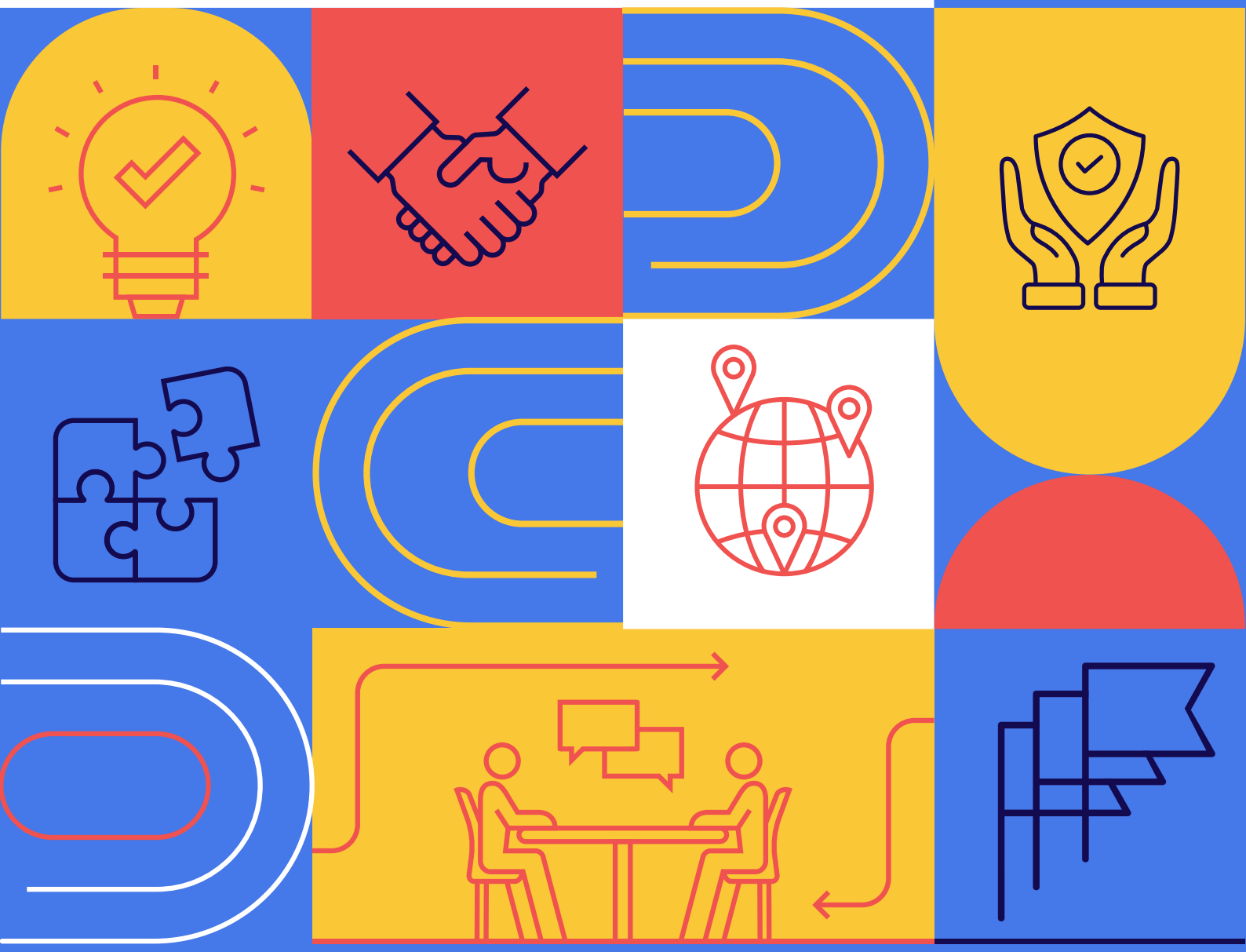
One-Stop-Shop thematic case digest

RIGHT TO OBJECT AND RIGHT TO ERASURE

Alessandro Mantelero

Associate Professor of Private Law and Law & Technology at Polytechnic University of Turin;
EC Jean Monnet Chair in Mediterranean Digital Societies and Law

9 December 2022



The case digest was commissioned as part of the EDPB's Support Pool of Experts initiative, which aims to support cooperation among SAs by providing expertise and tools related to enforcement.

Legal studies by external providers

The EDPB may commission contractors to provide legal studies on specific topics.
The views expressed in the legal studies are those of their authors and they do not necessarily reflect the official position of the EDPB. The EDPB does not guarantee the accuracy of the information included in the legal studies. Neither the EDPB nor any person acting on the EDPB's behalf may be held responsible for any use which may be made of the information contained in the legal studies.
Some excerpts may be redacted from the legal studies as their publication would undermine the protection of legitimate interests, including, inter alia, the privacy and integrity of an individual regarding the protection of personal data in accordance with Regulation (EU) 2018/1725 and/or the commercial interests of a natural or legal person.

Thematic case digest

One-Stop-Shop mechanism and decisions

Foreword by EDPB

This thematic digest look at a selection of examples of final One-Stop-Shop decisions taken from the EDPB's public register. The Register was consulted between 20 August and 13 November 2022. The thematic case digest analyses decisions relating to Articles 17 (right to erasure) and 21 (right to object) of the GDPR.

The OSS thematic digest is a valuable resource to showcase how SAs work together to enforce the GDPR. It offers an exceptional opportunity to read final decisions taken by, and involving, different SAs relating to two specific data subject rights.

The OSS thematic digest was produced within the framework of the EDPB Support Pool of Experts, a strategic initiative of the EDPB that helps Supervisory Authorities increase their capacity to supervise and enforce the safeguarding of personal data.

The One-Stop-Shop Mechanism explained

The One-Stop-Shop (OSS) mechanism demands cooperation between the Lead Supervisory Authority (LSA) and the Concerned Supervisory Authorities (CSAs). The LSA leads the investigation and plays a key role in the process of reaching a coordinated decision between the SAs.

The LSA investigates the case while taking into account national procedural rules, ensuring that individuals can exercise their rights. It shall cooperate with the other Supervisory Authorities concerned and endeavour to reach consensus. In particular, it can gather information from another SA via mutual assistance or by conducting a joint investigation. The Internal Market Information system (IMI) supports the authorities in exchanging relevant information.

The LSA then prepares a draft decision, which it submits to the CSAs. They have the right to object. This either leads to a revised draft decision or, if no consensus can be found, the EDPB acts as a dispute resolution body and issues a binding decision. In such a case, the LSA must adopt its final decision on the basis of the EDPB's decision.

I. Scope and methodology

This analysis of the decisions relating to Articles 17 and 21 of the GDPR, adopted by Supervisory Authorities (SAs) acting as Lead Supervisory Authorities (LSAs) pursuant to Article 60 GDPR (One Stop Shop Decisions), shows that most cases do not entail very critical breaches of these provisions and serious implications for data subjects. However, it possible to identify the main shortcomings related to different aspects of enabling and exercising the right to object and the right to erasure.

The analysis is based on the information gathered and the outcomes of the relevant inspection activities carried out as referred to by the Supervisory Authorities in their final decisions. This may entail some limitations in having a comprehensive view of individual cases.

Finally, since in the vast majority of decided cases the right to erasure is associate with a prior exercise of the right to object, the case law on Article 21 GDPR is discussed before the decisions relating to Article 17, following the most common sequence of requests that the Supervisory Authorities have to deal with and whose order contributes to shaping their decisions.

II. The right to object

1. The right to object and its relationship with the right to erasure in data subject complaints

The application of Article 21 (right to object) is often combined with the exercise of the right to erasure, as enshrined in Article 17. Article 17(1)(c) recognises this right when the data subject objects to processing pursuant to Article 21(1) and there are no overriding legitimate grounds for data processing,[1] or when the data subject objects to data processing performed for direct marketing purposes (Article 21(2) GDPR).

Most of the cases decided by Supervisory Authorities under Article 21 deal with the use of personal data for direct marketing (Article 21(2)) rather than objections to the processing of data in the performance of tasks carried out in the public interest, in the exercise of official authority vested in the controller, or on the basis of legitimate interests (Article 21(1)).

Thus, in the cases examined, there is a frequent link between the request to stop any further processing of personal data for marketing purposes[2] and the request to erase previously collected data.

Against this background, two main sets of issues characterise the case law on Article 21, as emerging from the decisions adopted within the cooperation mechanism provided for in Article

1 See Section III.3 below.
2 Article 21(2) and Article 21(3) GDPR.

60 GDPR: (i) issues concerning effective exercising of the right to object by data subjects, and (ii) issues relating to the procedure adopted by data controllers and processors in handling complaints from data subjects.

2. Exercise of the right to object

We will highlight three particular elements relevant to the exercise of the right to object: (i) the information provided to the data subject about the right to object,[3] (ii) the solutions – including technical solutions – adopted to make the exercise of this right easier, and (iii) the implementation of appropriate procedures to handle such requests. The first two elements are discussed in this section, while the last one in Section II.3.

Several cases concern non-compliance with the GDPR because the controller did not provide data subjects with any **information on the right to object**, in contrast with Article 13(2)(b) [EDPBI:ES:OSS:D:2021:263].[4] One such example was provided by a case decided in 2021 where the complainant received direct marketing by email from a bank without receiving information about the right to object to the processing of personal data for direct marketing purposes, pursuant to Article 21(4) GDPR [EDPBI:NO:OSS:D:2021:292].

Data subjects were targeted with direct marketing emails without having the option to opt out when registering their email addresses, and were only able to do so by changing their preferences once they had accessed the online banking service, or by contacting customer service.[5]

This case is also relevant in highlighting some recurring shortcomings in the **technical and organisational solutions** adopted by controllers in dealing with this type of request. These include lack of capacity and backlogs in customer service departments [EDPBI:NO:OSS:D:2021:292], as well as incorrect processing of objection requests [EDPBI:EE:OSS:D:2019:55], where the data subject's request was not properly registered resulting in the implementation of the objection with regard to only one account in a case of multiple user accounts and technical errors within the system [EDPBI:CZ.OSS:D:2021:312] creating delays in complying with Article 21.[6]

It is worth noting that the controller is required to facilitate the exercise of data subject rights[7] and that, in the context of information society services, the right to object may be exercised by automated means using technical solutions.[8]

3 See also, inter alia, CJEU, case C-201/14, Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF), para 33.

4 See Recital 70 relating to the right to object for direct marketing.

5 In this case, the LSA issued a reprimand and ordered the controller to implement measures to ensure that personal data is no longer processed for direct marketing when so requested by data subjects and to ensure that data subject requests under Article 15-22 GDPR are answered within the time limits set in Article 12(3) GDPR.

6 See also Article 12(3) GDPR.

7 See Article 29 Working Party guidelines on transparency under Regulation (EU) 2016/679, adopted on 29 November 2017 and revised on 11 April 2018, available at https://ec.europa.eu/newsroom/article29/items/622227/en, accessed 10.10.2022, 26-27. These guidelines were endorsed by the EDPB on 25 May 2018.

8 See Article 21(5) GDPR.

Although shortcomings regarding the exercise of the right to object are often part of a broader lack of compliance by data controllers, a focus on the design of the legal and technical solutions used to enable the exercising of this right plays a crucial role in terms of compliance.[9]

Finally, as regards how this right can be exercised, in the cases reviewed the data subjects were not asked for a request in legal terms, as even a generic request not to receive further marketing messages (such as "I ask for a guarantee that this will not repeat itself", EDPBI:NO:OSS:D:2021:292) could be considered appropriate.

3. Complaints handling procedure

Most of the cases decided under Article 60 show deficiencies in the internal procedure adopted to deal with such requests,[10] including related aspects such as the accuracy of the procedure and internal communication,[11] the timeframe for processing requests,[12] and accountability (e.g. evidence that a system for receiving/tracking complaints has been put in place).[13]

Legal design elements play an important role in enabling the right to object in relation to this procedural dimension. **Cumbersome procedures** and **language barriers** should be avoided.[14] This should prevent cases such as the one when a contact email address was provided for the exercise of data subjects' rights, but an automated response referred the data subject to the "Contact us" form on the website, thus setting up a cumbersome procedure instead of directly handling the requests through the contact email [EDPBI:FR:OSS:D:2022:326].

The design of interaction with the data subject must therefore be carefully considered, using a clear and easily accessible form (see Article 12 GDPR)[15] and avoiding any misunderstanding.

For example, when using a no-reply email address for marketing purposes, data subjects must be informed in a clear manner and in the body of such emails that the message does not allow replies to the sender and, therefore, that any objections expressed by replying will be ineffective.[16]
In addition, emails acknowledging receipt of objection requests must provide data subjects with timely information on the timeframe for implementation of their requests; data subjects

9 See e.g. EDPBI:FR:OSS:D:2019:73; EDPBI:FR:OSS:D:2019:8.
10 See EDPBI:DEBE:OSS:D:2021:184; EDPBI:ES:OSS:D:2021:263; EDPBI:NO:OSS:D:2021:292; EDPBI:CZ.OSS:D:2021:312; EDPBI:FR:OSS:D:2022:326.
11 See EDPBI:UK:OSS:D:2019:31.
12 See EDPBI:DEBE:OSS:D:2018:9.
13 See EDPBI:CY:OSS:D:2019:57; EDPBI:CY:OSS:D:2019:58; EDPBI:FR:OSS:D:2020:84.
14 See Article 12 GDPR. See also Article 29 Working Party, Guidelines on transparency under Regulation (EU) 2016/679, adopted on 29 November 2017 and revised on 11 April 2018, available at https://ec.europa.eu/newsroom/article29/items/622227/en, accessed 10.10.2022, 10. These guidelines were endorsed by the EDPB on 25 May 2018.
15 See Article 12 GDPR. See also EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted - version for public consultation, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en, accessed 20.11.2022, 42-44.
16 See e.g. EDPBI:FR:OSS:D:2019:8.

must then be correctly informed about the outcome of the exercise of their rights.[17]

Specific procedures to process objection requests – including appropriate technical solutions – must therefore be adopted by data controllers, involving data processors according to the task distribution relating to processing operations,[18] being aware that an incorrect task allocation may delay an appropriate response.[19]

In addition, the technical solutions implemented must be effective and **designed with the different types of data subject in mind.** For example, it is inappropriate to use an unsubscribe link at the bottom of direct marketing emails referring to a specific customer account page, since prospects who do not have a customer account cannot unsubscribe via this link. Here, a link that directly unsubscribes the user is much more effective than referring to the customer account.[20]

Although setting up specific procedures for exercising the right to object is desirable, it is worth noting that this should not limit data subjects' possibilities to send requests to the controller in other ways. However, **informal requests**, such as through a tweet on Twitter, can legitimately be disregarded by the controller when other more formal channels, such as email, are available [**EDPBI:SE:OSS:D:2021:276**].

Establishing specific and appropriate procedures that data subjects can use for their requests helps handle them carefully, whereas leaving room for the initiative may lead to difficulties, such as when data subjects' requests are sent using a different email address than the one used to create the personal account.[21]

Finally, to ensure effective regulatory compliance, **accountability** plays a crucial role in terms of record-keeping of the objection requests and their outcome,[22] and **data controller** is responsible for mistakes of its employees in dealing with data subjects' requests, and the employee's fault is irrelevant in assessing compliance with the GDPR and proving accountability in the cases examined [**EDPBI:DEBE:OSS:D:2021:184**].

17 See EDPBI:EE:OSS:D:2019:55 and EDPBI:FR:OSS:D:2019:41.
18 See e.g. EDPBI:FR:OSS:D:2020:84, EDPBI:MT:OSS:D:2019:60, and EDPBI:EE:OSS:D:2019:55.
19 See EDPBI:UK:OSS:D:2019:31 in a case where the customer care officer had forwarded the data subject's request to the wrong department.
20 See e.g. EDPBI:FR:OSS:D:2020:84.
21 See also EDPBI:MT:OSS:D:2019:60 and Section III.2 on the right to erasure.
22 See also EDPBI:CY:OSS:D:2019:57; EDPBI:CY:OSS:D:2019:58.

III. The right to erasure

1. The right to erasure in case law under Article 60 GDPR

Despite the significant development of the right to be forgotten in the online context after the Google Spain case, [23] very few decisions have been adopted over the years by Supervisory Authorities on this topic under Article 60 GDPR [24] . The large majority of the cases deal with requests for: (i) erasure as a result of objecting to the processing of data for marketing purposes [e.g., EDPBI:CZ:OSS:D:2021:312], [25] including unsolicited emails [e.g., EDPBI:NO:OSS:D:2022:314], and (ii) erasure of accounts/profiles relating to services no longer used. [26]

As the cases examined largely concern fairly basic situations, at least from the point of view of compliance with Article 17, the main considerations are: (i) bottlenecks and shortcomings in the internal complaints handling procedure, and (ii) the presence of an overriding legitimate interest or other conditions justifying the processing despite the request for erasure. In view of the large number of requests they receive, data controllers usually put in place partially or fully automated procedures to deal with them.

As for the right to object, complaint procedures can be divided into two main steps: the exercise of the right based on the data subject's request (see para III.2) and the complaints handling procedure (see para III.3). As a result, the issues related to these two phases are different, focusing more on the correct identification of the data subject as far as erasure requests are concerned, and more on the classification of requests and internal organisation as regards the complaint handling phase.

2. The exercise of the right to erasure

As in cases relating to the right to object, the data controller must **facilitate the exercise of the data subject's right** [27] without creating cumbersome procedures. In this regard, critical issues concern the identification of the data subject and the **proof of identification**. [28]

Although Article 12(6) allows the data controller to ask for additional information in event of reasonable doubt as to the identity of a data subject, a specific assessment is required to determine whether a reasonable doubt exists. [29]

23 CJEU, case C 131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, available at https://curia.europa.eu.

24 This is probably due to the fact that many of them are handled as local cases under Article 56(2) GDPR. See the Internal EDPB Document 1/2019 on handling cases with only local impacts under Article 56.2 GDPR, Example 11, page 10.

25 See also EDPBI:DEBE:OSS:D:2018:9 and Section II.1.

26 See e.g. EDPBI:DESL:OSS:D:2019:11

27 Article 12.2 GDPR.

28 See e.g. EDPBI:DK:OSS:D:2019:69.

29 See also Recital 64 GDPR and Article 29 Working Party, Guidelines on the right to "data portability" (wp242rev.01), available at https://ec.europa.eu/newsroom/article29/items/611233/en, accessed 10.10.2022, 13, and EDPBI:FR:OSS:D:2019:3 (the online nature of the customer relationship cannot in itself imply such a reasonable doubt and be a sufficient reason to require a proof of identity; the latter must be justified by specific

Additional information for the purposes of Article 12(6) should therefore be justified on a case-by-case basis. Requiring a copy of a national ID card by default is not acceptable.[30] The undue request of identity documents as a condition for the exercise of the right to erasure violates the principle of data minimisation pursuant to Article 5(1)(c) of the GDPR. Failure to comply with such a request cannot therefore justify delaying the erasure of the data and, as the data subject's personal data could have been deleted at the time of the request, the continued processing of personal information after receipt of the erasure request constitutes an infringement of Article 6(1).[31]

A common argument used to justify the need to provide an official identity document relates to the problem raised by sending the erasure request via **an email address other than the one used at the registration stage**. Although in such cases the identity of the data subject may be uncertain on the basis of the sole email address, other solutions more in line with the minimisation principle are available. It would, for example, be disproportionate to require a copy of an identity document in the event where the data subject made their request within an area where they are already authenticated[32] .

Conversely, it is possible, for example, to provide a unique identifier to users at the end of the registration process,[33] to inform users that only requests from an email address linked to their profile will be taken into account, to provide a password hotline in order to change the account login details,[34] to use other means of identification, such as via an online call,[35] or to identify the claimant by asking for additional information related to the service (e.g. current and previous nicknames, date of account registration, secret questions) [**EDPBI:EE:OSS:D:2021:294**].

In the case of robot-generated requests, the measures taken by data controllers to cope with the increased workload generated by these types of requests, cannot limit the exercise of the subject's rights by adopting **semi-automated procedures for sending erasure requests** that lead to disregarding any requests that do not follow the instructions. [36]

Furthermore, in the cases of Article 17(1) GDPR, including ones in which the data subject withdraws consent (Article 17(1)(b))or objects to processing under Article 17(1)(c), a specific

circumstances, such as suspicion of identity theft or account piracy). These guidelines were endorsed by the EDPB on 25 May 2018.

30 See also EDPBI:FR:OSS:D:2019:3 (the practice of requiring individuals to "systematically provide a copy of an identity document for exercising their rights [...] does not, in view of its systematic nature, comply with the text [of the applicable law]") and EDPBI:IE:OSS:D:2020:166 (in a case where the standard procedure of the data controller was to ask for the submission of a copy of a national identity card for all erasure requests, the LSAs had made it clear that "the request for a copy of a national identity card was not made on foot of any specific doubt as to the complainant's identity, but rather was a result of the policy that was in place in Groupon at the time") and EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted - version for public consultation, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en, accessed 20.11.2022, 23-27.

31 See EDPBI:IE:OSS:D:2020:166.

32 See EDPBI:FR:OSS:D:2019:3.

33 See EDPBI:DK:OSS:D:2019:69

34 See also EDPBI:LU:OSS:D:2019:14 and EDPBI:LU:OSS:D:2020:94.

35 See also EDPBI:MT:OSS:D:2019:26.

36 See EDPBI:DK:OSS:D:2020:151.

request of erasure from the data subject is not necessary, as there is an independent obligation arising for the data controller to delete data regardless of the request[37] [EDPBI:DEBE:OSS:D:2021:229].

3. The complaints handling procedure

An effective exercise of the rights to erasure requires adequate management of the internal processes. This is especially true when requests are on a large scale, as in the case of erasure based on objections to data processing for marketing purposes. In this context, different types of shortcomings may occur that jeopardise the effective exercise of the data subject's right.

The main shortcomings detected by the LSAs can be classified under two categories, namely **procedural shortcomings and human errors**, where the former are more impactful in terms of GDPR compliance as they affect all requests handled, while the latter are case specific.

Among the procedural shortcomings, the most serious concerned the **complete absence of a specific procedure to deal with erasure requests,**[38] while the most frequent case concerns delays in the erasure process due to **poor internal organisation**[39] or technical malfunction, which is why, for example, the data controller must adopt appropriate technical solutions not to leave an old contact email address unmonitored (e.g., automatic reply informing about the new contact email address or an automatic re-directing to the correct email) [EDPBI:MT:OSS:D:2021:212].[40]

The relationship between data controller and data processor, if not properly managed, may also lead to l**ack of coordination/instructions in the handling of requests**, with the result that the effective exercise of the right to erasure may be impaired [e.g. EDPBI:CY:OSS:D:2021:305 in a case of an oral request for erasure, where the LSA emphasised that both the data controller and the provider must facilitate the exercise of the right of erasure by properly training their employees and, as far as the controller is concerned, adopting clear instructions on the handling of the erasure requests; and EDPBI:DEBE:OSS:D:2021:374 in a case where the data processor treated a data subject's request internally instead of forwarding it to the controller, as required by the nature of the service and task allocation].

37 See EDPBI:DEBE:OSS:D:2021:229 as well as the EDPB Opinion 39/2021 on whether Article 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject, paragraph 22 ("Article 17 GDPR provides for both (i) an independent right for data subjects and (ii) an independent obligation for the controller. In this regard, Article 17 GDPR does not require the data subject to take any specific action, it merely outlines that the data subject "has the right to obtain" erasure and the data controller "has the obligation to erase" if one of cases set forth in Article 17(1) GDPR applies") and paragraph 23 ("some cases set forth in Article 17(1) GDPR clearly refer to scenarios that the controllers must detect as part of their obligation for erasure, independently of whether or not the data subjects are aware of these cases").

38 See also e.g. EDPBI:MT:OSS:D:2019:60.

39 See also EDPBI:DEBE:OSS:D:2018:10 in a case where the erasure request was not handled in a timely manner as there were two separate databases, managed by the customer care and the in-house shop management, and the account was deactivated on the former, but the request was not forwarded to the shop management.

40 See also EDPBI:CZ:OSS:D:2021:312; EDPBI:FR:OSS:D:2020:105.

In some limited cases, **inadequate technological solutions** are the main reason for the failure to fully meet the data subject's requests, such as when documents sent by users via email to the data controller have been stored by generating URL links making their subsequent deletion more difficult [EDPBI:FR:OSS:D:2021:202, in a case where customers' driving licenses were accessible via any browser without required authentication by entering a URL that linked to the software used for data storage].[41]

Finally, in several cases, the data controller complied with the data subject's request for erasure but **did not inform the data subject** of the erasure (Article 12(3) GDPR) [EDPBI:LU:OSS:D:2021:240 [42]] or this information was provided with delay.[43]

With regard to the controller's obligation to inform the data subject about the action taken on the requests received (Article 12(3) GDPR), the case law considered has also clarified that, when the controller notifies the data subject that the request has been granted, the erasure has been initiated and how long it will take at most, no confirmation that the erasure had been carried out is required. This is unless the data subject requests otherwise, or it is otherwise indicated that the data subject wishes to be notified that the erasure has been carried out or that the erasure is not carried out within the specified time limit [EDPBI:SE:OSS:D:2021:303]
As regards **human errors**, they may concern requests inadvertently not processed or not forwarded to the competent department [EDPBI:DEBE:OSS:D:2020:130; EDPBI:CY:OSS:D:2021:267], as well as occasional misclassification of the data subject's requests [EDPBI:DEBE:OSS:D:2021:184; EDPBI:SE:OSS:D:2021:195] or misrepresentation of the data subject's position.[44]

In addition, a combination of procedural and human errors is likely to occur in the case of erasure **requests handled manually and not via digital communications and automated procedures** [EDPBI:SE:OSS:D:2021:178 in a case where the data subject was not informed about the results of the erasure request, as the request was handled manually, because it was received by mail, whereas the company used to handle requests through an automated digital system where notifications about measures taken were sent automatically].

Based on the case law of the LSAs and in the light of the EDPB guidelines, [45] data controllers are required to ensure the effectiveness of all data subjects' requests concerning the exercise the right of erasure, and personal data must be systematically erased when requested.
Against this background, the automation of the complaint process can reduce both the

41 See also EDPBI:FR:OSS:D:2020:193 where the data subject's request for erasure was addressed by assigning personal information a special status making then unusable by the data subject, but without erasing them from the database.

42 See also EDPBI:DEBE:OSS:D:2020:156, see also EDPBI:FR:OSS:D:2020:84.

43 See also EDPBI:HU:OSS:D:2020:118.

44 See also EDPBI:PL:OSS:D:2020:194, in a case of wrongful compliance with the data subject's request for erasure due to lack of the information on one of the several active processing operations concerning the data subject.

45 See Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, available at https://ec.europa.eu/newsroom/article29/items/611237/en, accessed 10.10.2022, 12; "[…] failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence".

procedural and human errors, by introducing user-friendly interfaces that support data subjects in formulating and providing better evidence of their requests, and by setting the decision-making process regarding erasure so as to be aligned with the tasks assigned under the GDPR to those handling personal data. This ensures more effective compliance with both the data subjects' requests and the GDPR, without prejudice to the human decision on each case, which remains in the hands of the persons tasked by the controller to make the final decision. In the most basic cases, such as erasure resulting from contract/service termination, full automation may be considered.

4. Overriding legitimate interest and other conditions justifying data processing despite a request for erasure

More complicated issues, entailing a case-by-case assessment and the involvement of a human decision-maker, arise in cases where the request for erasure cannot be accepted due to the presence of overriding legitimate grounds for the processing (Article 17(1)(c) GDPR), or where the right to erasure is not granted when processing is necessary under Article 17(3).
As to the first category of cases, they mostly deal with the prevalence of data **controllers' legitimate interest** [e.g. EDPBI:SE:OSS:D:2021:196 where the data subject's right to the erasure of banking information did not override the legitimate interest of the data controller in payment and fraud prevention, in a case involving the use of unique payment instrument identifiers to counter the abuse of free trial online services offered by a media company]. In this regard, it is worth noting that the decisions examined do not include cases of the exercise of right to be forgotten in the context of the activity of search engines, which are instead common in national and regional decisions of individual Supervisory Authorities.

Regarding the second category, i.e. cases where the right to erasure is not granted, the LSA decisions mainly concern **obligations under national laws** setting mandatory data retention periods [e.g., EDPBI:DK:OSS:D:2021:210 data retention required by the law with regard to customers' complaints and purchases].[46] Data controllers must i**nform data subjects about the legal grounds** for retaining their data, which justifies the rejection of any

erasure request [EDPBI:MT:OSS:D:2022:340, regarding anti-money laundering obligations; EDPBI:MT:OSS:D:2021:272, concerning various obligations under banking laws]. In these cases, **specific information on the source of the legal obligations** must also be provided to the data subject at the time of the request for erasure (Article 12.1) [EDPBI:MT:OSS:D:2021:272].

However, **legal obligations must be interpreted in line with data protection principles** and not abused to justify limitations to the rights of the data subject. In this sense, for example, the consumer's right to claim compensation for a defective product for two years after the delivery of the goods to the purchaser cannot justify a refusal to erase a customer's profile because of the use of an online form on the customer's page to exercise the right to complain, as it is possible to

46 See also CJEU, case C-398/15, Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni.

complain about a product in a different way with no need to maintain an active profile [see also EDPBI:DK:OSS:D:2020:171 and EDPBI:DK:OSS:D:2021:210 where it was deemed unnecessary to keep the customer account active for at least two years after the purchase for the exercise the right to complain under the customer protection law, as this right can be exercised by other means such as emails or telephone].

Legal obligations and the defence of legal claims (Article 17(3)(e) GDPR) related to consumer protection may also justify the retention of personal data processed in connection with orders during the time when purchasers may make their claims, or a competent supervisory body may carry out an inspection [EDPBI:CZ:OSS:D:2021:312].

Nonetheless, it is worth emphasising that, while under certain circumstances some personal data may be kept in intermediate storage in the presence of an erasure request, those that are not necessary in the context of fulfilment of such obligations or purposes under Article 17 must be deleted after the exercise of this right [EDPBI:FR:OSS:D:2021:279; EDPBI:FR:OSS:D:2021:310].

IV. Concluding remarks

Due to the nature of the cases decided, most of the complaints relating to Articles 17 and 21 concern minor violations and are often characterised by a collaborative approach on the part of the data controller, with spontaneous remediation of the infringement, including the adoption of new procedures fully compliant with the GDPR.

For this reason, discontinuation of data processing and erasure of personal data as a result of LSA investigations and active cooperation by data controllers make reprimands the main outcome in the case law examined. It is worth noting that, in presence of minor violations, the motivation of the remedy adopted in the final decision may be not sufficiently elaborated, by using general statements (see e.g., EDPBI:DEBE:OSS:D:2021:184 which refers to "the specific circumstances of the case under investigation"). Although in some cases the LSAs have imposed specific sanctions on data controllers, this is usually due to a large number of infringements of the GDPR, with a minor role played by violations of Articles 17 and 21. This also makes it difficult to identify in the Register a set of notable case studies focusing on these specific legal grounds.

Finally, it is worth noting that even where the violations of Article 17 are more serious, the LSAs may consider refraining from imposing a fine in consideration of the specific circumstances of the case [e.g. EDPBI:DEBW:OSS:D:2021:203 where the LSA took the following elements into account: "First of all, it must be seen that [the data controller] is a non-profit and thus not commercially active company which, apart from the managing sole shareholder, has no employees and is dependent on donations for its non-profit activities, which in 2020 amounted to only 10,603.00 Euros up to the time of the statement of 24 November 2020. In addition, did not act intentionally, but on the contrary, due to a lack of technical expertise, was convinced that the signature list had already been deleted and had thus complied with the complainant's request for erasure".

edpb.europa.eu