2025 Coordinated Enforcement Action

Implementation of the right to erasure by controllers

Adopted on 10 February 2026

Executive summary

In October 2020, the European Data Protection Board ('**EDPB**') decided to set up a Coordinated Enforcement Framework ('**CEF**') with a view to streamlining enforcement and cooperation among supervisory authorities at EDPB level. Since then, three CEF actions have been completed on the use of cloud services by public bodies, the designation and position of data protection officers and the right of access. For the fourth edition, the EDPB chose to take a look at the implementation by controllers of another data protection right, namely: the right to erasure. The right to erasure is one of the most frequently exercised data subject rights and has given rise to many complaints across the EEA and to a growing number of decisions from SAs.

Throughout 2025, 32 supervisory authorities ('**SAs**') across the EEA launched coordinated investigations into the compliance of controllers with the right to erasure under the GDPR[1], to examine how this right is implemented in practice by a broad range of controllers, in organisations of various sizes and across different sectors.

The CEF action was carried out at national level (1) as a fact-finding exercise, (2) to identify if a formal investigation is warranted, and/or (3) through a formal enforcement investigation or follow-up of an ongoing formal investigation. In this context, the SAs agreed on a questionnaire to guide their investigations and actions and to use when contacting controllers, and a total of 764 controllers responded to the questionnaire.

The present report aggregates the findings of all the SAs participating in the CEF action[2]. Seven recurring issues were identified by SAs, as set out below. The results confirmed some of the findings of the 2024 coordinated action on the right of access, for example when it comes to the lack of appropriate internal procedures to handle data subjects' requests, or the lack of sufficient information provided to data subjects. In addition, participating SAs reported specific findings related to the reliance by some controllers on inefficient anonymisation techniques to handle erasure requests as an alternative to deletion. SAs also noted inconsistent practices and the difficulties faced by controllers regarding the determination of retention periods and the deletion of personal data in back-ups.

As the right to erasure is not an absolute right, some controllers face difficulties in assessing and applying the applicable conditions for the exercise of this right, including in carrying out the different balancing tests between the right to erasure and other rights and freedoms.

While the overall level of compliance of the responding controllers has been assessed as "average" (depending on factors such as the size of the controller, the number of erasure requests received and its sector), a number of best practices have also been observed. The table below lists seven recurring issues that were identified during the coordinated action. Non-binding recommendations are also included for each issue. The report highlights in more detail additional recommendations, addressed either to controllers and/or SAs/the EDPB.

[1] And the corresponding right to erasure applicable to EU institutions under Regulation (EU) 2018/1725, which are supervised by the European Data Protection Supervisor (EDPS) who participated in this CEF action.
[2] The SAs' national reports are attached to this report and provide further detail on the results obtained and the analyses made at national level. These were submitted during September 2025 and represent the situation at that point in time.

List of recommendations for controllers and actions that SAs/EDPB may consider for each issue
Issue 1: Absence of a documented and updated internal procedure to handle erasure requests
• The SAs/EDPB may consider providing further templates and guidance, including flowcharts or checklists, to assist controllers in handling erasure requests. • Controllers: Establish and update internal procedures with clear deadlines and steps and allocating responsibilities among actors for handling and recording erasure requests.
Issue 2: Absence of, or inadequate training
• Controllers: Raise awareness and provide resources to enable regular role-specific training using various formats, if needed by relying on the existing resources published by SAs.
Issue 3: Insufficient information provided to data subjects
• The SAs/EDPB may consider making available a template form that data subjects could use to exercise their right to erasure, or giving more visibility to existing templates. • Controllers: The privacy notice should be regularly reviewed and updated to ensure that data subjects receive clear and understandable information on the exercise of the right to erasure.
Issue 4: Misuse of and legal uncertainty on the exceptions to deny erasure requests
• The SAs/EDPB may consider providing further targeted guidance and clarification on the correct application of the exceptions to deny erasure requests. • Controllers: Ensure that compliance or legal teams are involved in decision-making processes concerning the refusal or postponement of erasure requests.
Issue 5: Difficulties in defining and implementing data retention periods
• The SAs/EDPB may consider adopting further practical guidance on how to define and implement retention periods, also taking into account national legal obligations. • Controllers: When documenting retention periods for instance in the records of processing activities, clearly specify any applicable legal obligations justifying the retention of personal data for a defined period.
Issue 6: Deletion of personal data in the context of back-ups
• The SAs/EDPB may consider adopting further guidance to explain how controllers should practically deal with erasure in back-ups and what "without undue delay" means in this context. • Controllers: Follow established standards to erase and destroy data in a secure and structure manner.
Issue 7: Difficulties with anonymisation to respond to erasure requests
• The SAs/EDPB may consider continuing to issue practical actionable guidance on the subject. • The SAs/EDPB may consider providing more guidance to help controllers ensure that personal data can no longer be linked to an identifiable individual.

The CEF highlighted that extensive guidance documents and templates exist at national level to help controllers comply with the right of erasure, both general and targeted to specific contexts. Based on the CEF results, many SAs plan to carry out further actions at their level to communicate and raise awareness on this right. Some additional EDPB-level actions could also be considered in the future, for example through the issuance of practical and actionable guidance to address the issues listed above and resolve the inconsistent practices that were observed. In doing so and in line with its Helsinki Statement of 2 July 2025, the EDPB would leverage on the guidance and templates identified at national level in the context of this CEF action.

This report also includes information about the participating SAs' actions relating to the right to erasure, both independently of and in context of the CEF action. Some of these actions are still ongoing, especially when formal investigations were launched. Accordingly, this report does not constitute a definitive statement of the actions carried out within the CEF action

Table of Contents

1 Introduction

In October 2020, the European Data Protection Board ('**EDPB'**) decided to set up a Coordinated Enforcement Framework ('**CEF**')[3]. The CEF is part of the first key action identified under the second pillar of its 2024-2027 Strategy[4], together with the creation of a Support Pool of Experts ('**SPE**'), aiming at streamlining enforcement and cooperation among supervisory authorities (collectively '**SAs**', or individually '**SA**').

In October 2024, the EDPB selected the topic '**Implementation of the right to erasure by controllers**' for its 2025 CEF action[5]. The EDPB decided to prioritise this topic given that this right is one of the most frequently exercised data protection rights and one about which SAs frequently receive complaints.

The EDPB and participating SAs announced the initiation of the action as of 5 March 2025[6]. Since then, 32 SAs across the EEA launched coordinated investigations into the compliance with the right to erasure. More specifically, nine SAs have initiated new **formal investigations or have continued ongoing ones**. Twenty-three SAs stated that the initial procedural framework of their action was **fact-finding**. Among them, fourteen indicated that they would determine **follow-up actions** based on the results.

The present report aggregates the findings of SAs participating in the CEF action and provides a state of play of their work. In particular, the first part of this report presents statistics regarding the controllers addressed by each SA, while the second part analyses the positive findings (such as best practices) but also the challenges and issues identified. In addition, it presents an overview of the actions already implemented or ongoing, including guidance, enforcement actions or potential actions by SAs. The SAs' national reports are annexed to this report and provide further detail on the results obtained and the analyses and observations made at national level[7].

With this fourth CEF action, the EDPB intends to:

- ensure that the right to erasure is effectively exercised by data subjects across the EEA,
- understand how controllers comply with the right to erasure in practice by analysing and comparing the processes they put in place,
- identify good practices and the most important challenges to the compliance with this right, in particular for further guidance on this topic,
- collect the experience and conclusions of the participating SAs under this CEF action for analysis.

[3] EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679 (EDPB, 20 October 2020).
[4] EDPB Strategy 2024-2027, adopted in April 2024.
[5] 'CEF 2025: EDPB selects topic for next year's Coordinated Action', 10 October 2024, available at https://www.edpb.europa.eu/news/news/2024/cef-2025-edpb-selects-topic-next-years-coordinated-action_en.
[6] 'CEF 2025: Launch of coordinated enforcement on the right to erasure', 5 March 2025, available at https://www.edpb.europa.eu/news/news/2025/cef-2025-launch-coordinated-enforcement-right-erasure_en.
[7] These national reports were submitted by participating SAs over the course of September 2025. They therefore represent the situation at this point in time. Furthermore, it should be noted that all seven German SAs participating in this CEF action (Baden-Württemberg, Brandenburg, Mecklenburg-Western Pomerania, North Rhine-Westphalia, Lower Saxony, Rhineland-Palatinate, and Federal (BfDI)) have drafted a common report with their consolidated findings. The findings presented in this consolidated report may not be valid for other German SAs which have not participated in this CEF action. Lastly, not all findings, impressions, possible explanations or solutions expressed in the participating German SAs' report are valid or apply fully to each participating German SA. Lastly, the Annex does not include a national report for AT SA, as AT SA provided some figures, which were used to calculate the aggregated figures in Section 3 of this CEF report, but not the rest of the national report template.

2 Background and methodology

2.1 Legal overview & background on EDPB's activities relating to the right to erasure

The right to erasure or right to be forgotten was codified in the GDPR, allowing its exercise based on more grounds than under Directive 95/46/EC. The right to erasure under Art. 17 GDPR[8] is still not an absolute right. This right can only be exercised based on one of the six following grounds:

- the personal data are no longer necessary in relation to the purposes for which they were collected or processed,
- the data subject withdraws consent on which the processing is based, and there is no other legal ground for the processing,
- the data subject successfully exercised their right to object, or the data subject objects to the direct marketing processing,
- the personal data have been unlawfully processed,
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law applying to the controller, or
- the personal data have been collected in relation to the offer of information society services to a minor based on consent.

The CJEU has already issued several rulings, clarifying some of the above grounds to exercise the right to erasure[9].

The controller can refuse to comply with an erasure request based on one the five exceptions set out in the GDPR:

- for exercising the right of freedom of expression and information,
- for compliance with a legal obligation which requires processing by Union or Member State law and applying to the controller or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,
- for reasons of public interest in the area of public health (Article 9(2)(h) and (i) and Article 9(3) GDPR),
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 89(2) GDPR in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing), or
- for the establishment, exercise or defence of legal claims.

[8] Art. 19 EUDPR applies to EUIs. This provision is, *mutatis mutandis*, identical to Art. 17 GDPR, except on the following: the data subject's exercise of the right to object is not mentioned in Art. 19(1)(c) EUDPR and the references to "Union or Member State law" do not appear.

[9] See in particular, Judgment of 27 October 2022, C-129/21, Proximus NV v Gegevensbeschermingsautoriteit, ECLI:EU:C:2022:833, on a subscriber's request to be removed from the directory and the application Art. 17(1)(b) and Art. 17(1)(d), Art. 17(2) and Art. 19 GDPR; Judgment of 7 December 2023, SCHUFA Holding, Joined Cases C 26/22 and C 64/22, ECLI:EU:C:2023:958, paras. 106-113, on Art. 17(1)(c) and 17(1)(d) GDPR.

There are several pending referrals before the CJEU to further clarify, among others, the conditions to exercise the right to erasure and the exceptions allowing to reject erasure requests[10].

Besides Art. 17 GDPR, Art. 12 GDPR[11] defines the modalities for the exercise of the rights of the data subject, including the right to erasure.

SAs receive many complaints from data subjects regarding the exercise of this right and a number of their decisions relate to this matter. SAs cooperate frequently as part of the one-stop-shop ('**OSS**') mechanism to handle the complaints they receive and reach consensus. At the date of publication of this report, more than 500 final decisions relating to the right to erasure are available in the EDPB register of OSS final decisions[12]. This makes this risk the most frequent topic that is covered by SAs in their final decisions. A "case digest" was published in 2023 to summarise the main findings of some of these decisions (commissioned through the SPE)[13] and is being updated with more recent decisions.

The EDPB adopted several documents where it provides guidance on some aspects of the right to erasure[14]. In addition, it published an 'SME Guide', which is addressed to smaller controllers and is available in 18 different EU languages. This guide sets out a checklist explaining what to do concerning data subject rights and how to handle data subject rights requests. More specifically, it includes a section dedicated to the right to erasure with a short video[15].

2.2 Methodology of the CEF action

Participating SAs first agreed on a questionnaire drafted in English designed to contact the respective controllers, which was then translated into the relevant EU languages and sent to the controllers of each SA's choice at national level. The questionnaire was drafted in a neutral manner to allow participating SAs to decide which controllers should be addressed (e.g. public or private sector, specific sectors or cross-sectoral approach), by which means to address them and in which procedural context (e.g. enforcement or fact-finding). The questionnaire covers a range of topics relating to the right to erasure, from the internal request-handling process put in place by to the implementation of the exceptions to the right to erasure and the steps taken to inform other controllers and data recipients about the erasure request. Lastly,

[10] The pending referrals include: Referral C-40/25 (CRIF, 23 Jan 2025) regarding onward transfers, Referral C-12/25 (Bisdom Gent, 9 January 2025) regarding the baptism registry, Referral C-474/24 (NADA Austria and Others, 4 July 2024), Referral C-312/24 (Darashev, 29 April 2024) regarding Articles 17(1)(a) and 17(1)(d) GDPR and the data added to the employee's human resources file and Referral C-655/23 (Quirin Privatbank, 7 November 2023) regarding onward transfers and illicit disclosure.
[11] Art. 14 of Regulation (EU) 2018/1725 (EUDPR) applies to the EU institutions, bodies, offices and agencies (EUIs), which are supervised by the European Data Protection Supervisor (EDPS). This provision is, *mutatis mutandis*, identical to Art. 12 GDPR, except on the following: the possibility to charge a reasonable fee to the data subject in certain situations (Art. 12 (5) lit. b GDPR) is **not** mirrored in Art. 14 (5) EUDPR.
[12] Available at https://www.edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en. Decisions can be filtered depending on the GDPR provision(s) they relate to. In this case, the search was done based on Art. 17 GDPR or with the tag "right to erasure".
[13] OSS Case Digest on the right to object and the right to erasure, 9 December 2022, Alessandro Mantelero, 9 December 2022, available at https://www.edpb.europa.eu/system/files/2023-02/one-stop-shop_case_digest_on_the_right_to_object_and_right_to_erasure_en.pdf.
[14] See for example, 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, where the EDPB's guidance on Articles 17(1) and 17(3) could still be relevant to a certain extent to controllers who are not search engines); Guidelines 01/2022 on data subjects rights – Right of access (which are especially relevant when it comes to the interpretation of Article 12 GDPR); Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (paras. 76-77, before public consultation); Guidelines 02/2025 on processing of personal data through blockchain technologies (before public consultation).
[15] The EDPB data protection guide for small business, available at https://www.edpb.europa.eu/sme-data-protection-guide/home_en.

the questionnaire included a number of open questions, allowing SAs to get deeper insights into the compliance of controllers with this right.

When reviewing the results of the survey, one has to bear in mind the following aspects:

- The questionnaire has been translated into twenty different languages, in which they were also answered. While translations have been proofread by SAs, the wording of the questions may have been understood or interpreted differently depending on language or cultural differences.
- Each participating supervisory authority developed its own strategy for the recipients of this commonly-built questionnaire.
- The SAs who decided to launch a formal investigation audited a smaller number of organisations (3-9).
- The SAs doing a fact-finding exercise had different strategies. Some SAs decided to contact a large number of controllers (hundreds for MT, LV and NL SAs, thousands for BG and PL SAs) while others targeted a smaller pool (e.g. less than 20 for LI, LU, EE, HU, PT and ES SAs).
- A few SAs made it possible for controllers to complete the survey without providing their identity (e.g. FI, LV, BG, MT SAs). In contrast, other SAs contacted previously identified controllers.
- Certain SAs targeted a specific sector or category of controllers: some targeted only the public sector (e.g. European Union institutions [16] for the EDPS, public administration for AT SA) while others focused on certain areas of the private sector (e.g. online casinos for DK SA, controllers having a customer loyalty program in the retail sector for EE and EL SAs). However, half of the participating SAs decided to contact controllers from both the public and private sectors.
- The survey was either mandatory or optional for controllers to complete, depending on whether the questionnaire was completed as part of an enforcement action.
- Since only certain questions were considered mandatory, some SAs decided not to include all the questions of the commonly built questionnaire. In addition, some SAs slightly modified certain questions (e.g. to tailor them to specific controllers or sectors or adjust them to a pure enforcement context). A few SAs sent follow-up questions to responding controllers to clarify certain points.
- Some SAs asked controllers to provide documentation on their internal processes and analysed such documentation in light of the controllers' input, while others did not.
- Lastly, each SA collected between 3 and 155 answers to the questionnaire.

[16] This refers to EU institutions, bodies, offices and agencies.

3 Some figures

This section provides figures on the controllers which responded to the survey and the data they provided[17].

3.1 Responding controllers and their processing activities

A total of **764 controllers responded across the EEA**[18]. This year, certain SAs decided to contact a specific sector of activity or category of organisations. For instance, the EDPS and AT SA only contacted public-sector organisations, while ten SAs[19] decided to only contact private sector organisations. Finally, the other participating SAs chose organisations from both public and private sector. In total, 431 answers were processed from the public sector, 325 answers from the private sector and 8 from "other sectors"[20].

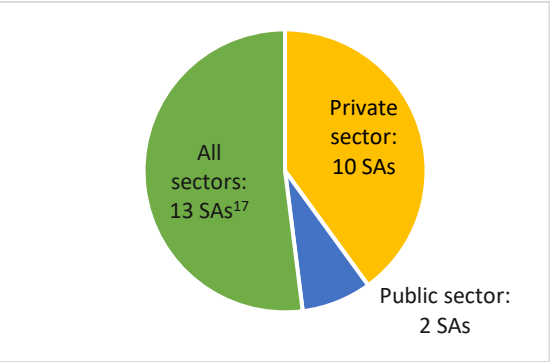

Figure 1: Sector of activities targeted by participant supervisory authorities

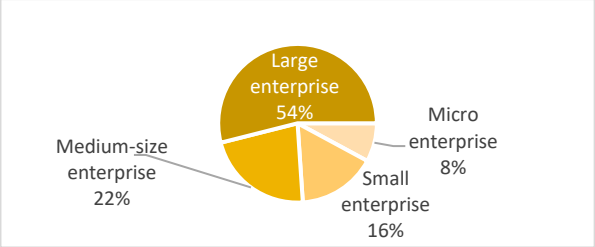

Figure 2: Repartition of private entities

enterprises to large companies[21].

Finally, the public sector was represented by local authorities (about half of public sector's answers), administrative authorities and agencies (about a third), various types of educational institution (e.g. school, university, etc) and, finally ministries.

About 3% of the answers received came from NGOs. Then, for the private sector, the sample size contained controllers of all sizes, from micro

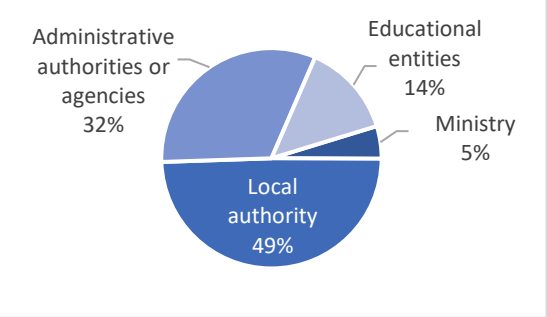

Figure 3: Repartition of public entities

[17] No figure was included in this section for CY SA. While 7 German SAs participated (Baden-Württemberg, Brandenburg, Mecklenburg-Western Pomerania, North Rhine-Westphalia, Lower Saxony, Rhineland-Palatinate, and Federal (BfDI), they provided a unique common report and thus are artificially counted as "1" SA in this graph.
[18] In total 7943 controllers were contacted by all the participating SAs. Four SAs, which were among the five who contacted the most controllers, had a significantly lower response rate (between 0.6% and 14%) than other SAs carrying out a fact-finding exercise (at least 60%). Identified factors that may have played a role in the gap in response rate are: the lack of controllers' resources, the voluntary nature of the questionnaire, the absence of a specific procedure in handling or documenting the erasure requests received, the fear of controllers that the SAs may open an investigation, the timing of the request (i.e. during summer holidays), the outdated contact information of certain controllers and, in some Member States, a possible distrust towards public administrations.
The nine SAs conducting formal investigations encountered no gap between the controllers contacted and those responding. Finally, ES SA received twice more answers than the number of controllers contacted as some of them spread the invitation, inviting several additional health departments and hospitals to participate.
All in all, each SA processed between 3 and 155 answers for a total of 764 answers.
[19] CZ, DK, EL, EE, FR, HR, HU, LU, LT, MT SA.
[20] These controllers were qualified as "other sectors" for different reasons, for example as a private entity providing a public service.
[21]

Participating SAs relied on a wide array of criteria when deciding whom to interview or audit, considering factors such as the sector of activity (see **Error! Reference source not found.**Figure 5), the size of the entity, and the number of data subjects concerned by the processing activities of the controllers. In particular, 19 SAs selected controllers affecting more than a million data subjects.

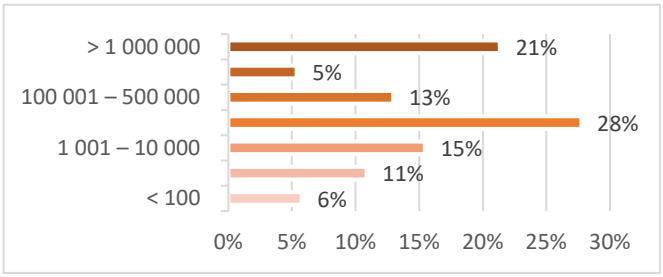

Figure 4: Repartition of controllers per range of concerned data subjects in their processing

Thus, the responding controllers were active in multiple sectors [22]. Following public administration from which more than 300 answers were gathered, the most represented sectors were the following: Health, Education, Finance and Retail. The responding controllers belonged to the following categories of entities:

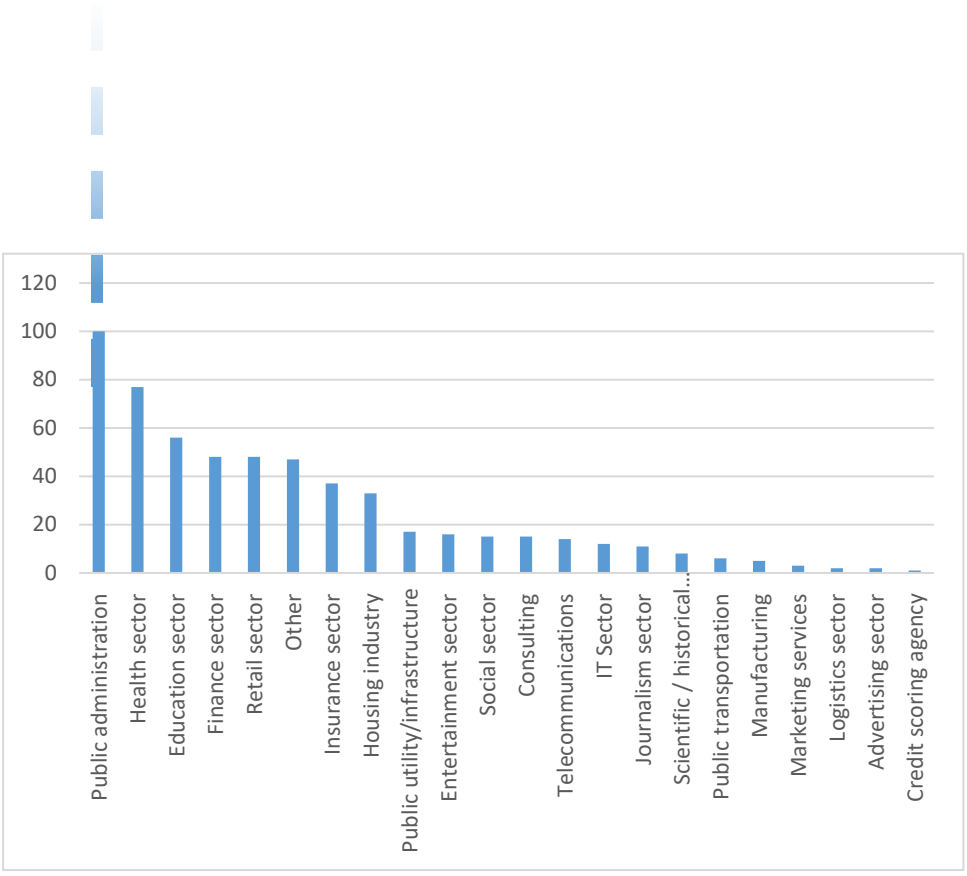

Figure 5: Main sectors of participating controllers

[22] For more detail, please see the national reports in the Annex. Controllers can be active in more than one sector.

Finally, while various sectors were addressed in this CEF, it is interesting to note that[23]:

- About 42% of the responding controllers processed personal data of children.
- About 42% of the responding controllers processed personal data of vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people).

3.2 Erasure requests reported by responding controllers

Taking into account this variety of profiles, it is noteworthy that the majority of the enquired controllers had not received a single request for erasure in the last two years.

While controllers were often chosen due to being in certain particular situations (for instance: processing sensitive data, processing a very large amount of data, etc.), about 70% of controllers still had received less than 10 requests per year.

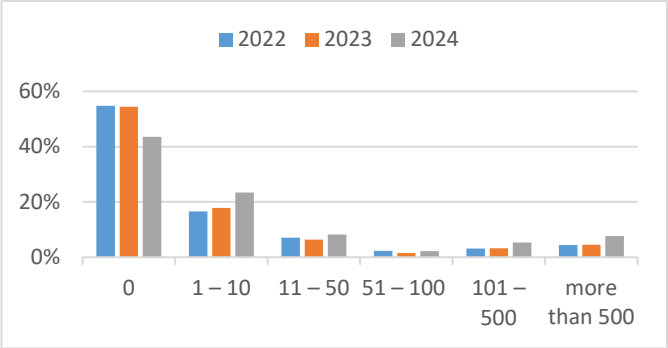

Figure 6: How many Art. 17 GDPR requests for erasure did the responding controllers receive per year?

When looking at the profile of the category of data subjects mainly concerned by the processing activities and at the data subjects who submit erasure requests more prevalently (see Figure 7), it appears that certain profiles are less likely to exercise their rights (e.g. applicants in public services, citizens toward public services, contractors, or job applicants/employees) while others seem less hesitant to do so (e.g. (potential) customers).

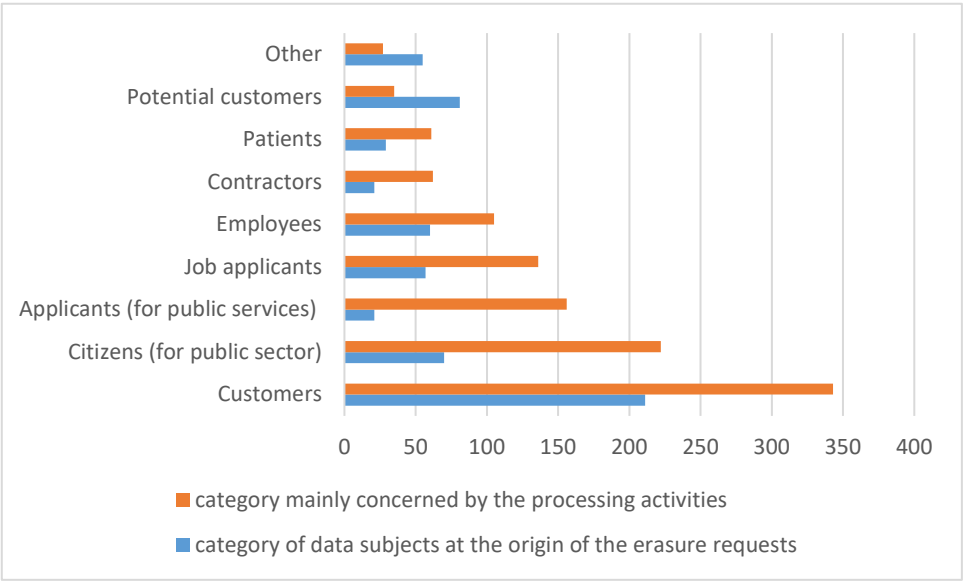

Figure 7: Profile of data subjects involved in the processing and of data subjects asking for erasure

[23] Please take note that some controllers may have considered children in "Vulnerable subjects" while others didn't.

Regardless of the context, 7 SAs noted that the parents or guardians of vulnerable subjects, as well as vulnerable subjects themselves were overrepresented in the requests, showing the importance of data subjects' rights for the more vulnerable individuals.

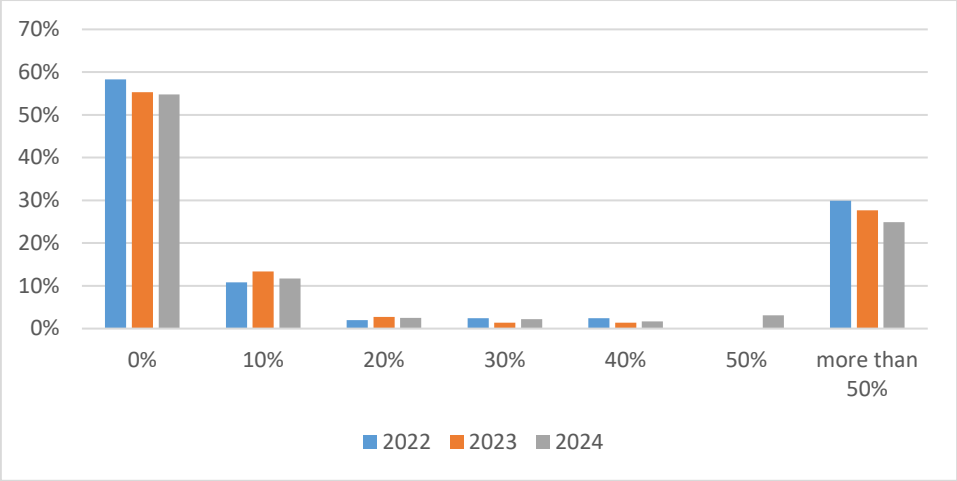

Figure 8: Out of received requests, what was the approximative percentage of rejected requests?

SAs enquired about the rejection of requests per controllers and answers showed two opposing trends: either controllers rarely rejected requests or controller rejected requests more than 50% of the time. The SAs who carried out enforcement actions noted that the rejection of requests by responding controllers was overall justified. This leads to the hypothesis that organisations that regularly refuse erasure requests can rely one of the exemptions provided by Article 17(3) GDPR. This is consistent with Figure 8 showing requests being either (almost) systematically accepted or very largely refused.

4 Positive findings and challenges identified

4.1 Level of compliance

According to almost two thirds of the participating SAs, the level of compliance can be assessed as "average", whereas a few SAs evaluated the level of compliance as "high". This is consistent with the findings from the SAs carrying out enforcement actions, who indicated that erasure requests are usually taken into account and, when refused, such refusal seems to be based on one of the GDPR exceptions. Many controllers also implement various good practices, as described below.

The following section discusses in more detail the recurring issues that SAs encountered.

The data collected indicate that the degree of compliance may vary depending on the size and type of the controller, the sector, the type of data processed, the number of erasure requests received and the number of data subjects affected. Larger organisations generally receive a higher number of requests and tend to have more formalised and structured internal procedures, including technical and organisational measures, to ensure compliance with data

protection requirements, including the compliance with requests exercising the right to erasure.

The results reported by SAs that compared the private and public sectors showed that private-sector controllers are generally better positioned, with clearer internal processes, established guidelines, and more frequent employee training.

Some SAs did not distinguish between different types of controllers and therefore could not report on potential differences.

In summary, differences in sector, size, and processing activities clearly influence not only the number of erasure requests received but also the overall level of compliance observed.

4.2 Challenges identified during the CEF action

The following sections detail some of the challenges identified during the CEF action, either by the participating SAs or by respondents themselves, which the EDPB considers to be the most relevant or the most frequent. For each challenge identified below, a list of non-binding recommendations is included for controllers, SAs and the EDPB, without prejudice to the provisions of the GDPR/EUDPR and to SAs' powers under data protection law. Neither these challenges nor these recommendations are exhaustive, but they include those that the EDPB considers the most relevant. This section also highlights a number of best practices implemented by some responding controllers. Additional findings, recommendations and best practices can be found in the respective SA's national reports provided in the Annex.

4.2.1 Issue 1: Absence of a documented and updated internal procedure to handle erasure requests

As many as seventeen SAs raised concerns regarding controllers not having any internal procedure or practice in place to handle erasure requests or having an incomplete or irregularly reviewed procedure. This finding confirms the conclusion of the CEF of 2024, where this issue was also flagged by many SAs when assessing compliance of controllers with the right of access[24].

While the GDPR does not explicitly require controllers to adopt a particular procedure or process for handling erasure requests, a clear and efficient process helps controllers to respond to requests within the legal deadline[25] and adequately address them[26]. More generally, a documented procedure is also useful for controllers to demonstrate compliance with their GDPR obligations, in line with the accountability principle (Art. 5(2) and 24 GDPR). As mentioned above, the level of internal process and formalisation in place seems to depend on the number of erasure requests already received, the size and the sector of the responding controllers as well as the complexity of the personal data processed. Typically, small-sized controllers which receive zero or a negligible number of erasure requests are unlikely to have anything in place.

[24] 2024 Coordinated Enforcement Action, Implementation of the right of access by controllers, adopted on 16 January 2025 ("CEF 2024 report"), Section 4.2.3 on "Lack of documented internal procedures".
[25] See with respect to the right of access, Guidelines 01/2022 on data subjects rights – Right of access ('Guidelines 01/2022'), Section 5.3 on "timing for the provision of access", which interprets the requirements of Article 12(4) GPDR on the legal deadline.
[26] See with respect to the right of access, Guidelines 01/2022, para 6.

The absence of internal procedures poses the risk that requests might be handled subjectively and inconsistently. This risk is particularly relevant for the right to erasure: as this right is not absolute, there is a need to check, on the one hand, whether the data subjects can rely on one of the applicable conditions to exercise their right (Art. 17(1) GDPR), and, on the other hand, whether one of the exceptions applies to deny (fully or partially) the erasure request (Art. 17(3) GDPR). To mitigate this risk, an internal procedure could explain in simple terms the criteria that the relevant team(s) should uniformly apply when assessing erasure requests. In that regard, a few SAs reported that the assessment carried out by some controllers to apply Art. 17(1)(a) GDPR (to check if the personal data is "no longer necessary" and needs to be erased) is inconsistent. While some controllers implement formal assessments that include checking the legal basis, the retention period and the purpose for the concerned processing, others rely only on informal internal consultations or verifying GDPR general principles (e.g. data minimisation) without documented steps. Similarly, some SAs reported

inconsistent practices when it comes to withdrawal of consent (Art. 17(1)(b) GDPR) or exercise of the right to object (Art. 17(1)(c) GDPR).

Some controllers report that they regularly review their internal procedures, for example by integrating them into the scope of their compliance audits and by auditing them annually. Others carry out a review every five years, do so only when they detect a problem or when a need to update it arises or they do not review them at all. This seems to indicate inconsistent practices across controllers on this matter.

When asked about the process in place to handle erasure requests, some responding controllers do not even report relying on their record of processing activities ('ROPA'). In that regard, a few SAs noted the difficulties of certain controllers in identifying the personal data which fall under the scope of erasure requests. This challenge is very similar to the issue identified during the CEF of 2024 on the right of access regarding the lack of awareness about the scope of the right of access[27]. These difficulties are associated with the absence of a structured process to map the relevant personal data. This may result in controllers not fully complying with the right to erasure due to an inability to locate all of the relevant data on their systems/databases. For example, one controller was of the opinion that the personal data included in emails was by default out-of-scope. More generally, many controllers also excluded back-up data by default, without providing a justification for doing so (see Issue 6). Because of the uncertainty some controllers seem to have on the scope of right to erasure, they sometimes ask data subjects to clarify to which specific data their erasure request relates.

A few SAs also highlighted that certain controllers had difficulties with differentiating between closing an online user account or profile and the right to erasure[28]. Some controllers seemed to consider that by offering data subjects the possibility to delete their account, profile or even mobile app while keeping the user account (and possible additional personal data) in their internal systems, they were complying with a request for erasure. This confusion ultimately undermines the effectiveness of the right to erasure.

[27] CEF 2024 report, Section 4.2.1.

[28] See the EDPB Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites, adopted on 3 December 2025.

Regarding this challenge, as a result of the CEF, SAs/EDPB may consider the following actions:

- Continuing to develop ready-to-use templates for controllers to respond to erasure requests in different use cases (e.g. in case the request is granted or rejected). Some of the existing templates are referred to in Section 5.
- Continuing to develop guidance, and advertise existing one[29], to help controllers handle erasure requests internally, with a suggested frequency for regular review of the procedure.
- Continuing to raise awareness on the scope of erasure requests and on the distinction between the right to erasure and the deletion of a user account.

Recommendations for controllers to address this challenge:

- Establish and update internal procedures with clear deadlines and steps, and allocating responsibilities among the different actors for handling and recording erasure requests.
- Map personal data and storage locations (including, when possible, by relying on the ROPA) to have a clear overview of which personal data fall under the scope and where to search upon receipt of an erasure request.
- Develop codes of conduct, pursuant to Art. 40 GDPR to identify standardised procedures for the effective application of the right to erasure.

Best practices implemented by some controllers:

- Involve a team which is in charge of handling erasure requests (e.g. the legal team), coordinating if necessary with other teams.
- Use of software or systems where records are generated automatically as proof of deletion when an erasure request is granted.
- Use Key Performance Indicators (KPI) to monitor the handling of erasure requests, such as the percentage of requests answered within one month or three months (in case of an extension); submit the KPI reports to the management for the evaluation and improvement of the process.
- Define relevant technical and legal terms of the right to erasure in everyday language understood by the relevant staff members.

4.2.2 Issue 2: Absence, or inadequate training of staff members

A recurring challenge identified among several controllers concerns the absence of, or inadequacy of staff training. In many cases, data protection training is either not conducted regularly or limited to general sessions held on an annual basis. This may be due to the relatively low number of erasure requests received or limited resources (time, budget, personnel) available to organise such training.

As a consequence, significant gaps were observed in employee awareness and monitoring regarding the handling of erasure requests. In particular, staff members generally lack specific training on Article 17 GDPR and have insufficient knowledge of the internal procedures for processing such requests (if internal procedures exist, see Issue 1). This can lead to difficulties

[29] Similarly, see the Flowchart included as an annex to Guidelines 01/2022 to help controllers handle access requests.

in correctly identifying and handling erasure requests. As a result, controllers may face difficulties in recognising when data subjects are exercising their right to erasure, which can lead to failures to respond within the legal deadline or to forward the request to the responsible person or organisational unit. A lack of knowledge can create additional workload for staff members, as they first need to familiarise themselves with the relevant requirements. It may also result in important legal exceptions or requirements not being identified or being recognised too late. No or insufficient training can further lead to incorrect or incomplete erasure of personal data. This also increases the risk of complaints, as data subjects are more likely to contact the supervisory authority when they receive no or insufficient responses. Inconsistent handling of erasure requests may also undermine trust in the controller's data protection practices.

Recommendations for controllers to address this challenge:

- To address the identified challenges, controllers should ensure that staff are adequately trained and equipped, also regarding internal procedures to handle erasure requests in accordance with Article 17 GDPR. Key measures include:
- Raise awareness and provide resources: Controllers should recognise the importance of proper training as well as awareness-raising measures and allocate sufficient resources and tools to support it (if appropriate by relying on all the guidance available, as described in Section 5).
- Provide clear information on the right to erasure, particularly from the perspective of employees dealing with data subject requests.
- Train staff regularly: Training should be conducted as soon as the relevant staff members join the organisation of the controller and from then on, frequently, including refresher sessions.
- Consider the use of e-learning tools: Controllers may complement in-person training with e-learning tools and programmes for self-study.
- To strengthen compliance, it is essential for all controllers to implement mandatory, role-specific training for employees involved in handling erasure requests.

Best practices implemented by some controllers:

- Organise internal training sessions and test the participants on the content of the session at the end, ensure the effectivity of the training in practice.
- As part of the training process, test staff members on fake requests to verify that the process is correctly followed.

4.2.3 Issue 3: Insufficient information provided to data subjects

Thirteen SAs noted that some controllers provide insufficient information to data subjects with respect to the right to erasure. This issue was found to be more prominent with smaller-sized controllers which reported having received zero or very few requests.

More specifically, data subjects are not systematically informed about the existence of this right, even if required under Articles 13(2)(b) and 14(2)(c) GDPR. Insufficient information may result in a general lack of awareness on the part of data subjects about their data protection rights, ultimately leading to less erasure requests and less control over their personal data.

When they do bring this right to the attention of data subjects, controllers do not always provide instructions to facilitate its exercise or do not ensure that these instructions are clear and easily accessible (Art. 12(1) and 12(2) GDPR[30]). The level of detail and instructions provided varied between controllers, with some controllers offering multiple means for data subjects to understand their rights and the procedure for requesting erasure. In contrast, some controllers provide information only when asked by data subjects requesting erasure.

Insufficient information relating to the conditions for exercising the right to erasure was observed. As this right is not absolute, it is important for data subjects to understand under which conditions their erasure request can be granted. In that regard, the legal basis on which the controller relies for its processing activities matters (e.g. Art. 17(1)(b), (c), (e), (f) GDPR), making it crucial for data subjects to know which legal bases are used in their specific case (Art. 13(1)(c), 14(1)(c) GDPR). More generally, some controllers do not explain which conditions data subjects have to fulfil to exercise their right successfully, which may ultimately undermine its effectiveness.

Insufficient information on the process itself was also reported. Some controllers do not explain to data subjects the procedure that has to be followed to submit a request for erasure (e.g. mentioning who to contact and which communications channel(s) to use[31]).

Furthermore, upon receiving an erasure request, some controllers do not inform data subjects when they need more time to handle their erasure request (up to two additional months instead of the one-month legal deadline, under Art. 12(3) GDPR). Later on in the process, some controllers do not provide justifications when refusing to grant an erasure request (see Issue 4). In addition, some controllers do not inform data subjects about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy if they do not take action regarding the request of the data subject (Art. 12(4) GDPR). In that regard, having an internal procedure with templates can help controllers provide all the necessary information to data subjects (see Issue 1).

The topic of transparency will be further examined during the next Coordinated Enforcement action of the EDPB in 2026, which will focus on "Compliance with the obligations of transparency and information (Articles 12, 13 and 14 GDPR)"[32].

Regarding this challenge, as a result of the CEF, SAs/EDPB may consider the following actions:

- Making available a template form that data subjects could use to exercise their right to erasure (e.g. specifying the applicable conditions to fulfil) or giving more visibility to existing templates.
- Making available templates to help controllers respond to erasure requests and making sure that all the relevant information is provided to data subjects throughout the process.

Recommendations for controllers to address this challenge:

- Review and, if appropriate, complement privacy notices to mention the right to erasure, its scope and explain the process to exercise it.

[30] See also Recital 59 GDPR.
[31] See Guidelines 01/2022, paras. 52-56.
[32] https://www.edpb.europa.eu/news/news/2025/coordinated-enforcement-framework-edpb-selects-topic-2026_en

- Make sure to include in an easily accessible manner the contact details or the channel to use for data subjects to submit their erasure request.
- Prepare (if available based on the documents mentioned above) different templates to respond to erasure requests in different use cases.

Best practices implemented by some controllers:

- Offer data subjects different and user-friendly communication channels to submit an erasure request (e.g. through an online portal, app interface, by email, by phone, etc.)33.
- Acknowledge the receipt of an erasure request and provide an estimated response time to process the request (even if this is the one-month legal deadline) to enhance transparency34.
- Publish FAQs, help centres and/or web forms to make it easier for data subjects to understand their right to erasure and submit a request.
- Leave the possibility for data subjects to first make a request for access if they wish to know which personal data will be subject to erasure.
- Inform data subjects submitting an erasure request about the consequences of definitive deletion of their data (e.g. use of certain services, access request which cannot be fulfilled).

4.2.4 Issue 4: Misuse of and legal uncertainty on the exceptions to deny erasure requests

More than a dozen of SAs noted difficulties associated with the application of the exceptions to deny erasure requests. Several controllers demonstrated uncertainty or inconsistency in applying the exceptions under Article 17(3) GDPR. The verification of conditions for exceptions varies widely among controllers, and in some cases, exceptions are treated as automatically applicable without conducting a case-by-case assessment. This seems to indicate that some controllers could overuse some exceptions, without assessing the merits of each erasure request.

In addition, in some use cases controllers do not implement appropriate measures to safeguard the rights of data subjects where erasure could not be granted immediately.

Example 1: The controller is not certain if the erasure request is going to be granted and needs time to analyse the request. In such a case, a restriction of processing under Art. 18 GDPR could be applied.

Example 2: The controller intends to comply with the erasure request but requires additional time to implement it technically. In such cases, anonymisation of the data could serve as a technical safeguard (see Issue 7).

In cases where erasure requests are lawfully denied under Article 17(3) GDPR, some controllers do not consistently implement measures to ensure continued compliance with the principles laid out in Article 5 GDPR, such as data minimisation, storage limitation, and integrity and confidentiality. Appropriate technical and organisational measures — such as restriction of processing (Art. 18 GDPR), or segregation of data within specific systems — are

[33] See Guidelines 01/2022, para. 53.
[34] See Guidelines 01/2022, para. 57. Also see CEF 2024 report, page 19.

not always applied, which can lead to the continued risk of improper use or access to personal data.

Furthermore, in some cases, extremely high rejection rates were reported, which may indicate unreliable or inconsistent practices in assessing erasure requests.

These shortcomings may be attributed to legal uncertainty regarding the interpretation of Article 17(3) GDPR, insufficient legal guidance, and the absence of clear internal procedures. Limited involvement of legal or compliance departments in decision-making and a lack of awareness of alternative protective measures may further contribute to the problem.

A few SAs noted that some controllers do not document the application of an exception to reject erasure requests, even though this could contribute to fulfilling their accountability obligation (Art. 5(2) and 24 GDPR). Some controllers were also unable to provide the number of erasure requests that they rejected in the past years or to provide accurate figures on this topic.

With respect to the application of Article 17(3)(a) GDPR, for example, in several reported cases, data subjects exercised their right to erasure concerning personal data published by online newspapers or similar media outlets. These publications can include full names and photographs. However, despite receiving erasure requests, some controllers fail to delete the personal data or to provide sufficient justification for their refusal, citing freedom of expression without a documented balancing assessment.

With respect to the application of Article 17(3)(b) GDPR, another challenge concerns the reconciliation between the obligation to comply with the right to erasure and the legal duty to retain certain personal data. Some controllers fail to adequately assess the specific legal obligations applicable to each individual case, which may result in data being stored longer than necessary (see Issue 5).

Some controllers demonstrate a lack of understanding when balancing interests under Article 17(3)(c) GDPR. In particular, erasure requests are sometimes refused on the grounds of legitimate interest without proper assessment or documentation of the balancing test.

Regarding this challenge, as a result of the CEF, SAs/EDPB may consider the following actions:

- Providing further targeted guidance and clarification on the correct application of Article 17(3) GDPR, including examples and practical criteria for assessing proportionality.

Recommendations for controllers to address this challenge:

- Document legal reasonings and justifications in writing when relying on exceptions to erasure (e.g. through a record of requests).
- Involve compliance or legal teams in decision-making processes concerning the refusal or postponement of erasure requests.

4.2.5 Issue 5: Difficulties in defining and implementing data retention periods

Under the principle of "storage limitation", personal data are retained for a specific period that is not longer than necessary, depending on the processing purpose (Art. 5(1)(e) GDPR).

According to a few SAs, some of the responding controllers, especially those of small size, encountered difficulties in determining the appropriate retention periods for the specific processing they carry out[35]. Retention periods can stem, among others, from a variety of European or national laws or regulations, which can be general or sector- or service-specific and can be phrased very differently (e.g. obligation to keep the data for a certain period, or to delete it after a specific date; statute of limitations applying to different fields of law such as for contractual, commercial, tax, social or archiving matters). For example, one controller was unable to distinguish the appropriate retention periods for different processing operations and instead applied the longest period applicable to one processing activity to all of them. Similarly, another one active in a regulated sector implemented a retention period applying to certain kinds of protected data by default, without having assessed whether this period was appropriate for the different processing activities. On the positive side, other responding controllers had internal documentation in place to map and implement the retention periods applicable to the various processing purposes such as a retention policy or schedule.

This issue has an impact on the exercise of the right to erasure and its handling by controllers.

Firstly, the principle of storage limitation is linked to the exercise of this right: one of the grounds allowing data subjects to exercise this right is when the controller is subject to a national or EU legal obligation requiring it to erase data (Art. 17(1)(e) GDPR). A second ground is also when "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed" (Art. 17(1)(a) GDPR). This presupposes that controllers are clear about their (objective) need to retain the concerned personal data (if any) and the retention period applicable to avoid keeping the data longer than necessary. In that regard, having a retention policy or schedule can help to determine when it is required to delete personal data. A few SAs raised some concerns, as a number of controllers did not have a structured procedure in place to assess whether the personal data subject to an erasure request is still necessary for the defined purposes, leaving it to individual staff members to make this difficult assessment without a starting point (this is linked to Issue 1 above).

Secondly, some responding controllers do not inform data subjects about the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period (Art. 13(2)(a) and 14(2)(a))[36]. This means that data subjects often have little information as to whether and for how long the continued processing of their data is really needed. This may contribute to creating confusion among data subjects about their ability to exercise their right to erasure, similarly to Issue 3.

[35] On this topic, also see a related problematic issue that was reported in the Coordinated Enforcement of 2024 on the right to erasure in Section 4.2.2 "Indefinite, excessive or inconsistent retention periods relating to access requests".
[36] See also WP29 Guidelines on transparency under Regulation 2016/679, adopted on 11 April 2018, WP260 rev.01, endorsed by the EDPB during its first plenary meeting in 2018, pages 38-39. Also see CEF 2024 Report, Section 4.2.7 on "Provision of insufficiently detailed or tailored information to data subject", which noted that in the context of the response to the right of access, retention periods (Art. 15 (1)(d) GDPR) are often only specified in very general terms, without distinguishing between processing activities or data categories.

Thirdly, controllers can reject an erasure request to the extent that the concerned personal data is necessary for compliance with a legal obligation (either at national or European level) (Art. 17(3)(a) GDPR). It was reported that some controllers were not aware of the legal obligations applicable to them.

Regarding this challenge, as a result of the CEF, SAs/EDPB may consider the following actions:

- Providing more guidance and continuing to raise awareness on the requirement to keep personal data only for an appropriate duration and to inform data subjects about retention periods or the criteria underlying such periods.
- Providing more practical guidance on how retention periods interact with the right to erasure.
- Providing more practical guidance on how to define and implement retention periods, also taking into account national legal obligations (e.g. with templates or use cases), if necessary in coordination with other competent regulators.

Recommendations for controllers to address this challenge:

- When documenting the retention periods in the ROPA, specify if there are any legal obligations to retain personal data for a certain period.
- Maintain and update retention policy specifying the applicable retention periods.

Best practices implemented by some controllers:

- Specify in privacy notices both the specific data retention periods and the criteria for determining it (e.g. the applicable legal obligation), which enhances transparency for data subjects
- Use a “data deletion matrix” that cross-indexes the type of data being processed, the associated legal basis, and the retention period.

4.2.6 Issue 6: Deletion of personal data in the context of back-ups

Back-up is an important tool to protect the integrity of the personal data when the controller is affected by a security incident (for example ransomware). It is therefore important to protect the integrity of the back-up. Depending on the technical settings and risks, it might not always be advisable to modify or delete information from back-ups. But, in that case, organisations should have appropriate procedures to keep track of erasure requests and comply with them on restored systems, as much as possible, in case of a data breach affecting the integrity of the organisation’s system.

Half of the responding SAs raised concerns regarding the deletion of personal data in this context. Many controllers were found not to have specific procedures and measures in place to handle erasure requests in the context of back-ups, relying either on automatic deletion measures (not specific to the erasure requests received) or on the implementation of retention periods applicable to the concerned back-ups.

When deletion was applied, inconsistent practices were observed from one controller to another, as SAs have identified a wide range of methods used by controllers for deleting personal data from back-ups, each working to varying degrees of efficiency. For instance, an interesting solution implemented by a controller consists of relying on a tool that, upon

reaching a pre-determined end-date (retention period), extracts all the personal data relating to a data subject from all systems of the organisation. The data is then moved away from employees' access to an anonymised and separate system where it will be permanently erased one month later. The complexity of the deletion process is further evidenced by the fact some controllers stated they face problems while deleting data in older information systems or large cloud solutions.

Some of the controllers' practices were automatic in nature. Some stated that data from back-ups is only deleted when it is automatically overwritten by another back-up or when updating or deleting the back-up at set intervals, for instance, one month. Some controllers further raised concerns over technical aspects, stating that in certain situations it may not be possible to simply change parts of the data, especially when the back-up must be preserved as a whole.

Some controllers were found to rely on the retention periods they implement for their back-ups to ensure that back-ups are wiped after a specific period of time. However, in practice, retention periods can vary significantly within organisations and from one controller to another (also see Issue 5). In the absence of concrete retention periods, one SA identified a practice where controllers rely on internal procedures deleting personal data in increments spanning long periods of time. The SA found that this procedure creates difficulties to conclude whether deletion triggered by a data subject's erasure request takes place "without undue delay", as per the requirement of Article 17(1) GDPR.

Conversely, while the solutions presented above involve automation to some extent, some SAs observed a common practice of processing erasure requests fully manually. While this brings forward the advantage of human oversight, it may require increased manual effort.

<u>As a result of the CEF, the EDPB may consider the following actions:</u>

- Providing more guidance and recommendations to explain how controllers should practically deal with erasure in back-ups and what is meant by "without undue delay" in this context.

<u>Recommendations for controllers to address this challenge:</u>

- Follow established standards to erase and destroy data in a secure and structured manner.
- Verify that erasure has been carried out and be able to demonstrate such erasure.

<u>Best practices implemented by some controllers:</u>

- To mitigate the structural impact deletion brings to back-ups, some controllers replace the personal data they wish to delete with strings of random characters.
- Rely on tools that automatically extracts all personal data from internal systems and transfers them to back-ups inaccessible to employees. Ensure that personal data is afterwards deleted or fully anonymised.

4.2.7 Issue 7: Difficulties with anonymisation to respond to erasure requests

Recital 26 GDPR states that information is anonymous when it does not relate to an identified or identifiable natural person. This includes, among others, personal data rendered anonymous in such a manner that individuals are no longer identifiable. A common practice among responding controllers is relying upon anonymisation as a substitute for a permanent deletion of personal data[37]. This may be the case in situations where controllers wish to retain some data, even in anonymised form, for analytical and statistical purposes. A possible explanation identified by one of the SAs could be related to the technical limitations imposed by some controllers' information system making them believe anonymisation to be a simpler solution.

As regards the practical implementation of the anonymisation process, several SAs noted that controllers may be uncertain about what legally and technically constitutes anonymisation. The need for clearer guidance on both what legally constitutes anonymisation as well as appropriate technical solutions has been expressed by multiple controllers. The EDPB is currently working on Guidelines on anonymisation taking into account the recent clarifications offered by the CJEU in its SRB ruling[38]. In this context, the EDPB also organised a stakeholder event on pseudonymisation and anonymisation[39].

Multiple SAs found that controllers relying on anonymisation for deletion have various degrees of success in correctly implementing it. For example, in some cases, they only apply basic

pseudonymisation or partial masking, although such a process would not fulfil the requirements of the GDPR regarding deletion.

As regards to the actual technical measures employed by responding controllers, their difficulties could also originate from insufficiently fixed and clear technical standards defining what constitutes "state of the art" when it comes to anonymisation. The size of controllers does not seem to be systematically correlated to the sophistication of the technical standards implemented. For instance, some mid-sized controllers deployed strong anonymisation methods while some large controllers used weaker masking techniques.

Regarding this challenge, as a result of the CEF, SAs/EDPB may consider the following actions:

- Continuing issuing practical actionable guidance on the subject.
- Helping ensure a proper information of controllers about the most relevant EDPB guidance on the matter.

Best practices implemented by some controllers

- Implement technical standards such as ISO/IEC 27001 and ISO 9001 on management systems, as they help organisations improve their processes and accountability.
- While not completely implementing the standards mentioned above, some controllers nonetheless based their security policy on them.

[37] Judgment of 20 December 2017, C-434/16, Nowak v Data Protection Commissioner, ECLI:EU:C:2017:994, para. 55.: in this case the CJEU mentions the erasure of examination scripts (in copy) as entailing that they are "destroyed".
[38] Judgment of 4 September 2025, C-413/23 P, EDPS v. SRB, ECLI:EU:C:2025:645.
[39] https://www.edpb.europa.eu/news/news/2025/anonymisation-and-pseudonymisation-take-part-stakeholder-event_en

5 Actions taken by SAs relating to the right to erasure

This section maps out the actions carried out by SAs at national level in relation to the right to erasure – both independently from and in the course of this CEF action. However, this section does not aim to present a comprehensive overview of all actions conducted by SAs, nor does it list ongoing actions that are not finalised and on which SAs have not yet publicly communicated. Each individual report of the participating SAs detailing their respective actions is available in the Annex.

5.1 Complaints-related trends

Several SAs identified a general upward trend in complaints relating to data subject rights since the entry into force of the GDPR[40]. For instance, EE SA and LU SA stated that this growth is likely attributed to a greater awareness among data subjects of their rights. Similarly, both CY SA and PT SA stated that the number of erasure requests is small but rising. Conversely, HU SA and LI SA noticed that the number of complaints relating to the right to erasure remained relatively constant.

A significant number of SAs further provided the share erasure requests have out of the total number of complaints received. On the higher end, NL SA and LU SA noted that erasure requests account for around 19% of the total number of complaints received. DK SA provided a similar estimate (around 15%) while further noting that some of the cases analysed may also address other data protection issues[41]. Both LI SA and SI SA estimate that around 10% of the complaints received concern the right to erasure. On the lower end, ES SA stated that by mid-2025, the proportion of complaints on the right to erasure received this year represented around 5% of the total. Similarly, HU SA estimates that around 40 to 45% of the total number of complaints relate to data subject rights out of which 10-15% directly concern the right to erasure.

5.2 Enforcement actions

SAs have several powers at their disposal in accordance with Art. 58 GDPR, including corrective powers such as issuing reprimands or orders to comply or fines, for cases of non-compliance with the requirements of Art. 12 and 17 GDPR. In accordance with Art. 83(5) GDPR, if a controller does not fulfil its obligations in respect of data subjects' rights pursuant to Art. 12 to 22 GDPR, it can be subject to administrative fines up to 20 million euros, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher[42].

As a general observation, a number of SAs noted that the exercise of corrective powers with respect to the right to erasure often stems from individual complaints[43]. One SA found that the majority of complaints received concern delays or refusals by controllers to erase personal

[40] See for example CZ SA's, IT SA's, LT SA's and LU SA's national reports.
[41] The fact that complaints also relate to other data subject rights has also been noted by other SAs such as HU and IE SAs.
[42] However, in some Member States, some public-sector controllers cannot be fined under the GDPR due to restrictions imposed by the national legislator.
[43] See for instance DE SAs, CZ SA's national reports.

data. Various factors play a key role in determining the outcome of complaints-based procedures. Some controllers may be under a legal obligation to retain certain personal data, one SA noting that in the majority of complaints it was concluded that there should be no deletion and the erasure requests can be lawfully rejected. Procedures based on complaints might be closed without corrective measures being imposed if during the investigation the controller complies with the data subject's request. In this regard, one SA (IE SA) noted that most of the complaints were resolved through amicable settlements.

Of the participating SAs, several have already taken actions towards controllers concerning the right to erasure prior to the launch of this CEF. For instance, FI SA issued an administrative fine of 75.000 euros to a private parking enforcement company for, among others, failing to delete the personal data once no longer necessary for the purposes initially collected[44]. The Helsinki Administrative Court upheld the orders and reprimands issued by FI SA while reducing the administrative fine to 70.000 euros. Later, the Supreme Administrative Court rejected the data controller's application for leave to appeal against the decision of the Helsinki Administrative court[45]. Furthermore, NL SA has taken corrective actions as a result of infringements of Art 17 GDPR, notably, issuing a fine of 6.000 Euros to a controller for ignoring requests for removal or personal data and not having a method in place for dealing with removal requests[46].

Several SAs issued compliance or erasure orders, obligating controllers to erase the personal data of data subjects. For instance, HU SA received a complaint pertaining to a video depicting members of the controller and the data subject in an altercation. Despite the data subject being considered an "exceptional public figure" due to their activities in a social movement, the SA found that the video itself could not be considered a public debate, nor did it serve a public interest and hence ordered the controller to erase it without delay. Further MT SA issued a compliance order to a vehicle insurer to erase the personal data of a data subject who never entered into an insurance contract with it but only requested a quotation, stating that no legislation requiring the controller to keep the data existed[47]. Lastly, FI SA issued a decision where it found that a data subject had the right to have their personal data removed from an Internet forum due to being underage at the time the messages had been posted.

As part of this CEF action, as many as nine SAs launched or continued formal investigations (AT, DK, some DE SAs, PT, FR, SI, LT, CY SAs). In addition, after the publication of this CEF report, several other SAs are planning to take immediate enforcement and/or awareness raising actions. For instance, HU SA, EDPS and LU SA plan to inform the respondents about the publication of the report. More generally, IE SA is planning to continue engaging controllers informally regarding their responsibilities under Article 17 GDPR. Some of the participating DE SAs are considering potential actions against controllers who failed to provide answers to the questionnaire while HR SA is considering doing so in the future. LU SA and HU SA are also considering launching formal investigations following the findings of this CEF.

[44] FI SA: https://tietosuoja.fi/-/yritykselle-seuraamusmaksu-tietosuojarikkomuksista-pysakoinninvalvontamaksujen-yhteydessa?languageId=en_US
[45] FI SA: https://tietosuoja.fi/en/-/the-supreme-administrative-court-did-not-grant-parkkipate-oy-leave-to-appeal-the-administrative-court-decision-concerning-the-office-of-the-data-protection-ombudsman-s-decisions-will-remain-in-force
[46] NL SA: https://www.autoriteitpersoonsgegevens.nl/en/current/fine-for-recruitment-company-for-ignoring-requests-for-removal
[47] MT SA, https://idpc.org.mt/wp-content/uploads/2024/01/CDP_COMP_84_2023.pdf

5.3 Guidance

A significant number of SAs have issued either general or targeted guidance on the right to erasure. Some of the general guidance published concerned other data subject rights as well. For instance, MT SA issued a fact sheet containing a description of data subject's rights, the means and requirements for exercising them[48]. Similarly, ES SA published a series of webpages dedicated to each of the data subject rights and the means to exercise them[49]. The table below presents a non-exhaustive list of the guidance issued by SAs on the right to erasure.

Topic	General guidance on the right to erasure	Targeted guidance / other
Description	Several SAs have issued general guidance on the right to erasure in various formats, which are addressed to data subjects, controllers, or both: 1) **DE SAs**[50] **DK SA**[51], **EL SA**[52], **ES SA**[53], **FI SA**[54], **FR SA**[55], **IT SA**[56], **LI SA**[57], **LU SA**[58] **NL SA**[59], **PT SA**[60], **SE SA**[61], published some content	**BG SA** established a dedicated phone line where individuals can seek guidance on GDPR-related matters, including the right to erasure. Furthermore, the BG SA issued targeted guidance tailored to children[70] as well as, for example, on the right to erasure in the context of processing personal data for journalistic purposes[71]. **DE SAs** issued targeted guidance including among others an educational video teaching youths how to delete posts on the internet[72], guidelines on police authorities[73] and on the storage of telecommunication traffic data[74].

[48] MT SA, https://idpc.org.mt/for-individuals/your-rights/#:~:text=In%20the%20event%20that%20you,able%20to%20investigate%20your%20complaint.&text=The%20right%20to%20get%20your,child%20for%20an%20online%20service
[49] ES SA, https://www.aepd.es/derechos-y-deberes/ejerce-tus-derechos
[50] DE SA (Fed), https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Betroffenenrechte/Betroffenenrechte_L%C3%B6schung_Vergessenwerden.html; DE-BW SA, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/03/Betroffenenrechte.pdf
[51] DK SA, https://www.datatilsynet.dk/regler-og-vejledning/behandlingssikkerhed/sletning
[52] EL SA, https://awareness.SA.gr/
[53] ES SA, https://www.aepd.es/derechos-y-deberes/ejerce-tus-derechos
[54] FI SA, https://tietosuoja.fi/en/if-you-would-like-to-have-all-of-your-data-erased
[55] FR SA, see for example, https://www.cnil.fr/fr/falc-droit-effacement and https://www.cnil.fr/fr/falc-droit-effacement
[56] IT SA, https://www.garanteprivacy.it/i-miei-diritti/diritti/oblio
[57] LI SA, https://www.datenschutzstelle.li/datenschutz/themen-z/loeschfristen
[58] LU SA, https://cnpd.public.lu/fr/particuliers/vos-droits/droit-oubli.html
[59] NL SA, see for example, https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacyrechten-avg/recht-op-gegevens-verwijderen; https://www.autoriteitpersoonsgegevens.nl/jij-en-jouw-online-gegevens/jouw-privacyrechten/jouw-gegevens-laten-verwijderen
[60] PT SA, https://www.cnpd.pt/organizacoes/orientacoes-e-recomendacoes/
[61] SE SA, https://www.imy.se/privatperson/dataskydd/dina-rattigheter/radering/
[70] BG SA, https://cpdp.bg/en/children-and-their-personal-data/
[71] BG SA, https://cpdp.bg/%d1%81%d1%82%d0%b0%d0%bd%d0%be%d0%b2%d0%b8%d1%89%d0%b5-%d0%bd%d0%b0-%d0%ba%d0%b7%d0%bb%d0%b4-%d0%be%d1%82%d0%bd%d0%be%d1%81%d0%bd%d0%be-%d0%bf%d1%80%d0%b0%d0%b2%d0%be%d1%82%d0%be-%d0%b4%d0%b0/?hilite=%D0%BF%D1%80%D0%B0%D0%B2%D0%BE+%D0%B4%D0%B0+%D0%B1%D1%8A%D0%B4%D0%B5%D1%88+%D0%B7%D0%B0%D0%B1%D1%80%D0%B0%D0%B2%D0%B5%D0%BD
[72] DE SA (Fed), https://www.bfdi.bund.de/SharedDocs/Videos/DE/Pixi/Wissen_DF_Folge-6.html?nn=411490
[73] DE SA (NW), https://www.ldi.nrw.de/datenschutz/sicherheit-und-justiz/polizei/speichern-und-loeschen-personenbezogener-daten-nach-dem
[74] DE SA (Fed), https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/DatenschutzpraxisLeitfadenVerkehrsdaten.html

	on their website on the right to erasure. 2) **SI SA** [62] issued guidelines on data subject rights. 3) The **DE SAs** issued a standardised data protection framework [63] and a short paper on the right to erasure[64]. 4) **DE SAs** [65] and **NL SA**[66] issued data erasure request forms for data subjects. 5) **HU SA** [67] issued a resolution / position paper on the erasure of personal data. 6) **MT SA**[68] and **EDPS**[69] have issued factsheets on data subject's rights, including the right to erasure.	**DK SA** recorded a series of podcasts[75] covering relevant data protection topics. Episode 6 was dedicated to the right to erasure[76]. **EL SA** developed, as part of the wider public sector reform, an online assistant [77] (named Wizard) for assisting individuals in exercising their rights. Furthermore, as part of the byDefault project, the EL SA created an online toolkit tailored to the needs of SMEs[78], an e-platform and digital library dedicated to knowledge sharing[79] and an educational programme along with a physical board game for primary and secondary school students[80]. **ES SA** established a new virtual assistance chatbot, available 24/7, that contains a section for data subject rights. It offers forms for exercising such rights[81]. **FI SA** issued targeted guidance for SMEs[82] and offers sector-specific Q&As on their website. **IE SA** issued a Q&A on the amendment or erasure of medical records[83]. **HR SA** in collaboration with **IT SA** and several universities formed the ARC2 Consortium which developed Olivia, a virtual teacher and assistant

[62] SI SA, https://www.ip-rs.si/publikacije/priro%C4%8Dniki-in-smernice/smernice-po-splo%C5%A1ni-uredbi-o-varstvu-podatkov-gdpr/vodnik-po-varstvu-osebnih-podatkov-za-posameznike
[63] DE SAs (DSK), see for example, Module 60 "Deletion and Destruction", https://www.ldi.nrw.de/datenschutz/medien-und-technik/standard-datenschutzmodell
[64] DE SAs (DSK), Short Paper No. 11- Right to erasure / "Right to be forgotten", https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_11.pdf
[65] DE SA (MV), https://www.datenschutz-mv.de/datenschutz/publikationen/muster/.
[66] NL SA, https://www.autoriteitpersoonsgegevens.nl/documenten/voorbeeldbrief-verwijdering.
[67] HU SA, https://www.naih.hu/adatvedelmi-allasfoglalasok/file/58-allasfoglalas-szemelyes-adatok-torlesevel-esadathordozok-megsemmisitesevel-kapcsolatban
[68] MT SA,https://idpc.org.mt/for-individuals/your-rights/#:~:text=In%20the%20event%20that%20you,able%20to%20investigate%20your%20complaint.&text=The%20right%20to%20get%20your,child%20for%20an%20online%20service
[69] EDPS, https://www.edps.europa.eu/system/files/2022-01/22-01-21_infographic_dataproday22_en.pdf
[75] DK SA, https://www.datatilsynet.dk/regler-og-vejledning/podcast
[76] DK SA, https://www.datatilsynet.dk/regler-og-vejledning/podcast/sletning-hvornaar-og-hvordan
[77] EL SA, https://www.SA.gr/el/polites/gkpd/wizard_politon
[78] EL SA, https://bydesign.dpa.gr/questionnaires/fe630b8d-6dae-4537-b865-e8e924ebf344/en
[79] EL SA, https://collab.SA.gr/
[80] EL SA, https://www.dpa.gr/en/enimerwtiko/themes/tzimaniousen
[81] ES SA, https://www.aepd.es/
[82] FI SA, https://www.tietosuojaapkyrityksille.fi/ohjesivut/oikeus-poistaa-tiedot-ja-tulla-unohdetuksi/
[83] IE SA, https://dataprotection.ie/en/can-i-use-gdpr-have-my-medical-records-amended-or-erased#medical

		covering data protection and incorporating various materials on the right of erasure[84]. **NL SA** issued targeted guidance on the right of erasure covering multiple aspects, such as health data[85], exercising the right of erasure on the internet[86], with police[87], judicial authorities[88] and Europol[89].

6 Possible follow-ups and conclusion

This coordinated action enabled participating SAs to gather key insights on the practical implementation of the right to erasure by the responding controllers. The results confirmed some of the findings of the coordinated action that was carried out in 2024 on the right of access, for example when it comes to the lack of internal procedures to handle data subjects' requests, or the lack of sufficient information provided to data subjects. In addition, participating SAs reported specific findings regarding the right to erasure, such as the reliance by some of the responding controllers on anonymisation techniques to handle erasure requests. Some SAs also noted inconsistent practices, and the difficulties faced by controllers regarding the determination of retention periods or the deletion of personal data in back-ups. As the right to erasure is not an absolute right, some controllers struggle to assess and apply the applicable conditions for the exercise of this right, including in carrying out the different balancing tests between the right to erasure and other rights and freedoms.

The CEF highlighted that a lot of guidance exists at national level to help controllers comply with the right to erasure, both generally and in specific contexts. Based on the CEF results, seventeen SAs and some of the participating DE SAs plan to carry out actions at their level to communicate and raise awareness with respect to the right to erasure, including publishing more online guidance, online training sessions and/or conferences and workshops. A few SAs will also consider adopting guidance targeted to specific sectors/services (e.g. mobile apps).

In addition, the EDPB will consider if additional awareness-raising actions should be carried out at EU level, including through the preparation of additional practical and actionable guidance with use cases, examples and best practices, in the form of guidelines or through other formats such as Q&As, in line with the Helsinki Statement[90]. In that regard, the extensive guidance and templates already available at national level will be leveraged at EDPB level where appropriate. Special attention will be paid to the topics explained in Section 4 and the inconsistent practices observed across the EEA, such as the application of exceptions to the right to erasure, the identification and implementation of retention periods and erasure in back-

[84] HR SA and IT SA, https://olivia-gdpr-arc.eu/hr
[85] NL SA, https://www.autoriteitpersoonsgegevens.nl/themas/gezondheid/gezondheidsgegevens-in-een-dossier/rechten-bij-het-dossier-met-gezondheidsgegevens
[86] NL SA,https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme-apparaten/persoonsgegevens-op-internet/persoonsgegevens-publiceren-en-verwijderen-internet
[87] NL SA, https://www.autoriteitpersoonsgegevens.nl/themas/politie-en-justitie/politie-bijzondere-opsporing-en-justitie/uw-privacyrechten-bij-politie-bijzondere-opsporing-en-justitie
[88] NL SA, https://www.autoriteitpersoonsgegevens.nl/en/themes/police-and-judicial-authorities/police-special-investigation-services-and-judicial-authorities/your-privacy-rights-with-the-police-special-investigation-services-and-judicial-authorities
[89] NL SA,https://www.autoriteitpersoonsgegevens.nl/themas/politie-en-justitie/europol-eurojust-en-eom/europol#uw-rechten-bij-europol
[90] The EDPB Helsinki Statement on enhanced clarity, support and engagement, adopted on 3 July 2025.

ups. Besides, the EDPB will strive to provide clarifications on the application of Article 17 GDPR and the interactions and differences between the right to erasure with other rights (right to restrict processing, right to object and right to restriction of processing), which was deemed important by a few controllers.

The present report is the state of play, at the end of 2025, of the CEF action regarding the implementation of the right to erasure by controllers. It may need to be subsequently updated to take into account the progress of procedures which have not yet been completed to date and /or given the issues identified.

Annex 1 National reports by Supervisory Authorities