EDPB Support Pool of Experts Programme

One-Stop-Shop thematic case digest

Right to object and right to erasure

by Ass. Prof. Alessandro MANTELERO

Document submitted on 26 May 2026 by Ass. Prof. Alessandro Mantelero[1]

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

One-Stop-Shop mechanism and decisions

Foreword by EDPB

This thematic digest looks at a selection of examples of final One-Stop-Shop decisions taken from the EDPB's public register. 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.

Contents

I. Scope and methodology 5

II. Common issues 6

III. The right to object 8

1. The right to object and its relationship with the right to erasure in data subject requests 8

2. Exercise of the right to object 8

3. Data subjects' requests: handling procedures 9

IV. The right to erasure 11

1. The right to erasure in case law under Article 60 GDPR 11

2. The exercise of the right to erasure 13

3. Data subjects' requests: handling procedures 15

4. Conditions justifying data processing despite a request for erasure 18

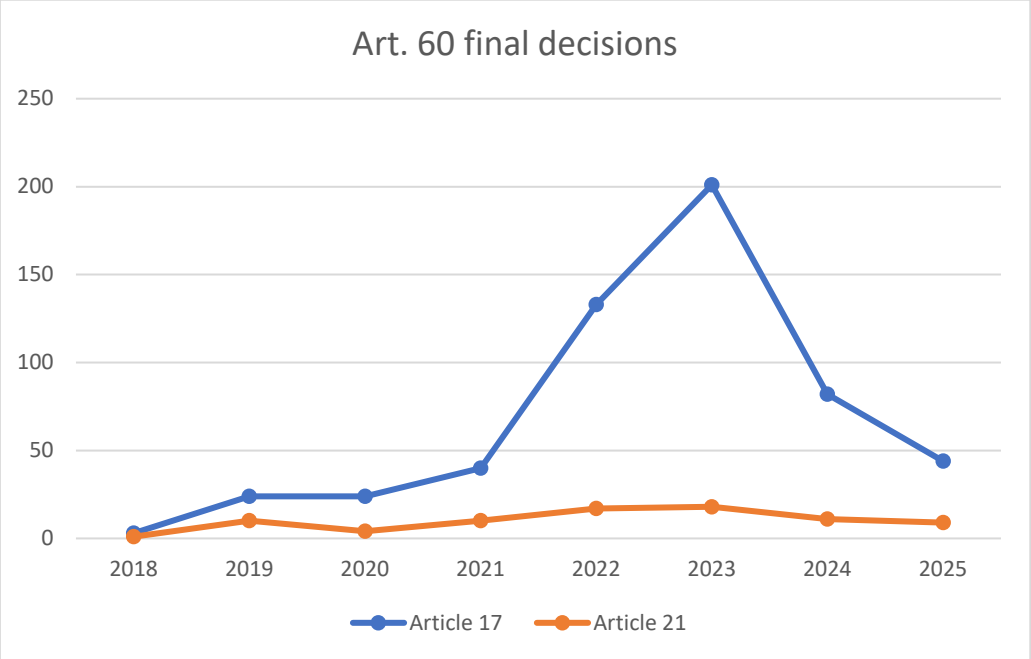
V. Concluding remarks 21

I. Scope and methodology

This analysis of the decisions relating to Articles 17 and 21 of the GDPR, adopted by Supervisory Authorities (SAs) 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 is 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.

The examined corpus comprises the final **One-Stop-Shop decisions that are available in the EDPB's public register**.[2] The relevant cases were extracted using Articles 17 and 21 of the GDPR as the main legal references. The analysis was carried out in two stages. The first version of this digest, which covered decisions adopted between 2018 and November 2022, was published in December 2022. A second set of decisions was examined between October 2025 and January 2026, covering those adopted until January 2026. The entire selected corpus comprises **551 decisions relating to Article 17 and 80 relating to Article 21**, which are distributed as follows:



Given the variability of individual cases and data subjects' reactions to data processing, several factors can affect the data shown in the graph. However, the distribution of cases per year suggests a consistent trend for Article 21 cases, while Article 17 cases show a peak in 2022 and 2023, followed by a decline towards normalization. Analysis of data

[2] The register is available at https://www.edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en.

relating to Article 17 and the LSAs reveals that Irish cases (i.e. cases involving the Irish SA as the LSA) have the greatest impact on the total number of Article 17 cases, with 84 in 2022, 150 in 2023, and 35 in 2024. This is not the case for Article 21, where more LSAs determine the total annual number of cases.

All the decisions have been read and classified, but only the most relevant have been included in this digest, as many of them address similar issues and elaborate similar arguments. In addition, a limited number of cases that were decided at a national level have been referenced in the footnotes based on feedback received by the Supervisory Authorities in response to a specific call made in 2025; from these decisions, only the most relevant cases in relation to emerging trends in the final decisions adopted under Article 60 on the right to object and the right to erasure have been selected.

Finally, since the right to erasure is often associated 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 a common sequence of requests that the Supervisory Authorities have to deal with and whose order contributes to shaping their decisions.

This case digest is divided into five main sections. After this introductory section on scope and methodology, the second section addresses issues common to the two rights under consideration concerning the management of the data subject requests and, more broadly, procedural matters. Sections III and IV focus on the right to object and the right to erasure, respectively. They consider how these rights are exercised and the specific problems that arise when managing requests from data subjects. Some concluding remarks are made in the final section.

II. Common issues

Analysing how the rights to object and to erasure are exercised reveals common issues regarding the manner in which related requests are received and managed by data controllers. Further details are provided in the following sections with respect to each of these rights (see sections III.3 and IV.3), but these common issues can be grouped into two main categories: **errors** and **cumbersome procedures**. With regard to the former, it is possible to distinguish between (i) poor design of data processing and management, and (ii) errors, including human errors, when implementing existing procedures and errors in their functioning.

A common procedural issue, which is not limited to the two rights examined but is relevant to all data subjects' rights, concerns the **identification of the data subject**. Several data controllers have adopted a strict approach to this, systematically requiring official identity documents to be provided. In this respect, it is worth highlighting the distinction between cases involving the risk of unauthorised disclosure of personal data, and those in which this risk does not exist. According to this view, strong authentication

should be limited to requests concerning the right of access, but not for the right to object[3] (and the same exclusion could be extended to the right to erasure).

Another important group of issues concerns the One-Stop-Shop (OSS) mechanism itself and some criticisms that have emerged over the years. These issues should be considered in light of the reform of the OSS mechanism.

Furthermore, even in light of Regulation 2025/2518,[4] it is important to highlight that a significant portion of cases are resolved through **spontaneous compliance** – often after the Supervisory Authority begins its investigation – or through an amicable settlement. Regarding the latter, the **amicable settlement procedure** widely used by the Irish Supervisory Authority has proven effective in many cases.[5] If such procedures are allowed by national law and implemented correctly and promptly, they could reduce the workload of the Supervisory Authorities and provide a faster response to requests from data subjects.[6] In this respect, simply initiating this procedure often prompts the data controller to reconsider their position and comply with the data subject's requests. In this scenario, the best practice for all SAs when addressing data subjects' requests should be to attempt an amicable resolution by default if suitable.[7]

The role of amicable settlements is also relevant in light of other emerging features of the One-Stop-Shop (OSS) mechanism. More specifically, the vast majority of cases examined concern **minor or trivial issues**.[8] In these cases, the procedure set out in Article 60 is often disproportionate and causes delays.[9]

Finally, in an effort to simplify the existing procedure and reduce its impact on the workload of the Supervisory Authorities, it seems that numerous authorities are using **standard templates** for decisions relating to cases involving minor and trivial issues. A potential step forward would be for all the authorities to harmonise this by creating a template that at least covers the key elements.

---

[3] See EDPBI:SE:OSS:D:2025:1757 ('[…] in the case of an objection to certain processing operations under Article 21 of the GDPR […], IMY [i.e. Swedish Authority for Privacy Protection] notes that there is normally no reason to authenticate, and sometimes even to identify, the data subject in order to satisfy the objection or request for information.'). See also, on this issue, EDPB. 2024. OSS Case Digest. Right of access, authored by Hanne Marie Motzfeldt, https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/one-stop-shop-case-digest-right-access_en, pp. 16-17.

[4] See Article 5 of Regulation (EU) 2025/2518 of the European Parliament and of the Council of 26 November 2025 laying down additional procedural rules on the enforcement of Regulation (EU) 2016/679. This article relates to early resolution of cross-border complaints which concern the exercise of data subjects' rights.

[5] See, e.g., EDPBI:IE:OSS:D:2022:464 and EDPBI:IE:OSS:D:2022:556.

[6] See also EDPB. 2022. Guidelines 06/2022 on the practical implementation of amicable settlements. Version 2.0. Adopted on 12 May 2022, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062022-practical-implementation-amicable_en.

[7] On whether an amicable settlement may or may not be pursued, see EDPB. 2022 (fn. 5), p. 7-8.

[8] See, e.g. EDPBI:LU:OSS:D:2023:946 and EDPBI:NL:OSS:D:2023:756. For examples of non-trivial cases where the burden of the procedure seems justified, even though the issue concerning Article 17 may be less crucial than those relating to other violations, see EDPBI:FR:OSS:D:2023:809, EDPBI:FR:OSS:D:2023:795, EDPBI:DEBY:OSS:D:2024:1594.

[9] But see now Article 6 of Regulation (EU) 2025/2518 on the simple cooperation procedure.

III. The right to object

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

The application of Article 21 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,[10] or when the data subject objects to data processing performed for direct marketing purposes (Article 21(2) GDPR).

Many of the cases decided by Supervisory Authorities under Article 21 deal with the use of personal data for direct marketing 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)).

In the cases examined there is a frequent link between the request to stop any further processing of personal data for marketing purposes[11] and the request to erase previously collected data.[12]

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 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, including the role of processors, in handling these requests 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,[13] (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 is in Section III.3.

During the first years after the GDPR became applicable, 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 violation of Article 13(2)(b) [EDPBI:ES:OSS:D:2021:263].[14] One such example was provided by a case decided in 2021 where the complainant received direct marketing by email from a bank without

[10] See Section IV.3 below.

[11] Article 21(2) and Article 21(3) GDPR.

[12] In this respect, it has also been stressed that the timeframe between the data subject's request for objection and the erasure of the data by the controller should be minimum. See EDPBI:DEBE:OSS:D:2018:9 ('its behavior is to be understood as advertising objection in the meaning of the art. 21 Abs. 2 GDPR. Such an advertising objection leads to a deletion obligation according to Article 17 (1)(c) 2nd alternative GDPR. The timeframe to be applied here is "immediately".').

[13] 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.

[14] See Recital 70 relating to the right to object for direct marketing.

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].[15]

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 the customer service.[16]

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.[17]

It is worth noting that the controller is required to facilitate the exercise of data subject rights[18] and that, in the context of information society services, the right to object may be exercised by automated means using technical solutions.[19]

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.[20]

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. Data subjects' requests: handling procedures

Most of the cases decided under Article 60 show deficiencies in the internal procedure adopted to deal with such requests,[21] including related aspects such as the accuracy of the procedure and internal communication,[22] the timeframe for processing requests,[23]

[15] See also EDPBI:SE:OSS:D:2024:1570.

[16] 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.

[17] See also Article 12(3) GDPR.

[18] See Article 12(2) GDPR. Also 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.

[19] See Article 21(5) GDPR.

[20] See e.g. EDPBI:FR:OSS:D:2019:73; EDPBI:FR:OSS:D:2019:8.

[21] 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.

[22] See EDPBI:UK:OSS:D:2019:31.

[23] See EDPBI:DEBE:OSS:D:2018:9.

and accountability (e.g. evidence that a system for receiving/tracking complaints has been put in place).[24]

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, as stressed mainly during the first years of the GDPR implementation.[25] 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 interactions with the data subject must therefore be carefully considered, using a clear and easily accessible form (see Article 12 GDPR)[26] 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.[27] At the same time, as recently stated [EDPBI:NL:OSS:D:2022:376] 'the GDPR does not prescribe that unsubscribing should always be possible using the reply function', but it is important that emails sent for marketing purposes include a clear link to the webpage where it is possible to unsubscribe.
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 must then be correctly informed about the outcome of the exercise of their rights.[28]

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,[29] being aware that an incorrect task allocation may delay an appropriate response.[30]

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

[24] See EDPBI:CY:OSS:D:2019:57; EDPBI:CY:OSS:D:2019:58; EDPBI:FR:OSS:D:2020:84.
[25] See Article 12(2) GDPR and 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.
[26] See Article 12 GDPR. See also EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 2.1, Adopted on 28 March 2023, available at https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf, 42-45.
[27] See e.g. EDPBI:FR:OSS:D:2019:8.
[28] See EDPBI:EE:OSS:D:2019:55 and EDPBI:FR:OSS:D:2019:41.
[29] See e.g. EDPBI:FR:OSS:D:2020:84, EDPBI:MT:OSS:D:2019:60, and EDPBI:EE:OSS:D:2019:55.
[30] 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.

unsubscribe via this link. Here, a link that directly unsubscribes the user is much more effective than referring to the customer account.[31]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 (now "X"), can legitimately be disregarded by the controller when other more formal channels, such as through an email, are available [EDPBI:SE:OSS:D:2021:276]. Although this interpretation was recently confirmed [e.g. EDPBI:SE:OSS:D:2024:1550: 'A data subject is not limited to use certain communication channels indicated by the controller as the preferable one, the data subject can also make requests by using other official communication channels of the controller'], it can be observed that this approach reflects an initial stage of GDPR implementation rather than the current situation, in which data subjects are more aware of their rights and the provision of specific, easily accessible channels for exercising their rights might be considered sufficient, reducing the burden on controllers to monitor a variety of different sources, which, in large organisations with many potential points of contact, may result in a cumbersome process.[32]

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.[33]

Finally, to ensure effective regulatory compliance, **accountability** plays a crucial role in terms of record-keeping of the objection requests and their outcome.[34] **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].

IV. 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,[35] very few decisions have been adopted between 2008 and November 2022 by Supervisory Authorities on this topic under Article 60 GDPR[36]. The

[31] See e.g. EDPBI:FR:OSS:D:2020:84.

[32] See also EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 2.1, Adopted on 28 March 2023, https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf, accessed 01.04.2026, para 54 ('it should be noted that the controller is not obliged to act on a request sent to a random or incorrect e-mail (or postal) address, not directly provided by the controller, or to any communication channel that is clearly not intended to receive requests regarding data subject's rights if the controller has provided an appropriate communication channel, that can be used by the data subject').

[33] See also EDPBI:MT:OSS:D:2019:60 and Section IV.2 on the right to erasure.

[34] See also EDPBI:CY:OSS:D:2019:57; EDPBI:CY:OSS:D:2019:58.

[35] 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.

[36] 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.

large majority of the cases involved 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],[37] including unsolicited emails [e.g., EDPBI:NO:OSS:D:2022:314], and (ii) erasure of accounts/profiles relating to services no longer used.[38]

In recent years, an interesting tendency has emerged in the examined decisions, which could be considered a kind of **'distorting effect'** of certain erasure requests. This means that the GDPR is being used for **purposes that are not primarily aimed at protecting personal data**.

The most evident cases in this respect concern the 'weaponisation' of the GDPR, as seen in the EDPBI:CY:OSS:D:2023:1032 case. In these cases, complaints are followed by lengthy interactions between the parties involved, primarily because the data subjects persist in making their claims without providing the specific evidence requested by the SA. While this risk is inherent in all legal claims, it would be necessary to introduce deterrents for frivolous claims.

In many other cases, the distortion lies in the instrumental use of the right to erasure to achieve different, indirect results that are the primary objective of the data subject's request. Data protection rights can therefore serve as a means of requesting the erasure of information relating to an old book [EDPBI:LU:OSS:D:2023:810, the data subject's request was to remove from a website 'the reference page of his book and his personal data related to his book and author status'; see also EDPBI:LU:OSS:D:2023:702], properties [EDPBI:DEHH:OSS:D:2023:1125], business activities [EDPBI:CY:OSS:D:2024:1426], flights [EDPB:SE:OSS:D:2025:1825], and unwanted packages [EDPBI:LU:OSS:D:2023:705].[39] Regardless of the outcome of these requests, some of which were rejected in the decided cases, it is clear that data protection is sometimes used instrumentally to protect other interests.

Finally, a group of cases deserves attention, e.g. EDPBI:SE:OSS:D:2023:763; they relate to social media, gaming and other online service accounts. In these cases, data subjects' requests for erasure are more related to account management than to issues directly focused on the deletion of their personal data.[40] These cases also emphasise the importance of **implementing self-service tools that facilitate the exercise of data subjects' rights**.[41] The use of such a tools should not only be encouraged, but also be

[37] See also EDPBI:DEBE:OSS:D:2018:9 and Section III.1.

[38] See e.g. EDPBI:DESL:OSS:D:2019:11.

[39] The broad use of the right to erasure has also raised doubts in certain cases about the existence of personal data processing, as in the case of the removal of aircraft data from Flightradar24 not to be tracked [EDPBI:SE:OSS:D:2025:1825].

[40] These cases cover various requests, including the deletion of fake accounts created by bad actors, the procedure for deleting or suspending account (e.g., failure by the data controller to communicate account erasure, suspension due to inappropriate behaviour in violation of the terms of use) as well as the deletion or change of a data subject's username [EDPBI:IE:OSS:D:2023:1054; EDPBI:IE:OSS:D:2023:990; EDPBI:FR:OSS:D:2023:981; EDPBI:IE:OSS:D:2023:966; EDPBI:IE:OSS:D:2023:941; EDPBI:IE:OSS:D:2023:908; EDPBI:IE:OSS:D:2023:843]. However, some cases concern the traditional exercise of the right to erasure, dealing with requests to remove content uploaded by third-party users. See, e.g., EDPBI:IE:OSS:D:2023:1069; EDPBI:IE:OSS:D:2023:1026.

[41] See also EDPB. 2023. Guidelines 01/2022 on data subject rights - Right of access. Version 2.1. Adopted on 28 March 2023, https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf paras 35b, 137, and 138.

considered as a mandatory preliminary step before any data processing compliance request. This would reduce the number of Article 60 procedures for minor issues.

As the examined cases largely concern fairly basic situations, at least from the point of view of compliance with Article 17, the main issue to consider are: (i) bottlenecks and shortcomings in the internal handling procedure for data subjects' requests, (ii) the delisting/erasure process, and (iii) the presence of an overriding legitimate interest or other conditions justifying the processing despite a 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 mentioned above.

As with the right to object, issues relating to data subjects' requests refer to two main activities: exercising the right (see IV.2) and handling requests (see IV.3)[42]. As a result, the issues related to these two activities 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 request 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**[43] without creating cumbersome procedures. In this regard, critical issues concern the identification of the data subject and the **proof of identification**.[44]

Although Article 12(6) allows the data controller to ask for additional information in the event of reasonable doubt as to the identity of a data subject, a specific assessment is required to determine whether a reasonable doubt exists.[45]

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.[46] The undue request of identity documents as a condition for the exercise of the right to

[42] See also EDPB. 2026. Coordinated Enforcement Action. Implementation of the right to erasure by controllers, https://www.edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-implementation-right-erasure_en.

[43] Article 12.2 GDPR.

[44] See e.g. EDPBI:DK:OSS:D:2019:69.

[45] 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 circumstances, such as suspicion of identity theft or account piracy). These guidelines were endorsed by the EDPB on 25 May 2018. Also see EDPB. 2023. Guidelines 01/2022 on data subject rights - Right of access, section 3.2 on "Identification and authentication".

[46] 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. See also EDPB. 2023. Guidelines 01/2022 on data subject rights - Right of access. Version 2.1. Adopted on 28 March 202. See also EDPBI:IE:OSS:D:2023:796; EDPBI:FR:OSS:D:2023:1012; EDPBI:IE:OSS:D:2023:1028; EDPBI:SE:OSS:D:2024:1527.

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).[47]

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[48], 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.[49]In more general terms, the authentication method must be 'relevant, appropriate and proportionate', taking into account 'the type of personal data processed (e.g. special categories of data), the nature of the request, the context in which the request is made, as well as any damage that may result from inappropriate disclosure' [EDPBI:FR:OSS:D:2024:1286]. Finally, when authentication is justified, attention must be paid to the means used to share identity documents in order to adequately protect them (see, for example, EDPBI:NO:OSS:D:2024:1126 in a case involving an ID card shared via an unencrypted email).

Conversely, it is possible, for example, to provide a unique identifier to users at the end of the registration process,[50] 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,[51] to use other means of identification, such as via an online call,[52] 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].

With regard to 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.[53]

Finally, 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 request of erasure from the data subject is not necessary, as there is an

[47] See EDPBI:IE:OSS:D:2020:166.
[48] On the contrary, no further identification measures have been necessary when the data subject has used the email account provided upon creation of the service account, see e.g. EDPBI:CY:OSS:D:2024:1120.
[49] See also EDPBI:FR:OSS:D:2019:3.
[50] See EDPBI:DK:OSS:D:2019:69.
[51] See also EDPBI:LU:OSS:D:2019:14 and EDPBI:LU:OSS:D:2020:94.
[52] See also EDPBI:MT:OSS:D:2019:26.
[53] See EDPBI:DK:OSS:D:2020:151.

independent obligation arising for the data controller to delete data regardless of the request[54] [EDPBI:DEBE:OSS:D:2021:229].

3. Data subjects' requests: handling procedures

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. 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**, and mainly characterised the initial implementation of the GDPR by some controllers[55].

The most frequent case concerns delays in the erasure process due to **poor internal organisation**[56] 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].[57]

The relationship between data controllers and data processors, if not properly managed, may also lead to **lack 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

[54] 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").

[55] See also e.g. EDPBI:MT:OSS:D:2019:60.

[56] 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). See also EDPBI:FR:OSS:D:2023:572.

[57] See also EDPBI:CZ:OSS:D:2021:312; EDPBI:FR:OSS:D:2020:105. EDPBI:FR:OSS:D:2020:105. See, more recently, EDPBI:FR:OSS:D:2023:999. In this case, a company did not consider implementing an automatic message to inform people sending emails to the old customer support address that it was no longer used, when setting up the new one. Although the old email address was no longer available on the company's website, it was still active and listed on different websites.

request internally instead of forwarding it to the controller, as required by the nature of the service and task allocation].[58]

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].[59]

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[60]] or this information was provided with delay.[61]

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].

Finally, a variety of errors in the processing and management of data subjects' requests (e.g. failure to record users' objections to marketing, technical errors when sending communications, unsynchronised databases, reading only part of the data subject' claim, etc.) can affect the data subject's rights.[62]

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.[63]

Human error when handling data subjects' requests can also include **failing to notify individuals of erasure**, **failing to communicate internally**, and **providing**

[58] See also EDPBI:BE:OSS:D:2025:1668, in a case involving a lack of synchronisation between the controller and third-party services when handling the request for erasure.
[59] 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.
[60] See also EDPBI:DEBE:OSS:D:2020:156, see also EDPBI:FR:OSS:D:2020:84.
[61] See also EDPBI:HU:OSS:D:2020:118.
[62] See, e.g., EDPBI:EE:OSS:D:2023:1029; EDPBI:FR:OSS:D:2023:1012; EDPBI:CY:OSS:D:2023:927; EDPBI:LU:OSS:D:2023:812; EDPBI:FR:OSS:D:2023:537; EDPBI:EE:OSS:D:2024:1445.
[63] 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.

data subjects with incorrect information on how to manage account deletion and similar issues.[64]

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,[65] data controllers are required to ensure the effectiveness of all data subjects' requests concerning the exercise of the right of erasure, and personal data must be systematically erased when requested.

Against this background, the automation of the controller's internal process can reduce both the 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.

Finally, a topic that has been little explored and potentially raises difficulties for controllers concerns **the proof that erasure has occurred**. In this regard, in considering the difficulties in providing proof of the non-existence of erased data, EDPBI:DE:OSS:D:2023:929[66] stressed that the 'data controller must be able to demonstrate compliance with personal data processing principles, in accordance with the liability principle set out in article 5.2 of the GDPR. In this respect and in this specific case, the data controller may in particular provide a screenshot showing a negative result, i.e. highlighting that the database no longer contains the personal data of the data subject requesting erasure, or that the user cannot be found and has been deleted.'

---

[64] See, e.g., EDPBI:SE:OSS:D:2022:1805; EDPBI:FR:OSS:D:2023:1082; EDPBI:IE:OSS:D:2023:1059; EDPBI:IE:OSS:D:2023:1042; EDPBI:IE:OSS:D:2023:1041; EDPBI:EE:OSS:D:2023:1015; EDPBI:FR:OSS:D:2023:998; EDPBI:IE:OSS:D:2023:914; EDPBI:IE:OSS:D:2023:835; EDPBI:IE:OSS:D:2023:794; EDPBI:DK:OSS:D:2023:696; EDPBI:SE:OSS:D:2023:694; EDPBI:PL:OSS:D:2023:681; EDPBI:SI:OSS:D:2024:1546; EDPBI:LU:OSS:D:2024:1390; EDPBI:LU:OSS:D:2024:1316; EDPBI:SE:OSS:D:2024:1270; EDPBI:FR:OSS:D:2024:1128.

[65] 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".

[66] See also EDPBI:CY:OSS:D:2023:927.

4. 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 data subject objects to the processing and 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) for other prevailing reasons.

As to the first category of cases, they mostly deal with the prevalence of data **controllers' legitimate interest**[67] [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]. Regarding the cases where prevailing interests take precedence over the right to erasure, the decisions examined include a limited number of cases of the exercise of right to be forgotten in the context of the activity of search engines,[68] which are more common in national and regional decisions of individual Supervisory Authorities. When considering the right to erasure in relation to online information, competing interests may restrict the exercise of this right. For example, in the case of online information concerning an imposed prison sentence of 30 years, which was handed down in 1993 and had since been served, the initial request to delete over 100 URLs was limited to only twelve due to public interest in the information [EDPBI:IE:OSS:D:2023:1085].[69]

[67] See also EDPB. 2025. One-stop-shop Case Digest Legitimate interest, by Dr. TJ McIntyre, available at https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/one-stop-shop-case-digest-legal-basis_en.

[68] See, e.g., EDPBI:IE:OSS:D:2023:996; EDPBI:IE:OSS:D:2023:903; EDPBI:IE:OSS:D:2023:890; EDPBI:IE:OSS:D:2023:844; EDPBI:IE:OSS:D:2023:771.

[69] At a national level, the public interest in receiving information is also often the basis for rejecting requests for erasure. For example, see the decision of the Conseil d'État (10ème - 9ème chambres réunies) on 30 June 2023, case no. 460269, https://www.legifrance.gouv.fr/ceta/id/CETATEXT000047773954/. This decision confirmed the French data protection authority's decision in a case regarding a complaint concerning the refusal of a request for erasure with regard to the 2010 annual report of the Mission interministérielle de vigilance et de lutte contre les dérives sectaires (Miviludes). The report warned the public about the risks associated with training in non-conventional therapeutic practices, citing those offered by the applicant at the time. The court ruled that this information, published online by Miviludes, forms part of its public interest mission to inform the public about the risks of sectarian practices. Therefore, it does not fall within the category of personal data processing that may be subject to the right to erasure under Article 17 of the GDPR. See also Raad van State, 6 August 2025, case No. 202204928/1/A3, in which the Dutch Council of State finally confirmed the initial decision of the Dutch Data Protection Authority, adopted on 12 July 2019. The case referred to an access to mental health services, followed by a request for the erasure of medical records (as the appellant decided not to start treatment, the only record was an interview between the appellant and a social psychiatric nurse), which was carried out, but a note of the removal request was kept in the system. The appellant asked to the Dutch DPA to remove this note under Article 17 of the GDPR. Based on the national legislation, the Council of State confirmed that data processing was necessary for reasons of public interest in the field of public health. This included the management and accountability of mental health services.

Regarding the **delisting process (also known as de-referencing)**,[70] additional issues arose concerning the range of search terms to be used for delisting [e.g. EDPBI:IE:OSS:D:2023:890 where the respondent explained that the previously delisted URL 'had in fact been delisted in 2020 against the particular search term submitted at the time. Regarding the remaining URLs, the Respondent explained that it had informed the Data Subject (in direct response to the delisting request made) that as they had included additional search terms other than their name(s) in the search criteria (in this case, place names), the returned URLs were not eligible for delisting against those search terms. However, following receipt of the DPC's correspondence and in the interests of amicably resolving the matter, the Respondent agreed to proactively delist the requested URLs from appearing in search results when using the Data Subject's previous legal name and their current legal name as search terms.'].

Another issue relating to the balancing of interests, which is also common for social media, concerns **the geographical scope of erasure**.[71] This is often limited to the EU – or EEA and UK [EDPBI:IE:OSS:D:2023:788] – or a specific country with regard to URL availability [e.g. EDPBI:IE:OSS:D:2023:833 where 'Respondent had taken steps to block from view the content in question [blogpost] from its Blogger platform in Spain, which is where the Data Subject was based.'].[72] However, the different geographical scope is not discussed or explained in detail in several decisions.[73]

Regarding the **nature of the interests** that can prevail over the data subject's request for erasure, they are heterogeneous and include not only the freedom of expression and information [EDPBI:BE:OSS:D:2024:1395],[74] but also other interests vested in legal obligations,[75] e.g. relating to debts [EDPBI:AT:OSS:D:2024:1418],[76] the storage of passenger name record (PNR) [EDPBI:SE:OSS:D:2025:1598], public registers [EDPBI:DEHH:OSS:D:2023:1125; EDPBI:DEHH:OSS:D:2024:1124; EDPBI:DEHH:OSS:D:2024:1266; EDPBI:DEHH:OSS:D:2025:1806],[77] or relating to the

[70] See also EDPB. 2019. Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1). Version 2.0. Adopted on 7 July 2020, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en, p. 5 ('As a result, both Article 17 and Article 21 GDPR can serve as a legal basis for delisting requests.').

[71] See also CJEU, Case C-507/17, *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)*, 24 September 2019, ECLI:EU:C:2019:772.

[72] See also EDPBI:IE:OSS:D:2023:758; EDPBI:IE:OSS:D:2023:757.

[73] See also EDPBI:IE:OSS:D:2023:1078; EDPBI:IE:OSS:D:2023:1064; EDPBI:IE:OSS:D:2023:1017; EDPBI:IE:OSS:D:2023:1001; EDPBI:IE:OSS:D:2023:833; EDPBI:IE:OSS:D:2023:788; EDPBI:IE:OSS:D:2023:758; EDPBI:IE:OSS:D:2023:757.

[74] On the balancing test between freedom of expression and the right to erasure, see also the decision of the Datenschutzbehörde (Austrian DPA), 2022-0.479.809, 29 March 2024, which refers to the relevant criteria set out in the case law of the ECHR and the CJEU.

[75] The relevance of interests vested in legal obligations is also acknowledged in decisions that are limited to the national level. See, e.g., a Dutch case decided by the Council of State (Uitspraak 202204928/1/A3, Raad van State) concerning an initial decision adopted by the national data protection authority regarding medical treatment and record-keeping.

[76] For similar cases at the national level decided by data protection authorities, see e.g. Information and Data Protection Commissioner (Malta), case CDP/COMP/57/2025.

[77] See also CJEU, Case C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*, 9 March 2017, OJ C 354, 26.10.2015. At national level, decisions in different countries recognise an overriding legitimate ground also to private registers with reference to the baptismal

nature of the contractual agreements and services provided [EDPBI:DE:OSS:D:2024:1285].

Regarding the 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].[78] Data controllers must **inform 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].

These **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 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 of 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].

registers and the interest of the Catholic Church in retaining personal data, having regard, on the one hand, to the purpose of the baptism register and the conditions under which it may be consulted, and, on the other hand, to the option open to any baptised person to have a note entered in the register stating their decision to renounce any connection with the Catholic religion. See, e.g., Conseil d'État (10ème - 9ème chambres réunies) on 2 February 2024, case no. 461093, which confirmed the decision of the French data protection authority. The same interpretation has been followed in Italy by the Garante in several decisions; see a list of them (in Italian) here: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1044304. But see the Belgian SA's decision no. 169/2023 of 19 December 2023, which ordered the Diocese of Ghent to comply with the complainant's requests to object to and erase his data. On 11 December 2024, the Market Court refers preliminary questions to the Court of Justice of the EU in the appeal that the diocese of Ghent filed against decision 169/2023, https://www.dataprotectionauthority.be/citizen/according-to-the-be-dpa-a-baptized-person-has-the-right-to-be-deleted-from-the-baptismal-register; see Request for a preliminary ruling from the Hof van beroep Brussel (Belgium) lodged on 9 January 2025 – Bisdom Gent VZW v Gegevensbeschermingsautoriteit; Interveners: JM and Others; Case C-12/25, Bisdom Gent, C/2025/1878), https://juris.curia.europa.eu/juris/document/document.jsf?text=&docid=297628&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=178617.

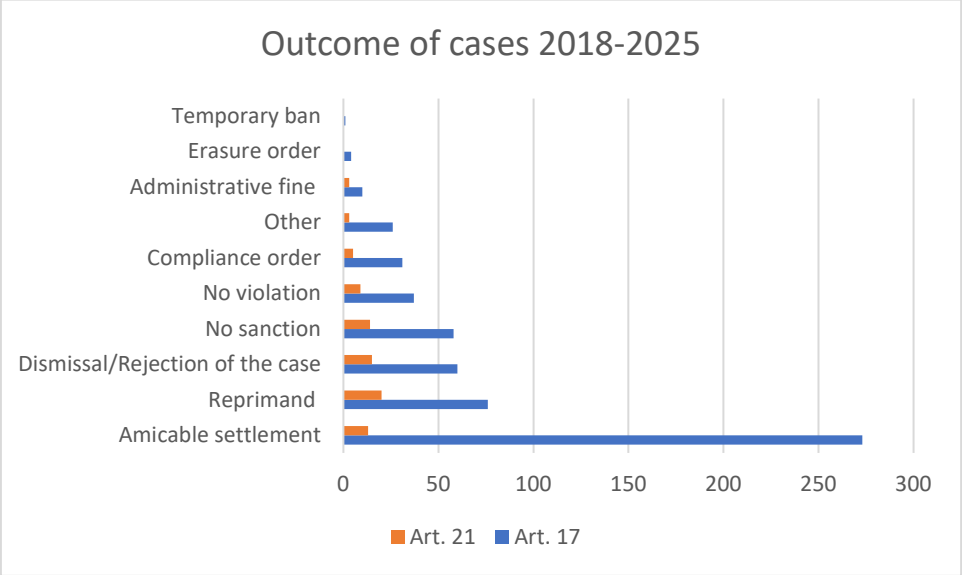
[78] See also CJEU, case C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni.

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].[79]

V. 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 these reasons, the main outcome for cases that are not resolved through an amicable settlement – often involving the discontinuation of data processing and the erasure of personal data – is a reprimand, as can be seen from the table below.



This emphasises that the GDPR and its implementation are **based on promoting values rather than punishment**. This approach prioritises effective, rights-oriented design, supervision and guidance over sanctions.

[79] It has also been noted that, when data was originally collected in the aftermath of an alleged violation by a data subject of the controller's contractual documentation, but the reasons for its collection and retention are no longer applicable and there is merely an abstract possibility of potential future lawsuits, the continued storage of the data cannot be considered legitimate once the underlying incident has been closed. See, e.g., Higher Regional Court of Karlsruhe (Oberlandesgericht Karlsruhe), Germany, case no. 14 U 150/23, 15 January 2025, https://www.landesrecht-bw.de/bsbw/document/NJRE001597671 (the operator of an internet platform originally collected personal data following an alleged violation of the terms of use, community standards, and criminal provisions by the plaintiff. The purpose was to investigate, document, and support any further measures, such as temporarily or permanently suspending the account and, if necessary, terminating the contractual relationship. However, this purpose ceased to exist when it became apparent that the content in question had not been posted by the plaintiff herself, but by unknown third parties in the course of a hacking attack.).

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.

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"].

With regard to the remedies provided to data subjects and the entire procedure set out in Article 60, one critical issue that has emerged is the **length of the procedure**. Despite the limited nature of the potential prejudice suffered by the data subject, it often takes many months or even years before some cases are closed [see, e.g., EDPBI:IE:OSS:D:2023:1080; EDPBI:IE:OSS:D:2023:1081; EDPBI:IE:OSS:D:2023:1073]. In this respect, the new procedural rules recently adopted by the EU legislator may alleviate this issue, as they aim to ensure swift and effective coordination between Supervisory Authorities.

Finally, it is worth noting that Supervisory Authorities in one country are paying attention to the decisions adopted by other countries and, in some cases, explicitly refer to them [see, e.g., EDPBI:CY:OSS:D:2024:1120]. This emphasises **the importance of the online repository** created by the EDPB, and the importance of carrying out thematic analyses of this body of decisions, in order to make Supervisory Authorities aware of the main trends and thus achieve a more harmonised application of the GDPR.


EDPB
European
Data Protection
Board