used by authorities like police or customs to control the identity of individuals. It is based on three assumptions:

**Assumption 1.** *The **verifier** (authority) and the **prover** (individual) meet physically.*

**Assumption 2.** *The prover owns an identification document which was created by a trusted authority.*

**Assumption 3.** *The provider is able to check that the prover's face (or any other biometrics) matches the photo on the document and that the document is official.*

Each assumption ensures an important property for the verification. Assumption 1 ensures the liveness of the verification. Assumption 2 ensures that the document is unique and that there is a low probability of document forgery. Assumption 3 binds the prover with the document. If any of those assumptions is not verified, then this verification technique is not safe.

## 3.1 Using ID documents during remote verification

If identity proofing is proportionate, relevant and if the data controller and data subject agree to meet physically, then the verification based on ID documents is appropriate. However, regarding access requests by electronic means, Article 15 of the GDPR stipulates that

> *Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.*

Therefore, it is likely that all the interactions between the controller and the subject are remote. This breaks Assumption 1 and data controllers should not use classical verification based ID documents. In this case, other techniques need to be used to verify the identity of the subject sending the request.

Remote identity proofing protocols are possible and have been discussed and analyzed by ENISA in [ENI21, ENI22].

The DPA of the German Land Baden-Württemberg[1] is actually recommending the use of remote identity proofing. It recommends the intake of a video along with the producing of the ID card, while admitting this technique might pose concerns in terms of data collection. The DPA recommends, in such cases, allowing for a real-time video chat with the requesting person. The use of video in establishing the identity of the requested person could pass the test of proportionality when the data requested is particularly sensitive, such as e.g. medical data.

**Recommendation 3.** *The guidelines should mention explicitly remote identity proofing and explain when this kind of technique has to be used. The guidelines are not precise enough and there is a high risk that data controllers keep using unsafe identity proofing techniques.*

## 3.2 Using ID documents for special categories of data

73. It should be emphasised that using a **copy of an identity document** as a part of the authentication process **creates a risk for the security of personal data and may lead to unauthorised or unlawful processing, and as such it should be considered inappropriate, unless it is strictly necessary, suitable, and in line with national law**. In such cases the controllers should have systems in place that ensure a level of security appropriate to mitigate the higher risks for the rights and freedoms of the data subject to receive such data. It is also important to note that identification by means of an identity card does not necessarily help in the online context (e.g. with the use of pseudonyms) if the person concerned cannot contribute any other evidence, e.g. further characteristics matching to the user account.
77. (...) under certain circumstances, verification on the basis of an ID may be a justified and proportionate measure, for example for entities **processing special categories of personal data** or undertaking data processing which may pose a risk for data subject (e.g. medical or health information) (...).

"Necessity" and "suitability" of the request of ID document are principles that need further interpretation criteria, as the ones proposed below, to be assessed in a case by case analysis by the data controller, as explained by the Irish DPA [2]:

- **sensitivity of data**: where the category of information relating to that individual is **sensitive in nature** and where the information on the official ID can be corroborated with the categories of personal data and its identifiers already held and known by the data controller, such as a chosen username, address, an email address, a cookie or mobile identifier.

[1] German Land Baden-Württemberg DPA https://www.lda.brandenburg.de/sixcms/media.php/9/TB_2020_web.pdf
[2] Irish DPAhttps://media-exp1.licdn.com/dms/document/C4E1FAQE71sheLwITPQ/feedshare-document-pdf-analyzed/0/1645691176304?e=1646481600&v=beta&t=Cs1G5taNCxQ3USPGLsu2vReO1maKaI3GPv-lznrO8Tk

- **non-sensitivity of data**: where no special category personal data is held, confirmation of other data can be sufficient, e.g. the postal address, email account.
- **subsidiary data**: an ID document contains sensitive information on a data subject [3]. As such, it should only be asked as a last recourse. The identity of the data subject could be verify based on other user specific information, such as subscription details, name, email, postal address, phone number, phone call [DRW+19, BMMS20].

**Recommendation 4.** *The guidelines need to provide operationable criteria on the necessity and suitability of the request of ID documents in Paragrapg 73.*

### 3.3 Blackening information on ID documents

Hiding information on a copy of an ID card seems to be appropriate to implement the proportionality principle. Indeed, the data controller does not need to learn information on the data subject making the request that it does not know already. Blackening information is discussed in the guidelines:

> 75. In any case, information on the ID that is not necessary for confirming the identity of the data subject, such as the access and serial-number, nationality, size, eye colour, photo and machine-readable zone, may be **blackened or hidden** by the data subject before submitting it to the controller, except where national legislation requires a full unredacted copy of the identity card (see para. 77 below). Generally, the date of issue or expiry date, the issuing authority and the full name matching with the online account are sufficient for the controller to verify the identity, always provided that the authenticity of the copy and the relation to the applicant are ensured. Additional information such as the birth date of the data subject may only be required in case the risk of mistaken identity persists, if the controller is able to compare it with the information it already processes.

However, blackening information on an ID document hampers the security of the verification and it breaks somehow Assumption 3. Blackening out information on an ID document can be assimilated to document tampering. It complicates the task of the person in charge of verifying that the document is authentic, because the document has been edited by the subject. Adversaries can edit an existing document to forge a new one to impersonate a subject to a data controller. A person in charge of verifying a request (typically a DPO) will have to distinguish genuine ID documents blackened by legitimate subjects from those forged by an adversary.

The findings of the study conducted by Bulafieri in 2020 [BMMS20] on verification procedures of ID documents are particularly relevant with respect to this question. The ID card of one of the authors was modified to appear as being clearly tampered with (i.e., false), with the first ID card being redacted (hiding the non-required information as per this paragraph) and, in case it was not accepted, then the non-redacted ID card would be used. Out of the 25 controllers to whom the ID card was sent to, 21 accepted the ID card, while 4 refused the redacted ID card, but only to then accept the non-redacted one; therefore, they were able to receive data each time while using the tampered document. This study concluded that serious doubts arose regarding whether controllers had the correct technology and expertise to conduct an efficient assessment of the veracity of ID cards. **The EDPB may consider assessing which verification procedures of ID documents are needed to avoid data breaches**.

**Recommendation 5.** *The guidelines should change its position concerning blackening information on ID documents. Blackening information cannot be recommended because it weakens the verification of the ID documents. Such practice should be discouraged and should disappear.*

[3] Dutch DPA https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_dpg.pdf

### 3.4 Transferability

> 78 - Taking the above into account, where an ID is requested (and this is both in line with national law and justified and proportionate under the GDPR), **the controller must implement safeguards to prevent unlawful processing of the ID**. Notwithstanding any applicable national provisions regarding ID verification, this may include not making a copy or deletion of a copy of an ID immediately after the successful verification of the identity of the data subject. This is because further storage of a copy of an ID is likely to amount to an infringement, in light of the principles of purpose limitation and storage limitation (Art. 5(1)(b) and (e) GDPR) and any possible national legislation with regards to processing of the national identification number (Art. 87). The EDPB recommends, as good practice, that the controller, after checking the ID card, makes a note e.g. " ID card was checked " to avoid unnecessary copying or storage of copies of ID cards.

Transferability is defined by Menezes, van Oorschot and Vanstone [MvOV96] as the property that a data controller cannot reuse a verification exchange with a data subject sending a request to successfully impersonate the subject to another data controller. This question is partially discussed in the guidelines.

Secure deletion of the copy of ID documents is indeed a method to reduce the risk of later impersonation and to implement transferability.

**Recommendation 6.** *The guidelines should recommend that the procedure used by the data controller respects the transferability property. It ensures that the data controller can not impersonate any subjects sending a request and it minimizes the risks of impersonation in case of a data breach. Transferability is relevant when ID documents are used during the verification but it also applied to any verification method.*

## 4 On additional information and proportionality

### 4.1 Clarification on Recital 64

Recital 64 gives some elements on the amount of information which can be collected in order to verify the identity of subject who requests access.

> Recital 64
>
> 1. The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers.
> 2. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

The second part of the recital needs to be clarified in the view of the elements provided in the previous section. Dedicated verification procedures are needed to verify that a request is legitimate. *These verification procedures are based on data that both the controller and the subject know.* It is important to understand whether or not a data controller can collect data in order to verify potential subject access requests.

Let us consider the case of a data controller who controls a website on which the data subjects gets registered. Data subjects access the website using a login and a password. We consider two different cases. On the first case, the data controller has implemented multiple-factor authentication (MFA) using the phone number of the subjects. The controller has collected the subjects phone numbers for the web authentication. This mechanism can be re-used to verify subject access requests as suggested in the guidelines:

63. (...) insofar as a digital communication channel already exists between the data subject and the controller and without prejudice to Art. 12(6) GDPR, the controllers must implement or **re-use an authentication procedure** in order to ascertain the identity of the data subjects requesting their personal data or exercising the rights granted by the GDPR.

In the second case, the data controller has not implemented multiple-factor authentication. The controller is not asking the subject to provide any data when she registers. However, the data controller wants to verify the identity of the subject using multiple-factor authentication to verify subject access requests. In order to implement MFA, the controller needs to collect the phone number of the subject. Does Recital 64 prevents controllers from collecting these data for the sole purpose of verifying subject access requests.

**Recommendation 7.** *The guidelines should clarify how data controllers can apply Recital 64 when they are implementing their procedures to handle subject access requests.*

## 4.2 Reasonable doubts and the proportionality assessment

62. If the controller has **reasonable doubts** concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject (Art. 12(6))
65. In cases where the controller requests the provision of additional information necessary to confirm the identity of the data subject, the controller shall each time assess what information will allow it to confirm the data subject's identity and possibly ask additional questions to the requesting person or **request the data subject to present some additional identification elements, if it is proportionate** (see section 3.3). **Such additional information should not be more than the information initially needed for the verification of the data subject's identity (authentication)**. In general, the fact that the controller may request additional information to assess the data subject's identity **cannot lead to excessive demands and to the collection of personal data which are not relevant or necessary** to strengthen the link between the individual and the personal data requested
69. (...) if the controller has reasonable grounds for doubting the identity of the requesting person, it may request additional information to confirm the data subject's identity. However, the controller must at the same time ensure that it does not collect more personal data than is necessary to enable identification of the requesting person. Therefore, **the controller shall carry out a proportionality assessment**, which must take into account the type of personal data being processed (e.g. special categories of data or not), the nature of the request, the context within which the request is being made, as well as any damage that could result from improper disclosure. When assessing proportionality, it should be remembered to avoid excessive data collection while ensuring an adequate level of processing security.

The **Proportionality Assessment**, already requested by DPAs [4], is a commendable practice to confirm whether the controller has reasonable doubts on the identity of the requester and make use of less data-driven proofs and thus prevent *abusive identity check risks*. This assessment should be recorded and also given to the data subject.

It is relevant to consider what **reasonable doubts** are to avoid systematic complaints and errors from data controllers. **A more granular threshold is needed**, in line with Recital 64. In fact, several complaints reported by DPAs reflect the confusion regarding "reasonable doubts" even when controllers already have information on the data subject, e.g. a postal address [5], an email account [6] used to register the user, a qualified electronic signature [7], though an ID document was still asked.

[4] https://gdprhub.eu/index.php?title=Datatilsynet_-_2018-7320-0166
[5] https://gdprhub.eu/VG_Berlin_-_1_K_90.19
[6] https://www.aepd.es/es/documento/td-00013-2021.pdf
[7] https://gdprhub.eu/index.php?title=BVwG_-_W274_2237071-1

**Recommendation 8.** *The guidelines need to provide minimum and maximum threshold on the concept of reasonable doubts on the identity of the data subject.*

### 4.3 Accountless users

The guidelines need to provide more clarification on the case of accountless users. Many online interactions occur when data subjects are not registered on the websites of data controllers. Still, data controllers collect and process information on the accountless subjects. The data are associated to pseudonyms or other unique identifiers such as IP addresses or cookies (which are personal data under Recital 30 of the GDPR). In this case, the guidelines provide the following recommendations:

> 66 As a consequence, where information collected online is linked to **pseudonyms or other unique identifiers**, the controller can implement **appropriate procedures** enabling the requesting person to make a data access request and receive the data relating to them.

The exercise of the right of access in the situation of accountless users proves to be impossible as explained in [JNO+21] and demonstrated in [ALS22]. In general, accountless users are disempowered to access their own personal data, and cannot verify the lawfulness of the processing and tracking, nor are they able to exercise further their rights when issuing a SAR with **IP address or a cookie ID**, since their requests are often *denied*. There are several basis to deny the requests in this case:

- The subject is unable to prove that she is the only subject to have used the identifier.
- The subject cannot prove she has used the identifier.

It is very relevant to read the guidelines on data subject requests provided by IAB Europe (leading European-level industry association for the interactive advertising ecosystem) [8] to understand how companies are going to handle subject access requests. Three following paragraphs are particularly important.

> It is also relevant where a single browser or device is shared by several individuals, resulting in a cookie ID being assigned to several individuals. Companies may ask individuals to visit the companies' website and fill in a **form** to verify their identity and that the device ID was assigned to their device or access their website portal that verifies the device ID, pursuant to Article 12(6) GDPR.
>
> It's important to note here that this verification process again raises a challenge for digital marketing companies. If a company maintains non-pseudonymised personal data, such as email addresses, it may send a verification link to the email account provided by the individual, ensuring that the data subject is the owner of that email address.
>
> There is no way for digital marketing companies holding only pseudonymised to verify the individual in this manner. However, despite not having the individual's name and address, there is potential that a digital marketing company should not refuse to provide data to the data subject and should instead attempt to verify the individual's right to the data, which includes taking reasonable steps at authenticating the data subject. **Digital marketing companies which only process pseudonymous data should respond only to data subject requests tied to the identifier they use. These identifiers may include cookie IDs and mobile device IDs. If the data subject sends in her name, email address, or IP Address, digital marketing companies should first request additional information from the data subject**. This may include the actual cookie or mobile identifier20 from the individual, which digital marketing companies are entitled to receive under Article 12(6) GDPR

[8] https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf page 9 and 10.

Internet users will need to provide a lot of personal data, which might trigger *privacy invasion risks*. Additional information can consist of ID documents, credit card numbers, utility bills, or taking part in a phone interview [Pav19], etc to submit a verifiable access request. Some of these data are more revealing then the information that the website already holds.

These users will need to rely on the content of the privacy policies of the visited organizations to be informed on what information is collected when these users visit their website. In the work of [ALS22] the authors found that the processing of IP addresses is unclear from the privacy policies and that some organizations do not even present privacy policies.

This lack of oversight regarding accountless users creates opportunities for IP-address based tracking wherein GDPR transparency rights to information and access do not suffice to expose this kind of tracking, as concluded in [ALS22].

**Recommendation 9.** *The guidelines do not address the very frequent scenario of accountless users. The guidelines need clarify how data controllers handle requests from accountless users.*

# References


[AD18] Jef Ausloos and Pierre Dewitte. Shattering one-way mirrors – data subject access rights in practice. *International Data Privacy Law*, 8(1):4–28, 2018.

[AFC17] AFCDP. Données personnelles - Index AFCDP du Droit d'accès. Technical report, 2017. In french.

[ALS22] Supriya Adhatarao, Cédric Lauradoux, and Cristiana Santos. Why IP-based Subject Access Requests Are Denied? In *Privacy Symposium 2022*, 2022. To appear.

[AMMG17] Hadi Asghari, Rene L.P. Mahieu, Prateek Mittal, and Rachel Greenstadt. The Right of Access as a tool for Privacy Governance. In *Proceedings of Hot Topics in Privacy Enhancing Technologies (HotPETs 2017)*, 2017.

[BFB+19] Coline Boniface, Imane Fouad, Nataliia Bielova, Cédric Lauradoux, and Cristiana Santos. Security Analysis of Subject Access Request Procedures How to authenticate data subjects safely when they request for their data. In *Annual Privacy Forum*, volume 11498 of *Lecture Notes in Computer Science*, pages 1–20, Rome, Italy, June 2019. Springer.

[BMMS20] Luca Bufalieri, Massimo La Morgia, Alessandro Mei, and Julinda Stefa. GDPR: When the Right to Access Personal Data Becomes a Threat. In *2020 IEEE International Conference on Web Services, ICWS 2020*, pages 75–83, Beijing, China, October 2020. IEEE.

[CHP19] Matteo Cagnazzo, Thorsten Holz, and Norbert Pohlmann. GDPiRated - Stealing Personal Information On- and Offline. In *Computer Security - ESORICS 2019 - 24th European Symposium on Research in Computer Security*, volume 11736 of *Lecture Notes in Computer Science*, pages 367–386, Luxembourg, September 2019. Springer.

[CRB19] Stefano Calzavara, Alvise Rabitti, and Michele Bugliesi. Sub-session hijacking on the web: Root causes and prevention. *J. Comput. Secur.*, 27:233–257, 2019.

[DMQ+] 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. In *Privacy Enhancing Technologies, PETS 2022*, volume 8555 of *Lecture Notes in Computer Science*, page To appear. Springer.

[DRW+19] 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 *Fourteenth Symposium on Usable Privacy and Security (SOUPS)*, page 371–386, Santa Clara, CA, USA, August 2019. ACM, USENIX Association.

[ENI21] Remote ID Proofing. Technical report, ENISA, March 2021.

[ENI22] Remote ID Proofing: Attacks & Countermeasures. Technical report, ENISA, January 2022.

[Eur22] European Data Protection Board. Guidelines 01/2022 on data subject rights - Right of access. Technical report, January 2022.

[GDP] GDPR Implementation Working Group. Data Subject Requests. Technical report, IAB Europe, April.

[JNO+21] Scott Jordan, Yoshimichi Nakatsuka, Ercan Ozturk, Andrew J. Paverd, and G. Tsudik. Viceroy: Gdpr-/ccpa-compliant enforcement of verifiable accountless consumer requests. *ArXiv*, abs/2105.06942, 2021.

[KLH20] 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, New York, NY, USA, 2020. Association for Computing Machinery.

[MvOV96] Alfred Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[Pav19] James Pavur. GDPArrrrr: Using Privacy Laws to Steal Identities. In *Blackhat USA*, page https://arxiv.org/abs/1912.00731, Las Vegas, NV, USA, 2019. Arxiv.

[UTD+19] Tobias Urban, Dennis Tatang, Martin Degeling, Thorsten Holz, and Norbert Pohlmann. A Study on Subject Data Access in Online Advertising After the GDPR. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology - ESORICS 2019 International Workshops, DPM 2019 and CBT 2019*, volume 11737 of *Lecture Notes in Computer Science*, pages 61–79, Luxembourg, September 2019. Springer.