Annex 1:

National Reports on the CEF Right to erasure

BG SA

Name of Supervisory Authority: Bulgarian DPA

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. **Fact finding:** Yes
b. Fact finding + determining follow-up action based on the results:
c. New formal investigation[1]: [N.A.]
d. Ongoing investigation: [N.A.]

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? [no]
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. [no]
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? [no]

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
The same questionnaire was used for all controllers

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
The same questionnaire was used for all controllers

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?
No

Part I - Information about the controllers addressed

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 6
b. Private sector: 16
c. Other:1

[1] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

a. If so, what were the other sectors? Education (Military education)

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector: 4
b. Health sector: 1
c. Social sector:
d. Insurance sector:
e. Finance sector: 2
f. IT sector: 1
g. Retail sector:
h. Logistics sector: 2
i. Public transportation:
j. Telecommunications:
k. Postal services:
l. Advertising sector: 2
m. Marketing services:
n. Entertainment sector:
o. Information / journalism sector:
p. Scientific / historical research:
q. Credit scoring agency:
r. Public utility/infrastructure provider (e.g. energy): 1
s. Housing industry:
t. Manufacturing: 1
u. Consulting: 3
v. Public administration: 3
w. Other (please specify): 3 (wholesale trade – 1, auto services – 1, facility management, including activities: maintenance of administrative buildings, equipment and installations in the building funds; current and major cleaning, hospital food - 1)

11. Please specify the category in which the responding controllers fall[2]:

a. Micro enterprise: 5
b. Small enterprise: 5
c. Medium-size enterprise: 2
d. Large enterprise (more than 250 employees): 4
e. Non-profit organisation: 2
f. Ministry:
g. Local authority:
h. Administrative authority/agency/office (e.g. job center): 3
i. School/university/educational institution: 2
j. Other (please specify):

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers:

[2] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

b. Customers: 8
c. Contractors:
d. Job applicants: 3
e. Employees: 7
f. Applicants (for public services):
g. Citizens (for public sector): 2
h. Patients: 1
i. Other (please specify): *(2) children – 1, children and students - 1*

12.b. According to the responding controllers, are those data subjects also:

a. Children: 5
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 7
c. Non applicable: 11

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: 7
b. 101 – 1 000: 4
c. 1 001 – 10 000: 3
d. 10 001 – 100 000: 1
e. 100 001 – 500 000: 3
f. 500 001 – 1 000 000:
g. > 1 000 000: 4

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 20
b. Payment data: 14
c. Identification data: 22
d. Marketing data: 4
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 4
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 2
g. Other, please specify:

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year
☐ 3 years - Yes
☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received

between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	2023	2022
0	[14]	[14]	[14]
1 – 10	[2]	[2]	[0]
11 – 50	[0]	[0]	[0]
51 – 100	[0]	[0]	[1]
101 – 500	[0]	[0]	[0]
more than 500	[3]	[2]	[3]

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	2024-2023	2024-2022
0	[14]	[14]	[14]

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
[0]

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 1 year
☐ **3 years** - Yes
☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	2023	2022
0%	[17 responding controllers]	[17]	[17]
10%	[0]	[0]	[0]
20%	[0]	[0]	[0]
30%	[0]	[0]	[0]
40%	[0]	[0]	[0]
more than 50%	[4]	[3]	[4]

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?
☐ **Yes**
☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
[0]

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 1 year
☐ 3 years
☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	16	14	14
10%	1	0	0
20%	0	0	0
30%	0	0	0
40%	0	0	0
more than 50%	3	3	4

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
0

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers:
b. Customers:
c. Contractors:
d. Job applicants: 2
e. Employees:
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients:
i. Other: 3

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: No

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High - Yes
c. Average
d. Low
e. Very low
f. Too diverse levels to qualify

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

Respondents answers show that while SMEs' generally receive a lower number of requests (or none) more of them tend to provide data protection training for their employees rather than big organisations do. It also shows, that SMEs' tend to review the procedures in place more often than big organisations. This could be due to the large difference in received requests, while large organisaitons receive a high number of requests for erasure in line with the adopted procedures, SME's due to their low number of requests may rarely if at all implement their procedures and conduct regular training and procedural oversight as a precautionary measure. Control oversight is also a large component in this as the lower number of requests shows to lead to stricter measures and regular monitoring of activities, as large organisations show to monitor processes only when needed.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

No

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).

A large amount of the respondents, almost 43% have not provided answers to questions 3.1 to 3.11. due to lack of requests for erasures. Our analysis shows, that from the rest of the respondents while having described their internal procedures for processing requests for erasure, and not having any mishandling, unlawful processing or violations of the protection of personal data, a lot of them do not have an adequate procedure in place. It is also notable that almost all of the controllers who have received requests and have answered questions 3.1 to 3.11 have shown to use legitimate interest as basis for refusal of requests or further processing.

24. Are there any leading or best practices of the controllers having responded that you would like to share?

Among the respondents who use technical means for the processing of requests, there are 2 notable practices: first the process of requesting erasure of data in digital platforms has been automated, having the data and profile of users be deleted immediately without any delay or need for further action (records are also generated automatically as proof of deletion), the second practice is the option to request, and have approved erasure of data prior to the expiration of the storage period (except in cases where storage is required by law).

We have noticed that controllers are generally accommodating when receiving requests for erasure through unofficial channels. They have indicated that they process these requests even if they are submitted via incorrect communication channels. They also take timely measures to notify the person in the event of a delay in the processing of the request or when they need further verification. We've also observed that controllers have made significant efforts to facilitate the request process for data subjects.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.

A large amount of the respondents, almost 43% have not provided answers to questions 4.1 to 4.5.1. Among the rest of the respondents almost half have no regular methods established for informing data subjects of their rights. This shows insufficient information provided by data controllers to citizens about their rights, especially during the data collection process. In addition, many citizens remain unaware of their rights and the procedures for submitting erasure requests. This suggests that controllers may not effectively disseminate information about the mechanisms for exercising the right to erasure or may not have sufficient resources for effective dissemination (right of access to data, right of rectification, right to restriction of processing). The lack of prior information could be connected to the lack of requests for erasure received from most of the respondents.

26. Are there any leading or best practices of the controllers having responded that you would like to share?

We have noticed that controllers are generally accommodating when receiving requests for erasure through unofficial channels. They have indicated that they process these requests even if they are submitted via incorrect communication channels. Additionally, while not required controllers have established multiple channels for submission of requests under Art 17 GDPR intended to ease data subjects when exercising their rights. They also take timely measures to notify the person in the event of a delay in the processing of the request or when they need further verification. We've also observed that controllers have made significant efforts to facilitate the request process for data subjects. Many have provided comprehensive online information on how to make a request, offered telephone support for further inquiries, and trained employees to assist individuals directly in stores.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers

Among the 23 respondents, 20 of them have stated they do not use technical means for the processing of requests under article 17 GDPR. Among the other respondents they have stated to implement technical means in line with ISO standards. This difference in the means used for the processing of requests could be due to the significant difference in means and resources available to SME's and public authorities compared to large organisations, as well as the sector (field) of activity of the controllers.

28. Are there any leading or best practices of the controllers having responded that you would like to share?

Among the respondents who use technical means for the processing of requests, there are 2 notable practices: first the process of requesting erasure of data in digital platforms has been automated, having the data and profile of users be deleted immediately without any delay or need for further action (records are also generated automatically as proof of deletion), the second practice is the option to request, and have approved erasure of data prior to the expiration of the storage period (except in cases where storage is required by law). Some controllers have shared they use software tailored specifically for their processing activities and internal systems allowing to better protect personal data and review requests from data subjects.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

The Commission for personal data protection has established a dedicated telephone line for citizen guidance, available every working day, to assist individuals with inquiries about personal data protection and Regulation (EU) 2016/679. Through this telephone line, people call in to receive advice on how to exercise their rights in front of various entities. Our experts explain the process and assist data subjects on how to better understand and exercise their rights.
We have published multiple guidance and information campaigns where we have given guidance to children and parents in the digital age: The CPDP has contributed with multiple publications, guidance notes, flyers, informative videos and a contest designed specifically for children to help raise awareness about the importance of digital safety and privacy. Available links here (BG) (https://cpdp.bg/home-default/%d0%b4%d0%b5%d1%86%d0%b0%d1%82%d0%b0-%d0%b8-%d1%82%d0%b5%d1%85%d0%bd%d0%b8%d1%82%d0%b5-%d0%bb%d0%b8%d1%87%d0%bd%d0%b8-%d0%b4%d0%b0%d0%bd%d0%bd%d0%b8/?hilite=%D0%B4%D0%B5%D1%86%D0%BO). "Your personal data and the internet - advices for children"(EN) (https://cpdp.bg/en/your-personal-data-and-the-internet-advices-for-children/?hilite=children) "GDPR and your rights. Data protection, a fundamental right for every EU data subject - EDPB brochure" (EN) (https://cpdp.bg/en/gdpr-and-your-rights-data-protection-a-fundamental-right-for-every-eu-data-subject-edpb-brochure/).

Other sources available in Bulgarian:
Clarifications on the practical application of the General Data Protection Regulation by local authorities (municipalities) Разяснения относно практическото приложение на Общия регламент относно защита на данните от органите на местното самоуправление (общините) (https://cpdp.bg/home-default/%d1%80%d0%b0%d0%b7%d1%8f%d1%81%d0%bd%d0%b5%d0%bd%d0%b8%d1%8f-%d0%be%d1%82%d0%bd%d0%be%d1%81%d0%bd%d0%be-%d0%bf%d1%80%d0%b0%d0%ba%d1%82%d0%b8%d1%87%d0%b5%d1%81%d0%ba%d0%be%d1%82%d0%be-%d0%bf%d1%80-2/?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)
Opinion of the CPDP on the right to be forgotten in the context of the processing of personal data for journalistic purposes Становище на КЗЛД относно правото „да бъдеш забравен" в контекста на обработване на лични данни за журналистически цели (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)
CPDP factsheet 'New developments concerning the rights of natural persons under Regulation (EU) 2016/679' Информационна брошура на КЗЛД „Нови моменти относно правата на физическите лица съгласно Регламент (ЕС) 2016/679" (https://cpdp.bg/home-

default/%d0%b8%d0%bd%d1%84%d0%be%d1%80%d0%bc%d0%b0%d1%86%d0%b8%d0%be%d0%bd%d0%bd%d0%b0-%d0%b1%d1%80%d0%be%d1%88%d1%83%d1%80%d0%b0-%d0%bd%d0%b0-%d0%ba%d0%b7%d0%bb%d0%b4-%d0%bd%d0%be%d0%b2%d0%b8-%d0%bc%d0%be/?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)
Practical issues of personal data protection after 25 May 2018 Практически въпроси на защитата на личните данни след 25 май 2018 г. (https://cpdp.bg/home-default/%d0%bf%d1%80%d0%b0%d0%ba%d1%82%d0%b8%d1%87%d0%b5%d1%81%d0%ba%d0%b8-%d0%b2%d1%8a%d0%bf%d1%80%d0%be%d1%81%d0%b8-%d0%bd%d0%b0-%d0%b7%d0%b0%d1%89%d0%b8%d1%82%d0%b0%d1%82%d0%b0-%d0%bd%d0%b0-%d0%bb%d0%b8/?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)
Opinion of the CPDP on the exercise of the rights to erasure, rectification or blocking of personal data by persons included in the lists supporting registration with the CEC Становище на КЗЛД относно упражняване на правата за заличаване, коригиране или блокиране на лични данни от лицата, включени в списъците за подкрепа на регистрацията в ЦИК (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-%d1%83%d0%bf%d1%80%d0%b0%d0%b6%d0%bd%d1%8f%d0%b2%d0%b0%d0%bd/?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)
Opinion of the CPDP on the deletion of personal data from the court's database Становище на КЗЛД относно заличаване на лични данни от базата данни на съда (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%b7%d0%b0%d0%bb%d0%b8%d1%87%d0%b0%d0%b2%d0%b0%d0%bd%d0%b5/?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)
Ten practical steps to implement the General Data Protection Regulation (updated and supplemented version) Десет практически стъпки за прилагане на Общия регламент относно защитата на данните (актуализиран и допълнен вариант) (https://cpdp.bg/home-default/%d0%b4%d0%b5%d1%81%d0%b5%d1%82-%d0%bf%d1%80%d0%b0%d0%ba%d1%82%d0%b8%d1%87%d0%b5%d1%81%d0%ba%d0%b8-%d1%81%d1%82%d1%8a%d0%bf%d0%ba%d0%b8-%d0%b7%d0%b0-%d0%bf%d1%80%d0%b8%d0%bb%d0%b0%d0%b3%d0%b0%d0%bd/?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)

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.
No

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?
Analysis on an annual base on the cases handled by the Bulgarian SA can be found at: https://cpdp.bg/home-default/%d0%b8%d0%bd%d1%81%d1%82%d0%b8%d1%82%d1%83%d1%86%d0%b8%d1%8f%d1%82%d0%b0/%d0%b3%d0%be%d0%b4%d0%b8%d1%88%d0%bd%d0%b8-%d0%be%d1%82%d1%87%d0%b5%d1%82%d0%b8-%d0%bd%d0%b0-%d0%ba%d0%b7%d0%bb%d0%b4/
(Available in Bulgarian)

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).
We are planning on continuing an information campaign focused on the results of the coordinated enforcement on the right of erasure. The campaign aims to raise public awareness about citizens' right of erasure held by both public and private sector entities. Our goal is to educate individuals on how they can exercise and better understand this right. By doing so, we hope to empower citizens with the knowledge needed to effectively manage their personal data and ensure transparency in data handling practices.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes: Yes
   If "Yes", please specify: *(please select one or more answers)*
   i. More online guidance: Yes
   ii. Online or remote training sessions: Yes
   iii. Conferences organised:
   iv. Others: please specify:

b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes:
b. No: Yes

35. Are there any other observations that you would like to share?
No

CY SA

Name of Supervisory Authority: Cyprus SA

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding:
b. Fact finding + determining follow-up action based on the results:
c. New formal investigation[3]:
d. Ongoing investigation: Yes

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? N/A
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. N/A
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? N/A

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
N/A

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
N/A

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?
CY SA contributes to the final report, providing its input on the right to erasure and describing any issues observed at national level during investigations that have been conducted through the years. Also, any reference to "controllers" concerning stakeholders that we have contacted in the framework of our investigations.

Part I - Information about the controllers addressed

6. How many controllers did you contact?
N/A

[3] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

7. Out of the contacted controllers, how many controllers responded?

*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

N/A

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

N/A

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: N/A
b. Private sector: N/A
c. Other: N/A
    b. If so, what were the other sectors? N/A

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector:
b. Health sector:
c. Social sector:
d. Insurance sector:
e. Finance sector: Yes
f. IT sector: Yes
g. Retail sector:
h. Logistics sector:
i. Public transportation:
j. Telecommunications:
k. Postal services:
l. Advertising sector:
m. Marketing services:
n. Entertainment sector: Yes
o. Information / journalism sector: Yes
p. Scientific / historical research:
q. Credit scoring agency: Yes
r. Public utility/infrastructure provider (e.g. energy):
s. Housing industry:
t. Manufacturing:
u. Consulting:
v. Public administration: Yes
w. Other (please specify): Political party Yes

11. Please specify the category in which the responding controllers fall[4]:

a. Micro enterprise:

[4] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

b. Small enterprise: Yes
c. Medium-size enterprise: Yes
d. Large enterprise (more than 250 employees): Yes
e. Non-profit organisation:
f. Ministry:
g. Local authority: Yes
h. Administrative authority/agency/office (e.g. job center):
i. School/university/educational institution:
j. Other (please specify):

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers:
b. Customers: Yes
c. Contractors: Yes
d. Job applicants:
e. Employees:
f. Applicants (for public services):
g. Citizens (for public sector): Yes
h. Patients:
i. Other (please specify):
a.

12.b. According to the responding controllers, are those data subjects also:

a. Children:
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people):
c. Non applicable: Yes

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers: N/A

a. < 100:
b. 101 – 1 000:
c. 1 001 – 10 000:
d. 10 001 – 100 000:
e. 100 001 – 500 000:
f. 500 001 – 1 000 000:
g. > 1 000 000:

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: Yes
b. Payment data: Yes
c. Identification data: Yes
d. Marketing data:
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data:
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: Yes

g. Other, please specify:

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*): N/A

☐ 1 year

☐ 3 years

☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)? N/A

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
N/A

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*): N/A

☐ 1 year

☐ 3 years

☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).* N/A

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified? N/A

☐ Yes

☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

N/A

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*): N/A

☐ 1 year

☐ 3 years

☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*
N/A

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
N/A

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers:
b. Customers: Yes
c. Contractors: Yes
d. Job applicants:
e. Employees:
f. Applicants (for public services):
g. Citizens (for public sector): Yes
h. Patients:
i. Other:

18.b. Were the following groups over-represented in the requests received? N/A

c. Parents or guardians on behalf of (a) child(ren): Yes / No
d. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: Yes / No

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
N/A

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
c. Average Yes
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

No.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

k. Name the issue(s) identified and briefly describe it.
l. Which provision(s) of the GDPR (or national laws) does this concern?
m. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
n. What are differences that you have encountered between controllers in your Member State?
o. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

a. The information regarding the erasure request is not provided in a timely manner and/or in the one-month period.
b. Article 12 GDPR
c. It appears that there are no written policies/ procedures concerning the actions taken when receiving a request or these policies are not shared to the staff.
d. –
e. Apply and follow written procedures and inform the staff accordingly.

a. Online newspapers publish excessive personal data, e.g. photos and names of data subjects. Even though the right to erasure is exercised, however they do not proceed with deletion of the personal data and do not provide with the reasons why.
b. Article 17 GDPR
c. The controllers do not balance (correctly) freedom of expression and the right to protection of personal data.
d. –
e. DPO involvement

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

No.

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to sub questions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).

24. Are there any leading or best practices of the controllers having responded that you would like to share?

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.
26. Are there any leading or best practices of the controllers having responded that you would like to share?

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers
28. Are there any leading or best practices of the controllers having responded that you would like to share?

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?
If yes, please provide the date, link to the guidance, and a short description of the guidance.
No.

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.
Our SA has conducted informal contacts, ex officio or complaint-based investigations and enforcement actions such as cases where our SA issued an order to erase personal data. There was compliance from the controllers.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?
The number of complaints received regarding the right to erasure was significantly less than the number of complaints regarding access request. The number is growing every year.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).
N/A

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes:
   If "Yes", please specify: *(please select one or more answers)*
   i. More online guidance:
   ii. Online or remote training sessions: Yes
   iii. Conferences organised: Yes
   iv. Others: please specify:
b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes:
b. No:

35. Are there any other observations that you would like to share?

CZ SA

Name of Supervisory Authority: Úřad pro ochranu osobních údajů / Office for Personal Data Protection (CZ SA)

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding:
b. Fact finding + determining follow-up action based on the results: Yes
c. New formal investigation[5]:
d. Ongoing investigation:

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? Yes
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. No
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? Yes, although we can't exclude the possibility of launching formal investigation(s), we are not currently planning any. We are going to publish our findings from this action.

b.

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
We used the same questionnaire for all controllers; we made no changes to the questionnaire.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
Not applicable.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?
Our method consisted of a fact-finding exercise with no changes to the questionnaire. The respondents were not anonymous. Based on the collected answers, we are going to publish our findings from this action.

Part I - Information about the controllers addressed

[5] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

6. How many controllers did you contact?
20 controllers.

7. Out of the contacted controllers, how many controllers responded?
*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*
All of them, i.e. 20 controllers.

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?
Not applicable.

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector:
b. Private sector: 20 responding controllers.
c. Other: If so, what were the other sectors?

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector:
b. Health sector: 2 responding controllers
c. Social sector:
d. Insurance sector:
e. Finance sector:
f. IT sector:
g. Retail sector: 18 responding controllers
h. Logistics sector:
i. Public transportation:
j. Telecommunications:
k. Postal services:
l. Advertising sector:
m. Marketing services:
n. Entertainment sector:
o. Information / journalism sector:
p. Scientific / historical research:
q. Credit scoring agency:
r. Public utility/infrastructure provider (e.g. energy):
s. Housing industry:
t. Manufacturing:
u. Consulting:
v. Public administration:
w. Other (please specify):

11. Please specify the category in which the responding controllers fall[6]:

[6] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

a. Micro enterprise:
b. Small enterprise:
c. Medium-size enterprise: 6 responding controllers
d. Large enterprise (more than 250 employees): 14 responding controllers
e. Non-profit organisation:
f. Ministry:
g. Local authority:
h. Administrative authority/agency/office (e.g. job center):
i. School/university/educational institution:
j. Other (please specify):

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers:
b. Customers: 19 responding controllers
c. Contractors:
d. Job applicants:
e. Employees:
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients: 1 responding controllers
i. Other (please specify):

12.b. According to the responding controllers, are those data subjects also:

a. Children: 2 responding controllers
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 3 responding controllers
c. Non applicable: 17 responding controllers

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100:
b. 101 – 1 000:
c. 1 001 – 10 000:
d. 10 001 – 100 000:
e. 100 001 – 500 000: 5 responding controllers
f. 500 001 – 1 000 000: 8 responding controllers
g. > 1 000 000: 7 responding controllers

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 19 responding controllers
b. Payment data: 8 responding controllers
c. Identification data: 16 responding controllers
d. Marketing data: 16 responding controllers
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 3 responding controllers

f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences:
g. Other, please specify:

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☒ 3 years - Yes

☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	1 responding controller	1 responding controller	2 responding controllers
1 – 10	4 responding controllers	4 responding controllers	4 responding controllers
11 – 50	7 responding controllers	8 responding controllers	7 responding controllers
51 – 100	0 responding controllers	0 responding controllers	0 responding controllers
101 – 500	3 responding controllers	3 responding controllers	3 responding controllers
more than 500	5 responding controllers	4 responding controllers	4 responding controllers

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0	1 responding controller	0 responding controllers	0 responding controllers

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

0 responding controllers.

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year
☒ 3 years
☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	**2023**	**2022**
0%	17 responding controllers	18 responding controllers	18 responding controllers
10%	2 responding controllers	1 responding controller	1 responding controller
20%	0 responding controllers	0 responding controllers	0 responding controllers
30%	0 responding controllers	0 responding controllers	0 responding controllers
40%	0 responding controllers	0 responding controllers	0 responding controllers
more than 50%	1 responding controller	1 responding controller	1 responding controller

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?
☐ Yes
☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
0 responding controllers.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 1 year
☒ 3 years
☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	9 responding controllers	9 responding controllers	10 responding controllers
10%	5 responding controllers	4 responding controllers	5 responding controllers

20%	2 responding controllers	2 responding controllers	0 responding controllers
30%	1 responding controller	0 responding controllers	2 responding controllers
40%	0 responding controllers	1 responding controller	0 responding controllers
more than 50%	3 responding controllers	4 responding controllers	3 responding controllers

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
0 responding controllers.

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 2 responding controllers
b. Customers: 17 responding controllers
c. Contractors:
d. Job applicants:
e. Employees:
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients: 1
i. Other:

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: No

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes, collected results seems to be consistent in regard to the processing activities of the responding controllers.

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High Yes
c. Average
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

No, we approached twenty controllers from private sector with focus on online retail. All of them fall into a category of medium-size or large enterprises. Approximate numbers of all data subjects concerned by the processing activities of the responding controllers range from hundred thousand to more than a million. However, collected data does not indicate that differences between respondents are necessarily dependent on the size of an enterprise or on the overall number of all data subjects concerned by the processing activities.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

a) In general, we did not identify singular substantive issue relating to internal procedures, internal organisation and training or request handling. All of the responding controllers developed internal instructions regarding the right to erasure under Art. 17 GDPR, but not all of the responding controllers regularly review and adjust said procedures that implement Art. 17 GDPR. A quarter of respondents do so only in response to a change in regulations or detecting a problem. They mostly train their staff at the beginning of employment and then once a year or as needed in case of changes in internal procedures or legal framework, but there were also cases where no training was held.
The responding controllers have internal procedures on how to handle a request for erasure which relates to personal data that are processed jointly or by their processor. They mostly monitor the handling of requests under Art. 17 GDPR specifically or as customer request in wide. The average time to fully comply with Art. 17 GDPR requests is one week, but it can take up to three or four weeks in more difficult cases. Only a quarter of the responding controllers extended the one-month deadline according to Art. 12(3) second sentence GDPR for the requests received in rare cases. The most common reason for extension was the need to acquire additional information necessary to confirm the identity of the data subject, a complexity of the request or a technical difficulty due to multiple information systems.
Only a smaller part of the responding controllers stated that they inform data subjects about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy if they don't take action regarding the request of the data subject.
b) Art. 17 GDPR in general and Art. 12(4) GDPR specifically.

c) There is no explanation apparent from the data we collected, it seems to be just a matter of individual internal procedures set up. It is also possible that the abovementioned findings were made due to the limitations of a fact-finding exercise and questionnaire itself.
d) We have not encountered any major differences between controllers, but some differences in internal procedures obviously stem from specific information systems used by the controllers.
e) Solution to the identified issues could lay in publishing our findings from this action.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

In the area of request handling, best practices involved an implementation of different communication channels (email, paper documents, telephone); notification of receipt of the request and the expected deadline for its processing; informing the data subject about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to sub questions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).
Most of the responding controllers regularly evaluate the purposes of processing and the period for which personal data are to be legitimately processed. The erasure of personal data is in some cases carried out automatically, mostly in cases where personal data is processed for direct marketing purposes or in cases where the data subject initiates deletion through a user account interface. The responding controllers stated that they assess whether personal data (that are subject to an erasure request) are no longer necessary for the purposes for which they were collected or otherwise processed according to Art. 17(1)(a) GDPR, in accordance with internal guidelines and the retention periods set. Their procedure also depends on the volume of requests received.
If the data subject withdraws consent according to Art. 17(1)(b) GDPR, and there is no other legal ground for processing, then personal data are deleted. Most of the controllers stated, that if the data subject objected to the processing in accordance with Art. 17(1)(c) GDPR, then they did not refuse to comply with the request for erasure. The remaining controllers stated that they have refused the request for erasure due to an exception according to Art. 17(3) GDPR.
The most applied exception to Art. 17(3) GDPR was compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject (Art. 17(3)(b) GDPR) or the establishment, exercise or defence of legal claims (Art. 17(3)(e) GDPR). Some of the responding controllers stated that in some minor cases they did not apply any exception, which seems to be in contradiction to responses made by other controllers, who carry out similar business activities and

operate within the same legal framework. These contradictions in collected answers may exist due to the small number of requests received by the respondents or specificity of received requests, e.g. requests related to personal data processed for direct marketing purposes, both of which may have skewed our data. If the right to erasure cannot be granted immediately, the responding controllers stated that to safeguard data subjects' rights they limited processing of the personal data to mere storage.

The responding controllers stated that they comply with their notification obligation relating to the right to erasure to data recipients (Art.19 GDPR) and that they inform all data recipients, but only a certain part of respondents stated they also inform data subjects about those recipients. This may be due to the fact that data subjects did not request information about data recipients, but some of the responding controllers inform data subjects about data recipients even without an explicit legal obligation.
In a situation where the data subject submits a request that contains both a request for access and a request for erasure the controllers apply different approaches. Most commonly, they process the data subject's request for access and then handle the data subject's request for erasure, informing the data subject separately depending on the subject matter that's being handled. Small number of respondents stated that they process data subject's request for access and then data subject's request for erasure and that they inform data subject at once. Only rarely do the controllers process the data subject's request for access, inform the data subject, confirm the next step and then process the data subject's request for erasure.

24. Are there any leading or best practices of the controllers having responded that you would like to share?
We would like to point out the practice of controllers facilitating the exercise of data subject rights by automatically informing data subjects about recipients of their personal data in context of their request for erasure or, in the situation when the data subject submits a request that contains both a request for access and a request for erasure, the practice of controllers facilitating the exercise of data subject rights by processing a request for access first and asking the data subject to confirm his request for erasure afterwards.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.
All the responding controllers have published contact details on their websites through which requests for erasure can be made. Usually, the contact details are accompanied by a more detailed description of the procedure, the rights of data subjects and possible exceptions. However, in some cases the contact in question is an email address that is not highlighted in any way and that is easy to miss in the rest of the text.

Most of the responding controllers stated that the contact information through which a request can be submitted is an e-mail address or another electronic method of submitting a request. Only a smaller part of respondents stated that a request can be submitted by post (paper document) or by telephone. All of them stated that they

respond to requests electronically, by e-mail, or via the user account interface. Less than a third stated that they responded to the request by post (paper document).

Most of the responding controllers, but not all, stated that they send confirmation of receipt of the request, indicating the expected time frame for its processing.

26. Are there any leading or best practices of the controllers having responded that you would like to share?
We would like to highlight the practice of providing contact details for submitting a request for erasure on websites as clearly as possible, so that it is not necessary to search for them within the entire content of the website. We also consider allowing usage of multiple communications channels to be good practice. As we have already stated, we consider sending an acknowledgement of receipt with an estimated processing time to be good practice.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers.
Only a fifth of the responding controllers stated that they follow a technical standard when deleting personal data. The others proceed according to internal guidelines and legal standards. From a technical point of view, the controllers delete personal data mainly by permanently deleting (overwriting) data and anonymizing it through hashing functions. In the case of physical media, erasure procedure is done via destroying or shredding said media. For this purpose, respondents mostly use their own internal systems, and to a lesser extent, specialized tools. Most of the responding controllers do not involve external services in the deletion process, except in cases where data are stored in a processor's system or if the controller in question is a part of a multinational group and the erasure is performed by the parent company.
More than a third of the responding controllers perform deletion through permanent data deletion and anonymization, depending on the type of information system. Some controllers perform deletion only through permanent data deletion and some only through anonymization. In relation to anonymization, the controllers stated that this is technically a simpler solution, and in some cases, it is apparently the only option available to ensure data continuity in information systems and to ensure that the data in question can be used for analytical and statistical purposes.
Most of the responding controllers stated that personal data are also deleted from backups and other information systems, but at the same time some of them stated that data from backups are deleted only when they are automatically overwritten by another backup. Deleting specific data from a backup is obviously problematic, as it may jeopardize the integrity of the backup data. In the view of the above, there are certain doubts about the consistency of the answers given. Similar doubts arise in cases where the controllers stated that they apply the same erasure procedures that they use for their main systems even for erasure of backups. In other words, it depends on whether they consider automatic backup overwriting to be a different procedure or not.
The complexity of the erasure process is evidenced by the fact that the responding controllers consistently stated that they face problems while deleting data in older

information systems, within large cloud solutions, or while ensuring the right to erasure when restoring backups.

28. Are there any leading or best practices of the controllers having responded that you would like to share?
Not applicable.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?
If yes, please provide the date, link to the guidance, and a short description of the guidance.
Not applicable.

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.

We deal with the right to erasure ("right to be forgotten") during our formal investigations and administrative proceedings, especially in reaction to complaints lodged by data subjects.

Standard course of action in cases of complaints lodged by data subjects that are related to right to erasure is to send a letter addressed to the concerned controller, that notifies them about a possible infringement of GDPR and that also contains advice on how to remedy this possible situation. If that is not sufficient, we might issue a decision stating that the controller needs to react to the right of erasure request accordingly in a certain time period (corrective measure) and we can also impose a fine within the same decision.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?

We often receive complex complaints in which right to erasure may play a role but does not necessarily make up the entire subject matter of the complaint. We can provide information regarding the volume of complaints related to this matter from the beginning of 2020 to July of 2025. We received 173 complaints in 2020, 104 in 2021, 187 in 2022, 192 in 2023, 121 in 2024 and 106 complaints from January 2025 to July

2025, i.e. 883 complaints during the period of question. This year, we have recorded an increasing number of complaints related to the matter at hand.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).

Based on the collected answers, we are going to publish our findings from this action. We can't exclude the possibility that formal investigation(s) will follow, but no formal investigations are currently planned.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes: Yes
   If "Yes", please specify: *(please select one or more answers)*
   i. More online guidance: Yes
   ii. Online or remote training sessions:
   iii. Conferences organised:
   iv. Others: please specify:
b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes: Yes, EDPB should adopt guidelines on the subject of right to erasure.
b. No:

35. Are there any other observations that you would like to share?
No.

DE SAs

Name of Supervisory Authority: DE SAs

Consolidated report for all participating German SAs, i.e. Baden-Württemberg, Brandenburg, Mecklenburg-Western Pomerania, North Rhine-Westphalia, Lower Saxony, Rhineland-Palatinate, and Federal (BfDI)

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding: Yes
b. Fact finding + determining follow-up action based on the results: Yes
c. New formal investigation[7]: Yes
d. Ongoing investigation: No

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? Yes
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. Yes, partially. Some SAs will incorporate the results of the CEF survey into further dialogue with the controllers, e.g. to achieve shorter retention periods in specific sectors.
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? Yes, the controller's responses will be taken into account in future consultations and supervision. The identified issues and challenges will be brought to the attention of the controllers.

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
Same questionnaire for all controllers.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
No exclusions or changes.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?

[7] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

For clarification, this National Report consolidates the contributions of the seven German supervisory authorities (SAs) participating in the CEF 2025 Action. The findings presented herein cannot be assumed to apply to other German SAs which did not take part in this CEF Action.
Furthermore, the participating German SAs did not each approach the same number, type, or sector of controllers. Accordingly, not all findings set out in Part II of this Report apply to all responding controllers. Likewise, the findings, observations, possible explanations, and proposed solutions should not be regarded as valid or fully applicable in equal measure to each of the participating German SAs.
This National Report does not constitute a legally binding assessment.

Part I - Information about the controllers addressed

6. How many controllers did you contact?
61

7. Out of the contacted controllers, how many controllers responded?
*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

60

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?
No, the missing controller is unresponsive.

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 22
b. Private sector: 38
c. Other: -
    c. If so, what were the other sectors? -

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector: 3
b. Health sector: 5
c. Social sector: 1
d. Insurance sector: 9
e. Finance sector: -
f. IT sector: 1
g. Retail sector: -
h. Logistics sector: -
i. Public transportation: -
j. Telecommunications: -
k. Postal services: -
l. Advertising sector: -
m. Marketing services: -

n. Entertainment sector: -
o. Information / journalism sector: -
p. Scientific / historical research: 1
q. Credit scoring agency: -
r. Public utility/infrastructure provider (e.g. energy): 2
s. Housing industry: 11
t. Manufacturing: 2
u. Consulting: 8 (legal consulting)
v. Public administration: 14
w. Other (please specify):
- tourism (2 responding controllers)
- recruitment agency (1 responding controller).

11. Please specify the category in which the responding controllers fall[8]:

a. Micro enterprise: 4
b. Small enterprise: 9
c. Medium-size enterprise: 10
d. Large enterprise (more than 250 employees): 13
e. Non-profit organisation: 2
f. Ministry: -
g. Local authority: 11
h. Administrative authority/agency/office (e.g. job center): 3
i. School/university/educational institution: 4
j. Other (please specify):

- Statutory Health Insurance Company (1 responding controller)
- Organisation of medical professionals in health insurance (1 responding controller)
- Public-law institution with legal capacity (2 responding controllers)

12.a. Which category of data subjects is <u>mainly</u> concerned by the processing activities of the responding controllers?

a. Potential customers: 4
b. Customers: 30
c. Contractors: 3
d. Job applicants: 13
e. Employees: 3
f. Applicants (for public services): 1
g. Citizens (for public sector): 2
h. Patients: 2
i. Other (please specify):
- Clients (2 responding controllers)
- Students (3 responding controllers)
- Insurance Members (1 responding controller)
- Study participants, contracted doctors and therapist (2 responding controllers)

[8] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

Note: Some controller provided multiple answers.

12.b. According to the responding controllers, are those data subjects also:

a. Children: 36
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 30
c. Non applicable: 9

Note: Some controller provided multiple answers.

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: 1
b. 101 – 1 000: 3
c. 1 001 – 10 000: 17 (1 controller noted that the figure refers to the number of people affected each year, archive excluded)
d. 10 001 – 100 000: 14
e. 100 001 – 500 000: 8
f. 500 001 – 1 000 000: 4
g. > 1 000 000: 12

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 54
b. Payment data: 27
c. Identification data: 26
d. Marketing data: 4
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 18
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 1
g. Other, please specify:

- Data in the context of legal work / mandate-related data (3 responding controllers)
- Student data, e.g. exam and application data (2 responding controllers)
- insurance contract data (2 responding controllers)
- Information about training and careers (1 responding controller)
- Human resources management (1 responding controller)
- Research data and personnel file data (1 responding controller).

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years

☒ other, specify: 6 SAs provided figures for three years (2022, 2023, 2024), while 1 SA provided figures only for 2024. This should be taken into account when considering the figures presented below.

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	24	18	18
1 – 10	17	12	12
11 – 50	7	4	4
51 – 100	4	2	2
101 – 500	2	-	-
more than 500	6	4	4

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0	19	18	16

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
None

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years

☒ other, specify: 6 SAs provided figures for three years (2022, 2023, 2024), while 1 SA provided figures only for 2024. This should be taken into account when considering the figures presented below.

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	**2023**	**2022**
0%	27	12	13
10%	-	-	-

20%	-	-	-
30%	1	1	1
40%	1	1	1
more than 50%	7	8	7

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?
☒Yes
☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

None.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 1 year
☐ 3 years
☒ other, specify: 6 SAs provided figures for three years (2022, 2023, 2024), while 1 SA provided figures only for 2024. This should be taken into account when considering the figures presented below.

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	26	13	14
10%	3	1	2
20%	1	1	1
30%	1	2	-
40%	1	-	1
more than 50%	3	4	3

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
1 controller

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 16
b. Customers: 23
c. Contractors: 2
d. Job applicants: 7
e. Employees: 5

f. Applicants (for public services): -
g. Citizens (for public sector): 2
h. Patients: 3
i. Other: 4

- students including former ones (2 responding controller)
- Statutory Health Insurance Members (1 responding controller)

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: Yes

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
c. Average
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

- The number of erasure requests tended to be higher for larger organisations, for those subject to more special legal provisions, and for those processing data of a greater number of data subjects.

- The responding controllers in the public sector seem to be slightly less aware of retention periods and granting the right to erasure.

- In the healthcare sector, over 40% of erasure requests are rejected, primarily due to statutory retention periods, for example § 630f (3) of the German Civil Code (BGB).

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

Issue 1: Internal Guidelines

a. Issue identified

Some controllers stated that they have not developed any specific internal instructions/guidelines/recommendations or similar documents on the right to erasure, as they have not received any requests to date.

The employee processing the request must decide on each request on a case-by-case basis.

Some controllers only have the instruction to contact a responsible person or forward the requests to this person (head of the company; data protection officer) without further general guidelines.

b. GDPR or national law provisions

Art. 17, Art. 24 (1), Art. 5 (2) GDPR.

c. Potential explanation

The controllers have justified this by stating that they had received few or no requests for erasure to date. Consequently, they did not consider the implementation of internal procedures to be necessary.

d. Differences between controllers in your Member State?

-

e. Possible solutions

Guidance and recommendations regarding the fact that the implementation of pre-defined procedures are a substantial part of the responsibility of the controllers according to Art. 24 (1) and Art. 5 (2) GDPR, regardless of the actual number of data subjects' rights being exercised.

Prescribed procedures/work instructions ensure a uniform approach, providing legal certainty for individual employees.

Issue 2: Reviewing Process

a. Issue identified

There is often an inadequate process for reviewing and adapting the procedures used to implement Art. 17 of the GDPR.

b. GDPR or national law provisions

Art. 17, Art. 24 (1) GDPR and where applicable special legal provisions (e.g. § 110a SGB IV, § 284 SGB V, 304 SGB V, 107 SGB XI)

c. Potential explanation

It is possible that the controllers do not realise that the processes need to be reviewed as they are currently receiving few or no requests for erasure.

d. Differences between controllers in your Member State

Companies with external data protection officers perform better in this area.

e. Possible solutions

Supervisory Authorities should raise awareness among controllers that reviewing and updating processes is necessary not only in response to a high number of erasure requests, but also due to changes in legislation, case law, or data processing practices. In addition to the right to erasure, Art.17 GDPR also stipulates the obligation of the controller to erase personal data without undue delay under the conditions specified therein. Guidelines and specific work instructions also serve as a preventive measure to ensure legal certainty in this regard.

Issue 3: DPO's Role

a. Issue identified

Systematic oversight and the role of the Data Protection Officer (DPO) in fulfilling data subject rights: it seems some organisations require the DPO to not only oversee the fulfilment of the right to erasure but actually conduct the process, leading to self-control and a collision of interests. Other controllers seem to delegate the fulfilment of data subject rights to a number of personnel for their field of activity each, leading to possible inconsistencies in regards to whether, when or how the right to erasure is granted.

b. GDPR or national law provisions

Art. 5 (2), Art. 12, Art. 39 GDPR

c. Potential explanation

We assume the lack of proper internal processes might be due to a lack of prioritizing data protection on the highest level of management. In most cases this might also correlate with the low to zero number of erasure requests received

d. Differences between controllers in your Member State?

-

e. Possible solutions

Notify controllers of the alleged infringements found, issue guidance and engage in a counselling process.

Issue 4: Training

a. Issue identified

Some controllers stated that they did not provide regular data protection training for their staff. In most cases, training only occurs on an ad hoc basis or less than once a year.

b. GDPR or national law provisions

Art. 32, 39(1) (b) GDPR

c. Potential explanation

One possible explanation is that these controllers provide data protection officers with insufficient resources to carry out their tasks.

d. Differences between controllers in your Member State?

-

e. Possible solutions

The responsible controllers must be aware of the problem and support the data protection officer accordingly, e.g. by providing sufficient resources and support tools. Another possible solution would be to develop e-learning tools and programmes designed for self-study.

Issue 5: Selecting Data

a. Issue identified

There is often an inadequate process in place for selecting data for erasure. Controllers often find it challenging to identify all locations where personal data is stored across different systems. This further complicates data identification and retrieval and this can be time-consuming.

b. GDPR or national law provisions

Art. 5, 6, 12 (3), 17 (1) and (2), 19 GDPR

c. Potential explanation

Controllers cite the complexity of data processing systems as a possible reason for the difficulty of selecting which data to erase. Particularly in cases involving complex storage, such as digital or paper files, multiple systems, databases, and similar arrangements (mixed media storage). Additionally, several parties within the controller, the processors and, where applicable, the joint controllers must coordinate their actions.

d. Differences between controllers in your Member State?

e. Possible solutions

The controllers must document their processing activities better, especially the storage locations (for digital and paper-based files) by using the record of processing activities. Defining suitable search criteria could make finding information easier.

The use of cross-system search tools can help identify and locate data relating to a specific data subject.

Issue 6: Case-by-Case Handling

a. Issue identified

Requests regarding the right to erasure are mostly dealt with on a case-by-case basis. This might be challenging for controllers because individual case reviews are likely to be labour-intensive, especially for complex requests.

b. GDPR or national law provisions

Art. 17GDPR

c. Potential explanation

Lack of clear structures and processes.

d. Differences between controllers in your Member State?

-

e. Possible solutions

Uniform standards and processes on the right to erasure, e.g. based on the records of processing activities

Issue 7: Group Structures

a. Issue identified
In large enterprises operating in a corporate structure, certain data (mainly contact data) is shared between the group companies if the data subject is a client of various group companies. Those data are stored in a joint master data management system. Due to the group structures of the controllers, a request for erasure must be checked for every single group company to see whether the joint master data management is affected. If this is the case, it is checked whether and which data is still required by other controllers in the group.
b. GDPR or national law provisions
Art. 17, 19, 26, 28 GDPR
c. Potential explanation
High technical challenges due to the volume of data.
d. Differences between controllers in your Member State?
-
e. Possible solutions
-

Issue 8: Withdrawal of Consent (health data)
a. Issue identified
Another challenge is the assertion of the right to erasure in connection with the withdrawal of consent as the legal basis for the processing of health data. In private health insurance, health data is largely processed on the basis of consent pursuant to Art. 6 (1) (a) GDPR and the exception to the prohibition on processing in Art. 9 (2) (a) GDPR. Withdrawal of consent is then regularly accompanied by the cancellation of the contractual relationship, as there is no other exception to the processing prohibition of Art. 9 (1) GDPR than consent for processing
b. GDPR or national law provisions
Art. 6 (1) (a) (b) in conjunction with Art. 9 (2) (a) GDPR
c. Potential explanation
Lack of legally compliant exemption from the processing prohibition in Art. 9 (1) GDPR for the processing of health data in private health insurance for the purpose of the initiation and performance of a contract.
d. Differences between controllers in your Member State?
-
e. Possible solutions
Common understanding of the legal exemptions for such data processing.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

- Develop and publish Checklists / internal guidelines / recommendations / work instructions or diagrams for the internal procedures regarding incoming requests for erasure, outlining the individual work steps and responsibilities and taking into account the various data protection requirements of Art. 17 GDPR (deadlines; identity verification; procedure with several controllers; reasons for erasure; exceptions; notification obligation pursuant to Art. 19 GDPR) / Set binding regulations that apply throughout the organisation to facilitate handling of Art. 17 GDPR requests.

c.

- Identification of the data concerned by comparison with the record of processing activities (Art. 30 GDPR); this makes it easier for them to identify the relevant data sources and storage locations
- Structured data storage facilitates the processing of erasure requests.

- If the data cannot yet be deleted due to existing retention periods, processing is restricted (Art. 18 GDPR) and the data subject is informed accordingly.

- Conduct semi-annual data protection audits involving the data protection officer.

- Offer and conduct regular and ad hoc training for employees.

- Data protection coordinators/data protection managers serve as the interface between specialist departments and data protection officers.

- Highlight variations in the process depending on data category (special categories under Art. 9 GDPR) or special groups (children / vulnerable subjects).

- Consider establishing a (certified) data protection compliance management system for procedural processes.

- Regularly monitor, review, and adapt procedures regarding Art. 17 GDPR based on process changes affecting the deletion workflow, such as the introduction of new software for processing personal data.

- Maintain and provide information in a centralized “data protection knowledge pool.”

- Appoint a designated “data protection coordinator” in each organizational unit.

- Apply the four-eye principle when processing erasure requests.

- In case of uncertainty, contact the data subject to clarify, for example, the scope of the erasure request. Instructing employees to identify potential erasure requests by interpretation, if necessary.

- Define relevant technical and legal terms in everyday language understood by the relevant employees.

- If a processor is involved, connect an interface (e.g. an API) to automate the erasure process.

- Deletion is mostly carried out by using technical standards, (e.g., ISO/IEC).

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).

Issue 1: Legal Compliance

a. Issue identified

Failure to consider the legal obligations applicable to the individual case and hence storage of data longer than necessary.

Depending on the sector or industry, there are diverse and extensive legal provisions regarding retention periods, as well as a broad range of storage requirements and legal exceptions.

b. GDPR or national law provisions

Art. 17 (1) GDPR and where applicable special legal provisions (e.g. § 110a SGB IV, § 284 SGB V, 304 SGB V, 107 SGB XI), Section 257 of the German Commercial Code (HGB) and Section 147 of the German Fiscal Code (AO))

c. Potential explanation

There is no uniform retention period, as different laws, risks, business areas, and data protection principles must be taken into account.

In complex cases, external advice or expertise may be necessary, incurring additional costs

d. Differences between controllers in your Member State?

-

e. Possible solutions

Even templates and guidance do not completely exempt from a case-by-case examination. Standardization of erasure periods in various special laws could lead to a simplification of the individual case examination. Maintain and update internal lists specifying retention periods. Record the retention period and the legal basis in the record of processing activities.

Issue 2: Understanding of Terminology

a. Issue identified

Some controllers had a poor understanding of the terms 'objection', 'withdraw' and 'overriding legitimate grounds'. In particular, ‘withdraw’ and ‘objection’ were often used in the wrong context, i.e. in connection with the wrong legal basis. For example, in the case of withdrawal, reference is made to the legal basis of Article 6(1) (b) of the GDPR.

b. GDPR or national law provisions

Art. 4, 6, 7, 17, 21 GDPR

c. Potential explanation

-

d. Differences between controllers in your Member State?

Some controllers use the terms correctly, in accordance with their meaning.

e. Possible solutions

Firstly, the controllers must be made aware of the problem. Data protection officers would also need training.

24. Are there any leading or best practices of the controllers having responded that you would like to share?

- The assessment of Art. 17(1) (a) of the GDPR is based on the classification of the category of data subject (e.g. former employees, applicants, clients and newsletter subscribers) and the categories of personal data being processed.

- In the case of a combined request for access and erasure, some controllers described a two-step procedure that allows data subjects time to review the information provided in accordance with Art. 15 of the GDPR after receiving it. Only then the data will be erased.

- If data cannot be deleted immediately due to legal or contractual obligations (e.g. under commercial law), processing may be restricted in line with Article 18 GDPR by revoking access rights and marking the relevant data records accordingly, ensuring they are only retained for the sole purpose of fulfilling the storage obligations.

- The legal department, data protection experts, and the data protection officer are consulted in the event of complex legal issues.

- Systematic evaluation is carried out regularly to ensure compliance with reporting obligations, e.g., pursuant to Art. 19 GDPR.

- Automate or streamline processes—for example, by using templates—to facilitate compliance with obligations such as the notification requirement under Art. 19 GDPR.

d.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.

Issue 1: Information Obligations and Facilitation of Data Subject Rights

a. Issue identified

Some controllers do not provide data subjects with any instructions or only with the criteria for determining storage periods, despite existing legal provisions, and fail to concisely inform them on how to exercise their right to erasure, including accessible channels, which may explain the low number of erasure requests received.

b. GDPR or national law provisions

Art. 5 (1) (a), Art. 12, 13 (2) (a) and Art. 14 (2) (a) GDPR

c. Potential explanation

The controllers might be unaware of the difference between the alternatives mentioned in Art. 13 (2) (a) as well as in Art. 14 (2) (a) GDPR.

We assume the lack of proper internal processes might be due to a lack of prioritizing data protection on the highest level of management. In most cases this might also correlate with the low to zero number of erasure request received.
d. Differences between controllers in your Member State?
Controllers of the public sector seem to have slightly more issues here.
e. Possible solutions
Raise awareness among controllers about the need to provide clear and concise information to data subjects, particularly regarding profession-specific retention obligations, and offer guidance, counselling, instructions on the procedures for exercising the right to erasure, e.g. including identification requirements to ensure requests are handled efficiently .

26. Are there any leading or best practices of the controllers having responded that you would like to share?

- Controllers offer various communication channels to data subjects. Some controllers offer the possibility to submit requests for erasure via customer online portals.

e.

- The website, forms and/or privacy policy should provide additional guidance specific to the target group regarding Art. 17 GDPR, including applicable legal retention periods.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers

Issue 1: Backups
a. Issue identified
No proper deletion processes of backup data. Some controllers do not delete or remove personal data from backups at all. Furthermore, they have not implemented a process to ensure that previously restricted or deleted data will not be restored when backups are reinstalled.
b. GDPR or national law provisions
Art. 5 (1) a, e, Art. 17, Art. 25 and Art. 32 GDPR
c. Potential explanation
It is technically challenging to delete data selectively from backups in a way that ensures data security. In particular, deleting data from backups can conflict with the integrity of the backups themselves. Controllers, especially those with high security requirements, tend to prioritise integrity of the backups.
In the unlikely event that the system needs to be restored from an unadjusted backup, the technical/organizational challenge would be to perform the repeated deletions of the affected documents and thus also personal data in order to restore the state at the time of the event that required the system to be reinstalled, which can only be done by documenting the deletion processes. Some controllers are unaware of this fact.
Differences between controllers in your Member State?
-
e. Possible solutions

Issue guidance and engage in a counselling process.

Issue 2: Selective Deletion

a. Issue identified

One challenge for controllers is that some processing systems lack tools that allow for the selective deletion of specific data. Without these tools, manual deletion would be necessary, which could be time-consuming or even impossible, depending on the amount of data and the processing system

b. GDPR or national law provisions

Art. 17, 25 GDPR

c. Potential explanation

One possible explanation is that some systems/software have become so complex that it is difficult to develop or retrofit such tools.

d. Differences between controllers in your Member State?

-

e. Possible solutions

Appropriate tools in the standard software and automated erasure procedures within the systems should be driven forward.

Issue 3: Permanent Deletion

a. Issue identified

Permanently deleting digital data from IT-systems and providing evidence that it cannot be recovered poses a problem for some controllers.

b. GDPR or national law provisions

Art. 17, 25 GDPR and special legal provisions (e.g. § 110a SGB IV, § 284 SGB V, 304 SGB V, 107 SGB XI)

c. Potential explanation

The physical destruction of paper files or data storages is naturally easier to handle than the erasure of digital files within a system Therefore it is difficult to develop or retrofit such software solution.

d. Differences between controllers in your Member State?

-

e. Possible solutions

Possible solutions could be uniform standards for setting up an IT-infrastructure for controllers (e.g. by the Federal Office for Information Security (BSI)) and the provision of software that simplifies the digital erasure of data.

Issue 4: Anonymization

a. Issue identified

Controllers faced issues to implement anonymization techniques that are state of the art.

b. GDPR or national law provisions

Art. 32 and recital 26 of the GDPR

c. Potential explanation
Data can potentially be re-identified; there are no fixed standards defining what constitutes a sufficient 'state of the art'.
Anonymisation of data is required by law in the context of statistical collection or research data.
d. Differences between controllers in your Member State?
This is particularly relevant in the healthcare and education sector.
e. Possible solutions
Practical guidance.

28. Are there any leading or best practices of the controllers having responded that you would like to share?

- Use of technical standards, e.g., ISO/IEC.
- Implementation of an internal IT ticketing system, with each erasure request being assigned a unique ticket.
- Use cross-system search tools to identify and locate data relating to a specific data subject.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?
If yes, please provide the date, link to the guidance, and a short description of the guidance.

Institution	Title	Date	Link	Short description
DSK Joint committee of the German Data Protection Supervisory Authorities	Short paper No. 11 – Right to erasure / "Right to be forgotten"	17.12.2018	https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_11.pdf	This short paper serves as a first orientation concerning the right to erasure, in particular for the non-public sector, and describes as how the German Data Protection Conference (DSK) considers the GDPR should be applied in practice.
DSK	Standard Data Protection Model (SDM)	2021 (Version 2.0)	https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-	This module is part of the standard Data Protection Model (SDM) and describes the processes for erasure and destroying personal data especially

	Module 60 “Deletion and Destruction”		V2.0_L%C3%B6schen_und_Vernichten_V1.0a.pdf and https://www.ldi.nrw.de/datenschutz/medien-und-technik/standard-datenschutzmodell	with reference to legal requirements and the different methods of erasure.
LfDI BW Commissioner for Data Protection and Freedom of Information Baden-Württemberg	Digitale Kehrwoche (“Digital Week of Sweeping“)	2025	Digitale Kehrwoche: Bucket-List | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg	The right to erasure is a fundamental data subject right enshrined in the GDPR. At the same time, everyone can play a part in reducing the circulation of personal data. To raise awareness and promote responsible data practices, the State Commissioner has launched the 'Digital Cleaning Week' initiative.
LfDI BW	The deletion concept: how to delete data correctly	15.04.2021	https://www.baden-wuerttemberg.datenschutz.de/video-loeschkonzept-wie-loesche-ich-daten-richtig/	Anyone processing personal data must also delete it. Why is this necessary? When and how should data be deleted? What happens if this is not done properly? This article provides useful information and tips for creating a deletion concept. In addition to the video we have an Excel spreadsheet designed to help create processing directories and deletion concepts.
LDA Brandenburg Commissioner for Data Protection and Access to Files of Brandenburg	Template Art. 17 GDPR		https://www.lda.brandenburg.de/sixcms/media.php/9/03d_Loeschung_Feb19_KW.pdf	Template on our website that data subjects can use to submit a request for erasure to a controller.
LfDI MV Commissioner for Data Protection and Freedom of Information Mecklenburg-Western Pomerania	Form to exercise the right to object and the right to deletion concerning Apple Look Around		https://www.datenschutz-mv.de/datenschutz/publikationen/muster/	

LDI NRW Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia	Guidelines for Police authorities		https://www.ldi.nrw.de/datenschutz/sicherheit-und-justiz/polizei/speichern-und-loeschen-personenbezogener-daten-nach-dem	Storage and deletion of personal data under the North Rhine-Westphalia Police Act
BfDI Federal Commissioner for data Protection and Freedom of Information	The right to data protection	September 2024	https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Flyer/Recht-auf-Datenschutz.pdf?__blob=publicationFile&v=13	Brief overview of the right to data protection in Germany, e.g. what rights data subjects have (right to information, correction or erasure of their data).
BfDI	The right to erasure / "Right to be forgotten" (Art. 17 GDPR)	Current publication on the BfDI homepage	https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Betroffenenrechte/Betroffenenrechte_L%C3%B6schung_Vergessenwerden.html	The information deals with the rights of data subjects in connection with the erasure of their personal data. It is among other things explained that under certain conditions people can request the erasure of their data, how data subjects can enforce their rights and what exceptions exist.
BfDI	FAQ Employee data protection / "Data protection for job applications" / "Return respectively erasure of application documents"	Current publication on the BfDI homepage	https://www.bfdi.bund.de/DE/Buerger/Basiswissen/Beschaeftigte/Beschaeftigte_node.html	Brief overview of the rights and obligations of employees in relation to data protection. One FAQ addresses explicitly the return respectively erasure of application documents.
BfDI	Archival law and data protection	March 2023	https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/Archivrecht.pdf?__blob=publicationFile&v=11	An overview of the legal provisions and requirements to be observed when dealing with archives and archived data. Among other things, the right to erasure with exceptions is explained.
BfDI	How long can the statutory health insurance	Current publication on the BfDI homepage	https://www.bfdi.bund.de/DE/Buerger/Inhalte/GesundheitSoziales/IhreRecht	Explanations of the special provisions in German social law regarding the right to erasure.

	company keep my data?		e/L%C3%B6schfristen.html	
BfDI	Pixi Video - Episode 6 (Tips for emergencies)	Current publication on the BfDI homepage	https://www.bfdi.bund.de/SharedDocs/Videos/DE/Pixi/Wissen_DF_Folge-6.html?nn=411490	The video primarily provides children and young people simple instructions on how to delete posts on the internet.
BfDI	Guideline for data protection-compliant storage of traffic data	30.09.2022	https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Datenschutzpraxis/LeitfadenVerkehrsdaten.html	These guideline deals with the storage period of telecommunications traffic data, which is assessed as appropriate. Note: The guideline does not immediately concern the GDPR but the ePrivacy Directive.

Further Guidance from Other Organizations:

Institution	**Title**	**Date**	**Link**	**Short description**
German Association for Data Protection and Data Security (GDD) e.V (Die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.)	Data carrier destruction in compliance with data protection regulations – in accordance with the state of the art –	2019	https://www.gdd.de/wp-content/uploads/2023/06/Datenschutzgerechte-Datentraegervernichtung-4.-Aufl.-2019.pdf	This guide addresses the secure and data protection-compliant destruction of various data carriers. Note: BfDI contributed to the creation of this document
German Insurance Association (Gesamtverband der Versicherungs-wirtschaft)	Code of Conduct	29.06.2018		The code owner is the German Insurance Association (Gesamtverband der Versicherungswirtschaft). The German data protection supervisory authorities and the Federation of German Consumer Organisations (vzbv) were involved in the drafting process in an advisory capacity. A revised version is currently undergoing the approval process. The code of conduct contains provisions on deletion and notification obligations.

Credit Agencies in Germany	Code of Conduct	25.05.2024	https://www.die-wirtschaftsauskunfteien.de/code-of-conduct	The major credit agencies in Germany have adopted a code of conduct for the verification and storage periods of personal data by credit agencies

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.

- Enforcement actions e.g. pursuant to Art. 58 (2)(b) (c) (f) and (g). This includes, for example, a request to set initial retention periods, after which the data must be deleted or archived / an order to delete personal data / order to comply with Art. 17 GDPR / warnings / reprimands / imposing a fine / inspections.
- SAs receive numerous complaints relating to the right to erasure, which regularly lead to complaint-based investigations.
- SAs provide guidance to both data subjects and controllers, e.g. regarding the right to erasure and retention periods. All SAs participate in regularly informal contacts and consultations with controllers of all sectors in regards to their processing activities to ensure that the right to erasure is properly granted.
- In some cases, controllers comply with the SAs requests, voluntarily, making formal enforcement measures unnecessary.
- On-sight investigation, e.g. regarding internal processes.
- Ex officio investigations.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?
No statistics of sufficient detail are available to provide an answer to this question.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).

Some of the participating German SAs consider carrying out one or more of the following actions:

- Obtain additional information and provide preventive recommendations.
- Incorporation responses into ongoing advisory activities.
- Notify controllers of alleged infringements found according to Article 58 (1) (d) GDPR and provide guidance with recommendations.
- Invite controllers to counselling meeting concerning the CEF action results and letters received from the DPA.
- Provide individual guidance and recommendations to optimise processes. If applicable, a notice pursuant to Art. 58 (1) (d) GDPR will be issued in individual cases
- Conduct ongoing investigations into storage periods.
- One controller that did not respond to the survey is going to be subject to an administrative act ordering them to respond to the questionnaire or pay a fine.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes: Yes

If "Yes", please specify: *(please select one or more answers)*

i. More online guidance: -
ii. Online or remote training sessions: -
iii. Conferences organised: -
iv. Others: please specify: Yes

Some of the participating German SAs consider carrying out one or more of the following actions:

- Publish recommendations on how to handle requests for erasure.
- Provide further guidance to the controllers involved in the CEF action.
- Offer a consultation with the responding controllers to answer their questions that might arise.
- Incorporate the controller's responses into the ongoing advisory activities.

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes: Guidance for controllers to assess request for erasure in compliance with Art. 12 and Art.17 GDPR and on the grounds of the right to erasure including a concept for erasure at the level of the EDPB in addition to e.g. the “Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR”.
b. No: -

35. Are there any other observations that you would like to share?

DK SA

Name of Supervisory Authority: The Danish Data Protection Agency

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding:
b. Fact finding + determining follow-up action based on the results:
c. New formal investigation[9]: Yes
d. Ongoing investigation:

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? N/A
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. N/A
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? N/A

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.

The Danish DPA used the same questionnaire for all controllers.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.

The Danish DPA included all the questions from the consolidated questionnaire.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?

The Danish DPA added a question (6.4) on whether the controllers were aware of the webpage regarding the right to erasure on the Danish DPA's website.

Part I - Information about the controllers addressed

6. How many controllers did you contact?

[9] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

Six controllers.

7. Out of the contacted controllers, how many controllers responded?

*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

The Danish DPA received six complete answers.

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

N/A

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: -
b. Private sector: 6 responding controllers
c. Other: -
d. If so, what were the other sectors?

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector: -
b. Health sector: -
c. Social sector: -
d. Insurance sector: -
e. Finance sector: -
f. IT sector: -
g. Retail sector: -
h. Logistics sector: -
i. Public transportation: -
j. Telecommunications: -
k. Postal services: -
l. Advertising sector: -
m. Marketing services: -
n. Entertainment sector: 4 responding controllers
o. Information / journalism sector: -
p. Scientific / historical research: -
q. Credit scoring agency: -
r. Public utility/infrastructure provider (e.g. energy): -
s. Housing industry: -
t. Manufacturing: -
u. Consulting: -
v. Public administration: -
w. Other (please specify): 2 responding controllers

The Danish DPA only asked Danish controllers providing online casinos to Danish data subject. The controllers either clicked off "Entertainment sector" or "Other" specifying that they worked with online casino.

11. Please specify the category in which the responding controllers fall[10]:

a. Micro enterprise: -
b. Small enterprise: 2 responding controllers
c. Medium-size enterprise: 3 responding controllers
d. Large enterprise (more than 250 employees): 1 responding controller
e. Non-profit organisation: -
f. Ministry: -
g. Local authority: -
h. Administrative authority/agency/office (e.g. job center): -
i. School/university/educational institution: -
j. Other (please specify): -

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers: -
b. Customers: 6 responding controllers
c. Contractors: -
d. Job applicants: -
e. Employees: -
f. Applicants (for public services): -
g. Citizens (for public sector): -
h. Patients: -
i. Other (please specify): -

12.b. According to the responding controllers, are those data subjects also:

a. Children: -
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 1 responding controller
c. Non applicable: 5 responding controllers

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: -
b. 101 – 1 000: -
c. 1 001 – 10 000: 1 responding controller
d. 10 001 – 100 000: -
e. 100 001 – 500 000: 4 responding controllers
f. 500 001 – 1 000 000: -
g. > 1 000 000: 1 responding controller

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 6 responding controllers
b. Payment data: 5 responding controllers

[10] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

c. Identification data: 6 responding controllers
d. Marketing data: 5 responding controllers
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: -
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: -
g. Other, please specify: 2 responding controllers (confidential information + statistical information on online behaviour)

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years - Yes

☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	1 responding controllers	1 responding controllers	1 responding controllers
1 – 10	4 responding controllers	4 responding controllers	3 responding controllers
11 – 50	-	-	1 responding controllers
51 – 100	-	-	-
101 – 500	1 responding controllers	1 responding controllers	1 responding controllers
more than 500	-	-	-

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0	1 responding controller	1 responding controller	1 responding controller

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
All six controllers provided the figures for this question.

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 1 year
☐ 3 years - Yes
☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	**2023**	**2022**
0%	2 responding controllers	2 responding controllers	2 responding controllers
10%	1 responding controller	1 responding controller	1 responding controller
20%	-	-	-
30%	-	-	-
40%	-	-	-
more than 50%	3 responding controllers	3 responding controllers	3 responding controllers

One controller clicking off "0%" (2022-2024) did not receive any requests.

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?
☐Yes: Yes
☐ No, if so: -

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
All six controllers provided the figures for this question.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 1 year
☐ 3 years - Yes
☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	2023	2022
0%	5 responding controllers	5 responding controllers	5 responding controllers
10%	-	-	-
20%	-	-	-
30%	-	-	-
40%	-	-	-
more than 50%	1 responding controller	1 responding controller	1 responding controller

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
All six controllers provided the figures for this question.

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: -
b. Customers: 5
c. Contractors: -
d. Job applicants: -
e. Employees: -
f. Applicants (for public services): -
g. Citizens (for public sector): -
h. Patients: -
i. Other: 1 (did not receive any)

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: No

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes, the Danish DPA expected the numbers on rejections to be high since this sector is obligated by national laws to store personal data for a longer period due to e.g. anti-money laundering purposes.

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
c. Average Yes

d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

The Danish DPA asked six controllers in the same sector and therefore no different types of controllers.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

Overall the workflow of the responding controllers is compliant with the GDPR. The Danish DPA did not identify any main issues or challenges.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

The Danish DPA noticed that the processing times for all the controllers were short and that none of them extended the one-month legal deadline. Furthermore, the Danish DPA noticed that the controllers had appointed an organisation unit with the leading role for handling requests for erasure.
Most of the controllers also had an overview over the processing of personal data within the organisation, some had a privacy management system.

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).
Consent

a. Name the issue(s) identified and briefly describe it.

Some of the controllers indicated that if the data subject withdraw their consent the controller would find a new legal basis instead of deleting the data.

b. Which provision(s) of the GDPR (or national laws) does this concern?

Article 17(1)(b) GDPR

c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?

It is the understanding of the Danish DPA, that some of the controllers are confused as to what is meant by legal basis within the meaning of the GDPR. The controllers therefore have issues identifying the correct legal basis before processing personal data.

d. What are differences that you have encountered between controllers in your Member State?

The Danish DPA did not identify any significant differences.

e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

The Danish DPA will consider whether to draw attention to this issue in the final letters to the participating controllers.

24. Are there any leading or best practices of the controllers having responded that you would like to share?

The Danish DPA finds it positive that the controllers are aware of the national legislation affecting the right to erasure.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.

The Danish DPA has not identified any main issues or challenges.

26. Are there any leading or best practices of the controllers having responded that you would like to share?

The Danish DPA has not identified any best practices.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers

The Danish DPA has not identified any main issues or challenges.

28. Are there any leading or best practices of the controllers having responded that you would like to share?

The Danish DPA has not identified any best practices.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

The Danish DPA has published some guidance regarding the right to erasure, including a webpage, guidance and a podcast.

Webpage (updated regularly): https://www.datatilsynet.dk/regler-og-vejledning/behandlingssikkerhed/sletning

Guidance (July 2018): Registreredes rettigheder.pdf

Podcast (2019): Podcast: #6 Sletning - hvornår og hvordan?

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.

The right to erasure is part of the ongoing supervisory activities of the Danish DPA. The Danish DPA is regularly handling complaints, initiating ex officio investigations and publishing or updating guidance regarding the right to erasure.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?

The Danish DPA has been registering the subject matter of complaints for cases finished since September 2023. In the period from 1 September 2023 to 27 August 2025 (approximately two years), the agency has completed 3536 GDPR related complaint cases (complaints related to other legislation are not included in this number). Out of these 3536 complaints, 532 cases relate to article 17, corresponding to approximately 15 % of these complaints.

The Danish DPA notes that these complaints may, however, also address other data protection issues.

In the majority of the complaints, the Danish DPA has concluded that there should be no deletion with reference to national legislation, e.g. the obligations for public authorities to keep records or the Danish Bookkeeping Act.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).

The formal investigations will impact the day-to-day work of the Danish DPA to ensure that the data protection rules are complied with, including consideration of which cases the Danish DPA should address on its own initiative.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes:
   If "Yes", please specify: *(please select one or more answers)*
   i. More online guidance: -
   ii. Online or remote training sessions: -
   iii. Conferences organised: -
   iv. Others: please specify: -
b. No: Yes

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes: -
b. No: Yes

35. Are there any other observations that you would like to share?
The Danish DPA has no further comments.

EDPS

Name of Supervisory Authority: EDPS

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding: N/A
b. Fact finding + determining follow-up action based on the results: Fact finding + determining follow-up action based on the results:
c. New formal investigation[11]: N/A
d. Ongoing investigation: N/A

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? Yes
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. No
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? Yes. The survey's findings will provide the EDPS with critical data to identify the EUIs handling the largest number of data subject erasure requests and will enable the EDPS to focus more effectively its enforcements actions.

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
The EDPS sent the same questionnaire to all controllers, i.e. all EU institutions, bodies, offices and agencies (EUIs).

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
a) In view of the fixed number and homogeneous nature of the entities (EU public administrations) it supervises, the EDPS was able to reply to several questions without surveying the EUIs. To complete this report, the EDPS relied on additional information gathered by the EDPS in the course of its supervisory activities.
Therefore, the EDPS decided to send a short questionnaire to all EUIs to gather statistics on the number of data subject erasure requests they received in 2022, 2023 and 2024, and calculate the percentage of those requests in comparison to the ones rejected or linked with Article 23 EUDPR the right to object. Thus, the EDPS used questions 1.2, 1.3. and 1.4 from the EDPB questionnaire, which correspond to sections 1.8 (How many requests for erasure were received in the timeframe specified for 2022, 2023 and 2024), 1.9 (What was the percentage of the data subject erasure

[11] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

requests received in 2022, 2023 and 2024 that were rejected) and 1.10 (What was the percentage of the data subject erasure requests received in 2022, 2023 and 2024 that were linked to the exercise of the right to object) of this report.
b) The processing of personal data by EUIs does not fall within the GDPR but within Regulation (EU) 2018/1725 (EUDPR). Therefore, the questions sent to the EUIs were adapted accordingly. For the same reason, where appropriate, this report includes a reference to the relevant provisions of the EUDPR.
Moreover, to complement the relevant statistics, the EDPS added the following question to the questionnaire sent to the EUIs: 'What is the approximate current number of staff members (permanent and non-permanent) in the EUIs'. This is because the EUDPR applies to the processing of personal data by all Union institutions and bodies (Article 2(1) EUDPR). It follows, that a large number of data subjects who will be able to invoke the EUDPR will be staff members (also reflected in Article 68 EUDPR), making the above question pertinent.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?

General remark:
In the majority of processing operations by EUIs, the processing is carried out because it is either necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the EUI or necessary for compliance with a legal obligation to which the controller is subject. Article 19 EUDPR sets out a data subject's right to erasure of personal data processed by EUIs. In accordance with Article 19(3) EUDPR, paragraphs 1 and 2 of that Article do not apply to the extent that the processing is necessary, among others, for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This entails that the right to erasure does not apply in the majority of processing operations by EUIs (of course under the condition that the processing of the personal data at stake is necessary, proportionate and lawful, and that the appropriate retention period set for that processing has not passed).
For Part II (Substantive issues regarding controllers' level of compliance):
- the EDPS' replies do not result from the direct inputs provided by EUIs (see above section 4).
- for the sake of selectiveness, the EDPS picked a number of relevant issues for each of the sections.

Part I - Information about the controllers addressed

6. How many controllers did you contact?
75

All EUIs (75), via their DPOs. (The list of the 75 EUIs is available here: https://www.edps.europa.eu/data-protection/eu-institutions-dpo/network-dpos_en).

7. Out of the contacted controllers, how many controllers responded?

*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

65

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?
We do not have information in this regard.

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector:

All 75 surveyed EUIs belong to the public sector

b. Private sector: N/A
c. Other: N/A

10. Please specify the sector ("core business") in which the responding controllers mainly operate:
Public administration:
All respondents are EU institutions, bodies, offices and agencies (EUIs).

11. Please specify the category in which the responding controllers fall[12]:
Other (please specify):
All respondents are EU Institutions, bodies, offices and agencies (EUIs).

bb.

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?
Other (please specify):
The data subjects concerned by the EUIs' processing activities are EUI staff members and their family members, as well as any individual interacting with EUIs (for example, if they register to an EUI newsletter).

12.b. According to the responding controllers, are those data subjects also:

a. Children: N/A
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): N/A
c. Non applicable:

The survey findings cannot provide a direct response regarding Question 12.b, as it was not part of the questionnaire shared with the EUIs. As a related point, EUIs may handle the personal data of data subjects in vulnerable categories, including children.

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: N/A
b. 101 – 1 000: N/A
c. 1 001 – 10 000: N/A

[12] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

d. 10 001 – 100 000:

All EUIs process personal data of their staff members, amounting to approximately 60 000 staff members in total.

a. 100 001 – 500 000: N/A
b. 500 001 – 1 000 000: N/A
c. > 1 000 000: N/A

As any individual may have interactions with EUIs, if only when consulting the latter's websites, it is impossible to provide an estimate of the data subjects, other than EUI staff members, that are concerned by the EUIs' processing activities.

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data:

All EUIs, among others for HR management of their staff.

b. Payment data:

All EUIs, among others for payroll management of their staff.

c. Identification data:

All EUIs, among others for HR management of their staff.

d. Marketing data:

Some EUIs, among others for marketing activities to promote the work of the EUI.

e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data:

(For EUIs: the relevant provision is Art. 11 EUDPR)

All EUIs, among others for sick leave/invalidity management, possible accommodations for
staff members with disabilities, etc.

f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences:

(For EUIs, the relevant provision is Art. 11 EUDPR)
All EUIs, if only when collecting extracts of criminal record of staff members in the hiring process.

g. Other, please specify: N/A

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐3 years - Yes

☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received

between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	2023	2022
0	9	2	19
1 – 10	28	6	2
11 – 50	2	0	0
51 – 100	1	0	0
101 – 500	2	0	0
more than 500	0	0	0

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	2024-2023	2024-2022
0	9	2	19

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
None- All EUIs provided figures for this question.

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 1 year
☐ 3 years- Yes
☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	2023	2022
0%	23	3	11
10%	0	2	0
20%	1	0	1
30%	1	0	0
40%	1	0	0
more than 50%	6	2	0

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?
☐ Yes
× No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

No information in this regard.

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
None- All EUIs provided figures for this question.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 1 year
×3 years
☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	30	5	9
10%	1	0	0
20%	1	1	0
30%	0	0	0
40%	0	0	0
more than 50%	2	0	0

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
None- All EUIs provided figures for this question.

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?
Other:
We do not have information in this regard.

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: No

The survey findings cannot provide a direct response regarding Question 18.b, as it was not part of the questionnaire shared with the EUIs. As a related point, EUIs may handle the personal data of data subjects in vulnerable categories, including children.

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*
High

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

The survey results do not allow the EDPS to draw comprehensive conclusions on the matter.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:
Name the issue(s) identified and briefly describe it.
The majority of the respondent controllers have general instructions in place on how to handle the right to erasure or data subjects' requests overall. However, not all EUIs that replied to the questionnaire operate with specific internal instructions/guidelines for handling data erasure requests. Controllers justify the absence of specific written instructions/guidelines given the very reduced number of requests for erasure they have received. This may result in inconsistent implementation of the right to erasure, insufficient monitoring of the process (including compliance with deadlines) as well as difficulties in demonstrating compliance vis-à-vis the supervisory authority or in case of litigation.

Which provision(s) of the GDPR (or national laws) does this concern?
- Article 19 EUDPR (Right to erasure): The substantive right that is being undermined.
- Article 27 EUDPR (Data protection by design and by default): Setting out the obligation for controllers to implement the necessary organisational measures to protect data subjects' rights from the outset, and have documented and reviewed procedures in place.
- Article 4(2) EUDPR (Principle of Accountability): Failing to demonstrate compliance with the data protection principles.

Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
According to the survey findings, the most common reason is **the low volume of requests**, with institutions having received few or no erasure requests.

What are differences that you have encountered between controllers in your Member State?
It is important to clarify that these survey findings pertain to EUIs as the responsible controller and not to a specific Member State. The main distinction appears to be the number of requests for erasure. Very few EUIs, and not necessarily the biggest, have received between 100 and 500 requests for erasure per year, while the vast majority received up to 10 requests or no request at all in the last 3 years.

What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?
For EUIs that deal with a significant amount of requests for erasure, **having a central register of these requests**, which the DPOs maintain or at least have access to (even if they are not responsible for handling those), could provide an appropriate solution. This register would help monitor the requests for erasure and ensure that the applicable rules (such as, deadlines, ID authentication of the requester, confirmation of data deletion across all systems) be implemented in a consistent and effective manner. This approach would support the EUIs in their responsibility to ensure and demonstrate compliance. It would also facilitate the performance by the DPO of their task to monitor compliance (Article 45(1)(b) EUDPR).

The EUIs as the responsible controllers could **develop standardised procedures** for handling data erasure requests and **share their documentation and best practices** within their EUIs' network. In this way, smaller EUIs could benefit from standardised templates for handling erasure requests.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

A good practice is adopting formal internal instructions/ guidelines describing how to handle requests on data subject's rights, which will provide guidance on the specific procedure for a data erasure request, and contain a set of detailed templates with options to be used to reply to the data subjects for each step of the procedure (acknowledgment of receipt of the request, request for clarification (if applicable), final reply, etc.).
Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).

a. Issue(s)

Based on the EUIs' responses, **a significant number of EUIs lack practical experience in handling the more complex provisions of the right to erasure**. This includes cases falling under Article 19(1)(c), Article 19(2) (data made public), Article 19(3) (exceptions) EUDPR, as well as combined requests for erasure and access. There is no standardised and unified process in place to deal with these related cases. This may result in inconsistent handling of the right to erasure request, insufficient monitoring of the process (including compliance with deadlines) as well as difficulties in demonstrating compliance vis-à-vis the supervisory authority or in case of litigation. The grounds applicable to the right to erasure provided on Article 19(3) EUDPR require a thorough assessment by the controller.
In addition, **combined data erasure and access request bring additional challenges to the controllers**, which require a complex handling of the two

competing data protection rights. In accordance with the EDPB Guidelines on 01/2022, the controller "should reflect the situation at the moment when the request was received by the controller"[13], and should not proceed with the deletion of data before providing access to the data subject[14].

b. Relevant Provisions

- Article 19(1) EUDPR (Right to erasure).
- Article 19(2) (Erasure of personal data made public).
- Article 19(3) EUDPR (Exceptions to the right to erasure).
- Article 21 EUDPR (Notification obligation regarding rectification or erasure of personal data or restriction of processing).

c.) Potential explanation why this has been an issue for EUIs

Based on the survey findings provided, many EUIs rarely face complex erasure requests. Therefore, because of the low volume of requests, they lack practical experience.

d.) Differences between EUIs

Differences in the data protection implementation and practice emerge among the EUIs. The main distinction appears to be the difference in number requests to erasure received.

e.) What are possible solutions to the issue(s)?

When handling a request to erasure under Article 19(1)(c) EUDPR, **controllers need to make a case-by-case assessment** and they should have a **thorough and robust justification for "compelling grounds"**, where applicable. The EUI's founding legal act or public interest mandate while being the basis for its processing, might not in itself be a "compelling ground" that overrides the data subject right to erasure. The EUIs must articulate why the continued processing of that specific data is greatly necessary for its public interest task that supersedes the individual's specific right. This practice demonstrates a genuine application of the proportionality principle and a true balancing of the competing interests.

The EUIs as the responsible controllers should implement a **formal, standardised workflow for handling combined requests** of erasure and access. This process must be **sequential.** The EUIs first grant the request for access and only then proceed with the erasure. This means that upon receiving a combined request, the controller's obligation is to continue processing the personal data in question and not delete it. First, they should handle the right of access. After providing access, the controller must assess whether the erasure request is applicable under Article 19 EUDPR (including the exceptions), and if so proceed with the deletion of the data.

24. Are there any leading or best practices of the controllers having responded that you would like to share?

Even when a refusal for data deletion was issued on the basis of Article 19(1)(c) EUDPR, a best practice applied by an EUI was to still implement **mitigating**

[13] EDPB Guidelines 01/2022 on data subject rights - Right of access, Version 2.1, adopted on 28 March 2023, pg. 5

[14] idem, pg. 19

measures to protect the data subject's interests, such as redacting personal data (i.e. names) in the documents that were made public.

A leading practice applied by an EUI when having to deal with combined requests for access and erasure, was to ask the data subject for confirmation if they still wished to erase the data, after they have received and reviewed it, following their right of access. This approach prevents irreversible data loss and fully respects both rights.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.

a. Issue(s)

The survey results do not allow the EDPS to draw comprehensive conclusions on the matter.

b.) Relevant Provisions

- Article 19(1) EUDPR (Right to erasure).
- Article 14(2) EUDPR (Facilitating rights).
- Article 14(3) EUDPR (Timeline for response).
- Article 15(2)(b) EUDPR (Information on rights).
- Article 4(1)(a) EUDPR (Principle of transparency).

c.) Potential explanation why this has been an issue for EUIs

The survey results do not allow the EDPS to draw comprehensive conclusions on the matter.

d.) Differences between EUIs

The survey results do not allow the EDPS to draw comprehensive conclusions on the matter. Potentially the differences might be similar to the ones cited in the above sections (21d and 23d).

e.) What are possible solutions to the issue(s)?

Not applicable.

26. Are there any leading or best practices of the controllers having responded that you would like to share?

According to the survey results, **almost all respondent controllers indicated that they send an acknowledgment of receipt after a data subject submits an erasure request**. This practice facilitates the individuals' data subject rights and is in line with the principle of transparency (Art. 4(1)(a) EUDPR) and the obligation to facilitate the individual's rights in accordance with Article 14(2) EUDPR.

Another key procedure the controllers apply is a **comprehensive communication workflow for managing erasure requests**. This process begins immediately with an acknowledgment of receipt that also provides instructions. It continues by transparently guiding the data subject through all necessary steps, including identity confirmation, notifying them of internal data sharing required to fulfil the request, and asking for clarification if needed. Notably, this practice also involves proactively

informing the individual of their right to complain to the EDPS and providing them with the relevant privacy statement, ensuring full transparency and facilitation of their rights.

The adoption and publication of clear instructions for submitting erasure requests is another recommended approach. To actively comply with the obligation under Article 14(2)(b) EUDPR to "facilitate the exercise of rights", EUIs must develop simple, clear, and easy-to-find instructions on how an individual can submit a request for data erasure. This guidance should be published across multiple channels to ensure accessibility, such as on the EUI's official website: in a dedicated and clearly labelled data protection section on the EUI's official website and in their privacy statements. The instructions should specify the designated point of contact (e.g., a functional mailbox like the DPO's or a web form), and the basic information an individual may need to provide to help the EUI locate their data.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers

a. Issue(s)

The challenges that EUIs might face are related to **accountability**. Specifically, when demonstrating that data has been adequately erased, including from backups, and that there is a clear and documented process in place for managing data deletion.

b.) Relevant Provisions

- Article 19 EUDPR (Right to erasure).
- Article 4(1)(f) EUDPR (Principle of integrity and confidentiality).
- Article 4(1)(e) EUDPR (Principle of storage limitation).
- Article 27 EUDPR (Data protection by design and by default).

c.) Potential explanation why this has been an issue for EUIs

The low number of requests to erasure received by the controllers.

d.) Differences between EUIs

The survey results do not allow the EDPS to draw comprehensive conclusions on the matter.

e.) What are possible solutions to the issue(s)?

Controllers should implement **secure erasure techniques and procedures**, that render data permanently irrecoverable, including on **backups**.

28. Are there any leading or best practices of the controllers having responded that you would like to share?

Showing accountability and adopting automated workflows to handle data subject deletion requests.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in

specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

The EDPS published a Factsheet on data subject rights, including the right to erasure, in 2022: (https://www.edps.europa.eu/system/files/2022-01/22-01-21_infographic_dataproday22_en.pdf)

The EDPS thematic guidelines include a section on data subject rights, including the right to erasure in so far as this right applies to the processing at stake (e.g., https://www.edps.europa.eu/system/files/2025-10/25-10_28_revised_genai_orientations_en.pdf, and https://www.edps.europa.eu/sites/default/files/publication/14-02-25_gl_ds_rights_en.pdf)

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.
Yes, in the context of complaint-based investigations. In cases where the EDPS has found in its decision that an EUI concerned has infringed Article 19 EUDPR, the EUI proceeded with complying with complainant's request to erase their personal data. In cases where the EDPS has found in its decision that an EUI has not infringed Article 19 EUDPR, the EDPS' decision nevertheless helped to raise awareness on when and how the right to erasure applies.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?
While EUIs' compliance with data subject rights is consistently a prevalent issue raised in complaints submitted to the EDPS, less than 30 complaints submitted since entry into force of EUDPR in December 2018 specifically concerned right of erasure.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).
The results of this exercise will be shared with the DPOs and the controllers.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?
Yes: More guidance and online or remote training sessions for EUI controllers and staff members.

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?
No

35. Are there any other observations that you would like to share?
No

EE SA

Name of Supervisory Authority: Estonian Data Protection Inspectorate

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding: Fact finding in the context of customer loyalty programs in retail sector (with a focus on gas stations and grocery store chains)
b. Fact finding + determining follow-up action based on the results:
c. New formal investigation[15]:
d. Ongoing investigation:

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? [**yes** / partially / no]
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. **[no** / yes; if yes: free text]
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? [**no** / yes; if yes: free text]

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
We used the same questionnaire for all controllers.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
Since our fact finding exercise concerned client programs the data subject groups were limited to customers and only private sector was targeted, therefore answers to some questions were known to us. For this reason we did not include questions 1.2, 1.3, 1.5 and 1.11 in our questionnaire and the list of options was shortened for question 1.4. However, we are able to provide the answers to these questions in the report.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?
Our fact-finding exercise concerned client programs used in the retail sector (with the focus on bigger grocery store chains and gas station chains.)

Part I - Information about the controllers addressed

[15] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

6. How many controllers did you contact?
12

7. Out of the contacted controllers, how many controllers responded?
*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*
12
8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?
-
9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 0
b. Private sector: 12
c. Other: -If so, what were the other sectors? -

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector: [Response, e.g. 4 responding controllers]
b. Health sector:
c. Social sector:
d. Insurance sector:
e. Finance sector:
f. IT sector:
g. Retail sector: 12 responding controllers
h. Logistics sector:
i. Public transportation:
j. Telecommunications:
k. Postal services:
l. Advertising sector:
m. Marketing services:
n. Entertainment sector:
o. Information / journalism sector:
p. Scientific / historical research:
q. Credit scoring agency:
r. Public utility/infrastructure provider (e.g. energy):
s. Housing industry:
t. Manufacturing:
u. Consulting:
v. Public administration:
w. Other (please specify):

11. Please specify the category in which the responding controllers fall[16]:

a. Micro enterprise: [Response, e.g. 4 responding controllers]
b. Small enterprise:

[16] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

c. Medium-size enterprise: 2 responding controllers
d. Large enterprise (more than 250 employees): 10 responding controllers
e. Non-profit organisation:
f. Ministry:
g. Local authority:
h. Administrative authority/agency/office (e.g. job center):
i. School/university/educational institution:
j. Other (please specify):

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?
Potential customers: [Response, e.g. 4 responding controllers]

a. Customers: 12 responding controllers
b. Contractors:
c. Job applicants:
d. Employees:
e. Applicants (for public services):
f. Citizens (for public sector):
g. Patients:
h. Other (please specify): [*to be completed*]

12.b. According to the responding controllers, are those data subjects also:

a. Children: 7 responding controllers
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 9 responding controllers
c. Non applicable: 1 controller explained that it doesn´t process the data of children or vulnerable adults; 1 controller explained that they allow anyone over the age of 14 join the loyalty program but do not categorize the customers based on status (asylum seekers etc); 1 controller explained that it is possible that data subjects include vulnerable people but they are not deducting these characteristics based on the personal data they process within the customer loyalty programs.

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: [Response, e.g. 4 responding controllers]
b. 101 – 1 000:
c. 1 001 – 10 000: 1 responding controllers
d. 10 001 – 100 000: 3 responding controllers
e. 100 001 – 500 000: 6 responding controllers
f. 500 001 – 1 000 000: 2 responding controllers
g. > 1 000 000:

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 11 responding controllers
b. Payment data: ***9 responding controllers***

c. Identification data: ***12 responding*** controllers

d. Marketing data: 9 responding controllers

e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 1 responding controller

f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences:

g. Other, please specify: 2 responding controllers (data about purchase history)

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐3 years: Yes

☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	0	0	0
1 – 10	7	8	6
11 – 50	1	1	3
51 – 100	1	1	0
101 – 500	1	0	1
more than 500	1	1	0

15.c. <u>For the SAs which asked figures relating to several years</u>, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0	1	1	1

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

We asked figures for 3 years, however one controller was not able to provide figures for the year 2022.

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years- Yes

☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	**2023**	**2022**
0%	11	12	11
10%	1		
20%			
30%			
40%			
more than 50%			

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?

☐ Yes

☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

We asked figures for 3 years, however one controller was not able to provide figures for the year 2022.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

Yes 3 years

☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	12	12	11
10%			
20%			

30%			
40%			
more than 50%			

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

We asked figures for 3 years, however one controller was not able to provide figures for the year 2022.

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?
We omitted this question, please refer to the answer under question 4. Only customer data was concerned regarding our fact-finding exercise.

a. Potential customers: [Response, e.g. 2 responding controllers]
b. Customers:
c. Contractors:
d. Job applicants:
e. Employees:
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients:
i. Other:

18.b. Were the following groups over-represented in the requests received? .

a. Parents or guardians on behalf of (a) child(ren): Yes / No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: Yes / No

Comment: Some controllers explained that they don´t categorize requests for erasure based on age or other factors and are therefore not able to provide information about whether the clients submitting the requests would fall into any groups referred in this question.

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes.

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
c. Average
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?
Our fact-finding exercise focused solely on private sector entities. However, we noticed differences between bigger and smaller entities. Smaller companies have put less emphasis on establishing processes to ensure compliance with data protection requirements, including the right to erasure.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

1)

a. Name the issue(s) identified and briefly describe it.

Training: Two responding controllers do not carry out internal data protection training at all. Some controllers carry out trainings but only on a strictly yearly basis. This fixed training schedule does not consider the need to offer training to new employees as soon as they start in their positions, which might result in a gap in adequate handling of erasure requests.

b. Which provision(s) of the GDPR (or national laws) does this concern?

Articles 17 and 5(1) of the GDPR.

Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?

Some controllers explained that since little or no erasure requests have been received, they have not recognized the need to carry out training for handling erasure requests.

c. What are differences that you have encountered between controllers in your Member State?

Smaller companies offer less training and have less thought-out processes in place for handling erasure requests compared to bigger companies.

d. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

Base-level training should be offered in any case, a solution that some companies use is offering an e-course which includes training on handling erasure requests.

2)

a. Name the issue(s) identified and briefly describe it.

Identification: Some controllers require a digitally signed request to be submitted in all cases where data erasure is requested. This could result in a possible breach of the principles relating to the processing of

personal data, e.g. the data minimisation principle, which states that collected data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

b. Which provision(s) of the GDPR (or national laws) does this concern?
Article 17 of the GDPR in connection with the data minimisation principle pursuant to article 5(1)(c).

c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
The need to sufficiently authenticate the correct data subject is important to avoid deleting the personal data of a wrong data subject, however proportional approach should be chosen.

d. What are differences that you have encountered between controllers in your Member State? -

e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?
The controllers who require digitally signed erasure requests in all cases should analyse whether it is possible to offer alternative methods for authentication (e.g through an existing self-service portal or an app) that would not require the data subject to essentially provide more personal data before deleting it (as digital containers contain the personal identification number of the data subject).

3)

a. Name the issue(s) identified and briefly describe it.
Rejections: Most controllers indicated that there have been no rejections to erasure requests in the last three years (question 1.9). However, from other answers it was clear that there are several relevant grounds for potential rejections, e.g. the need to retain personal data for legal claims, for example in cases where a customer uses a self-service check-out option but doesn´t pay for their purchase, AML regulations and data retention requirements of the national Accounting Act. It seems that controllers might not categorize certain rejections (e.g justified rejections, as per art 17 (3)) as rejections or corresponding requests as valid data subjects´ requests that require an answer on their part, which in turn could result in inadequate information being shared with the data subject.

b. Which provision(s) of the GDPR (or national laws) does this concern?
Article 17 of the GDPR, art 12(1) and art 5(1)(a).

c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
Lack of having thoroughly thought-out processes in place for dealing with erasure requests and informing the data subjects about the outcome of the requests, lack of awareness about how to process erasure requests, including requests for which there are justified grounds for (partial or full) refusal of erasure.

d. What are differences that you have encountered between controllers in your Member State?
The degree of detail with which the controllers had mapped out their processes for handling requests varied to a large extent.

e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?
Some controllers should reassess their process for handling requests and grounds for rejecting those requests, including how to ensure the data subjects are adequately informed in cases where there are grounds for (partially) retaining the data subjects´ personal data.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?
One controller uses automated processes for handling erasure requests that result in immediate deletion of personal data for certain services. When a user submits a valid request for deletion via a dedicated system interface, the related personal data shall be immediately and securely removed from the system without further manual intervention. In addition, based on the answers we received, it appears that most controllers handle erasure requests fairly quickly, in many cases within two weeks.
Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).
From the answers we received, it appears that an „all or nothing“ approach to personal data erasure seems to be prevalent for most data controllers. With a few exceptions, data controllers have not put in place measures to safeguard data subjects´ rights in case the right to erasure cannot be granted immediately. In addition, for several controllers the division of roles and the procedure for handling data subjects´ requests for erasure has not been mapped out for cases where additional data processors are used for processing the customers´ personal data. The same lack of clarity applies for verifying conditions for exceptions under 17(3) GDPR and for implementation of article 17(2) GDPR if the personal data is made public.

24. Are there any leading or best practices of the controllers having responded that you would like to share?
One controller uses a centralised tool to manage consents. The withdrawal of consent is subject to an automatic process that enforces the termination of all processing based on consent. One controller has not found itself in most of the situations described in questions 3.1 to 3.11 but has thoroughly visualized the process for cases where different exceptions to the right to erasure might be relevant in the future or where personal data would be disclosed to the public. Regarding customer loyalty programs they have identified a potential risk point of publishing the names of the winner of raffles or campaigns. In such cases, there are specific conditions for participation based on which the participant gives their separate consent to the disclosure of his/her name (and has a clear possibility to not do so) or the controller stipulates in the terms and conditions of the raffle that the winner will be contacted directly and the name will not be disclosed. In case the name is disclosed and a request for erasure of the disclosed data is received, the controller would immediately

remove the data from their channels (e.g. website, social media) and if necessary, contact third parties (e.g. platform operators, search engines) to request the removal of data, document the steps taken and inform the data subject in accordance with Article 12(3) GDPR.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.

Many controllers provided very generic answers about their personal data retention policies. Based on the answers it appears that several controllers have not assessed appropriate data retention periods in specific processing contexts (in the current case regarding customer loyalty programs). Some controllers do not provide information on processing time/expected processing time to data subjects when the data subject submits a request for erasure.

26. Are there any leading or best practices of the controllers having responded that you would like to share?

Nearly all controllers send an acknowledgement of receipt of erasure requests to the data subjects. Many replying controllers have several different channels made available to data subjects for submitting a request for deletion, e.g. e-mail, web forms, app interface. One controller described the active role of the customer service team in supporting data subjects by providing direct assistance and guiding individuals through the process, answering questions and ensuring that users understand how to exercise their right to erasure.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers

When describing how the controller erases personal data technically in a way that cannot be recovered, several controllers provided very short and generic descriptions. Some controllers simply mentioned that they ensure technically secure deletion based on the processes of the cloud service providers in accordance with the data processing agreements. Some controllers also stated that they do not rely on external processors for handling customer personal data and the deletion of such data (question 5.4) but from answers to other questions it was apparent that they have engaged processors for the processing of customer data. This could point to a problem of controllers relying on external data processors without having a clear overview of the data processing these processors are carrying out and the procedure for deletion of personal data.

Several controllers explained that a different deletion process is applied to backups in cases where the backup must be complete or it is not possible to specifically modify a part of the backup without backing it up again. This seems to be a wider issue, in the sense that it is difficult to ensure deletion of personal data from backups if the backup must be preserved as a whole and cannot be changed in parts.

28. Are there any leading or best practices of the controllers having responded that you would like to share?

Three controllers pointed out that they act in accordance with the international standard ISO/IEC 27001.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?
The EDPI has not issued specific guidance on the right to erasure, however it is an aspect that has been included in trainings carried out by our SA. We have also published a special section dedicated to data subjects´ rights, including right to erasure, on our website.

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.
There has been many complaint-based investigations regarding the right to erasure.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?
We do not have available statistics regarding the number of complaints relating to article 17 GDPR. As a general observation the number of complaints has grown since the entry into force of GDPR as data subjects have become more aware of their rights in general, however we have not noticed a bigger volume of article 17 complaints in proportion to other types of complaints.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).
We are planning on sending out general observations and further recommendations to the controllers with reference to the EDPB final report addressed to the controllers we sent the questionnaire to.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes:
   If "Yes", please specify: *(please select one or more answers)*

i. More online guidance:
ii. Online or remote training sessions: Yes
iii. Conferences organised:
iv. Others: please specify:

b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes: Based on the feedback from the controllers that participated in the fact finding exercise, practical guidelines clarifying different aspects of the right to erasure would be useful.
b. No:

35. Are there any other observations that you would like to share?
No.

EL SA

Name of Supervisory Authority: Hellenic Data Protection Authority

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding:
b. Fact finding + determining follow-up action based on the results: Yes
c. New formal investigation[17]:
d. Ongoing investigation:

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)?

Yes

- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available.

The Authority will examine whether formal investigations will be launched in the near future.

- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how?

If eventually no formal investigations are decided, our enforcement activities will be nevertheless impacted by the conclusions drawn by this exercise, e.g. in the sense that our case handling officers will be taking into account the findings of this exercise during the performance of their duties, examining complaints relating to the area of marketing strategies and reward/loyalty programs/cards.

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.

We used the same questionnaire for all chosen controllers.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.

N/A

[17] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?

The Hellenic DPA decided to address the questionnaire to data controllers that collect and process personal data within the framework of marketing strategies consisting in reward/loyalty programs and/or the issuance of reward/loyalty cards, which encourage their users to shop at specific businesses by offering them various benefits (e.g. discounts, gifts, offers). In these cases, data controllers often address personalized advertisements to cardholders, after having previously analyzed their purchases and consumer habits, a practice that consists in profiling. The Hellenic DPA is interested in exploring how the deletion of the retained inferred personal data is implemented in such cases.

Part I - Information about the controllers addressed

6. How many controllers did you contact?
35 controllers

7. Out of the contacted controllers, how many controllers responded?
*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

29

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

5 of the controllers did not respond to the questionnaire despite having been urged to do so by our Authority more than one time. 1 controller replied that they won't reply, because the data controller responsible for the marketing activities of the Greek company is located in Germany.

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector:
b. Private sector: 29
c. Other: If so, what were the other sectors?

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector:
b. Health sector:
c. Social sector:
d. Insurance sector: [1]
e. Finance sector: [3]
f. IT sector:
g. Retail sector: [10]
h. Logistics sector:

i. Public transportation:
j. Telecommunications: [1]
k. Postal services:
l. Advertising sector:
m. Marketing services:
n. Entertainment sector:
o. Information / journalism sector:
p. Scientific / historical research:
q. Credit scoring agency:
r. Public utility/infrastructure provider (e.g. energy): [3]
s. Housing industry:
t. Manufacturing:]
u. Consulting:
v. Public administration:
w. Other (please specify): [11].
    a. 4 controllers are Petroleum Products Trading Companies,
    b. 1 Controller is an airline company,
    c. 1 Controller is a tobacco company,
    d. 1 Controller is a Cosmetics Manufacturing and Trading Company,
    e. 1 Controller is a wholesale company,
    f. 1 Controller is a company organizing and conducting gambling games,
    g. 1 Controller is a company engaged in the granting of franchises and the provision of related consulting services,
    h. 1 Controller is a company engaged in the participation in other companies, including companies whose purpose and exclusive object is ship ownership and the operation of vessels in Greece and abroad.

11. Please specify the category in which the responding controllers fall[18]:
a. Micro enterprise:
b. Small enterprise:
c. Medium-size enterprise (up to 250 employees): [3]
d. Large enterprise (more than 250 employees): [26]
e. Non-profit organisation:
f. Ministry:
g. Local authority:
h. Administrative authority/agency/office (e.g. job center):
i. School/university/educational institution:
j. Other (please specify):

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?
a. Potential customers:
b. Customers: [29 responding controllers]
c. Contractors:

[18] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

d. Job applicants:
e. Employees:
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients:
i. Other (please specify):

It should be noted that 2 responding controllers mistakenly opted for “Other” in this question, one of them clarifying that it processes mainly personal data of employees, customers, partners, suppliers, and third parties such as participants in activities and relatives of employees and another controller that it processes mainly personal data of customers, potential customers and employees.
We presumed that this is a misunderstanding of the question by the two responding controllers, who are referring to their overall data processing and not on the scope of this questionnaire, and therefore counted them in “b. Customers”.

12.b. According to the responding controllers, are those data subjects also:

a. Children: [3 responding controllers]
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): [7 responding controllers]
c. Non applicable: [20 responding controllers]

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: 0
b. 101 – 1 000: [1 responding controller]
c. 1 001 – 10 000: [3 responding controllers]
d. 10 001 – 100 000: [2 responding controllers]
e. 100 001 – 500 000: [4 responding controllers]
f. 500 001 – 1 000 000: [6 responding controllers]
g. > 1 000 000: [13 responding controllers]

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: [29 responding controllers]
b. Payment data: [12 responding controllers]
c. Identification data: [23 responding controllers]
d. Marketing data: [23 responding controllers]
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: [0, although 1 responding controller mistakenly answered “yes” referring to employee data]
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: [0 responding controllers]
g. Other, please specify: [3 responding controllers: Data from the use of credit and debit cards at merchants participating in the loyalty programs]

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years- Yes

☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	[7 responding controllers]	[6 responding controllers]	[9 responding controllers]
1 – 10	[5 responding controllers]	[7 responding controllers]	[6 responding controllers]
11 – 50	[6 responding controllers]	[5 responding controllers]	[3 responding controllers]
51 – 100	[3 responding controllers]	[3 responding controllers]	[5 responding controllers]
101 – 500	[4 responding controllers]	[5 responding controllers]	[3 responding controllers]
more than 500	[4 responding controllers]	[3 responding controllers]	[3 responding controllers]

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0	7	6	6

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
[0 responding controllers]

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years - Yes

☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	**2023**	**2022**
0%	[26 responding controllers]	[26 responding controllers]	[26 responding controllers]
10%	[1 responding controller]	[1 responding controller]	[1 responding controller]
20%			
30%			
40%			
more than 50%	[2 responding controllers]	[2 responding controllers]	[2 responding controllers]

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?

☐ Yes

☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

[0 responding controllers]

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

Yes 3 years

☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	[17 responding controllers]	[18 responding controllers]	[21 responding controllers]
10%	[3 responding controllers]	[3 responding controllers]	[1 responding controller]
20%	[0 responding controllers]	[0 responding controllers]	[0 responding controllers]
30%	[0 responding controllers]	[0 responding controllers]	[0 responding controllers]
40%	[2 responding controllers]	[0 responding controllers]	[0 responding controllers]
more than 50%	[7 responding controllers]	[8 responding controllers]	[7 responding controllers]

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
[0 responding controllers]

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: [1 responding controller]
b. Customers: [24 responding controllers]
c. Contractors:
d. Job applicants: [2 responding controllers]
e. Employees: [1 responding controller]
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients:
i. Other: [5 responding controllers]

Similarly to our note in question 12a, the responding controllers that replied "job applicants" and "employees" in question 18a did so in error and we presumed that this is a misunderstanding of the question by them, who are referring to their overall data processing and not on the scope of this questionnaire.

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: No

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes, given that the controllers chosen for this exercise are active in the context of marketing strategies consisting in reward/loyalty programs and/or the issuance of reward/loyalty cards.

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
c. Average
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?
The level of compliance among the responding controllers was similar. Also, they all belonged to the private sector.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

We have not identified any particular issues regarding Questions 2.1 to 2.9, because all responding controllers have developed and are implementing internal procedures, internal organisation, training, etc regarding the right to erasure. As far as the review and adjustment of the procedures of implementing Art. 17 GDPR are concerned, we didn't identify any special issues, since 90% of the responding controllers review their procedures regularly (mostly once a year) or on an ad hoc basis. However, 2 controllers reported that they monitor or systematically control the handling of requests annually, which may be problematic.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

One responding controller is using KPIs to monitor its performance such as the percentage of requests answered within 1 month and the percentage of requests resolved within 3 months. These reports are submitted to Senior Management every six months for the evaluation and improvement of the process.
Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).
The main issues we have identified are the following:
Regarding art 17 (1) (a), 25% of the responding controllers state that they unconditionally accept all deletion requests without any assessment or evaluation procedure.

About 25% of the responding controllers state that they make use of documented data retention policies and of their Record of Processing Activities (RoPA), while also involving legal/business units, and relying on documented decision-making procedures.
The remaining 50% of the responding controllers make a partial assessment by making references to purpose and necessity or to compliance with law, but without referring to clear internal procedures or systematic documentation.
Regarding Article 17 (1) (b), about 30% of the responding controllers verify whether data processing was based solely on consent and if consent is the only legal basis, data are erased and the data subject is informed. If another legal basis exists, processing continues with clear documentation.
About 50% of the responding controllers directly proceed to erasure, without explicit reference to checking for alternative legal bases. (This is common for marketing purposes.).
About 20% of the responding controllers state that their processing does not rely on consent (e.g. loyalty programs or banking services based on contract) and, therefore, Article 17(1)(b) GDPR does not apply.
Regarding Article 17 (1) (c), we noticed that in marketing-related processing, requests are satisfied automatically, without a documented balancing test.
About 30% of the responding controllers, check whether overriding legitimate grounds exist before deciding.
Regarding Question 3.4, we noticed that the majority of the responding controllers (about 70%) have never refused an erasure request based on “compelling legitimate grounds“.
About 20% of the responding controllers respond theoretically, because they have not dealt with such requests.
Only a minority of the responding controllers (about 10%) have actually refused erasure, typically when required by legal obligations (e.g., tax law, regulatory frameworks).
Regarding Question 3.5, we noticed that the implementation of Article 17 (2) for the majority of the responding controllers is mostly theoretical, since they claim not to make the data public and therefore consider Article 17 (2) not applicable in their case.
Regarding Question 3.6, about 50% of the responding controllers replied that they mostly apply the exception of compliance with a legal obligation (mostly tax, labour, insurance and statute of limitations legislation).
About 20% of the responding controllers replied that they apply the exception of establishment, exercise or defence of legal claims.
About 30% of the responding controllers replied that they apply no exceptions.
Regarding Question 3.8, we noticed that all (100%) of the responding controllers replied that they have never refused to erase personal data based on the exception of Article 17(3) (a) (right of freedom of expression and information).
Regarding Question 3.9, the majority of the responding controllers follow the approach of restricting processing pursuant Article 18 of the GDPR by applying either technical (masking, encryption, anonymization) or organisational measures (flagging).
Regarding Question 3.10, about 63% of the responding controllers actively notify recipients, using different methods, mostly email, followed by automated systems and SMS/same-channel notifications.

We also noticed that about 20% of the responding controllers replied that they have no recipients to whom they disclose the data, therefore Article 19 in not applicable in their case.
As far as question 3.11 is concerned, we noticed that the majority of the responding controllers prioritize the right of access and then evaluate the requests for erasure.

24. Are there any leading or best practices of the controllers having responded that you would like to share?

No.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.
We have identified that 2 of the 29 responding controllers do not provide the data subject with guidance or a description of the procedure to submit a request of erasure. The procedure to be followed is found in the privacy policy of 19 of the 29 responding controllers. Furthermore, 8 responding controllers state that they do not provide an acknowledgement of receipt of erasure requests to the data subject.

26. Are there any leading or best practices of the controllers having responded that you would like to share?
No.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers
Many controllers (15) have replied that instead of deleting the relevant data, they are anonymizing it, but only few of them are providing some clarifications into how they are ensuring the anonymization is irreversible.
Additionally, 6 controllers have replied that they do not delete personal data from backups or different databases, which probably warrants a follow-up clarification with the relevant controllers, in case this was a misunderstanding of the question, or a formal investigation.

28. Are there any leading or best practices of the controllers having responded that you would like to share?
8 responding controllers have mentioned that either they themselves or the relevant processor have implemented the ISO 27001 or their security policy is based on this standard.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

a. An online platform has been created (accessible through this link, only in Greek https://awareness.dpa.gr/), with the goal to inform and raise awareness among young citizens about the protection of their personal data and privacy issues, including their data protection rights and how to exercise them.
b. Within the framework of the Operational Program "Public Sector Reform 2014–2020", which includes the project "Extension and provision of services of the Integrated Information System for the management of requests submitted by citizens, businesses, public services, and other entities through the online portal of the Hellenic Data Protection Authority", an an online wizard was developed to assist citizens and entities in exercising their rights.(available here, only in Greek: https://www.dpa.gr/el/polites/gkpd/wizard_politon). This system aims to assist data subjects in properly exercising any of their rights vis-a-vis the Data Controller, in case they encounter an issue related to the legislation on the processing of their personal data. At the end/final step of the wizard, the system indicates all the information that the data subject needs to gather in order to substantiate the exercise of his/her right and provides the data subject with the option to download or print an appropriate rights request form.
c. As part of the byDesign project (for more information on this, see answer to Q.30) , a user-friendly online Toolkit (available here: https://bydesign.dpa.gr/questionnaires/fe630b8d-6dae-4537-b865-e8e924ebf344/en) has been developed particularly tailored to the needs of the SMEs, facilitating GDPR compliance with a set of context-aware templates of essential documents.
d. As part of the byDefault project (for more information on this, see answer to Q.30), the following activities were carried out:
d1 An e-platform and digital library has been created for knowledge sharing among DPOs and privacy professionals and is available at https://collab.dpa.gr
d2 the educational program and physical board game on data protection, which was created for primary and secondary school students, and its supporting material for teachers (available here https://www.dpa.gr/en/enimerwtiko/themes/tzimaniousen)
e. Training material on how data subjects can protect their data rights has been created, and a series of general and specialized seminars has been conducted

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.

The Hellenic Data Protection Authority, coordinated the following initiatives:

- A two-year project entitled “byDesign” funded by the European Union’s Citizens, Equality, Rights and Values (CERV) Program. The project’s goal was dual: on the one hand, to facilitate small and medium sized enterprises (SMEs) with regard to GDPR compliance, by offering a tailored compliance kit; and on the other hand to promote the creation of data protection by design compliant ICT products and services, by raising awareness of the relevant stakeholders.
- A two-year project entitled “byDefault” funded by the European Union’s Citizens, Equality, Rights and Values (CERV) Program. The project, identifying the needs for data protection and privacy education and for an open knowledge source for DPOs and privacy professionals, pursues two strategic goals: (i) To raise data protection and privacy awareness among the critical social group of children; (ii) To provide DPOs and privacy professionals with continuous support in their activities, beyond a basic level, aiming towards specialized guidance on selected key sectors.
- Several online awareness events were organized such as:
  - “Aware by default: promoting awareness of critical social and professional groups – byDefault” was held on 4 October 2023
  - “Presentation of the ‘byDefault’ project outcomes”, was held on Wednesday July 24th 2024 18th Data Protection Day, the Hellenic Data Protection Authority organized an Information Day event entitled “Topical data protection issues – recent developments” on 30 January 2024
  - “Presentation of the project ‘byDesign’ outcomes” was held for the purposes of making an overall assessment of the findings and results of the project and answering questions.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?

Since the entry into force of the GDPR, we have received 63 complaints regarding the right to erasure. However, it must be noted that:
a) the characterization of the complaints as regarding the violation of the right to erasure is made by the complainants themselves when filing the complaint and can, therefore, be wrong,
b) many of the complaints regard the right to request the dereferencing of links from search engine results returned following a search on the basis of one’s name, and
c) this number excludes the high volume of spam related complaints we have received, since they were often mainly submitted as right to object complaints, even though it can be argued that they are also related to the right of erasure.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).

The results of this CEF will be soon communicated to the Board of the Hellenic SA, that will then decide if further actions are required and determine a potential timeline for these actions.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes: Yes
   If "Yes", please specify: *(please select one or more answers)*
   i. More online guidance: [Yes]
   ii. Online or remote training sessions: [Yes]
   iii. Conferences organised: [Yes]
   iv. Others: please specify:
b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes:
   Guidelines on the right to erasure and the consideration of legal obligations preventing erasure could be developed, which would elaborate on the procedure of implementing the right to erasure with a special focus on guidance on how to successfully implement anonymization.
b. No:

35. Are there any other observations that you would like to share? N/A

ES SA

Name of Supervisory Authority: Spanish Data Protection Agency (AEPD)

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. **Fact finding**: Yes
b. Fact finding + determining follow-up action based on the results: New formal investigation[19]:
c. Ongoing investigation:

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? Yes
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. No
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? There are no provisions for this activity to impact on the enforcement activities.

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
The same questionnaire was used by all controllers

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.

All the questions included in the consolidated questionnaire were used in the survey

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?

No further comments.

Part I - Information about the controllers addressed

6. How many controllers did you contact?
17 controllers were contacted

[19] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

7. Out of the contacted controllers, how many controllers responded?

*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

43 controllers responded

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

One public regional body and an association contacted spread the invitation among the controllers inviting them to participate in several health departments and hospitals.

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 25 responding controllers
b. Private sector: 17 responding controllers
c. Other: 1 responding controllers

If so, what were the other sectors? Charity- NGO

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector:
b. **Health sector**: 34 responding controllers
c. **Social sector**:1 responding controller
d. Insurance sector:
e. **Finance sector**: 2 responding controllers
f. IT sector:
g. **Retail sector**: 1 responding controller
h. Logistics sector:
i. **Public transportation**: 1 responding controller
j. **Telecommunications**: 2 responding controllers
k. Postal services:
l. Advertising sector:
m. Marketing services:
n. Entertainment sector:
o. Information / journalism sector:
p. Scientific / historical research: [
q. **Credit scoring agency**: 1 responding controller
r. **Public utility/infrastructure provider (e.g. energy)**: 1 responding controller
s. Housing industry:
t. Manufacturing:
u. Consulting:
v. Public administration:
w. Other (please specify):

cc.

11. Please specify the category in which the responding controllers fall[20]:

a. Micro enterprise:
b. Small enterprise: 1 responding controller
c. Medium-size enterprise: 2 responding controller
d. Large enterprise (more than 250 employees): 7 responding controller
e. Non-profit organisation: 5 responding controller
f. Ministry:
g. Local authority:
h. Administrative authority/agency/office (e.g. job center): 27 responding controller
i. School/university/educational institution:
j. Other (please specify): 1 responding controller: company providing credit information services that does not have employees

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers: 1 responding controllers
b. Customers: 8 responding controllers
c. Contractors:
d. Job applicants:
e. Employees:
f. Applicants (for public services): 3 responding controllers
g. Citizens (for public sector): 3 responding controllers
h. Patients: 33 responding controllers
i. Other (please specify):1- partners, beneficiaries and volunteers

12.b. According to the responding controllers, are those data subjects also:

a. Children: 6 responding controllers
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 6 responding controllers
c. Non applicable:

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: 1 responding controller
b. 101 – 1 000: 2 responding controllers
c. 1 001 – 10 000: 2 responding controllers
d. 10 001 – 100 000: 5 responding controllers
e. 100 001 – 500 000: 17 responding controllers
f. 500 001 – 1 000 000: 2 responding controllers
g. > 1 000 000: 14 responding controllers

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 37 responding controllers
b. Payment data: 18 responding controllers

[20] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

c. Identification data: 43 responding controllers
d. Marketing data: 4 responding controllers
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 29 responding controllers
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 1 responding controller
g. Other, please specify: Financial information

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years

☐ other, specify: This CEF is the first time that we have asked controllers to provide figures for right of erasure.

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	4 responding controllers	41responding controller	4 responding controllers
1 – 10	6 responding controllers	5 responding controllers	
11 – 50			4 responding controllers
51 – 100	1 responding controller		
101 – 500	3 responding controllers	2 responding controllers	2 responding controllers
more than 500	5 responding controllers		

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	2024-2023	2024-2022
0	5 responding controllers	5 responding controllers	5 responding controllers

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

5 responding controllers did not provide any figures for this question.

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years

☐ other, specify: This CEF is the first time that we have asked controllers to provide figures for right of erasure

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	2023	2022
0%	7 responding controllers	5 responding controllers	2 responding controllers
10%	3 responding controllers	2 responding controllers	1 responding controller
20%	1 responding controller		
30%	3 responding controllers		
40%			
more than 50%	3 responding controllers	responding controllers	2 responding controllers

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?

☐ Yes

☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

7 responding controllers did not provide any figures for this question.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years

☐ other, specify: This CEF is the first time that we have asked controllers to provide figures for right of erasure

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	11 responding controllers	2 responding controllers	2 responding controllers
10%	3 responding controllers	1 responding controller	1 responding controller
20%	1 responding controller		
30%			
40%	1 responding controller	1 responding controller	1 responding controllr
more than 50%			

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

7 responding controllers did not provide any figures for this question.

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 3 responding controllers
b. Customers: 4 responding controllers
c. Contractors: 1 responding controller
d. Job applicants: 1 responding controller
e. Employees: 3 responding controllers
f. Applicants (for public services):
g. Citizens (for public sector): 1 responding controller
h. Patients: 7 responding controllers
i. Other: Debtor clients

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): 2 responding controllers
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: 2 responding controllers.

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?

Yes.

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
c. Average: Yes
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

Different approaches appear depending on the application is based on a commercial or contractual relationship or a medical history. While in the commercial or contractual relationship, in general, it is commonly answered by directly by de DPO, when it comes to a medical history it is necessary to count on the medical team criteria responsible for the information to answer the request.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

k. Name the issue(s) identified and briefly describe it.
l. Which provision(s) of the GDPR (or national laws) does this concern?
m. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
n. What are differences that you have encountered between controllers in your Member State?
o. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

In general terms, the responding controllers show a well designed procedure to deal with data subject rights applications, including regular revisions, training programmes. Different approaches appear depending on the application is referred to a commercial relationship or a medical history where specific regulations are identified and the medical team opinion is required. Additionally, some responding controllers have implemented an automated software to handle the data subject's requests.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

Adequate procedures for dealing with data subjects requests, regularly reviewed, together with training programmes show a robust way to handle requests to exercise the right to erasure in an appropriate manner.
Several training sessions on privacy issues, and the DPO office organizing additional training sessions for specific departments based on the needs identified in different areas, both online and in person seems to be an important approach to cover training necessities.
One responding controller reported the implementation of a platform so that consumers can exercise their rights autonomously and according to their rights, also with an automated and immediate response, once the consumer's identity has been validated. On this platform, they can view the history of requests sent, responses received, processing status, etc.

- *Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below*.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).
As in the previous paragraph, responding controllers show an appropriate approach to deal with these requests depending on the field company/body. Although in some cases automated solutions are used responding controllers indicate a regularly case by case revision the procedure. The function of the DPO appear to be permanently present in these revisions.
Regarding question 3.2 of the questionnaire about the provision in article 17 (1) (a), can be highlighted one response reporting that since withdrawal of consent prevents the processing of such data, once the data subject withdraws their consent, the data will no longer be used for these purposes. However, if there is a legal obligation requiring their retention, they are subject to the blocking process according to article 32 of the Spanish data protection law.
Regarding question 3.4 of the questionnaire about refusing an erasure request based in article 17(1)(c) GDPR based on its “overriding legitimate grounds for the processing one responding controllers from financial sector, reported that this rejection is mainly related to deletion requests from active clients or those with outstanding debts.
Regarding question 3.3 of the questionnaire it has been reported that if the data subject specifies their objection request in accordance with Article 17(1)(c) on marketing, their data will be added to an advertising exclusion database and will not be included in any marketing actions, including those based on legitimate interests.
Technical measures are adopted in the systems to ensure the blocking of personal data when it must only be retained during the statute of limitations for the corresponding criminal, civil, commercial, and/or administrative liabilities, to address claims, or to defend against administrative or judicial actions.

24. Are there any leading or best practices of the controllers having responded that you would like to share?

Requests to de-index data from search engines are reported. In some cases, it has been also reported that YouTube had to be contacted to remove a former contributor's appearance from a video.
The conditions for exceptions under Art. 17/3) are evaluating in a case-by-case basis.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.
In most cases, information on how to exercise these rights is provided through the privacy policy available on the website including the conservation period. Multiple channels are provided for interested parties to exercise their rights.

26. Are there any leading or best practices of the controllers having responded that you would like to share?
As previously indicated: well-designed procedures regularly reviewed and trained personnel.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers
Most surveys indicate that no technical standards are used that comply with or adhere to regarding the deletion of personal data. However, some responding controller reported the use of ISO/IEC 27001 as well as ISO 9001.
Personal data is deleted from each system where it exists, using IT team support.
In the case of paper formats, a confidential document destruction company will handle with the deletion of personal information.
One responding controller reported the convenience of establishing control over contract cancellation platforms so that they do not include the cancellation of personal data by default, a request for which will be denied making it difficult to dedicate resources to genuine data deletion requests.
It has been also indicated that it would be advisable greater clarity from the authorities on how to act in specific cases and legal concepts such as limitations or exceptions to this right.
Regarding challenges based in the controller responding experience, they can be highlighted the following which requires specific training addressed to personnel involved:
Legal:
- It is necessary to communicate to the data subject, in simple and justified language, the reason why it is not possible to completely delete the data (for example, in some cases where it is not possible to delete the data because it is necessary to formulate, exercise, or defend claims).
- There may be situations in which the data subject's right to erasure coexists with other rights, and a balancing of rights is necessary.
• Organizational:
In some cases, data subjects use unofficial channels (for example, complaint forms or forms) to exercise these types of requests. This requires efforts to detect among the

complaints those that refer to requests to exercise rights and refer them to the area responsible for their management.
• Technical:
In some cases, there may be a system that is not designed to delete records easily, making it necessary to process the deletion process in a non-automated manner.

28. Are there any leading or best practices of the controllers having responded that you would like to share?
As previously indicated, well-designed procedures regularly reviewed and trained personnel can be highlighted as best practices.

Some responding controller from financial institution reported that, in general, the biggest challenge is managing secure deletion processes that do not affect our bank's overall operations, as well as determining appropriate retention periods that guarantee our ability to defend ourselves in the event of customer complaints or requests for information from the competent authorities.

In addition, a remark was made about some confusions observed in data subject requests regarding the right to object and the right to erasure.

As a suggestion it was reported that it would be of a great help to comply with this obligation to have tools that incorporate privacy by design and comply with the requirements of European data protection regulations when applying blocking, exclusion, and/or deletion of customer data, without involving the internal developments and risks to our business that come with the manual, internal management of these types of solutions.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

1: Section on AEPD´s website first level on the topic "knowing your rights" providing practical forms for exercising rights: https://www.aepd.es/derechos-y-deberes/ejerce-tus-derechos

2: FAQs on AEPD´s website include a section on "your rights" providing practical forms for exercising rights: https://www.aepd.es/preguntas-frecuentes/1-tus-derechos

3: New virtual assistance (24x7) via Chatbot on first level of AEPD´s web (https://www.aepd.es/), includes your rights section providing practical forms for exercising rights:

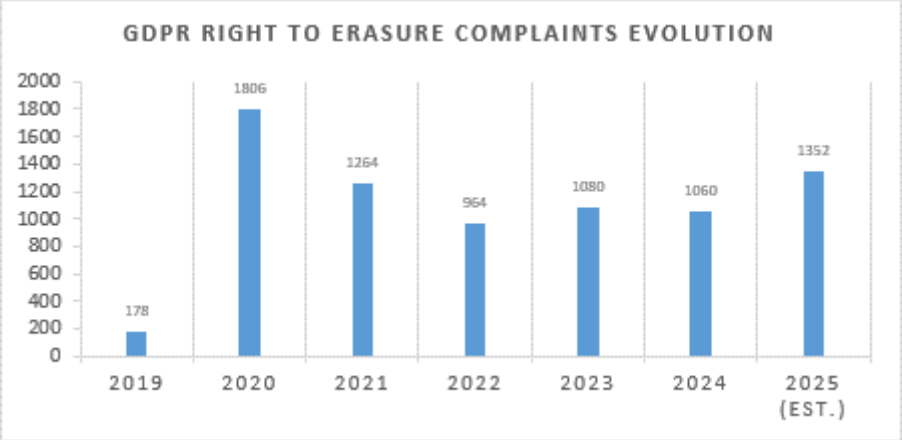
30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.

No actions were undertaken other than contacting the controllers to participate in the CEF.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?

Since the GDPR came into force, the Spanish SA has received over 7.000 complaints (7.028) regarding the right to erasure under Article 17 of the GDPR. The number of complaints reached a peak in 2020, with 1.806 complaints received. Then it decreased to stabilize around 1.000 complaints per year.

By mid-2025, 676 complaints have been received, which means that it is picking up and if it continues at this rate, the SA will have received around 1,352 complaints by the end of the year.



The volume of complaints regarding this right is approximately 8% of the total amount of complaints received, with a peak in 2020 where it represented the 17% of the complaints received that year. By mid-2025, it represents the 5% of the total complaints received so far this year.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).
None at this time but will reconsider after the overall results of this initiative.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes: Our strategic plan for the period 2025-2030 includes a line or work in order to make easier the exercise of rights and to power the role of DPD in the organisations. We think that this initiative might be useful in this framework after the experience of the overall SA opinions.
   If "Yes", please specify: *(please select one or more answers)*
   i. More online guidance: DPD specific channel, to answer doubts dealing with the exercise of rights
   ii. Online or remote training sessions: AEPD provides courses for the public sector and the promotion of contents related with the exercise of rights through associations representatives of private sector.
   iii. Conferences organised: Organized by AEPD or by other entities, the result of this CEF initiative should be spread.
   iv. Others: please specify:
b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes:

b. No: Not now, but after the result of this consultation, we will reconsider.

35. Are there any other observations that you would like to share?
No further remarks or observations.

FI SA

Name of Supervisory Authority: SA Finland (The Office of the Data Protection Ombudsman)

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding: Yes
b. Fact finding + determining follow-up action based on the results: Yes
c. New formal investigation[21]: No
d. Ongoing investigation: No

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? No, the responses were completely anonymous.
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. No.
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? No, it will not have any effect on our enforcement activities, as the questionnaire was carried out anonymously.

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.

Our SA sent the same questionnaire in both Finnish and Swedish to all controllers, as Finland is bilingual.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.

Questions 1.1 and 3.4 were removed. As the questionnaire was conducted anonymously, the option to provide internal guidelines and process charts was removed. Regarding Question 3.8, the respondents were not asked to provide the analysis that had been carried out at the time. Otherwise, the questionnaire was sent out as it was. No changes were made to the wording of the questions that would have significantly impacted the final results.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?

[21] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

This was the first year that our SA conducted the questionnaire anonymously. Since the questionnaire was anonymous, we anticipated that not all of the controllers to whom we sent the questionnaire would answer. However, we received many more answers than expected. Our experience of the anonymous questionnaire was very positive. We are confident that we received honest responses and feedback from controllers.
This year, our SA selected three sectors for our target audience: education, insurance and finance. In the finance sector, we chose to contact collection agencies. In the insurance sector, we sent the questionnaire to all insurance companies and authorised pension insurance companies. In the education sector, we contacted universities and universities of applied sciences. All operators in these sectors in Finland received the questionnaire. The selected sectors represent organisations from both the private and public sectors. When selecting the controllers to whom the questionnaire would be sent, we considered factors such as the prevalence of erasure requests in these sectors, as well as the targets of CEF measures in previous years.
As the questionnaire was anonymous, we do not intend to conduct formal investigations relating to the right to erasure in the near future, and the questionnaire will not affect our enforcement activities. However, we do plan to take follow-up action based on the results, with the aim of providing guidance on the right to erasure to controllers and specific sectors chosen this year.
We have identified some inadequacies in our use of the questionnaire. Upon analysing the responses, we realised that Questions 16.b and 17.b did not account for the possibility that some controllers had indicated in Question 15.b that they had not received any requests for erasure. As Questions 16.b and 17.b were mandatory and did not offer an alternative response option indicating that no requests had been received, those controllers who had not received any requests were still required to answer them. However, we were able to exclude those controllers who had not received any requests from the responses to Questions 16.b and 17.b. Therefore, the accuracy of the responses and tables presented in this report remains unaffected.

Part I - Information about the controllers addressed

6. How many controllers did you contact?

61

7. Out of the contacted controllers, how many controllers responded?

37

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

The main reason probably was that answering this year's questionnaire was not mandatory in any way, since the questionnaire was conducted anonymously. Thus, the gap was expected and an important reason why we sent the questionnaire to more controllers than we did in the previous years.

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 20 responding controllers
b. Private sector: 16 responding controllers
c. Other: 1 responding controllers
    d. If so, what were the other sectors? One company with a statutory duty.
    dd.

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector: 17 responding controllers
b. Health sector:
c. Social sector:
d. Insurance sector: 7 responding controllers
e. Finance sector: 9 responding controllers
f. IT sector:
g. Retail sector:
h. Logistics sector:
i. Public transportation:
j. Telecommunications:
k. Postal services:
l. Advertising sector:
m. Marketing services:
n. Entertainment sector:
o. Information / journalism sector:
p. Scientific / historical research: 2 responding controllers
q. Credit scoring agency:
r. Public utility/infrastructure provider (e.g. energy):
s. Housing industry:
t. Manufacturing:
u. Consulting:
v. Public administration: 1 responding controller
w. Other (please specify): 1 responding controller, covering both the education sector and scientific research.

11. Please specify the category in which the responding controllers fall[22]:

a. Micro enterprise: 2 responding controllers
b. Small enterprise: 3 responding controllers
c. Medium-size enterprise: 3 responding controllers
d. Large enterprise (more than 250 employees): 8 responding controllers
e. Non-profit organisation:
f. Ministry:
g. Local authority:
h. Administrative authority/agency/office (e.g. job center):
i. School/university/educational institution: 21 responding controllers

[22] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

j. Other (please specify):

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers:
b. Customers: 16 responding controllers
c. Contractors:
d. Job applicants:
e. Employees:
f. Applicants (for public services): 18 responding controllers
g. Citizens (for public sector):
h. Patients:
i. Other (please specify):

12.b. According to the responding controllers, are those data subjects also:

a. Children: 18 responding controllers
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 25 responding controllers
c. Non applicable: 8 responding controllers

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: 0 responding controllers
b. 101 – 1 000: 1 responding controller
c. 1 001 – 10 000: 4 responding controllers
d. 10 001 – 100 000: 16 responding controllers
e. 100 001 – 500 000: 7 responding controllers
f. 500 001 – 1 000 000: 2 responding controllers
g. > 1 000 000: 7 responding controllers

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 37 responding controllers
b. Payment data: 24 responding controllers
c. Identification data: 33 responding controllers
d. Marketing data: 14 responding controllers
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 16 responding controllers
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 9 responding controllers
g. Other, please specify: In total 6 controllers; 5 of them mentioned data in connection with scientific research; 1 respondent mentioned "ordered goods or services", 1 respondent mentioned "employment data", and 1 respondent mentioned "non-payment records".

15.a. For Question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☑ 3 years

☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	8	9	10
1 – 10	21	22	21
11 – 50	7	5	5
51 – 100	0	0	0
101 – 500	1	1	1
more than 500	0	0	0

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0	8 responding controllers	6 responding controllers	4 responding controllers

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

There were no such controllers, since we had marked the question mandatory.

16.a. For Question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☑ 3 years

☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	2023	2022
0%	12	12	10
10%	2	3	3
20%	1	1	1
30%	1	1	1
40%	1	1	2
more than 50%	12	10	10

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?

☐ Yes

☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

Our SA did not carry out an enforcement action.

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

As we mentioned in our response to Question 5, upon analysing the responses, we realised that we should have considered the fact that some controllers had answered Question 15.b stating that they had not received any requests from data subjects when designing Questions 16.b and 17.b. As these questions were mandatory, those controllers who had not received any requests were still required to answer them. However, we were able to exclude these controllers from the responses to Questions 16.b and 17.b. Consequently, the table for Question 16.b only contains the responses of those who did receive requests.

17.a. For Question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☑ 3 years

☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	2023	2022
0%	16	11	10
10%	9	10	10
20%	2	2	2
30%	0	0	0
40%	0	0	0
more than 50%	4	5	5

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

As previously mentioned, when we analysed the responses, we realised that we should have considered the fact that some controllers had answered Question 15.b stating that they had not received any requests from data subjects when designing Questions 16.b and 17.b. As these questions were mandatory, those controllers who had not received any requests were still required to answer them. However, we were able to exclude these controllers from the responses to Questions 16.b and 17.b. Consequently, the table for Question 17.b only contains the responses of those controllers who did receive requests.

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers:
b. Customers: 18 responding controllers
c. Contractors:
d. Job applicants:
e. Employees: 8 responding controllers
f. Applicants (for public services): 13 responding controllers
g. Citizens (for public sector):
h. Patients:
i. Other:

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): According to the respondents, just under 20 per cent of requests were made by parents or guardians on behalf of children. The proportion of children of under 18 years within the Finnish population is currently around 18 per cent. It is difficult to determine if this counts as notable over-representation.

b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: According to the respondents, 10 per cent of the requests were made by vulnerable subjects or guardians on behalf of a vulnerable subject. Whether this figure indicates over-representation depends on the share of vulnerable individuals within the controller's overall data subject population. As this baseline is not available, it is difficult to determine from this percentage alone whether vulnerable subjects are over-represented.

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?

Overall, the responses appeared consistent with the sectors in question and their processing activities. Controllers operating in the insurance sector or working as collection agencies reported that individuals submitting erasure requests were primarily their own customers or those of their clients. In the education sector, a broader range of individuals submitted erasure requests, including students,

customers, applicants for public services, and employees. In our opinion, this is also consistent with the nature of the sector and the processing activities carried out by the controllers.

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
c. Average
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

In our analysis, we focused on the differences between the private and public sectors. These differences also became apparent when we analysed the three chosen sectors individually. Universities and universities of applied sciences represent the public sector, while insurance companies, pension insurance companies and collection agencies represent the private sector.
Rejections were more common in the private sector. As our sample of private sector operators included insurance and pension insurance companies, as well as collection agencies, many of the rejections were based on statutory retention obligations and were therefore reasonable. It was also more common to fulfil erasure through anonymisation in the private sector. 75 per cent of the private sector respondents stated that they anonymise the data, compared to 40 per cent of public sector organisations.

Other differences were also present. All private sector operators had internal guidelines for processing erasure requests and erasing personal data. In the public sector, however, only around 75 per cent had similar guidelines, while a quarter did not. One reason given for this was that, as the processing of personal data is based on a compliance with a legal obligation, more detailed guidance than the legal definition is unnecessary. However, one respondent had noticed that their organisation's guidelines were inadequate, as they only covered requests for access to data and did not consider the right to erasure separately.

A similar pattern can be seen in the provision of training on requests for erasure: all private sector organisations provide training to their staff on Art. 17 GDPR. In the public sector, however, this figure is only 70 per cent. All private sector organisations also monitor or systematically control the handling of the requests under Art. 17 GDPR. In contrast, only 65 per cent of the public sector operators take such measures. Some of the public sector organisations that do not implement monitoring or control measures

cite the low number of erasure requests as an explanation. Some respondents stated that their organisation had identified a need for improvement in this area, and that development projects were currently in place to address this. In the private sector, 85 per cent of organisations regularly review and adjust their procedures for implementing Art. 17 GDPR. In contrast, only 25 per cent of public sector organisations do the same. One possible reason for the differences between the private and public sectors is the different amount of available resources.

It is also worth mentioning that most of the organisations (70 per cent) which stated that the data subjects who submitted requests for erasure were also parents or guardians on behalf of children or vulnerable subjects, or guardians of vulnerable subjects, were from the insurance sector. This is a reasonable conclusion, given that children are not usually subject to debt collection, and most students at universities and universities of applied sciences are of legal age.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.

In the higher education sector (universities and universities of applied sciences), requests for erasure are sometimes also made by people who participate in research projects. These requests are directed at individual researchers responsible for the projects who do not necessarily have a strong understanding of Data Protection Law. In situations like these, the requests for erasure can remain unnoticed by the DPO and the data protection unit.

One of the responding universities gave the following response: *"Sometimes technical issues occur when the data must be deleted manually from various locations, some of which may not be immediately recognised by the organisation. The large amount of manual labour poses a challenge."* There were, however, multiple responses from the controllers where manual labour was mentioned as an issue.

Yet another issue mentioned was adhering to legal retention periods in situations where the data are in practice only deleted manually. According to one responding university, this issue concerns particularly research data.

b. Which provision(s) of the GDPR (or national laws) does this concern?
ee.

In addition to Art. 17 GDPR, this challenge may concern, depending on circumstances of the particular case, Art. 89 GDPR, and/or national laws such as Sections 4(3) and 4(4) of the Finnish Data Protection Act (*tietosuojalaki*, 1050/2018), the Finnish Universities Act (*yliopistolaki*, 558/2009), and/or the Finnish Universities of Applied Sciences Act (*ammattikorkeakoululaki*, 932/2014).

c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?

According to one of the responding universities, *"We have a large and fragmented organisation where information flows face challenges. It can be difficult to find all the necessary people within the organisation in order to fulfil a request for erasure. In addition, nobody seems to fully know the procedure."*

Another university gave the following response: *"We have a significant number of different kinds of processes, tasks and services, and also lots of customer groups and IT systems. The person who requests for erasure does not necessarily understand how and where to make the request. It is possible that the request must be specified further. Moreover, the person making the request can simultaneously belong to multiple different categories of data subjects such as students, personnel and/or alumni. In addition, the university may have challenges in finding all the locations where the data subject's personal data have been stored. All these factors combined with the time limits may pose challenges."*

d. What are differences that you have encountered between controllers in your Member State?

While most controllers named at least one issue, there were also responding controllers who claimed not to have recognised any particular organisational problems.

Generally speaking, the controllers we contacted seemed to strive for GDPR compliance while acknowledging some room for improvement. Unfortunately, we cannot claim this applies to *all* responding controllers. See also Question 35 for more information on this.

e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

Our SA is planning to draft sector-specific guidelines for all three sectors that were selected to be approached in this CEF. The controllers in the field of higher education seem to have the biggest need for additional guidance as individual researchers and scientists are receiving requests from data subjects who are participating or who have participated in their research projects. In other words, many Art. 17 requests are not processed in a centralised manner by the DPO or the legal team, which creates the need for a more widespread awareness of data protection. A significant part of Art. 17 requests are, however, sent to the central administration of universities. There is a lot of variation depending on the situation.

One potential solution could also be that the universities and universities of applied sciences would increase their own efforts for awareness-raising among researchers, teaching staff, and students alike. Considering that the universities and universities of applied sciences have faced budget cuts in the past decade, the situation calls for cost-efficient and practical solutions.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

First a general remark on the responses in Part II about the leading or best practices; since this year's questionnaire was conducted anonymously and it was fully voluntary to respond, the answers we received were mostly very short and simple. The examples below are not groundbreaking but aim to give some light on the practical solutions the responding controllers have adopted in their operations.

- Having an internal team specifically intended for requests for erasure.
- Having guidelines with clearly defined roles, responsibilities and procedures within the organisation for handling data subjects' requests.
- Deleting data right after its retention period has passed.
- Informing the data subject after the reception of the request for erasure and again right after having fulfilled the request.
- If the DPO is not the one who handles requests for erasure, the DPO should at least monitor the procedure and adhering to the time frame.
- Evaluating and modifying the internal procedures regularly when needed, preferably at least once a year.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).

- For smaller organisations, the small number of Art. 17 requests has meant that there are no established practices for the processing of requests.
- Controllers that were contacted by our SA must adhere to statutory retention periods that often prevent the immediate fulfilment of Art. 17 requests. This is not an actual issue but may nevertheless cause dissatisfaction among data subjects.

24. Are there any leading or best practices of the controllers having responded that you would like to share?

- "If the personal data of the data subject cannot be erased due to e.g. legal or contractual obligations to store data, our organisation will make a decision and inform the data subject about it."

- "When conducting scientific research, anonymisation and/or pseudonymisation of personal data is done already during the research, not afterwards."

- "In situations concerning Art. 17(2) GDPR; if the personal data requested to be erased has been published online, we will not only delete the data from our own website but also contact Google and other search engines and request them to erase the data subject's personal data from their indexing and cache memory."

- "The applicability of Art. 17(3) GDPR is evaluated in co-operation between the DPO and the legal unit taking into account both the GDPR and domestic law. The decisions are supported with clear and concise documentation on the exemptions pursuant to Art. 17(3) and why it is necessary to retain the data vis-à-vis data subject's rights."

- "If the processing has solely been based on consent, all personal data of the data subject shall be erased after the consent has been withdrawn."

- "If the data subject objects to the processing of personal data pursuant to Art. 21 GDPR, the data shall be erased if there is no other ground for the processing than consent."

- "If there have been various grounds for processing, the withdrawal of consent will stop the processing of personal data for the purposes based on it. The controller is consequently going to evaluate if there are other grounds for the processing of the personal data for different purposes. The withdrawal of consent will be stored in the organisation's system."

- "In the event that the personal data cannot be erased due to e.g. legal or contractual obligations, our organisation will investigate if the visibility of the data can be limited."

- "Even if the request for erasure cannot be completely fulfilled, the data subject will no longer receive direct marketing and other communications from us."

- "If the request for erasure cannot be fulfilled, our organisation will evaluate the possibility to apply Art. 18 on the right to restriction of processing."

- "Regarding Art. 19 GDPR, we identify the recipient(s) [to whom the personal data has been disclosed], send them the request from the data subject and ask them to notify us when they have fulfilled the request for erasure on their part."

- "If the data subject submits a request that contains both a request for access and a request for erasure, the request for access will always be fulfilled before the fulfilment of the request for erasure."

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.

No alarming issues or challenges were identified in connection with communication with data subjects, but it must be admitted that not all responding controllers chose to answer the questions involving this theme. It is thus possible that the issues and challenges remain uncharted. For the context, there were 37 respondents to the mandatory questions of the first part of the CEF 2025 questionnaire. Here are the main findings about the communication with data subjects, i.e. the fourth part, including the answer rates:

- Over 78 per cent of the responding controllers [25 out of 32] had included the specific retention period(s) in their privacy notice. Almost as many responding controllers [24 out of 32] stated that their privacy notice provides the criteria used for determining the retention period(s).

- Over 87 per cent of the responding controllers [29 out of 33] answered that they send a confirmation of receipt to the data subject.

- Almost 68 per cent of the responding controllers [19 out of 28] answered having included information on [the expected] processing time of the request in the confirmation of receipt sent to the data subject.

- Around 94 per cent of the responding controllers [31 out of 33] receive Art. 17 requests via email.

- A little over 18 percent [6 out of 33] use a general online form.

- A little over 18 per cent [6 out of 33] use a specific online form for Art. 17 requests.

- Almost 58 per cent [19 out of 33] receive Art. 17 requests via paper mail.

- Seven responding controllers also mentioned receiving requests for erasure on the phone, at least one of them requiring verification prior to the phone call. It is not known to us if the other six organisations also require some kind of verification of identity.

26. Are there any leading or best practices of the controllers having responded that you would like to share?

- Having detailed instructions both in the privacy notice and in the customer portal for making the request.
- Also, the customer service gives advice on how to request for erasure of one's own personal data.
    - "If a data subject has notified us of wanting to request for erasure of their personal data, our organisation will send instructions via email."
- One of the universities that responded to the questionnaire mentioned that they include a description of data subject rights in their research briefing template.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers

- The vast majority of responding controllers [26 out of 30] do not comply or adhere to any technical standards when erasing personal data. The four controllers who answered yes, adhere to ISO 27001.

- There were a few responding controllers unsure of if or how their organisation erases personal data in a way that the data cannot be retrieved.

- There were also controllers that admitted having back-ups with separate retention periods.

- An interesting finding was that 19 out of 29 responding controllers answered "No" to Question 5.3 ("Does your organisation use technical tools (e.g. software) to process Art. 17 GDPR requests?"). It seems more common that the requests are processed fully manually, which probably has both its advantages, such as human oversight, and disadvantages (e.g. bigger manual effort required).
- One responding controller answered that the inter-dependency of different retention periods poses a technical challenge: "For historic reasons [that were not further elaborated], the organisation is unable to differentiate between various retention periods, which is why the customer's personal data will be erased only after the longest retention period has passed."

28. Are there any leading or best practices of the controllers having responded that you would like to share?

- 14 out of 30 responding controllers have engaged a service provider to perform the deletion of personal data. In these cases, technical support function has been either fully or partly outsourced to data processors through Data Processing Agreements. There was, however, much variation in the responses to Question 5.4.
- One of the controllers has set an end date after which a tool automatically collects the personal data of a specific data subject from all the systems of the organisation. The data are moved away from the employees' disposal to an anonymisation system from where they will be erased one month later. After this, the data cannot be retrieved anymore.
- Another controller responded that if the personal data are to be anonymised, the technique is chosen on a case-to-case basis. The anonymised data may be needed later, e.g. for reporting and statistical purposes. The anonymised data will be erased if they are not needed.
- A third controller answered that their system will automatically run an anonymisation procedure at regular intervals.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

We have published targeted guidance in Finnish and English regarding storage periods and the right to erasure for organisations involved in hobby activities of children. Our SA had a two-year project called GDPR4CHLDRN ("GDPR for Children") together with TIEKE, the Finnish Information Society Development Centre. Both language versions were published online on 8 April 2024:

In English: Is your association storing unnecessary data on its members?
Available at https://tieke.fi/en/is-your-association-storing-unnecessary-data-on-its-members/
In Finnish: Eihän yhdistyksessänne säilytetä harrastajien tietoja turhaan? https://tieke.fi/henkilotietojen-sailytys-ja-poistaminen-yhdistyksissa/

Furthermore, on 17 October 2022, our SA has published targeted guidance for SMEs on the right to erasure. This was part of a project called GDPR2DSM ("GDPR to Digital Single Market"), also in co-operation with TIEKE. The targeted guidance is only available in Finnish on the TIEKE website:

Oikeus poistaa tiedot ja tulla unohdetuksi ('Right to Erasure and to be Forgotten')
Available at https://www.tietosuojaapkyrityksille.fi/ohjesivut/oikeus-poistaa-tiedot-ja-tulla-unohdetuksi/

In addition, the FI SA website provides general guidance for both data subjects and organisations in Finnish, Swedish and English. There is no specific publication date

available, but the information is updated when necessary. The content is the same in all three language versions.

General guidance for data subjects on the right to be forgotten:
In Finnish: https://tietosuoja.fi/kun-haluat-poistaa-tietosi
In Swedish: https://tietosuoja.fi/sv/nar-du-vill-avlagsna-alla-dina-uppgifter
In English: https://tietosuoja.fi/en/if-you-would-like-to-have-all-of-your-data-erased

General guidance for organisations on the data subjects' right to be forgotten:
In Finnish: https://tietosuoja.fi/oikeus-poistaa-tiedot
In Swedish: https://tietosuoja.fi/sv/ratten-att-radera-uppgifter
In English: https://tietosuoja.fi/en/right-to-erasure

Furthermore, there are sector-specific Q&As on our website that contain information on the right to erasure; e.g. the info package on health data includes the limitations to the data subject's right to be forgotten.

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.

There have been complaint-based investigations and enforcement actions, four of which have resulted in imposing an administrative fine to the controller. However, in all those four cases there had been other kinds of shortcomings than just a failure to comply with Art. 17. In addition, there have been many cases where our SA has issued a reprimand to the controller.

Here are three short examples of Art. 17 cases our SA has had in the past few years:

Our SA concluded in its decision in Case Record No. 2956/154/18 that the complainant had the right to have their personal data such as messages erased from a popular Finnish Internet forum. An important factor in the decision-making was the fact that the complainant had been underage at the time when he had posted the messages to the message board. Recital 65 was explicitly referred to in the decision. Our SA also concluded that there was no need to take Art. 17(3) GDPR or § 27 of the Finnish Data Protection Act (1050/2018) into consideration in this particular case. (The latter is the domestic provision that contains the exception for processing carried out for journalistic purposes or the purpose of academic artistic or literary expression pursuant to Art. 85 GDPR.)

In the Case Record No. 6652/154/19, the complainant had requested for erasure of his personal data from a controller that offers recruitment services. The controller had refused to fulfil the complainant's request, as its two-year, non-statutory retention period for job applicant data had not passed. The controller had responded that they need to retain the job applicants' personal data for two years in order to be able to defend themselves against potential discrimination claims such as alleged work

discrimination (Chapter 47, § 3 of the Finnish Criminal Code). Our SA concluded in its decision that retention periods should primarily be as short as possible, and that personal data should only be processed if there are no other reasonable ways to implement the purpose of processing. Thus, our SA stated that the controller had no grounds to retain the complainant's personal data for more than two years. However, our SA also concluded that, pursuant to Articles 17(3)(b) and 17(3)(e) GDPR, the controller had a ground not to fulfil the complainant's request for erasure, as the two-year retention period from the end of the recruitment process had not passed yet.

In the bundled case with Record No. 2477/161/21, one of the five questions was if the controller had had grounds pursuant to Art.17(3) GDPR to refuse the complainants' requests for erasure.
According to the controller that was a private parking enforcement company, it had left in total 28 requests for erasure unhandled due to the lack of information from the data subjects who had made the requests.

In its response to our SA's request for clarification, the controller had stated that the data subjects' requests for erasure or limitation of processing had not been fulfilled as the controller sees its legal obligations (pursuant to e.g. the Finnish Accounting Act) and potential legal follow-up procedures to prevent the erasure of personal data. The controller had stated that it will retain the data subjects' personal data as long as it possible and proportionate. In this context, the controller had especially referred to Art. 5(1)(e) GDPR.

The controller also told in its response to our SA that the data subjects' personal data will be retained pursuant to the Finnish Accounting Act to the extent that the data involve parking fines. In this context, the controller referred to Art. 17(3)(b) GDPR and Chapter 2 § 10(2) of the Finnish Accounting Act. (The latter provision states that "unless a longer retention period is provided for elsewhere in the law, the vouchers for the financial year, correspondence regarding transactions and other accounting material than that referred to in subsection 1 must be retained for at least six years after the end of the year during which the financial year ended, in compliance with the requirements of sections 6, 7 and 9".) According to the controller's response, the nature of private parking fines consequently allows the controller to retain the photographs of vehicles taken for the purpose of parking control, and the copies of the forms containing private parking fines sent to the data subjects.

The controller stated that the data will be erased once there are no grounds based on accounting legislation to retain the data. The controller also referred to Art. 17(3)(e) GDPR and told that it may initiate legal proceedings at the Finnish district courts in order to claim the private parking fees it had issued to the data subjects in question. (The controller had already initiated thousands of similar court cases in Finland.) Referring to the Access to Court principle, the controller stated that it is not bound by other limitation periods for initiating the court proceedings than the ones based on the Finnish Act on the Limitation of Debts (728/2003).

In Cases Record No. 3609/154/18, 6175/154/18, and 8321/154/18, and 4035/182/20 (all under the bundled case Record No. 2477/161/21), our SA ordered the controller

to comply with the data subjects' requests to exercise their rights to erasure of their personal data connected with the so-called private parking fines, to the extent that the data do not include entries based on the controller's obligations to keep accounting records. If there are such entries in the accounting records, the data must be erased six years after the end of the year during which the financial year ended. Pursuant to Art. 58(2)(c), our SA ordered the controller to comply with the data subjects' requests to exercise their right to erasure in Cases Record No. 6569/182/18 and 2669/154/19. Furthermore, pursuant to Art. 58(2)(d), our SA also ordered the controller to bring its processing operations into compliance with the provisions of the GDPR.

Our SA concluded that the controller had failed to comply with Art.17(1)(a) – in addition to a few other provisions of the GDPR, as this was a bundled case. The controller was also imposed an administrative fine of EUR 75,000 by our SA. Later, the Administrative Court of Helsinki lowered the amount to EUR 70,000. The other corrective powers used by our SA in its initial decision were not subjected to changes in the judgment of the Administrative Court.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?

Unfortunately, we do not have such data at our disposal because our current case management system has all cases dealing with data subjects' rights under the same category. Separating the requests for erasure from other requests would require an enormous amount of effort and manual labour.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).

Our SA is planning to publish both general and targeted online guidance based on the findings of this CEF. The guidance will be sent via email to all the controllers that were contacted, and it will be also published on our website. As the CEF 2025 questionnaire was sent to controllers in only a few different sectors, our SA will likely draft sector-specific guidance. We do not know yet the exact date of publication of the guidance, but the drafting will begin soon after this national report has been submitted.

There will be no corrective measures towards the contacted organisations, as the questionnaire was conducted fully anonymously.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes: If "Yes", please specify: *(please select one or more answers)*

i. More online guidance: Yes, both on our website and sent to the contacted controllers via email. See also Question 32 above.
ii. Online or remote training sessions: No
iii. Conferences organised: No
iv. Others: please specify: No

b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes: EDPB Guidelines on the Right to erasure could be useful in our daily work if they were drafted in a similar style to Guidelines 01/2022 on Right of Access, i.e. with lots of practical examples. One topic that was requested in the answers we received was the correct processing and erasure of back-up data.
b. No:

35. Are there any other observations that you would like to share?

One responding controller confessed anonymously that the culture within the organisation has become such that the data protection team is not necessarily informed about requests from data subjects, as the requests are perceived as "unpleasant" and "inconvenient for the research". According to the same respondent, the higher management of the organisation acts indifferently and sees data protection as a barrier. Consequently, researchers are given oral guidance by the management to carry on with their research activities even though this guidance is not compliant with the approach approved by the data protection team. This is particularly common in the field of medical research.
Another controller responded that in their field, requests for data subjects' right are being used with malicious intent, e.g. by sending a collecting agency a large number of Art. 17 requests within a short period of time in order to cause bottlenecks so that the organisation cannot adhere to the time frames set out in the GDPR.

FR SA

Name of Supervisory Authority: Commission nationale de l'informatique et des libertés (CNIL – French SA)

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding: No
b. Fact finding + determining follow-up action based on the results: No
c. New formal investigation[23]: Yes
d. Ongoing investigation: No

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? ~~[yes / partially / no]~~
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. ~~[no / yes; if yes: free text]~~
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? ~~[no / yes; if yes: free text]~~

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
We used the same questionnaire for all controllers, that was adapted by each investigation team during the onsite investigations.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
Most of the questions were asked but, due to the type of investigation chosen (onsite investigation), each investigation team had to adapt the questionnaire to the observations made during the investigation.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?
Due to calendar constraints, the CNIL was unfortunately not able to investigate controllers from the public sector, as initially planned. These additional investigations will take place in September, and their results will therefore not be taken into account in the context of these conclusions.
Moreover, we would like to indicate that all investigations were based on complaints received by the authority.

[23] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

Part I - Information about the controllers addressed

6. How many controllers did you contact?

6

7. Out of the contacted controllers, how many controllers responded?

*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

6

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

N/A

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 0
b. Private sector: 6
c. Other: 0
d. If so, what were the other sectors? N/A

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector: 0
b. Health sector: 0
c. Social sector: 0
d. Insurance sector: 0
e. Finance sector: 0
f. IT sector: 1
g. Retail sector: 0
h. Logistics sector: 0
i. Public transportation: 0
j. Telecommunications: 1
k. Postal services: 0
l. Advertising sector: 0
m. Marketing services: 1
n. Entertainment sector: 1
o. Information / journalism sector: 0
p. Scientific / historical research: 0
q. Credit scoring agency: 0
r. Public utility/infrastructure provider (e.g. energy): 0
s. Housing industry: 0
t. Manufacturing: 0
u. Consulting: 0
v. Public administration: 0
w. Other (please specify): 1 controller in the recruitment sector / 1 controller in the trade intermediary sector

11. Please specify the category in which the responding controllers fall[24]:

a. Micro enterprise: 0
b. Small enterprise: 1
c. Medium-size enterprise: 1
d. Large enterprise (more than 250 employees): 4
e. Non-profit organisation: 0
f. Ministry: 0
g. Local authority: 0
h. Administrative authority/agency/office (e.g. job center): 0
i. School/university/educational institution: 0
j. Other (please specify): 0

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers: 0
b. Customers: 4
c. Contractors: 0
d. Job applicants: 0
e. Employees: 1
f. Applicants (for public services): 0
g. Citizens (for public sector): 0
h. Patients: 0
i. Other (please specify): 1 job seeker

12.b. According to the responding controllers, are those data subjects also:

a. Children: 1
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 1
c. Non applicable: 5

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: 0
b. 101 – 1 000: 0
c. 1 001 – 10 000: 1
d. 10 001 – 100 000: 0
e. 100 001 – 500 000: 1
f. 500 001 – 1 000 000: 0
g. 1 000 000: 4

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 5
b. Payment data: 3
c. Identification data: 3
d. Marketing data: 2

[24] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 0
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 0
g. Other, please specify: 2 (for human resources data)

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 3 years - Yes

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	[Response, e.g. 10 responding controllers]		
1 – 10			
11 – 50	1	1	1
51 – 100			
101 – 500	1		
more than 500	4	3	3

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*) N/A

	2024*	**2024-2023**	**2024-2022**
0	[Response, e.g. 10 responding controllers]		

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
2 controllers had no statistics for the years 2023 and 2022 on the day of the investigation.

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 3 years- Yes

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	**2023**	**2022**
0%	3	3	3
10%			
20%		1	1
30%			
40%			
more than 50%	2		

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?
☐ No, if so: Only one controller simply did not handle the requests received from data subjects without providing any kind of justifications.

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
1 controller had no statistics available. 1 controller only had statistics for the year 2024.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 3 years

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	3	3	3
10%			
20%			
30%			1
40%	1	1	
more than 50%			

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
1 controller found that the question was not applicable for its processes. 1 controller had no statistics on the topic on the day of the investigation.

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 1

b. Customers: 4
c. Contractors:
d. Job applicants:
e. Employees: 1
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients:
i. Other: 2 controllers answered “job seekers”

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: No

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes

Part II – Substantive issues regarding controllers’ level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High Yes
c. Average
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

The CNIL had no opportunity to investigate in the public sector. However, the French SA identified differences between bigger and smaller companies where bigger companies seems to have a more formal process to ensure the right of erasure.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?

c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

a) The biggest issue is to have a clear difference between the right to erasure and the deletion of the data subject's user account. While these two notions sometimes overlap, they are not always identical. When a client/user wants to close its account, it often results in the deletion of all the personal data.
b) Articles 5.1.c and 17 of the GDPR.
c) The main explanation is that most of the personal data processed is useful for the management of the account, as controllers try to respect the data minimisation principle expressed in Article 5.1.c of the GDPR.
d) See above – question 20
e) There is no specific solution for this issue as long as the controller identified the real intention of the data subject's request. Also, this issue is mainly due to the fact that most investigations were carried on controllers with an online service.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?
Overall, the investigations were able to highlight a will for the controllers to formalize the processing of requests to exercise the right to erasure.
During the training process of new employees, it was found useful to test the employees on fake requests to verify that the process is correctly followed.
Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).
The main issue identified is the conciliation between the obligation to comply with the right to erasure and the legal obligation to retain some personal data (such as billing documents).
Apart from this hypothesis, the investigations carried out did not reveal any other cases of mobilization of an exception to the right to erasure.

24. Are there any leading or best practices of the controllers having responded that you would like to share?
In cases where the data subject exercised its right to object to processing, the controller erased all the personal data because the retaining of this personal data was not necessary anymore.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.
We did not identify any issue on the information given to the data subjects as the privacy policies were exhaustive on the right to erasure.

26. Are there any leading or best practices of the controllers having responded that you would like to share?
For customer account deletions, implementation of the possibility for them to do it themselves when logged-in to their account.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers
The main difficulty is to achieve a full anonymisation process without any possibility of re-identification. For example, using an anonymisation process but keeping a client/user ID on tickets or bills is an obstacle to a complete anonymisation process.

28. Are there any leading or best practices of the controllers having responded that you would like to share?
We did not notice any particular leading or best practice on the topic.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

The CNIL regularly publishes guidance and content relating to the right to erasure on its website, for example :
- general considerations relating to the right to erasure: "Le droit à l'effacement" (https://www.cnil.fr/fr/falc-droit-effacement)
- a more specific publication on the issue of online data deletion (https://www.cnil.fr/fr/comprendre-mes-droits/le-droit-leffacement-supprimer-vos-donnees-en-ligne)
- a more specific publication on the issue of requests addressed to webmasters (https://www.cnil.fr/fr/webmaster-ou-responsables-de-sites-comment-repondre-aux-demandes-de-suppression-de-donnees)

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.

Since 2018, the CNIL imposed sanctions regarding the right to erasure: 1 in 2020, 3 in 2021, 2 in 2022, 2 in 2023, 6 in 2024 and 2 in 2025. Failure to comply with the right to erasure, identified in particular on the basis of complaints, is also regularly subject to corrective measures such as formal notices or reprimands.

31. Are you able to provide some information on the complaints that you have received regarding the right to erasure since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?

Since the entry into force of GDPR, the complaints received regarding the right to erasure represent approximately 8% of all admissible complaints.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).

At this stage, the investigations are still ongoing for all the controllers. These investigations might lead to corrective measures.

The timeline for a formal investigation is not predefined. It typically lasts several months.

Further investigations on the subject of the right to erasure will also begin before the end of the year, in particular in the public sector.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes:
   If "Yes", please specify: *(please select one or more answers)*
   i. More online guidance:
   ii. Online or remote training sessions:
   iii. Conferences organised:
   iv. Others: please specify:
b. No: the investigations carried out within the framework of the CEF being still in progress, the CNIL has not yet arbitrated this point.

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes: Guidelines on the right to erasure could be published by the EDPB in order to help the controllers on good practices to implement, with an emphasis on the anonymisation process, in line with upcoming anonymisation guidelines. However, we noticed that the right to erasure is mostly well understood and enforced by the controllers.
b. No:

HR SA

Name of Supervisory Authority: CROATIAN PERSONAL DATA PROTECTION AGENCY

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding:
b. Fact finding + determining follow-up action based on the results: Yes
c. New formal investigation[25]:
d. Ongoing investigation:

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? Yes
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. No
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? It is possible that there will be an increase in surveillance activities.

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.

The same questionnaire were used for all controllers.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
Not applicable.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?
No comments.

Part I - Information about the controllers addressed

6. How many controllers did you contact?
30

7. Out of the contacted controllers, how many controllers responded?

[25] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

19

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

For now we have not indicated the main reason. In the following days we will make contact with all controllers who did not provide answers.

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector:
b. Private sector: Yes
c. Other:

If so, what were the other sectors?

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector:
b. Health sector:
c. Social sector:
d. Insurance sector:
e. Finance sector:
f. IT sector:
g. Retail sector:
h. Logistics sector:
i. Public transportation:
j. Telecommunications:
k. Postal services:
l. Advertising sector:
m. Marketing services:
n. Entertainment sector:
o. Information / journalism sector:
p. Scientific / historical research:
q. Credit scoring agency:
r. Public utility/infrastructure provider (e.g. energy):
s. Housing industry: Yes, 19
t. Manufacturing:
u. Consulting:
v. Public administration:
w. Other (please specify):

11. Please specify the category in which the responding controllers fall[26]:

a. Micro enterprise: 6
b. Small enterprise: 13

[26] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

c. Medium-size enterprise:
d. Large enterprise (more than 250 employees):
e. Non-profit organisation:
f. Ministry:
g. Local authority:
h. Administrative authority/agency/office (e.g. job center):
i. School/university/educational institution:
j. Other (please specify):

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers: Yes
b. Customers: Yes
c. Contractors: Yes
d. Job applicants:
e. Employees: Yes
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients:
i. Other (please specify): Yes

12.b. According to the responding controllers, are those data subjects also:

a. Children: [Response, e.g. 4 responding controllers]
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people):
c. Non applicable: Yes

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: 6 responding controllers
b. 101 – 1 000: 8 responding controllers
c. 1 001 – 10 000: 2 responding controllers
d. 10 001 – 100 000: 2 responding controllers
e. 100 001 – 500 000:
f. 500 001 – 1 000 000:
g. 1 000 000:

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: Yes
b. Payment data: Yes
c. Identification data: Yes
d. Marketing data: Yes
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data:
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences:
g. Other, please specify:

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years - Yes

☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0			
1 – 10	1		1
11 – 50		1	
51 – 100			
101 – 500			
more than 500			

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0	16	16	16

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

1

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years- Yes

☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	2023	2022
0%	1	1	1
10%			
20%			
30%			
40%			
more than 50%			

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?

☐ Yes

☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

N/A

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

1

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years

☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	2023	2022
0%			
10%	1		1
20%		1	
30%			
40%			
more than 50%			

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

1

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: Yes
b. Customers: Yes
c. Contractors:
d. Job applicants: Yes

e. Employees: Yes
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients:
i. Other:

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: No

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes it could be.

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
c. Average
d. Low -Yes
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?
N/A

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

Regarding overall analysis we see that there is misunderstanding of more provisions of the GDPR.
For e.g. Identification and understanding of data processor and joint controllers.
This could be because the lack of education and awareness. Although, all respondents have stated that the educate and have activities of rising awareness.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?
No

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).
Not identified.

24. Are there any leading or best practices of the controllers having responded that you would like to share?
No.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.
Not identified

26. Are there any leading or best practices of the controllers having responded that you would like to share?
No

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers
Some respondents have not properly understood questions 5.1 and 5.2 so there is clear indication that there is lack of technical knowledge and understanding of data deletion.

28. Are there any leading or best practices of the controllers having responded that you would like to share?
No.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?
HR SA has developed a portal for topic of data protection under ARC2 project which also has incorporated different materials for data erasure.
The project started in September 2022.
The tools and materials can be find here: https://olivia-gdpr-arc.eu/hr

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.
No

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?
From 25 May 2018 we have received 675 complaints.
Below you can find table what was the number of complaints during the years.

Year	Number of complaints
2025	62
2024	98
2023	55
2022	74
2021	123
2020	100
2019	112
2018	51

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).
We will issue information on our website about this action.
Also, we will send invitation to all controllers to make registration and learn more about data protection on our website – Olivia.

We are considering taking more actions in way of conducting investigations for all who have not provide answers in the following months.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes:
   If "Yes", please specify: *(please select one or more answers)*
   v. More online guidance: Yes
   vi. Online or remote training sessions:
   vii. Conferences organised:
   viii. Others: please specify: online education via Olivia https://olivia-gdpr-arc.eu/hr
b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes:
b. No: Yes

35. Are there any other observations that you would like to share?
No

HU SA

Name of Supervisory Authority: National Authority for Data Protection and Freedom of Information

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding:
b. Fact finding + determining follow-up action based on the results: Yes
c. New formal investigation[27]:
d. Ongoing investigation:

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? **Yes**
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. Yes, the Hungarian SA plans to do so for a limited number of data controllers in the dedicated departments of the Hungarian SA.
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how?

h.

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
The Hungarian SA used the same questionnaire for all data controllers contacted.
4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?

Part I - Information about the controllers addressed

6. How many controllers did you contact?
13 controllers

7. Out of the contacted controllers, how many controllers responded?

[27] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

13 controllers

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?
[N/A]

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector:
b. Private sector: 13 controllers
c. Other: [
e. If so, what were the other sectors?

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector:
b. Health sector:
c. Social sector:
d. Insurance sector:
e. Finance sector: 13 controllers
f. IT sector:
g. Retail sector:
h. Logistics sector:
i. Public transportation:
j. Telecommunications:
k. Postal services:
l. Advertising sector:
m. Marketing services:
n. Entertainment sector:
o. Information / journalism sector:
p. Scientific / historical research:
q. Credit scoring agency:
r. Public utility/infrastructure provider (e.g. energy):
s. Housing industry:
t. Manufacturing:
u. Consulting:
v. Public administration:
w. Other (please specify):

11. Please specify the category in which the responding controllers fall[28]:

a. Micro enterprise:
b. Small enterprise: 1 controller
c. Medium-size enterprise: 1 controller

[28] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

d. Large enterprise (more than 250 employees): 11 controllers
e. Non-profit organisation:
f. Ministry:
g. Local authority:
h. Administrative authority/agency/office (e.g. job center):
i. School/university/educational institution:
j. Other (please specify):
   i.

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers:
b. Customers: 13 controllers
c. Contractors:
d. Job applicants:
e. Employees:
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients:
i. Other (please specify):

12.b. According to the responding controllers, are those data subjects also:

a. Children: 2 controllers
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 2 controllers
c. Non applicable: 11 controllers

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100:
b. 101 – 1 000:
c. 1 001 – 10 000: 1 controller
d. 10 001 – 100 000: 1 controller
e. 100 001 – 500 000: 4 controllers
f. 500 001 – 1 000 000: 3 controllers
g. > 1 000 000: 4 controllers

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 12 controllers
b. Payment data: 8 controllers
c. Identification data: 12 controllers
d. Marketing data: 8 controllers
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 1 controller
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences:
g. Other, please specify: 6 controllers

Most of the answers refer to personal data regarding the financial services provided to customers.

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years -Yes

☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	1 controller	2 controllers	3 controllers
1 – 10	3 controllers	3 controllers	1 controllers
11 – 50	5 controllers	4 controllers	4 controllers
51 – 100	1 controller		2 controllers
101 – 500	2 controllers	2 controllers	1 controller
more than 500	1 controller	1 controller	1 controller

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0	1 controller	1 controller	1 controller

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

1 controller

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ **3 years**- Yes

☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	2023	2022
0%	5 controllers	6 controllers	6 controllers
10%	1 controller	1 controller	1 controller
20%		1 controller	
30%	1 controller		1 controller
40%			
more than 50%	6 controllers]	4 controllers	4 controllers

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?

☐ Yes

☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

1 controller

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years - Yes

☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	2023	2022
0%	8 controllers	8 controllers	8 controllers
10%	3 controllers	1 controller	2 controllers
20%			
30%		2 controller	1 controller
40%	1 controller		
more than 50%	1 controller	1 controller	1 controller

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

1 controller

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 12 controllers
b. Customers: 11 controllers
c. Contractors:
d. Job applicants: 1 controllers
e. Employees: 3 controllers

f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients:
i. Other: 4 controllers

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): Yes / No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: Yes / No

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
In our opinion the answers are consistent with other actors in the financial sector. As expected, the two most relevant group of data subjects are the customers and the employees.

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High - Yes
c. Average
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

The banks surveyed were unanimous in reporting that because they process very large amounts of personal data in a number of IT systems, and in many cases the same personal data is processed for different purposes, on different legal bases and for different retention periods, a significant effort is required to fully comply with a request for erasure, so these challenges were reflected in their responses regardless of size, with no significant variation.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.

b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

1. One bank raised two concerns in relation to the processors' procedures. On the one hand, the bank reported its experience with some processors who charge extra fees for their cooperation in responding to data subjects' requests. Taking into account Article 12(5) GDPR, data controllers should provide this action free of charge. The bank is obviously aware that it cannot charge its own employees and costs incurred in connection with its own operations in complying with the erasure request. However, it has already been raised as a problem by the bank that the additional costs generated by the data subject's request in the processor-controller relationship should also be borne by the bank. According to the bank, it is not a solution for the data controller not to contract with these processors, as there is no real alternative to the services provided by these processors in a given case. The bank has not communicated the amount of this additional fee to the Hungarian authority, but the authority does not consider it at all likely that this amount would be significant for the bank's operations. In any case, the Hungarian authority believes that it may indeed be worth clarifying whether Article 12(5) of the GDPR should be interpreted as meaning that the processor cannot charge the controller an additional fee for cooperating with the data subject's request, or whether this only implies a cost exemption between the data subject and the controller.

2. Another problem identified by the same bank is that some processors are not in a "subordinate" role to the controller at all, as is implied by Article 28 of the GDPR. These processors determine in substance the conditions of the service they provide and do not give any leeway to data controllers to determine their role in fulfilling the data subject's requests. According to the Bank, the enforcement of the GDPR provisions would be facilitated if data processors were to have clear obligations to cooperate. Indeed, according to the Hungarian authority, the obligation of processors to do so under Article 28(3)(e) GDPR is not sufficiently defined, given the wording ("to the extent possible", "assist"). Section 1.3.5 of the EDPB's Guideline 07/2020 on the definition of controller and processor under the GDPR, which deals with the application of Article 28(3)(e) GDPR, does not contain specific obligations in this respect. The content of the obligation of cooperation on the part of the data processor may also be worth clarifying when amending Guideline 07/2020

3. Another bank also reported a specific case involving data processors. In this bank, the data processor performing most of the tasks is its parent company. If a request for erasure is received by this bank (subsidiary), the data processor (parent company) fulfils the erasure request directly, without involving the data processor. The bank did not mention any problems in this context. In the assessment of the Hungarian authority, in the case of this bank, the data processor (the parent company) has provided the controller (the subsidiary) with adequate means to comply with the data subject's request for erasure in accordance with Article 28(3)(e) of the GDPR. At the

same time, the Hungarian authority considers that it may also be useful to stipulate in Guideline 07/2020 that where parent companies provide data processing services to subsidiaries, they should not abuse their position (i.e. as parent companies they may have a material and significant influence on the subsidiary's operations) and should ensure that GDPR Article 28 is fully applied in the context of their services to the subsidiary. The Hungarian authority notes that the Guidelines 07/2020 only mention the parent-subsidiary relationship in a tangential manner, but that the Guidelines do not contain any requirement of this nature.
22. Are there any leading or best practices of the controllers having responded that you would like to share?

According to the Hungarian authority's assessment, all banks have adequate procedures and organisational measures in place to deal with requests for erasure, but it did not find any particularly good practices worth mentioning.

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).

In the context of fulfilling the obligation under Article 19 of the GDPR, respondents have no specific practice at all. For some banks, the answers were vague and general, while for others the answers consisted of a repetition - almost verbatim - of the provision in Article 19 of the GDPR. The vast majority of banks strongly stated that they comply with this obligation, but did not provide any specific details of their procedures. The Hungarian authorities consider that the banks' replies do not convincingly demonstrate that all banks comply with this obligation

24. Are there any leading or best practices of the controllers having responded that you would like to share?

1. The bank monitors the predefined retention periods through its internally developed system, and once the retention period has expired and the personal data is no longer required for the purpose for which it was originally collected, such personal data is anonymized within the live systems.

2. Another bank reported on its practice of using technical solutions such as the "least privilege" principle, irrespective of the erasure request: in the case of data retention based on a legal obligation only, the employees' access rights are "hidden" by limiting the access to these personal data for employees who do not need to know them to perform their job duties

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.

In general, banks provide information on data subjects' rights, including the right to erasure, in their privacy notices available on their websites and in their branches; all banks provide information on the duration of data processing and communicate with data subjects and receive erasure requests through several channels. One bank reported that they do not provide specific information on erasure requests, but only contact details of the bank. In their experience, any kind of description or template only adds unnecessary complexity to the procedure for data subjects: if the contact details are readily available to the data subject, he or she can formulate his or her request in the most convenient way.
According to the responses received, only a quarter of the banks contacted enabled applications via the internet banking interface, although the Authority considers that, in this case, the banks have the means to clearly identify the data subject.

26. Are there any leading or best practices of the controllers having responded that you would like to share?

In addition to the general information in the privacy notice mentioned in the previous point, it is good practice to provide information on data subjects' rights, including the right to erasure, in all information materials where the data subject is informed about the processing of his or her data, such as marketing emails or other information letters. Another bank reported on its additional information practice of informing data subjects in other bank documents or telephone calls, where consent has been given, about the possibility to withdraw consent and how to do so, as well as the possibility to object in case of processing based on legitimate interests.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers

Based on the responses received, it can be deduced that where physical erasure is possible, all personal data relating to the data subject is erased at database level, where physical erasure is not possible, customer data is anonymised. In many cases, the largest banking applications or the database structures they manage date back decades, and because the developments in data protection have been delayed, privacy by design could not be enforced. On the one hand, this has led to database structures where full erasure would remove internal references to the database, which could lead to inconsistencies, and banks have therefore in some cases used anonymisation as an alternative to deletion, especially in situations where the preservation of data structure or data image structure is justified for technical or business operational reasons.

In several cases, we received the answer that erasure from backups, from different databases, cannot be done at the same time as the erasure request is fulfilled; for example, erasure from backups would, in the view of some banks, pose a security risk, as it would violate the principle of integrity, could allow for subsequent manipulation (which could harm the security of the financial system and the interests of customers); therefore they are stored in a closed system, with appropriate encryption and are only used to restore information in the event of a disaster. They are also limited in the case of archival storage solutions (e.g. tape backups, historical databases), where technical assurance of irrecoverability cannot always be fully achieved, but access to such layers is typically limited and recovery can be subject to information security controls and is purpose-specific.

28. Are there any leading or best practices of the controllers having responded that you would like to share?

Several banks have reported that they are in compliance with all applicable data security standards or national or EU regulations that govern the secure handling and erasure of data and information security controls. The majority of the data controllers surveyed use automation or IT solutions (software) to assist in the erasure process. The solutions differ in that they are used only to perform general erasure tasks, i.e. that at the end of the required retention period, a central automated procedure for all customers concerned performs, for example, anonymisation for all related IT systems, or can be used to handle individual requests.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

Title: Resolution on the erasure of personal data and destruction of data media

Date: 20 March 2019

Link: https://www.naih.hu/adatvedelmi-allasfoglalasok/file/58-allasfoglalas-szemelyes-adatok-torlesevel-esadathordozok-megsemmisitesevel-kapcsolatban

Short description: the Hungarian authority has stated in its position that the controller must erase the personal data of the data subject in such a way that it is no longer possible to retrieve them. According to the authority, it is not sufficient to "simply format" hard disks or other computer storage media. The free software referred to by the controller in its submission (DBAN, https://dban.org/) or any other "HDD wipe" software may be appropriate for this purpose.

In addition, as regards the destruction of data media, the Authority underlined that the professional destruction of data media is carried out by several operators. To guarantee professionalism, the Authority considers it important that the company has a certificate for this activity and that at the end of the process the data controller

receives an official destruction report. This will enable the data controller to prove at any time to the authorities and to the data subjects that the data medium and the personal data stored on it have been destroyed.

In addition, the authority has also stated that the onus is on the controller to prove that the personal data have been erased. The controller should document the erasure of personal data in writing in a conclusive manner. An appropriate way to do so may be to keep a record of the erasure. The record should contain all information necessary to prove that the erasure was carried out in accordance with the law.

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.

Since May 2018, the Hungarian authority has issued hundreds of decisions on whether data controllers acted properly when they did not comply with a data subject's request for erasure. In the vast majority of these cases, the authority ruled in favour of the data subjects and censured the data controllers. The Hungarian authority highlights two of these cases as examples.

In one of the cases, the data subjects complained that the data controller had uploaded a video of them to its YouTube channel without their knowledge and had not complied with their request for erasure. The authority found that the data subjects could be considered exceptional public figures in the light of the practice of the Hungarian Constitutional Court, because they were activists in a social movement, and they have been shaping the public debate on a given issue through their statements and the events they regularly organise. According to the Authority, although the persons concerned are undisputedly exceptional public figures, the statements made on the recording cannot be considered as public debate. The Authority concluded that the mere fact that the persons concerned are exceptional public figures does not in itself constitute a basis for the public disclosure of the recording. On the one hand, because it was taken on the beach, of them as private individuals, and on the other hand, because it captures an altercation between the data subjects and the members of the data controller, which cannot be defined as a public debate. The authority found that neither the sharing of information about private life nor the dispute between the parties contributed to the contestation of public affairs, did not serve the public interest, nor did the case raise a legitimate interest. The Authority considered the controller's arguments to be unfounded and accordingly ordered it to comply with the request for erasure without delay.

In another case, the data subject applied to the controller for the deletion of his user account created on the controller's website. In response, the controller informed the data subject of the extension of the procedural deadline due to the large number of requests. The controller finally complied with the request for deletion within the time limit, but did not inform the data subject. Finally, the controller informed the data subject of the erasure, after a considerable delay, only because the data subject had

asked the controller again about the erasure. However, the information provided by the controller at that time did not cover the fact that the erasure did not result in the cessation of the processing as a whole, and that certain personal data of the data subject were retained by the controller for further processing purposes. In the case, the Authority found that the controller had extended the time limit for the exercise of the data subject's rights without good reason, as the large number of requests in the GDPR does not mean what the controller claimed - that in general the controller receives a large number of requests from data subjects whose personal data it processes - but that the data subject whose request is extended has submitted a larger number of requests to the controller. In addition, the Authority found that Article 12(3) of the GDPR requires the controller not only to take action on the basis of a data subject's request, but also to inform the data subject of the action taken. The Authority also found shortcomings in the ex post information on the erasure, as the information on the measures taken must be comprehensive; i.e. in the specific case, not only that the account has been deleted, but also the exact personal data continued to be processed by the controller on the basis of a legal obligation or legitimate interest, the purpose of such processing and the envisaged duration of the processing of the account and the data processed in relation to the account after its deletion.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?

The document management software used by the Hungarian authority does not allow us to produce such a statement, so we can answer this question by estimation.

Taking into account the statistics of the last three years, every year the Hungarian authority receives between 1600 and 1800 complaints against a specific data controller for some kind of data protection breach.

The Authority estimates that 40-45% of the complaints are related to the exercise of data subjects' rights, while 10-15% of them are complaints in which the Hungarian authority is requested to act on the grounds of a breach of the right to erasure (the Authority considers it necessary to note that a complaint may also include a breach of different provisions of the GDPR, i.e. it may not only relate to a failure by the controller to exercise the data subject's rights, but may also raise issues such as the lack of an adequate legal basis for the processing of data concerning him or her, or the inadequacy of prior information).

The Hungarian authority does not perceive any increase or decrease in the exercise of the right or the right to erasure, which can be considered as a roughly constant proportion of all submissions.

The Hungarian authority does not have a specific procedure or set of procedures for taking action against a controller for the exercise of data subjects’ rights.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).

In accordance with its task under Article 57(1)(b) and (d) of the GDPR, the Hungarian authority will inform all the banks contacted of the report resulting from the CEF. The Hungarian authority will also publish an abbreviated notice containing the main findings and a link to the report on its website. The Hungarian authority plans to inform the banks within a month of the adoption of the report and to publish the Communication on its website.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes:
   If "Yes", please specify: *(please select one or more answers)*
   a. More online guidance:
   b. Online or remote training sessions:
   c. Conferences organised:
   d. Others: please specify:
b. **No.** The Hungarian authority does not yet plan to publish further guidance, organise a conference or training on this issue beyond the publication of the CEF report.

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. **Yes:** Based on the responses received from the banks contacted, the Hungarian authority considers that, in accordance with the EDPB's task under Article 70(1)(e) of the GDPR, the following may arise:

1. Clarify in Guideline 07/2020 the application of Article 28(3)(e) of the GDPR as to what kind of cooperation obligation is expected from the processor; and to set out the expectation in the case where the parent company provides a data processing service to the subsidiary.

2. If other Member States or the EDPB were to raise the possibility that it might be appropriate to issue guidelines on deletion, we consider that clarification is needed in the case of these guidelines, inter alia, on the following:
   i. Is Article 12(5) of the GDPR to be interpreted as meaning that the processor may not charge the controller any additional fee for cooperating with the data subject's request?
   ii. whether anonymisation can be considered equivalent to erasure, taking into account the IT

aspects (specific database structure, data image structure),

iii. in the case of tape or similar backups, what is expected of data controllers with regard to the execution of erasure requests.

b. No:

35. Are there any other observations that you would like to share?
There are no further comments from the Hungarian authority.

IE SA

Name of Supervisory Authority: Data Protection Commission Ireland

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding: [Yes]
b. Fact finding + determining follow-up action based on the results:
c. New formal investigation[29]:
d. Ongoing investigation:

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? [Yes]
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. [NO]
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? [NO]

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.

Yes All questionnaires issued to controllers were the same version.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.

Not applicable

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?

No

Part I - Information about the controllers addressed

6. How many controllers did you contact?

40

[29] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

7. Out of the contacted controllers, how many controllers responded?

*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

28

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

We engaged with all controllers in attempt to elicit the maximum number of responses. A number of controllers advised that they did not have the resources available to complete the Questionnaire. A small number of controllers declined to participate without giving any rationale.

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 7
b. Private sector: 21
c. Other: Not applicable
    f. If so, what were the other sectors? Not applicable

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector: 2
b. Health sector: 2
c. Social sector: 1
d. Insurance sector: 3
e. Finance sector: 3
f. IT sector: 5
g. Retail sector: 2
h. Logistics sector: 0
i. Public transportation: 1
j. Telecommunications: 2
k. Postal services: 0
l. Advertising sector: 0
m. Marketing services: 0
n. Entertainment sector: 1
o. Information / journalism sector: 1
p. Scientific / historical research: 0
q. Credit scoring agency: 0
r. Public utility/infrastructure provider (e.g. energy): 1
s. Housing industry: 0
t. Manufacturing: 0
u. Consulting: 0
v. Public administration: 1
w. Other (please specify): 3; Commercial Aviation (1), Technology (1), Transportation (1)

11. Please specify the category in which the responding controllers fall[30]:

a. Micro enterprise: 1
b. Small enterprise: 1
c. Medium-size enterprise: 3
d. Large enterprise (more than 250 employees): 14
e. Non-profit organisation: 3
f. Ministry: 0
g. Local authority: 2
h. Administrative authority/agency/office (e.g. job center): 2
i. School/university/educational institution: 1
j. Other (please specify): 1; Hospital

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers: 0
b. Customers: 19
c. Contractors: 0
d. Job applicants: 0
e. Employees: 0
f. Applicants (for public services): 1
g. Citizens (for public sector): 3
h. Patients: 2
i. Other (please specify): 3; Students (1), Users (2)

12.b. According to the responding controllers, are those data subjects also:

a. Children: 17
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 15
c. Non applicable: 10

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

d. < 100: 2
e. 101 – 1 000: 0
f. 1 001 – 10 000: 0
g. 10 001 – 100 000: 4
h. 100 001 – 500 000: 3
i. 500 001 – 1 000 000: 2
j. > 1 000 000: 16

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 24
b. Payment data: 16
c. Identification data: 18
d. Marketing data: 7

[30] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 8
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 4
g. Other, please specify: 6

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years -Yes

☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	2	4	5
1 – 10	7	4	4
11 – 50	6	7	6
51 – 100	1	2	2
101 – 500	2	2	3
more than 500	10	9	7

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0	2	6	11

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

All of the responding controllers provided a response to this question. However, one controller did not provide a response in respect of 2022.

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years- Yes

☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	**2023**	**2022**
0%	6	5	6
10%	7	8	7
20%	1	1	0
30%	0	0	0
40%	1	1	1
more than 50%	10	8	7

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?

☐ Yes

☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

Not applicable

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

One controller did not respond at all to this question. In addition, we note that one controller did not provide a response in respect of 2022.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

Yes 3 years

☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	16	13	14
10%	4	5	2
20%			
30%			
40%			
more than 50%	5	5	5

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

One controller did not respond at all to this question. In addition, we note that one controller did not provide a response in respect of 2022.

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 8
b. Customers: 19
c. Contractors: 4
d. Job applicants: 12
e. Employees: 6
f. Applicants (for public services): 2
g. Citizens (for public sector): 3
h. Patients: 2
i. Other: 6

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: No

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes, we found the results to be largely consistent across sectors and processing activities

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High - Yes
c. Average
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

Specific differences are described in further detail below in our response to questions 21 through 28. Overall, we observed a wide variation in the responses provided by data controllers. This varied according to the size of the data controller, the type of data processed, the sector within which the data controller operates, and the number of erasure requests received. However, we found the practices within the sectors to be largely consistent.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

We found that the respondents answered this section's questions quite well overall. We note there is no specific requirement obliging data controllers to adopt a particular procedure or pre-defined process for handling erasure requests, provided that they can comply with the time limits and produce a response compliant with the other requirements necessitated by data protection law.
We found that a large majority of responding controllers have some level of process in place for responding to right to erasure requests. The complexity of the procedures in place largely depend on the nature and size of the organisation, the complexity of the data processed, and the volume of erasure requests received. However, we found that many of the controllers had basic processes, as well as plans to acknowledge and track the requests received. In addition, the majority of controllers provided some level of training to staff who may receive or process requests for erasure. The frequency and specificity of training varied according to the volume of erasure requests and the size and complexity of the organisations.
A minority of responding controllers reported issues with responding to or taking action on erasure requests within one month as required by Article 12(3) GDPR. These issues were often linked to additional roadblocks in determining how to respond, such as needing to clarify requests with the data subject to determine what data is subject to the request, needing to consult with the creator of the data at issue, or with employees within the organisation responsible for maintaining the data record. The need to consult with multiple stakeholders and gather additional information appears to create a greater potential for delayed action in response to an erasure request.
A small minority of controllers responded to questions 2.1 through 2.9 by indicating that they never deny a request for erasure.
Many of the issues identified in our review could be addressed through the use of simple tools, especially in the case of small to medium size controllers. These could include the use of specific templates for the submission of erasure requests and more specific procedures for processing erasure requests. These tools might help decrease response time for those controllers struggling to respond within one month. Additional guidance for data controllers on processing these requests would also be of use.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

We note that one of the best practices observed, regardless of the size of the data controller, was the use of a web form or other template available online to data subjects to submit a request for erasure. These forms need not be complex. In addition, a template allows both the data subject and data controller to more quickly identify the data that is the subject of the request.
Regular training together with procedures acknowledging, logging and tracking requests for erasure were also noted to be part of many successful programs to handling requests made pursuant to Article 17.

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).

As with questions 2.1 to 2.9, we found that the respondents answered this section's questions quite well overall. We observed a wide disparity in the types of scenarios encountered by the respondents depending on their size as well as the type and purpose of the data undergoing processing.
Despite the disparities between controllers, we observed several common themes among the responses submitted. Many of the data controllers, for example, reported using some level of case-by-case analysis when determining whether personal data, subject to the erasure request, is no longer necessary to be retained. Further, most of the controllers surveyed reported employing retention schedules or policies to aid in determining when it is appropriate for the personal data to be deleted. A few of the data controllers reported a more detailed procedure for determining whether continued processing of the data remained necessary.
Of some concern were the data controllers who reported not having any processes in place, or reported the need to consult with various stakeholders, before making any determination. The lack of processes could lead to potential delays in responding to a request and shows potential non-compliance with Article 24(2).
We observed that very few of the data controllers rely on consent for their legal basis for processing personal data. The majority of controllers who do rely on consent for processing personal data responded that they make tools, such as online requests or in-application controls, available for data subjects to withdraw consent, allowing automatic removal of the data.
Only a portion of the responding controllers make personal data public. Those that do make data public indicated specific procedures in place for notifying data recipients when taking action on a request for erasure.
All of the controllers reported the intent to adhere to the requirements of Article 17(3) when determining whether an exception to the right to be forgotten applies. We did however note a concern among controllers who frequently rely on the restriction related to the "*right of freedom of expression and information*", as transposed into Irish law under section 43 of the Data Protection Act 2018, to refuse erasure requests. Although the majority of controllers who reported relying on this basis articulated

specific balancing tests that they undertake based on legal precedent, a response from a data controller potentially indicated a balancing test that may overweight freedom of expression over the rights and freedoms of the data subject. This raises a concern that some erasure requests may be denied inappropriately.
Several of the responding data controllers reported that one of their most commonly applied exceptions when refusing a request for erasure is compliance with a legal obligation. While in some instances the provisions of law that support these refusals is clearly established and supported by judicial decisions, in some cases the data controllers rely on their institutional understanding of the application of the particular act or regulation that forms the basis of their refusal. There is a potential that the lack of correct interpretation of the legal obligation may lead to inappropriate denials of requests for erasure.
As above, we are of the view that additional sector-specific guidance and/or consultation may be of use in ensuring data controllers are responding appropriately to requests for erasure.

24. Are there any leading or best practices of the controllers having responded that you would like to share?

Regardless of controller size or function, one of the leading practices we observed was the use of clearly defined retention policies. One responding controller explained that they employ a "data deletion matrix" that cross-indexes the type of data being processed, the associated legal basis, and the retention period. We note that the employment of clearly defined schedules can act as a significant aid to the individuals within an organisation tasked with responding to erasure requests.

Among the larger controllers handling a larger volume of requests, we observed that some of the best outcomes were associated with the use of designated teams to respond to erasure requests. The teams tasked with these responses usually receive additional specified training as well as becoming more familiar with legal requirements and the use of balancing tests where required.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.

In the responses to question 4.1 to 4.5.1 we observed that controllers have adopted various means of communicating with data subjects in regards to the right to be forgotten. Again, we note that there is no specific requirement obliging data controllers to provide data subjects with a specific procedure and/or instructions for exercising the right to be forgotten.
We observed that most of the responding controllers included some level of instruction to individuals as part of their privacy notice. The type of instruction and degree of guidance varied between controllers, with some controllers offering multiple means for data subjects to understand their rights and the procedures for requesting erasure. For example, controllers identified instructions available in the privacy notice itself, links to online FAQs, help centres, website explainers, and how-to videos.

The large majority of responding controllers provide data subjects with acknowledgement when a request for erasure is received and most controllers provide an estimate for processing time when a request is received. In addition, the majority of controllers provide data subjects with multiple channels to exercise their rights, including online, via templates, through email, or by post.
One notable issue we observed is that not all controllers identify specific retention policies in their privacy notices. While not required, the lack of either specified retention periods or a delineation of the criteria used to determine the applicable retention period may contribute to confusion on the part of data subjects regarding their ability to exercise their right to erasure.

26. Are there any leading or best practices of the controllers having responded that you would like to share?
Some of the leading practice we observed including providing data subjects with more than one form of guidance or instruction in how to exercise the right to be forgotten. The use of both the privacy notice in conjunction with FAQs and/or explainers, how-to-videos, help centres, web forms, and templates, makes it easier for the individual to submit a request for erasure. While we recognise that some of these tools would be not be feasible for smaller controllers to implement, we believe that the use of more specific instructions or FAQs would be of utility to the majority of controllers.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers
In the responses we received to Questions 5.1 to 5.6.1 we observed that approximately half of all responding controllers indicated that they utilise software or technical tools to process erasure requests. Of that number, approximately half use their own or external information technology service providers to implement that software. Similarly, approximately half reported adhering to technical standards or ISO certification. Only a minority of responding controllers reported utilising anonymisation or overwriting in lieu of erasing data.
The use of technical tools and reliance on service providers and/or IT departments raises a potential concern regarding the security of data processing in relation to the erasure and anonymisation of personal data, especially when the controller does not separately adhere to ISO or comparable standards. While the use of software or similar tools can expedite the processing of erasure request, it is important that the security of the personal data is maintained by all the parties involved in this process. Data controllers must ensure that appropriate technical and organizational measures are place to ensure data security is maintained.

The use of anonymisation by data controllers also presents a potential concern. As above, data controllers who rely on anonymisation should ensure that the anonymisation is effective and that once anonymised the data can no longer be re-associated with the individual data subject.

28. Are there any leading or best practices of the controllers having responded that you would like to share?

As noted above, it is essential that technical and organisational measures are in place to ensure the security of personal data. We note that the best practices in this regard include ensuring that any service providers adhere to the privacy policies and programs of the data controller on whose behalf they are acting.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

Can I Use the GDPR to have my medical records amended or erased? | Data Protection Commissioner. This is an FAQ published to the DPC's website with the intended audience of data subjects.

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.

The DPC has led various complaint based examinations, with most being amicably resolved with the data controller either agreeing to delete further personal data or upon detailed explanation for the retaining of personal data issuing to the individual the individual is satisfied with same. No enforcement action has been taken to date, though the DPC is considering same in relation to a number of complaints. The DPC's own-volition inquiry into MTCH Technology Services Limited (Tinder) is still ongoing.

The DPC handles numerous queries from data controllers, for example, in November 2024, the DPC received a query from a motor trade entity about requirements for deleting personal data. A response was issued, detailing Article 17 and data retention responsibilities.

The DPC has engaged informally with the health research community through the national Health Research Data Protection Network on the applicability of Article 17(3)(d) (where the right does not apply or purposes of scientific research where erasure renders the processing impossible or significantly impacts the achievement of processing objectives). A brief presentation was given at a Network meeting about the need to make an assessment when rejecting an erasure request on the grounds of Article 17(3)(d).

The DPC has regular engagements with data controllers responsible for the management of web browsers regarding specific individual delisting requests.

Otherwise, the DPC has had no other informal engagement of note with data controllers on Article 17. In comparison to the right of access, the right to erasure receives very few complaints or queries from controllers.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?

Over 3000 complaints related to Article 17 requests have been received since the GDPR's conception. The DPC notes a slight upward trend of complaints being received.

Each examination of a complaint related to the right to erasure is unique. As a result, it is not possible to quantify exactly how long the examination of any individual complaint will take. Some complaints, particularly those which are of a multi-faceted nature (i.e., a number of matters must be examined where multiple data protection related matters are raised, for example, a right to access request is accompanied by an alleged disclosure complaint alongside an erasure request), require in-depth examination and careful consideration of legal issues prior to conclusion.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).

The DPC has and will continue to engage informally with controllers regarding their responsibilities under Article 17. We will continue to work with controllers regarding policies and practices that ensure data subjects can exercise their right to be forgotten.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes:
   If "Yes", please specify: *(please select one or more answers)*
   a. More online guidance:
   b. Online or remote training sessions:
   c. Conferences organised: Yes—the DPC will continue to work with the network of data protection officers within its remit
   d. Others: please specify:
b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes: We would propose that the EDPB develop additional in-depth guidance on the right to erasure. We would propose that the guidance includes sector-specific sections and offer examples of best practices for data controllers.
b. No:

35. Are there any other observations that you would like to share?

IT SA

Name of Supervisory Authority: Garante per la protezione dei dati personali

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding: Yes
b. Fact finding + determining follow-up action based on the results:
c. New formal investigation[31]:
d. Ongoing investigation:

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? Yes
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. No
- **2.c**. If not, will this fact-finding activity impact your enforcement activities, and if so, how? No

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
The same questionnaire was used for all data controllers.
4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
Questions 2.1.a.1, 5.2, 5.3, 5.3.a, 5.4.a, 5.6 and 5.6.a were not included in the questionnaire.
Changes were made to the wording of the following questions:

- Question 2.1.a: the reference to uploading any attachments was removed.
- Question 5.5. a: the reference to the technical description of the technical methods of anonymisation was removed.

It should also be noted that, with regard to questions 1.8, 1.9 and 1.10, only the year 2024 was taken into consideration, with answers for previous years to be included only if no requests for erasure were received in 2024.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?
No

[31] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

Part I - Information about the controllers addressed

6. How many controllers did you contact?

42

7. Out of the contacted controllers, how many controllers responded?

*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

39

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

No

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 2
b. Private sector: 32
c. Other: 5
    g. If so, what were the other sectors? Private entities accredited with the Regional Health System which, as such, qualify as a public service provider.

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector:
b. Health sector: 7
c. Social sector:
d. Insurance sector: 10
e. Finance sector:
f. IT sector:
g. Retail sector: 1
h. Logistics sector:
i. Public transportation:
j. Telecommunications: 2
k. Postal services:
l. Advertising sector:
m. Marketing services:
n. Entertainment sector:
o. Information / journalism sector: 8
p. Scientific / historical research: 2
q. Credit scoring agency:
r. Public utility/infrastructure provider (e.g. energy): 5
s. Housing industry:
t. Manufacturing:
u. Consulting:
v. Public administration: 1
w. Other (please specify): 3

11. Please specify the category in which the responding controllers fall[32]:

a. Micro enterprise: 1
b. Small enterprise: 4
c. Medium-size enterprise: 8
d. Large enterprise (more than 250 employees): 22
e. Non-profit organisation: 1
f. Ministry:
g. Local authority:
h. Administrative authority/agency/office (e.g. job center): 1
i. School/university/educational institution:
j. Other (please specify): 2 public research entities

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers: 1
b. Customers: 20
c. Contractors: 1
d. Job applicants:
e. Employees:
f. Applicants (for public services): 2
g. Citizens (for public sector): 2
h. Patients: 7
i. Other (please specify): 6 data subjects mentioned in newspaper articles

12.b. According to the responding controllers, are those data subjects also:

a. Children: 3
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 6 data subjects mentioned in newspaper articles
c. Non applicable: 3

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: 1
b. 101 – 1 000:
c. 1 001 – 10 000: 2
d. 10 001 – 100 000: 3
e. 100 001 – 500 000: 6
f. 500 001 – 1 000 000: 3
g. > 1 000 000: 24

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 35
b. Payment data: 27
c. Identification data: 37

[32] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

d. Marketing data: 23
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 19
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 6
g. Other, please specify: 3

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☒ 1 year-Yes
☐ 3 years
☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	4	3	3
1 – 10	5	1	
11 – 50	8		
51 – 100	3		
101 – 500	10		
more than 500	9		

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0	4	3	3

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
0

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☒ 1 year- Yes
☐ 3 years

☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	**2023**	**2022**
0%	19		
10%	7		
20%	1		
30%			
40%	1		
more than 50%	11		

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?

☐ Yes

☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

0

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☒ 1 year - Yes

☐ 3 years

☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	18		
10%	12		
20%	1		
30%			
40%			
more than 50%	8		

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

0

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 16
b. Customers: 8
c. Contractors:
d. Job applicants:
e. Employees:
f. Applicants (for public services): 1
g. Citizens (for public sector): 3
h. Patients: 3
i. Other: 9

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: No

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
☒ Average - Yes
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?
The questionnaires revealed that, in general, controllers of larger sizes tend to receive a higher number of requests and therefore seem to be better structured in terms of internal procedures and measures, including technical ones, for responding to requests from data subjects.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.

i. Staff training: most data controllers reported that they carry out training initiatives for in-house staff at least once a year. However, there were some cases (about 20% of respondents) where training appeared to be mainly limited to the recruitment phase, with no subsequent regular initiatives to ensure continuous training. When subsquent training activities are provided, they are only occasional and not regularly scheduled, as they are linked to specific circumstances (e.g. change of role or duties, occurrence of special events, explicit request from an organisational unit).

ii. Monitoring/control of request management: the monitoring and systemic control of request management appeared to be poorly structured for some data controllers, also on account of the highly vague description given of the activity. In some cases, the description only referred to the monitoring of the channels through which requests were received, without mentioning any further control activities—implemented *in itinere* and/or *ex post*—on the correct management of the requests.

b. Which provision(s) of the GDPR (or national laws) does this concern?

i. Articles 24, 29 and 32 of the GDPR;

ii. Articles 24 and 32 GDPR;

c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?

i. The majority of cases in which training was mainly limited to the recruitment phase concerned data controllers classified as “large undertakings” with more than 250 employees. This may be due to greater difficulty in structuring a continuous training process within larger organisations with a higher level of internal complexity;

ii. Although having internal instructions/guidelines/recommendations on the management of requests, data controllers may not have implemented specific tools that allow for effective control over the correct handling of requests received.

d. What are differences that you have encountered between controllers in your Member State?

i. Except for the cases described above, no significant differences were identified between the data controllers who responded to the questionnaire, as a fairly uniform situation emerged, with training activities carried out on an annual basis;

ii. Based on the descriptions provided, three distinct solutions appear to be adopted by the respondents for monitoring and controlling the management of requests for erasure, which may be adopted alternatively depending on the specific data controller, namely: the use of registers; periodic reporting to senior management and/or the Data Protection Officer; and the performance of audits.

e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?
   i. Data controllers could design specific internal training plans, scheduling sessions on a regular and pre-established basis, thus ensuring continuous staff training and updating;
   ii. Data controllers could adopt technological and/or organisational solutions - including through the combined use of multiple tools - to ensure effective monitoring and control of the processing of requests (e.g. dedicated registers, audits, periodic reporting).

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

i. In addition to "basic" training on personal data protection and the exercise of the right referred to in Article 17 of the GDPR, some data controllers have provided specialist training sessions, tailored to the specific context/scope in which the controller's organisation or its individual organisational units operate
ii. Some data controllers report that they adopt technological tools that allow, on the one hand, for comprehensive and continuous monitoring throughout the entire request management phase (from receipt to fulfilment, including the implementation of specific alerts regarding the deadlines to be met) and, on the other hand, to produce statistics and reports for *ex post* checks on the activities carried out

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).

a) The issues identified, based on the responses provided, concern the following aspects:
- some data controllers were found to lack transparency towards users with regard to their policy on the erasure of processed data, with reference to the purposes (question 3.1);
- some data controllers do not explain what procedures they activate in the event of a request to object to processing; other data controllers did not provide explanations on the procedures for handling requests to object to processing, merely stating that they had never dealt with such cases; other data controllers who process data on the basis of consent and other legal grounds did not specify the cases and related procedures for handling cases of request to object and withdrawal of consent (question 3.3);

- some data controllers showed a lack of transparency in explaining the cases referred to in Article 17(2) (question 3.5);
- some data controllers, in relation to Article 19, responded by making reference to data subjects rather than recipients (question 3.10);

b) The relevant provisions linked to the above-mentioned issues are: Article 17(1)(a) (3.1); Article 17(1)(c) and Article 21(1) and (2) (3.3); Article 17(2) (3.5); Article 19 (3.10);
c) possible explanations for the issues outlined above, which mainly concern the lack of transparency and the poor level of detail in the description of procedures by some controllers, both in relation to data subjects (on erasure policies and procedures) and in relation to the Authority in responding to the questionnaire, are considered to be found in the size of the organisational structure of the controllers, as large organisations have more sophisticated internal processes and higher number of resources to be deployed for this type of activity and, for these reasons, are able to ensure compliance with the legislation and greater transparency,

d) as to the differences observed between data controllers, relating to the abovementioned issues, particularly concerning transparency and lack of accuracy, these can be attributed to the reasons set out in the previous point, relating, therefore, to the different sizes of the various organisational structures;

e) taking into account the critical issues identified, we believe that a valid solution could be to raise awareness among data controllers of the adoption of Codes of conduct, pursuant to Article 40 of the GDPR, in particular in order to identify procedures for the optimal management of requests for erasure in accordance with Article 17 of the Regulation, also considering the different nature of the subjects involved.

24. Are there any leading or best practices of the controllers having responded that you would like to share?
The best practices identified concern the effective setting up and description of erasure procedures. In particular:

- in relation to the provision of Article 17(1)(a) of the Regulation, some controllers catalogue personal data on the basis of predefined categories identified taking into account the purposes, and constantly update this practice; others provide for automatic batch erasure at the end of the specified period (question 3.1);
- in relation to the provision of Article 17(1)(b) of the Regulation, some controllers predetermine the cases of withdrawal of consent and the consequent obligations; others, in cases where processing is based on consent, use automated systems to withdraw consent, so as to change consent from “Yes” to “NO” and stop data processing (question 3.2);

- some controllers have described in detail the procedure for handling simultaneous requests for access and erasure, demonstrating particular care and sound criteria for managing the procedures (question 3.11).

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.

(a) The responses provided reveal three relevant issues that controllers face when handling requests for erasure received pursuant to Article 17 of the Regulation, whose common denominator is a lack of transparency towards data subjects. This concerns, in particular:

i. the absence, in some cases, of specific information for data subjects on how to exercise their rights under Articles 15-22 of the Regulation, including the right to erasure. This is because, in a few limited cases, it was revealed that: a) the aforementioned information is available on the controller's website, in the "Legal Information" section, rather than in the privacy section; b) the aforementioned information is provided in case unclear requests to exercise rights are received, or in case of a request from a person other than the data subject who is not entitled to represent them; c) data subjects are in any case assisted in the management of requests submitted, even informally, regarding the exercise of their rights; d) one data controller has stated that it does not provide details of the aforementioned information.

ii. the lack of indication, albeit in very limited cases, of the retention period of the personal data collected and/or the criteria for determining the aforementioned period in the information notice provided to data subjects. In fact, it is noted that almost all data controllers inform data subjects of the retention periods by indicating either the retention period alone, the criteria for determining that period alone, or both.

iii. the information provided to the data subject regarding the actual processing of the request for erasure sent by the data subject to the data controller and, in particular, the time frame for processing the aforementioned request. The responses provided show that most data controllers do not send confirmation of receipt of the request made by the data subject. Among the data controllers who do send such confirmation, only some also provide the data subject with an indication of the time frame for responding to the request for erasure.

It should also be noted that one controller indicated in the questionnaire that the erasure of data can also be carried out directly by the data subject by deleting their account; however, they did not specify whether this action results in the mere deactivation of the account or also in the actual erasure of all personal data.

(b) With regard to the issues identified, the relevant provisions are those concerning the principle of transparency, referred to in Article 5(1)(a) of the Regulation, as well as Article 12 of the Regulation. With regard to the first issue, the provisions of Article 13(2)(b) of the Regulation must also be taken into account, while as regards the second issue, Article 13(2)(a) of the Regulation must be referred to.

In general, the requirements also concern the broader principle of accountability laid down in Articles 5(2) and 24 of the Regulation.

(c) The possible explanations for the problems experienced, concerning the lack of transparency of the information provided to data subjects, are considered to be linked to the size and type of controller.

(d) Concerning the issues identified, no significant differences were found between the controllers who responded to the questionnaire.

(e) Promote actions aimed at raising awareness of how to handle requests for erasure pursuant to Article 17 of the Regulation, and of the close correlation with the observance of the principle of transparency towards data subjects, which must be respected at all stages of the handling of such requests, in order to make the data subject fully aware of their rights under the Regulation. To this end, targeted awareness-raising among controllers is also recommended, in relation to the type of controller, also with regard to the Guidelines on transparency.

j.

26. Are there any leading or best practices of the controllers having responded that you would like to share?

Among the best practices identified, it should be noted that some controllers stated that they provided data subjects with an online form to facilitate the submission of requests for erasure pursuant to Article 17 of the Regulation. Most controllers also indicated that the information provided to data subjects, with reference to the data retention period, specifies both the actual period and the criteria for determining it.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers

In a small number of cases, data controllers stated that they comply with certain technical standards and use a provider for data erasure-related processes. Approximately 50% of the controllers involved stated that they use anonymisation techniques. This choice is mainly driven by technical requirements and the need to preserve the integrity of CRMs. The measures adopted for anonymisation are varied, but in all cases aim to ensure the irreversibility of the process.

In this regard, it should be noted that the measures implemented have been described in a very generic manner and are based on the concept of anonymisation itself. Furthermore, in many cases, anonymisation does not appear to be a choice made within the scope of the controller's accountability, but rather a necessity due to the technical specificities of the applications in use.

Numerous controllers have expressed difficulties in implementing the right to erasure, mainly related to:

- the spreading of AI technologies;
- compliance with legal deadlines, especially when a large platform needs to be involved in order to accept the request;
- the procedure for identifying the data subject;
- the interpretation of the content of the request;
- balancing the right to be forgotten with other rights protected by law and with the retention obligations imposed on data controllers by sector regulations;
- the traceability of requests, which often come from various channels;

- difficulties mainly due to technical reasons.

28. Are there any leading or best practices of the controllers having responded that you would like to share?
Some controllers have expressed their intention to develop new tools to facilitate the management of requests to exercise rights (e.g. through specific features available on company websites or in apps). Others have stated that they have developed response templates for data subjects, structured according to the most frequent types of requests and specific procedures to ensure that requests are promptly directed to the relevant department. Many subjects involved have called for the issuance of guidelines or best practices regarding the implementation of Article 17 of the GDPR and the exceptions provided for therein, as well as the development of technological solutions for the management of erasure requests using AI.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?
If yes, please provide the date, link to the guidance, and a short description of the guidance.
On the Garante's website, there are information sheets on the data subjects' rights, which can be found at the following link: https://www.garanteprivacy.it/i-miei-diritti/diritti/oblio.

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.
No general activities have concerned the right to erasure. However, multiple fact-finding activities have been launched on individual cases and clarifications have been sent to data subjects who have contacted the Garante or reported possible violations.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?
There have been numerous requests for data erasure, mainly relating to certain sectors (e.g. marketing). Sometimes these requests mainly concern the exercise of the right to be forgotten, while in other cases the erasure is associated with additional requests made by the data subject, such as those relating the right to object.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).
No activities specifically aimed at respondents to the questionnaire.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes: Yes
   If "Yes", please specify: *(please select one or more answers)*
   a. More online guidance:
   b. Online or remote training sessions:
   c. Conferences organised:
   d. Others: please specify: some initiatives are being evaluated, also in light of the changes introduced by new technologies and which affect, among other things, the issue of erasure.
b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes: the development of guidelines on erasure which, not limited to de-indexing and right to be forgotten, cover all the cases referred to in Article 17 of the GDPR.
b. No:

35. Are there any other observations that you would like to share?
No

LI SA

Name of Supervisory Authority: Data Protection Authority of the Principality of Liechtenstein

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding:
b. Fact finding + determining follow-up action based on the results: Yes
c. New formal investigation[33]:
d. Ongoing investigation:

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? Yes
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. No
- **2.c**. If not, will this fact-finding activity impact your enforcement activities and if yes, how?

Based on the findings and results of the survey, the LI SA will, as part of its advisory activities, draw the attention of the controllers to the inadequate or missing processes and/or implementation of the relevant provisions of the GDPR. In addition, as in previous years, the LI SA will address the main issues identified at the next annual meeting of DPOs in Liechtenstein on 10th November 2025. This event provides a valuable opportunity to raise awareness and present practical findings to organisations and their DPOs. Although no enforcement actions are currently planned, the results of the survey will contribute to shaping future measures aimed at improving compliance in this area.

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.

We used the same questionnaire for all controllers.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.

Not applicable

[33] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?

No

Part I - Information about the controllers addressed

6. How many controllers did you contact?

5

7. Out of the contacted controllers, how many controllers responded?

*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

5

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

Not applicable

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 2 responding controllers
b. Private sector: 3 responding controllers
c. Other:

If so, what were the other sectors?

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector:
b. Health sector: 1 responding controller
c. Social sector:
d. Insurance sector: 1 responding controller
e. Finance sector: 1 responding controller
f. IT sector:
g. Retail sector:
h. Logistics sector:
i. Public transportation:
j. Telecommunications:
k. Postal services:
l. Advertising sector:
m. Marketing services:
n. Entertainment sector:
o. Information / journalism sector:
p. Scientific / historical research:
q. Credit scoring agency:

r. Public utility/infrastructure provider (e.g. energy): 1 responding controller
s. Housing industry:
t. Manufacturing: 1 responding controller
u. Consulting:
v. Public administration:
w. Other (please specify):

11. Please specify the category in which the responding controllers fall[34]:

a. Micro enterprise:
b. Small enterprise: *1* responding controller
c. Medium-size enterprise: 1 responding controller
d. Large enterprise (more than 250 employees): 3 responding controllers
e. Non-profit organisation:
f. Ministry:
g. Local authority:
h. Administrative authority/agency/office (e.g. job center):
i. School/university/educational institution:
j. Other (please specify):

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers:
b. Customers: 3 responding controllers
c. Contractors:
d. Job applicants:
e. Employees: 1 responding controller
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients: 1 responding controller
i. Other (please specify):

12.b. According to the responding controllers, are those data subjects also:

a. Children: 3 responding controllers
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 5 responding controllers
c. Non applicable:

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: 1 responding controller
b. 101 – 1 000:
c. 1 001 – 10 000:
d. 10 001 – 100 000: 2 responding controllers
e. 100 001 – 500 000: 2 responding controllers
f. 500 001 – 1 000 000:
g. > 1 000 000:

[34] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 5 responding controllers
b. Payment data: 4 responding controllers
c. Identification data: 3 responding controllers
d. Marketing data: 2 responding controllers
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 3 responding controllers
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 3 responding controllers
g. Other, please specify: 2 responding controllers

One controller specified that the processing activities include medical records and related documentation, while another controller referred to energy consumption data.

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year
☐ 3 years
☒ other, specify:

Figures were requested for up to three years in a tiered manner: figures for 2024 were mandatory; figures for 2023 were requested only if no application for 2024 had been submitted; and figures for 2022 were requested only if no applications for either 2023 or 2024 had been submitted. Therefore, depending on the circumstances of each controller, the number of years for which data were requested varied.

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	2 responding controllers	1 responding controller	1 responding controller
1 – 10	2 responding controllers	1 responding controller	
11 – 50	1 responding controller		
51 – 100			
101 – 500			
more than 500			

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0	2 responding controllers	1 responding controller	1 responding controller

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

All five controllers surveyed provided figures for this question.

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years

☒ other, specify:

The same figures collection period and tiered manner as in question 15.a. were applied.

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	**2023**	**2022**
0%	3 responding controllers	2 responding controllers	2 responding controllers
10%			
20%			
30%			
40%			
more than 50%	2 responding controllers	1 responding controllers	

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?

☐ Yes

☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

Not applicable

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

As per question 15.d., all five controllers surveyed provided figures.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years

☒ other, specify:

The same figures collection period and tiered manner as in questions 15.a. and 16.a. were applied.

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	3 responding controllers	3 responding controllers	3 responding controllers
10%	1 responding controller		
20%	1 responding controller		
30%			
40%			
more than 50%			

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

As per questions 15.d and 16.d, all five controllers surveyed provided figures.

18. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 1 responding controller
b. Customers: 1 responding controller
c. Contractors:
d. Job applicants: 1 responding controller
e. Employees: 1 responding controller
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients: 1 responding controller
i. Other:

Note: Among the five controllers surveyed, one reported receiving an equal number of erasure requests from both potential customers and job applicants. Another controller did not receive any erasure requests during the entire period (2022–2024) and therefore did not provide data for this question (see question 15.b.).

18.a. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No

b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: No

18.b. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes, the results are consistent with the sectors and processing activities of the responding controllers. The data indicates that erasure requests primarily come from groups that are typically involved in those sectors, such as patients in healthcare, employees in manufacturing and customers, potential customers and job applicants in finance and insurance. The absence of erasure requests from one controller during the entire 2022–2024 period (as noted in question 15.b.) explains some gaps in the data. Overall, the pattern of active groups submitting erasure requests reflects the profiles of the controllers and their typical data processing activities.

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
c. Average- Yes
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

Yes, significant differences were identified among the five controllers surveyed based on their sector (public vs. private), size and data processing activities. These differences directly impacted their level of compliance with GDPR provisions concerning the right to erasure in Article 17.

As mentioned in question 15.b., one public sector controller did not receive any erasure requests during the entire 2022–2024 period, likely due to the nature of their services (energy provider). The second public sector controller, active in the healthcare sector, received some erasure requests exclusively from patients, which reflects the sensitive nature of the data they handle.

On the other hand, private sector controllers generally reported a significantly higher volume and broader variety of erasure requests. These came from multiple categories of data subjects, such as potential customers, customers, job applicants and employees. For instance, the controllers in the finance and insurance sector, both medium to large size organisations, reported requests across several categories, with

the largest private sector controller surveyed receiving the highest number of requests, involving all four main groups of data subjects.

The size of the organisations also impacts the number and variety of requests. Larger organisations, particularly those processing data for up to 500.000 individuals, reported a higher number of erasure requests and from more varied groups compared to smaller or medium-sized controllers.

In summary, the differences in sector, size and processing activities clearly influence both the volume and variety of erasure requests received. These factors also affect how easily and consistently controllers are able to comply with the GDPR provisions concerning the right to erasure in Article 17.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

Issue: Inconsistent scope and review frequency of internal erasure request procedures

a.: All five controllers surveyed confirmed having internal procedures for handling erasure requests under Article 17 GDPR. However, the scope, structure and review frequency of these procedures vary significantly. Some controllers follow well-defined, multi-step processes that are reviewed annually or integrated into compliance audits. For example, one controller includes erasure procedures in its annually reviewed Code of Conduct. Others review their processes only every four to five years, primarily in the context of audits or external evaluations, or rely on informal, ad-hoc practices, often managed solely by the DPO, without written guidelines or regular reviews.

b.: Articles 5 (1) c and d, 17, 19, 24 and 25 GDPR

c.: A likely explanation for these inconsistencies is the low number of erasure requests received by some controllers, particularly in the public sector and among smaller organisations. Both public organisations reported very few or no erasure requests during the entire 2022–2024 period (see question 15.b). In circumstances where requests are infrequent, procedures tend to be less formalised, updated less regularly and often depend solely on the DPOs individual expertise.

d.: There are clear differences between sectors: Private sector controllers generally tend to implement more systematic and regularly reviewed procedures. For instance, one large private controller combines manual and automated processes tailored for specific cases, while also involving external legal counsel to ensure compliance with local data protection requirements. Another large private controller follows a structured, multi-step process that is reviewed on an annually basis. This process includes verification, retention checks and coordination with data processors. In contrast, public sector controllers tend to rely more on the expertise of their DPO or adhere to fixed audit cycles. This indicates that public sector practices generally tend to be more reactive and less systematic compared to those in the private sector.
e.: In order to address these inconsistencies, a practical solution would be to introduce a standardised minimum procedural framework for all controllers, regardless of size or sector. This framework should include mandatory identity verification, clear coordination protocols with processors and joint controllers, standardised communication templates, documentation of each processing step and an annual review cycle. This would help ensure that procedures are up to date and compliant with the GDPR.

Challenge: Gaps in employee training and monitoring erasure request handling

a.: While most controllers surveyed provide some form of employee training on handling erasure requests, the frequency and quality of this training vary widely. Some controllers offer regular and mandatory training sessions. For instance, one conducts 2-3 interactive sessions per year, while another provides onboarding and refresher e-learning courses every two years. Another controller also combines e-learning with face-to-face training on an annual basis. Furthermore, one mandates training during the onboarding process and on annual basis thereafter. This training must include supplementary sessions on privacy awareness. In contrast, a relatively smaller public sector controller, does not conduct any training at all.
b.: Articles 24, 25, 12 (3), 39 (1) b and 5 (1) c and e GDPR
c.: The gaps in training and monitoring of erasure request handling appear to be influenced by organisational size, available resources (e.g., budget, staff) and the perceived compliance risk. Larger private sector controllers have the capacity to implement structured training programs and monitoring systems. Smaller organisations tend to underestimate the importance of staff training. This is partly due to the fact that they receive a lower volume of erasure requests. One public controller explicitly reported that there had been no staff training and no monitoring structure. Furthermore, many erasure requests follow initial access requests under Article 15 GDPR, which may lead controllers to treat erasure as a secondary, rather than primary legal obligation.

d.: Among the five controllers surveyed, there are notable differences in how training and monitoring of erasure request handling are dealt with. Large private sector organisations, implement structured compliance with mandatory onboarding, regular refresher training, e-learning, awareness campaigns and centralised monitoring. A medium sized private sector organisation applies a mix of e-learning and face-to-face training, although monitoring is often conducted manually. In contrast, public sector organisations rely far more on reactive practices. While one large organisation offers some face-to-face training and oversight, a smaller organisation provides no training or structured monitoring at all, depending solely on the DPO. It is evident, that higher request volumes are indicative of robust monitoring and compliance processes,

whereas low or absent request volumes often correspond with weak or non-existent systems.

e.: To strengthen compliance, it is essential for all controllers to implement mandatory, role-specific training for employees involved in handling erasure requests. The implementation of centralised tracking systems to document every step of the erasure process will improve transparency and accountability. These measures will enhance transparency, accountability and consistency with GDPR requirements.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

No
Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).

Issue: Inconsistent criteria and lack of documentation when assessing whether data are "no longer necessary"
a.: Controllers take very different approaches deciding whether personal data are "no longer necessary" for the original processing purpose under Article 17 (1) a GDPR. While some controllers implement formal assessments that include lawful basis, retention periods and purpose verification, others rely only on informal consultations with the DPO or general principles (e.g. data minimisation) without documented steps. This can lead to inconsistency, the risks of unequal treatment and the possibility of non-compliance.
b.: Articles 5 (1) c and e, 17 (1) a, 24 and 25 GDPR.
c.: The primary reason for these variations is usually the lack of legal resources, the maturity of compliance and the level of data mapping within the organisation. Larger, well-resourced organisations often embed necessity checks into workflows, while smaller organisations often depend solely on the opinion of the DPO without formalised tools.
d.: A larger private sector controller and a medium-sized controller have implemented structured, multi-step reviews. These reviews assess each request against Article 17 (1) a. The reviews also cross-reference processing records, statutory retention periods and lawful bases for processing. In contrast, a smaller public sector controller tends to adopt a more informal approach, often relying exclusively on the input of the DPO. One large private sector controller adheres to general data minimisation principles but does not have a binding checklist or formal assessment. The healthcare and utility sectors, with their specific statutory retention rules (e.g. for medical records), influence the decision-making process in a distinct manner. Under Article 17 (3) b or c GDPR, paragraphs 1 and 2 shall not apply to the extent that processing is necessary for compliance with a legal obligation or for reasons of public interest in public health. The

continued retention of personal data is therefore permissible where these conditions apply and the processing relies on another legal basis. Generally, it could be observed, that controllers with a high volume of data processing usually employ auditable checklists and software tools for the determination of necessity, while low-volume controllers often rely on manual checks and experience.
e.: A practical solution for all controllers would be to adopt a documented checklist for assessing necessity. This checklist should include validation of the processing purpose, review of retention periods, verification of legal grounds for processing, and screening for any exceptions under Article 17 (3) GDPR. This is not just a best practice but a clear GDPR requirement: Article 5 (1) c and e GDPR demand data minimisation and storage limitation, Article 17 (1) a GDPR calls for erasure when data are no longer necessary and Article 24 GDPR mandates embedding these standards into routine processes.

Challenge: Lack of tested and standardised procedures for handling consent withdrawal or objections
a.: Some controllers have drafted a process for handling consent withdrawals and objections, but only a few have tested these in practice. Several controllers reported that they have never received such requests. Smaller public organisations tend to handle these informally by the DPO, sometimes complicated by sector-specific obligations, such as mandatory retention of medical records. None of the controllers surveyed have applied the “overriding legitimate grounds” balancing test under Art. 21 (1) GDPR in practice.
b.: Articles 17 (1) b and c, 21, 7 (3), 6 (1) a to f, 24 and 25 GDPR.
c.: The main factor contributing to this challenge is the low volume of consent withdrawal or objection requests. This leads to a lower prioritisation of formal workflows for the handling of them. For many controllers, consent is rarely the legal basis for processing, which reduces the urgency of establishing formal procedures for its withdrawal. On the other hand, very common data processing relying on consent like the sending of newsletters is typically organised by integrated consent management tools. Recipients can withdraw their original consent and unsubscribe from newsletters automatically, which simplifies the handling of such withdrawals for controllers substantially and reduces the need for additional formal procedures.
d.: Public sector controllers frequently document the intended steps for consent withdrawals and objections, even in cases where there is no practical application. Private sector controllers tend to adopt a similar approach, incorporating these procedures into their data protection or compliance frameworks. Smaller public sector organisations tend to handle these situations informally, relying on the DPO, without standardised templates and often face sector-specific legal constraints. Large private sector controllers without actual consent withdrawal cases have similarly not tested their procedures. In sectors with heavy regulatory oversight (e.g., finance), documented readiness is more common, whereas smaller entities depend on case-by-case discretion.
e.: To address this gap, controllers should develop templates and step-by-step workflows for managing consent withdrawals and objections, including criteria for the "overriding legitimate grounds" test. Articles 17 and 21 GDPR stipulate that personal data must be erased or restricted, unless exceptions apply. Article 24 GDPR mandates full documentation and the readiness to apply these legal tests.

Issue: Inconsistent application of exceptions and alternative measures when erasure is delayed or refused (Art. 17(3) GDPR)
a.: While many controllers apply exceptions under Article 17 (3) GDPR (e.g. legal obligations, ongoing proceedings for the establishment, exercise or defence of legal claims or public interest), the process for verifying these exceptions varies widely. Some controllers make a formal legal assessment and document their reasoning, while others treat the exceptions as automatically applying without any proportionality checks. Similarly, alternative measures applied, such as encryption or access restrictions, range from robust technical solutions to informal arrangements with minimal safeguards.
b.: Articles 17 (3), 18, 5 (1) c, e, (2), 24 and 25 GDPR.
c.: The variations in practice stem primarily from differences in process maturity and available technical resources. Large organisations often incorporate exception checks into their workflows and utilise technology to ensure a high level of data protection (e.g. encryption, anonymisation). Smaller organisations tend to be more reactive and may not have the same level of resources or technical tools as larger organisations, which can limit their ability to conduct rigorous and consistent checks and to provide the same safeguards.
d.: Large public and private controllers typically provide written legal justifications, involve compliance or legal teams in decision-making and apply strong technical measures such as anonymisation, encryption or strict access controls. Smaller public sector controllers often assume to have statutory obligations without conducting a proportionality analysis, relying solely on the DPO's oversight. In regulated private sectors, such as the financial industry, legal obligations and defence in litigation procedures frequently serve as the primary grounds for exceptions, while public controllers place greater emphasis on public interest or public authority tasks. Generally, high-volume controllers have clearly defined templates and procedures for dealing with exceptions, whereas low-volume controllers often resort to ad hoc approaches.
e.: To ensure fairness and compliance, controllers should develop templates that require a detailed legal reasoning, contain a rationale for establishing the necessity of data processed, and require the performance of a proportionality analysis whenever an exception to the right to erasure is claimed. In addition, technical restriction mechanisms must be consistently used and fully documented. Article 17 (3) GDPR makes it clear that erasure can only be refused when a specific exception applies, with full justification, and Article 18 GDPR requires processing restrictions where erasure is not possible. Additionally, Article 24 GDPR demands that these procedures be properly documented and integrated into organisational processes.

24. Are there any leading or best practices of the controllers having responded that you would like to share?
No

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.

Issue: Inconsistent provision of clear instructions for submitting erasure requests

a.: While most controllers surveyed provide some form of instructions for submitting erasure requests, the clarity, accessibility, and consistency of these instructions vary. Some controllers ensure that the instructions are clearly visible in their privacy notices or dedicated forms. In contrast, other controllers offer instructions in a reactive manner or in a dispersed state across different documents, making it more difficult for data subjects to find the necessary information. This inconsistency limits transparency and undermines the effective exercise of the right to erasure under Article 17 GDPR.

b.: Articles 12, 13, 17, 24 and 25 GDPR

c.: The discrepancies seem to stem from the size of the organisation, available resources and their prioritisation of compliance. Larger controllers, such as those in the private sector, have more resources to ensure that clear, accessible instructions are visible across all communication channels. Smaller controllers may lack dedicated resources and typically provide instructions reactively, making it harder for data subjects to easily exercise their rights.

d.: In practice, these differences are clearly visible in the survey responses. A large public sector controller integrates complete, easy-to-find instructions for data erasure into their privacy notices, allowing all affected individuals to access them effortlessly. A large private sector controller in the financial industry follows a similar practice, providing clear instructions in their privacy notices for all customer groups. Another large private controller additionally creates a robust multi-channel approach. In contrast, a small public sector controller in healthcare only provides instructions upon request and requires written submissions, which can create unnecessary barriers. A medium-sized private controller in the insurance industry provides contact details for the submission of erasure requests in privacy notices, contracts and forms. However, online visibility of this contact information is inconsistent and not always user-friendly.

e.: To comply with GDPR requirements, controllers must ensure that instructions for submitting erasure requests are clear, standardised and easily accessible across all communication channels. Such an approach would ensure compliance with the transparency duties under Articles 12 and 13 GDPR as well as the organisational-measure obligations under Article 24 GDPR.

Issue: Inconsistent practices in acknowledging receipt of erasure requests and providing processing-time information

a.: While it is not a legal duty as such, all five controllers surveyed, in both the private and public sector, send receipts of acknowledgement to the requesting data subjects. One controller noted that in some cases it may not send an acknowledgment if the request is processed immediately, so no separate confirmation is necessary. However, some controllers omit timeframe information. This can cause uncertainty for data subjects regarding the processing and completion of their requests.

b.: Article 12 (3) and 24 GDPR

c.: The differences in practices regarding the provision of receipts of acknowledgement appear to be driven by internal procedures, available resources and varying levels of perceived compliance risk. Larger controllers often have more formalised processes for the acknowledgement of data subject's requests, including the specification of processing times. Smaller organisations, particularly those with lower volumes of erasure requests, may not prioritise sending formal receipts of acknowledgement or providing explicit timeframes.

d.: The survey results clearly highlight the practical differences in acknowledgement practices. Large controllers in both the public and private sectors consistently acknowledge receipt of such requests in a formal way and provide a corresponding receipt of acknowledgement including an estimated processing timeframe to the data subjects. One of the surveyed controllers sends receipts of acknowledgements only on a case-by-case basis, although this does include an estimated timeframe. While most large organisations (in both the private and public sectors) clearly communicate on processing times, this practice is less consistent among small and medium-sized organisations. The response varies depending on the type of request and the communication channel used. There is also significant variation in response methods and the indication of estimated processing times. Some organisations reply via email or postal mail, while others use online forms or apps. These inconsistencies can result in diverging experiences for data subjects, with some receiving clear confirmation and timelines, while others are left uncertain about the status of their request.
e.: In order to meet the transparency and accountability requirements of Articles 12 (3) and 24 GDPR, it is recommended that all controllers should implement a standardised policy to acknowledge every erasure request formally and without undue delay. This acknowledgement should include the expected processing time, even if this is the statutory maximum one-month period provided in Article 12 (3) GDPR. By adopting this approach, controllers can ensure clarity for data subjects and enhance compliance with GDPR requirements.

26. Are there any leading or best practices of the controllers having responded that you would like to share?
No

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers

Issue: Different use of established technical standards for deleting personal data
a.: Among the five controllers surveyed, the use of recognised technical standards for data deletion varies. Only two large controllers, one large private sector and one large public sector organisation, have implemented certified deletion practices. The remaining controllers rely on internally developed methods without external benchmarks, resulting in inconsistent levels of security and demonstrability of compliance.
b.: Articles 17, 25 and 32 GDPR
c.: These differences arise from variations in sector specific needs, organisation size, available resources and external oversight. Controllers in high-risk or competitive sectors tend to pursue certifications to fulfil contractual obligations and meet customer and regulatory demands. Smaller organisations, working with older systems and tighter budgets often prioritise basic internal procedures over formal certified mechanisms.
d.: In practice, this split is clearly visible in the survey responses. The large private sector controller holds an ISO 27001 certification and works with specialist providers

for complex deletion tasks. A similar approach is adopted by a large public controller, which follows an externally audited framework, maintaining the GoodPriv@cy seal. In contrast, a small public sector, a mid-sized and another large private sector controller use internal procedures only, without any third-party verification.
e.: A practical solution would be, e.g. for DPAs or the EDPB, to promote or establish deletion standards that apply to all controllers regardless of size and sector. Under Articles 25 and 32 GDPR, all controllers are required to implement appropriate technical and organisational measures to ensure secure data deletion. Article 24 GDPR further obliges controllers to be able to demonstrate the effectiveness of such measures. The use of recognised standards or certified best-practice frameworks is one of the most effective ways to demonstrate compliance with these requirements.

Issue: Inconsistent use and quality of anonymisation as a substitute for deletion
a.: Controllers adopt a variety of approaches to anonymisation when used as an alternative to deletion. In some cases, the methods are technically robust and render re-identification impossible in line with Recital 26 GDPR; in others, they are weak enough that personal data may still be considered identifiable or anonymisation is not applied at all.
b.: Articles 17 and 6 GDPR, Recital 26 GDPR
c.: Anonymisation is often chosen when organisations want to retain data for analytical purposes or when system limitations make deletion difficult. In the absence of clear technical standards, some controllers implement genuinely irreversible anonymisation, while others apply only pseudonymisation or partial masking, which fails to meet the GDPR's threshold for taking data outside its scope. These differences may result from varying technical resources, levels of data protection expertise and risk assessments among controllers, which can lead to discrepancies in the practical application of anonymisation in compliance with the GDPR's requirements.
d.: The private sector mid-sized controller and a large private sector controller apply strong anonymisation methods to prevent re-identification. A large public and a large private sector controller both use weaker masking techniques, which leave re-identification risks. The smallest controller surveyed does not use anonymisation at all.
e.: Introducing (sector-specific) guidance on when to use anonymisation and how to perform it, along with training to distinguish between anonymisation and pseudonymisation, would help ensure that all controllers meet GDPR standards.

28. Are there any leading or best practices of the controllers having responded that you would like to share?
No

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

If yes, please provide the date, link to the guidance, and a short description of the guidance.

The LI SA has published detailed and practical information on the right to erasure pursuant to Article 17 GDPR on its website. This information covers both general principles and specific aspects of data retention and deletion, including the relevant legal bases and the various scenarios in which personal data must be erased. It clearly explains key data protection principles such as purpose limitation, data minimization and storage limitation as defined in Article 5 GDPR.
The information details the specific conditions under which the right to erasure applies, for example, when data is no longer needed for its original purpose, when the data subject withdraws consent or objects to processing, in cases of unlawful processing, or when there is a legal obligation to erase the data. It also emphasizes that the right to erasure is only applicable if no other legal basis for continued processing exists and if no exception of Article 17 (3) GDPR applies. Additionally, it provides dedicated information on the rights of children, particularly where data has been collected via online services, and elaborates on the "right to be forgotten" for data made public, for example online.
Furthermore, the information clarifies the exceptions to the right to erasure, especially when statutory retention obligations or other legal provisions override the erasure right. It offers detailed information on applicable statutory retention and deletion periods in Liechtenstein, explains both processes of deletion and anonymization, and provides practical recommendations for developing and implementing data deletion policies within organisations.
This information on the right to erasure, including legal background, implementation information and practical considerations, is available on the official website of the LI SA: https://www.datenschutzstelle.li/datenschutz/themen-z/loeschfristen.

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.

We have not taken any such action yet.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?

Since the GDPR entry into force, the LI SA has received occasional complaints related to or containing the right to erasure (Art. 17 GDPR). On average, such complaints amounted to around 4 to 5 per year, which corresponds to about 10% of all complaints received. While we are unable to provide more detailed statistics, the overall number of such complaints has remained relatively stable.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the

controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).

The LI SA will present the findings of the CEF 2025 on the implementation of the right to erasure under Article 17 GDPR at the upcoming annual meeting of DPOs in Liechtenstein on 10th November 2025. This event will provide a valuable opportunity to share insights, highlight good practices and foster open dialogue with DPOs across sectors.

At the same occasion the LI SA will also remind participants of the practical support services it offers, including guidance materials and consultation options.

At this stage, no formal corrective measures - such as, orders, or administrative fines - are planned on the basis of the CEF results. Instead, the focus lies on raising awareness, promoting transparency and building capacity within organisations.

Following the annual meeting, the LI SA will evaluate whether further action is needed, taking into account the feedback received and the outcomes of discussions with DPOs. Any additional steps, such as bilateral follow-ups with individual controllers, will be considered on a case-by-case basis and remain at the discretion of the LI SA.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes

If "Yes", please specify: *(please select one or more answers)*

a. More online guidance:
b. Online or remote training sessions:
c. Conferences organised:
d. Others: please specify: The LI SA will present the key findings identified of the CEF questionnaire at the upcoming annual meeting of DPOs in Liechtenstein on 10 November 2025. This presentation will provide a general overview of Article 17 GDPR and explore how the right to erasure is being implemented in practice. In addition to highlighting the main findings, the session will address broader issues related to the application, interpretation, and operational challenges of the right to erasure.

   Following the presentation, DPOs will have the opportunity to ask questions and take part in an open discussion, enabling the exchange of views, good practices, and practical experiences. This interactive session is intended to support organisations and their DPOs in enhancing their compliance with Article 17 GDPR.

b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes:
b. No

35. Are there any other observations that you would like to share?
No

LT SA

Name of Supervisory Authority: State Data Protection Inspectorate of the Republic of Lithuania (hereinafter – LT SA).

Introduction

1. What was the initial procedural framework of your action?
A new formal investigation[35]: Investigation concerning the implementation of the right to erasure by data controllers was included in the annual investigation plan of the LT SA. As a result of this investigation, a decision determining whether an infringement has occurred will be adopted in respect of each controller.

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question):
The action is not oriented towards fact-finding.

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
The same questionnaire was used for all controllers.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
All questions from the consolidated questionnaire were included.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?
No other general comments.

Part I - Information about the controllers addressed

6. How many controllers did you contact?
The LT SA contacted five controllers.

7. Out of the contacted controllers, how many controllers responded?
All five contacted controllers responded.

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?
No gap identified.

9. Please specify the sectors of activity of the responding controllers.

[35] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

a. Public sector: -
b. Private sector: 5 responding controllers.
c. Other: -

If so, what were the other sectors? No applicable.

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector: -
b. Health sector: -
c. Social sector: -
d. Insurance sector: -
e. Finance sector:3 responding controllers.
f. IT sector: -
g. Retail sector: 1 responding controller.
h. Logistics sector: -
i. Public transportation: -
j. Telecommunications: -
k. Postal services: -
l. Advertising sector: -
m. Marketing services: -
n. Entertainment sector: -
o. Information / journalism sector: -
p. Scientific / historical research: -
q. Credit scoring agency: -
r. Public utility/infrastructure provider (e.g. energy): 1 responding controller.
s. Housing industry: -
t. Manufacturing: -
u. Consulting: -
v. Public administration: -
w. Other (please specify): -

11. Please specify the category in which the responding controllers fall[36]:

a. Micro enterprise: 1 responding controller.
b. Small enterprise: -
c. Medium-size enterprise: 2 responding controllers.
d. Large enterprise (more than 250 employees): 2 responding controllers.
e. Non-profit organisation: -
f. Ministry: -
g. Local authority: -
h. Administrative authority/agency/office (e.g. job center): -
i. School/university/educational institution: -
j. Other (please specify): -

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

[36] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

a. Potential customers: -
b. Customers: 5 responding controllers.
c. Contractors: -
d. Job applicants: -
e. Employees: -
f. Applicants (for public services): -
g. Citizens (for public sector): -
h. Patients: -
i. Other (please specify): -

12.b. According to the responding controllers, are those data subjects also:

a. Children: 1 responding controller.
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 1 responding controller.
c. Non applicable: 4 responding controllers.

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: -
b. 101 – 1 000: -
c. 1 001 – 10 000: 1 responding controller.
d. 10 001 – 100 000: 1 responding controller.
e. 100 001 – 500 000: 1 responding controller.
f. 500 001 – 1 000 000: -
g. > 1 000 000: 2 responding controllers.

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 5 responding controllers.
b. Payment data: 5 responding controllers.
c. Identification data: 5 responding controllers.
d. Marketing data: 3 responding controllers.
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 1 responding controller.
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 1 responding controller.
g. Other, please specify: 2 responding controllers (financial data).

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures:

☐ 1 year -Yes
☐ 3 years
☐ other, specify: -

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?
Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	1 responding controller	1 responding controller	1 responding controller
1 – 10	1 responding controller	-	-
11 – 50	2 responding controllers	-	-
51 – 100	0	0	0
101 – 500	0	0	0
more than 500	1 responding controller	-	-

15.c. For the SAs which asked figures relating to several years, could you please complete this table? The LT SA requested data covering a one-year period.

	2024*	**2024-2023**	**2024-2022**
0	-	-	-

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
0 responding controller.

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 1 year- Yes
☐ 3 years
☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	2023	2022
0%	2 responding controllers	2 responding controllers	2 responding controllers
10%	0	0	0
20%	1 responding controller	-	-
30%	0	0	0
40%	0	0	0
more than 50%	2 responding controllers	-	-

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?
☐ Yes
Yes No, if so: The LT AS could not provide an answer, since the investigation is still ongoing.

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
0 responding controllers.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 1 year - Yes
☐ 3 years
☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	2023	2022
0%	3 responding controllers	3 responding controllers	3 responding controllers
10%	0	-	-
20%	0	-	-
30%	1 responding controller	-	-
40%	0	-	-
more than 50%	1 responding controller	-	-

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
0 responding controller.

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 1 responding controller.
b. Customers: 3 responding controllers.
c. Contractors: -
d. Job applicants: -
e. Employees: -
f. Applicants (for public services): -
g. Citizens (for public sector): -
h. Patients: -
i. Other: -

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: No

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes.

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
c. Average - Yes
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

There is a difference between those responding controllers who receive a large number of requests for erasure and those who do not. Responding controllers who receive a huge number of requests have a shorter deadline for processing requests for erasure, are better prepared to receive requests for erasure, and have recommended application forms.
There is also a difference between responding controllers subject to anti-money laundering (AML) requirements and responding controllers not subject to these requirements. In the case of AML requirements, greater emphasis is placed on identifying applicants, resulting in longer processing times.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

a) The problem is the lack of specific internal instructions on the implementation of the right to erasure. Some of the controllers do not have any instructions on how to implement the right to erasure request at all. One controller has indicated that he would decide how to implement the right to erasure request only upon receipt of such a request. The majority of the controllers indicated that the right to erasure request would be dealt with in a general manner and only one controller indicated that they had a procedure for implementing the right to erasure request.
b) This is related to the implementation of Art. 17 GDPR.
c) The reason why a large part of the controllers did not have specific instructions for the implementation of right to erasure request may be that the controllers did not receive such requests or the number of these requests was negligible and therefore did not assess the practical aspects of the implementation of this data subject's right and indicated that they follow the general instructions.
d) There is a difference between the controller who receives a large number of the right to erasure request and the controller who has not received any such requests. Having not received any the right to erasure requests in the last 3 years, the controller did not have instructions on the implementation of the right to erasure requests, while the controller, having received more than 500 the right to erasure requests, not only had instructions on the implementation of the right to erasure requests, but also noted the shortest deadline for the implementation of such requests. We also drew attention to the longer deadline for processing the right to erasure request for those controllers who are subject to stricter personal identification requirements related to the prevention of money laundering (AML), while the controller, who received the most notifications, paid much less attention to identifying applicants.
e) The existence of model instructions governing the implementation of the right to erasure requests and model forms for applying for the implementation of the right to erasure requests could be a possible solution to the problem (at EDPB level for the development of uniform practices).

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

The controller, who demonstrated best practice in terms of processing incoming requests and deadlines for the implementation of the right to erasure requests had proven instructions and contact forms. One of the controllers noted that the training of employees not only introduces employees to the requirements of the GDPR, but also uses knowledge tests. We believe that in certain cases (for example, if there is such a need in the activities of the organization) this is a positive example for more effective absorption of knowledge about the protection of personal data.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).

a) The responses of the controllers indicate that the main problems in determining whether or not the data to be deleted are covered by the exceptions provided for in Article 17(3) of the GDPR.
b) This concerns the application of the exceptions provided for in Article 17(3) of the GDPR.
c) The majority of the controllers indicated that the exceptions provided for in Article 17(3) of the GDPR did not apply because there were no requests for the deletion of data falling under the exceptions provided for in Article 17(3) of the GDPR.
d) When answering the question whether the controller has ever stood up to erase data on the basis of the right to freedom of expression and information (Article 17(3)(a) of the GDPR), all controllers indicated that no requests for erasure of data falling under the exceptions provided for in Article 17(3) of the GDPR were received. In addition, almost all controllers indicated that they had not refused to delete the data on the basis of Article 17(1)(c) of the GDPR (for 'overriding legitimate reasons'). It is apparent from the reply of the only controller who referred to the application of that paragraph that the concept of 'overriding legitimate reasons' was misunderstood. In the present case, therefore, no differences were found between the controllers.
e) The issues raised could lead to further clarifications at the level of the EDPB for controllers on the application of the exceptions provided for in Article 17(3) GDPR.

24. Are there any leading or best practices of the controllers having responded that you would like to share?

In response to a question on how to handle right to erasure requests in case where the data subject simultaneously requests access to and deletion to their data, the vast majority of the controllers indicated that they first provide the data subject with access to the data before the data is deleted.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.

a) Some of the controllers indicated that there are no detailed instructions on how to submit the right to erasure request and simply provide links to the privacy policy.
b) This is related to the implementation of Art. 17 GDPR.
c) As regards the reasons for not providing detailed instructions on the implementation of the right to erasure, one controller indicated that this would potentially deter data subjects from submitting requests for erasure of personal data. The majority of controllers do not pay sufficient attention to the creation and provision of instructions, as they consider it sufficient to refer to the general provisions of the privacy policy.
d) The vast majority of the controllers indicated that communication with data subjects takes place by e-mail. Another method of communication indicated is via the customer account.
e) A possible solution to the problems identified could be the development and availability of a template of the right to erasure request form.

26. Are there any leading or best practices of the controllers having responded that you would like to share?

The controller implementing the most of the right to erasure request has prepared application forms and has the shortest deadlines for processing the requests. Having a prepared template of the right to erasure request form would facilitate the application procedure and likely speed up the implementation of the requests.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers

a) The controllers are mainly concerned with the deletion of personal data contained in backups.
b) This is related to the implementation of Art. 17 GDPR.
c) The problem concerns the technical measures in place, the storage of back-ups and the archiving of data. The majority of controllers delete data when backups are updated or deleted, i.e. every 30 days.
d) Some controllers have indicated that they are anonymizing the data, while others are completely deleting the data. It should be noted that most anonymization is carried out by financial institutions on the basis of a legal obligation and in order to maintain the integrity of the analytical indicators and the database. The main issue for the controllers is the deletion of personal data contained in backups. Only 1 controller stated that he deletes data from backups without any reservations. A large number of the controllers, in particular the financial institutions, indicated that data was deleted by erasing or updating, by synchronizing backups (in most cases every 30 days), but some did not specify a deadline for erasing or updating backups or indicated that data

from backups were not deleted, and stated that due to legal requirements they could not fully exercise this right. Some of the controllers indicated that they are using anonymization, some are completely deleting the data. It should be noted that, according to the survey data, most often anonymization is applied by financial institutions, motivated by a legal obligation and the desire to maintain the integrity of analytical indicators and the database.

e) Providing additional information on the process of deleting personal data from backups could help solve the problem.

28. Are there any leading or best practices of the controllers having responded that you would like to share?

One of the controllers reported using data anonymisation in order to preserve the consistency analytical indicators and the overall integrity of the database. This approach could be considered a good practice, given that other controllers noted that deleting data from the database could damage the integrity of the database.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

We do not have already published guidance's on the implementation of the right to erasure.

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.

General consultations are regularly conducted by telephone and in writing. In 2025, training was given to health institutions on rights in general, which also addressed the topic of the right to be forgotten (Article 17 of the GDPR). During the last 5 years, 1 decision was adopted to order the erasure of personal data pursuant to Article 58(2)(g) of the GDPR.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?

Since 2019, the LT SA has issued 501 decisions on the right to erasure of personal data under Article 17 of the GDPR. Of these, 46 complaints were found to be justified, and 27 were affected, mostly in accordance with Article 58(2)(d), (c) and (b) of the GDPR).

When comparing the number of complaints received over the years, there is a clear upward trend in case concerning the right to erasure of personal data. Specifically, the LT SA received 109 complaints in 2025, 109 in 2024, 100 in 2023, 67 in 2022, 107 in 2021, and 66 in 2020.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).
The investigation is ongoing and there is no answer yet.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes:
   If **"Yes",** please specify: *(please select one or more answers)*
   a. More online guidance: -
   b. Online or remote training sessions: -
   c. Conferences organised: -
   d. Others: please specify: The results of the studies will be summarized and published on the LT SA website (in order to share good practices and to indicate any errors in practice).
b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes: More practical examples of data erasure are needed.

35. Are there any other observations that you would like to share?
No other observations

LU SA

Name of Supervisory Authority: CNPD (Commission nationale pour la protection des données)

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding: Yes
b. Fact finding + determining follow-up action based on the results: NO
c. New formal investigation[37]: NO
d. Ongoing investigation: NO

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? Yes
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. Yes, if deemed necessary internally. Further guidance on the right to erasure could also trigger the launch of new thematic investigations.
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? n/a

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
The same questionnaire was used for all controllers.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
n/a
5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?
No

Part I - Information about the controllers addressed

6. How many controllers did you contact?
6

7. Out of the contacted controllers, how many controllers responded?

[37] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

5

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

The controller that did not respond did not want to take part in the survey as it considered that answering to such questionnaire is time and money consuming and that such questionnaire is not reliable as controllers are not obliged to be honest and are not likely to admit their non-compliance with GDPR.

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 0
b. Private sector: 5
c. Other: n/a

If so, what were the other sectors? n/a

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector:
b. Health sector:
c. Social sector:
d. Insurance sector:
e. Finance sector:
f. IT sector:
g. Retail sector:
h. Logistics sector:
i. Public transportation:
j. Telecommunications:
k. Postal services:
l. Advertising sector:
m. Marketing services:
n. Entertainment sector: 2 responding controllers
o. Information / journalism sector:
p. Scientific / historical research:
q. Credit scoring agency:
r. Public utility/infrastructure provider (e.g. energy):
s. Housing industry: 3 responding controllers
t. Manufacturing:
u. Consulting:
v. Public administration:
w. Other (please specify):

11. Please specify the category in which the responding controllers fall[38]:

a. Micro enterprise: 2 responding controllers

[38] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

b. Small enterprise: 1 responding controller
c. Medium-size enterprise: 1 responding controller
d. Large enterprise (more than 250 employees): 1 responding controller
e. Non-profit organisation:
f. Ministry:
g. Local authority:
h. Administrative authority/agency/office (e.g. job center):
i. School/university/educational institution:
j. Other (please specify):

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers: 2 responding controllers
b. Customers: 3 responding controllers
c. Contractors:
d. Job applicants:
e. Employees:
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients:
i. Other (please specify):

12.b. According to the responding controllers, are those data subjects also:

a. Children:
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 1 responding controller
c. Non applicable:

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100:
b. 101 – 1 000: 2 responding controllers
c. 1 001 – 10 000:
d. 10 001 – 100 000: 1 responding controller
e. 100 001 – 500 000:
f. 500 001 – 1 000 000:
g. > 1 000 000: 2 responding controllers

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 4 responding controllers
b. Payment data: 2 responding controllers
c. Identification data: 4 responding controllers
d. Marketing data: 2 responding controllers
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 2 responding controllers (related to sexual life)

f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences:
g. Other, please specify:

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years- Yes

☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	2 responding controllers	1 responding controller	2 responding controllers
1 – 10	1 responding controller	2 responding controllers	1 responding controller
11 – 50	-	-	-
51 – 100	-	-	-
101 – 500	-	-	-
more than 500	2 responding controllers	2 responding controllers	2 responding controllers

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0	1 responding controller	-	1 responding controller

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
All the controllers answered to this question.

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years- Yes

☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	**2023**	**2022**
0%	2 responding controllers	3 responding controllers	2 responding controllers
10%	1 responding controller	1 responding controller	1 responding controller
20%	-	-	-
30%	-	-	-
40%	-	-	-
more than 50%	-	-	-

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?

☐ Yes

☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

All the controllers answered to this question.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐3 years - Yes

☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	2 responding controllers	2 responding controllers	2 responding controllers
10%	-	-	-
20%	-	-	-
30%	-	-	-
40%	-	-	-
more than 50%	2 responding controllers	2 responding controllers	2 responding controllers

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

All the controllers answered to this question.

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 1 responding controller
b. Customers: 4 responding controllers
c. Contractors: 1 responding controller
d. Job applicants: -
e. Employees: -
f. Applicants (for public services): -
g. Citizens (for public sector): -
h. Patients: -
i. Other: -

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: No

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
c. Average
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

It appears that larger companies have implemented structured process with a high level of maturity to process the requests for erasure and anticipate the specific requirements of Article 17 GDPR, especially when companies have to retain certain data. It also appears that smaller companies are not always aware of the necessity to keep some personal data (for example for legal reasons) or do not have a real overview of all the personal data they actually process.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

Questions 2.1. and 2.9.

a. Name the issue(s) identified and briefly describe it.
For smaller organisations, there is no structured / complete process description for processing requests for erasure (definition of the internal responsibilities, of the input channels, software, output channels). Moreover, smaller organisations do not regularly review their procedures for implementing Art. 17 GDPR.

b. Which provision(s) of the GDPR (or national laws) does this concern?
The GDPR does not contain concrete requirements for the processing of the requests for erasure; the process falls within the organizational discretion of the controller. However the data controllers are responsible for a fair and lawful processing of the data according to GDPR Article 5; GDPR Article 24 also explains that “the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.”

c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
A potential explanation may be the number of requests for erasure received that does not justify, for the data controller, a structured procedure and its regular review.

d. What are differences that you have encountered between controllers in your Member State?
This issue typically concerns the small organisations that do not process a lot of requests for erasure.

e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?
Controllers should have implemented a structured process for processing requests for erasure, in which at least the internal

responsibilities are defined and the procedures are outlined. For smaller controllers, documented procedures cannot always be required but an awareness around the requirements of Article 17 is expected.
Controllers can implement an escalation procedure for more complex requests. Requests could be for example escalated to (by order of priority) 1- managers, 2- specialized GDPR operators, 3- the local DPO contact with support, and 4- the legal department.
For more complex organisations, controllers can develop several entry channels to facilitate the data subject's exercise of their rights.

Deletion procedures should be ongoingly monitored in regard of effectiveness and practicability.

Question 2.3.

a. Name the issue(s) identified and briefly describe it.
Some organisations do not have implemented specific training related to Article 17 requests.

b. Which provision(s) of the GDPR (or national laws) does this concern?
The GDPR does not contain concrete requirements for the training of the staff regarding the processing of Article 17 requests; the process falls within the organizational discretion of the controller. However the data controllers are responsible for a fair and lawful processing of the data according to GDPR Article 5; GDPR Article 24 also explains that "the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation."

c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
A potential explanation may be the number of requests for erasure received that does not justify, for the data controller, specific training.

d. What are differences that you have encountered between controllers in your Member State?
This issue typically concerns the small organisations that do not process a lot of requests for erasure.

e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?
Controllers should train (internally or externally) the staff when onboarding them and when business needs require it. Specific help can also be provided by external specialists.

Question 2.4.

a. Name the issue(s) identified and briefly describe it.
Absence of a structured process to identify and select the data related to the data subject in smaller organisations.

b. Which provision(s) of the GDPR (or national laws) does this concern?
The GDPR does not contain concrete requirements for the processing of the requests for erasure; the process falls within the organizational discretion of the controller. However the data controllers are responsible for a fair and lawful processing of the data according to GDPR Article 5; GDPR Article 24 also explains that "the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation."

c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
A potential explanation may be that smaller organisations have less means to identify all the personal data they actually process (for example they are not obliged to maintain a register of processing activities).

d. What are differences that you have encountered between controllers in your Member State?
This issue typically concerns the small organisations that do not process a lot of requests for erasure.

e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?
Each controller must be aware of its respective processing operations, if necessary and when existing via the record of processing activities, and it has to be able to assign individual processing operations to the data subject.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

Question 2.4.
Some data controllers identify and link data to a data subject by referencing them in a database. Each new processing activity includes this referencing when designing it.
Question 2.6.
A controller explains it appoints IT personnel to regularly monitor and assess the effectiveness of (technical) deletion procedures. This personnel also assesses the necessity of all deletion holds the company has set on individual profiles.
Question 2.8.
Some data controllers verify if there are reasons that may lead to an extension of the one month deadline once they receive the request and immediately inform the data subject about the delay and the reasons of such a delay (for example: establishment, exercise or defence of legal claims ...)
Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).

Question 3.1.

a. Name the issue(s) identified and briefly describe it.
For smaller organisations, there is no structured procedure in place to assess whether some personal data is still necessary for the defined purposes.
There is no distinction made with the consent withdrawal and the right to object.

b. Which provision(s) of the GDPR (or national laws) does this concern?
Art. 17 (1) (a) GDPR
Art. 17 (1) (b) GDPR
Art. 17 (1) (c) GDPR

c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
A potential explanation may be the number of requests for erasure received that does not justify, for the data controller, a structured procedure and the anticipation of certain situations where consent withdrawal and the right to object are applicable.

d. What are differences that you have encountered between controllers in your Member State?
This issue typically concerns the small organisations that do not process a lot of requests for erasure.

e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?
Controllers should implement a structured and systematic procedure to make sure that personal data (that are subject to an erasure request) are no longer necessary for the purposes for which they were collected or otherwise processed. Data controllers should describe how they identify the initial purposes of the collection of the data (ex: for legal purposes, legitimate interest, fulfilment of a contract) and the processing activity related to the data subject to compare it with the current situation of the data subject (ex: subscription to certain services, accounting requirements...).
Controllers should identify situations where the consent withdrawal and the right to object are applicable and, if yes, implement a procedure to handle these situations.

24. Are there any leading or best practices of the controllers having responded that you would like to share?

Question 3.11.
Some organisations inform the data subjects about the consequences of definitive deletion of all their data (ex: use of certain services, access request which cannot be fulfilled). The data controller advises the data subject to first make a request for access and then, in a second step, to repeat their request for deletion.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.

Question 4.1. (1)

a. Name the issue(s) identified and briefly describe it.
   For most of the controllers, there are no instructions nor a description of the process for submitting a request for erasure or the instructions lack of completeness. For example the legal mentions may describe the procedure to exercise the right of access (or the "rights" in general) but not the right to erasure in particular.

b. Which provision(s) of the GDPR (or national laws) does this concern?
   Pursuant to GDPR Article 5(1)(a) of the GDPR, data must be processed in a transparent manner in relation to the data subject and pursuant to GDPR Article 12 (2) "The controller shall facilitate the exercise of data subject rights under Articles 15 to 22.".

c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
   A potential explanation may be the number of requests for erasure received that does not justify, for the data controller, to spend more time and budget to improve the communication with their data subjects.

d. What are differences that you have encountered between controllers in your Member State?
   This issue mainly concerns the small organisations that do not process a lot of requests for erasure.

e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?
   Controllers should facilitate the exercise of the right to erasure and more generally of the different rights by providing instructions and / or a description of the process for submitting a request.

Question 4.1. (2)

a. Name the issue(s) identified and briefly describe it.
   Some controllers confuse the right to erasure and the closure of a client account. They explain that the data subjects can easily delete their profile by browsing the user settings but this is actually different from the exercise of the right to erasure.

b. Which provision(s) of the GDPR (or national laws) does this concern?
A request to delete a profile/account is based on contractual law while a request to erase personal data is based on Article 17 of the GDPR.

c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
A potential explanation may be the lack of awareness of the controllers regarding the specificities of the right to erasure.

d. What are differences that you have encountered between controllers in your Member State?
Most of the data controllers make this confusion, regardless of their size.

e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?
Controllers should review their practice and clearly distinguish the closure or deletion of an account with the right to erasure.

26. Are there any leading or best practices of the controllers having responded that you would like to share?
-

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers
Question 5.6.

a. Name the issue(s) identified and briefly describe it.
For some data controllers, personal data subject to an Article 17 erasure request is deleted from the databases in use but not deleted from backups.

b. Which provision(s) of the GDPR (or national laws) does this concern?
The GDPR does not contain concrete requirements for the processing of the requests for erasure; the process falls within the organizational discretion of the controller. However the data controllers are responsible for a fair and lawful processing of the data according to GDPR Article 5; GDPR Article 32 (1) also explains that "the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: […] "(b) the ability to ensure the ongoing confidentiality".

c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
-

d. What are differences that you have encountered between controllers in your Member State?

-

e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?
When processing a request for erasure, data controllers, data controllers may delete the databases in use but not deleted from backups but they should implement additional measures to guarantee the security / confidentiality of the data which can include (depending on the context and the functioning of the backup system):
- the implementation of a deletion log that will allow database administrators to automatically delete data during backup restorations (this log must also comply with the data minimization principle).
- the limitation of the use of backup to no other purpose than restoring a technical environment.
- the performance of a risk and impact analysis on procedures and data protection to demonstrate to the supervisory authority that immediately deleting backup data is technically impossible; and document the security procedures and policies for this data (location, encryption, etc.).

28. Are there any leading or best practices of the controllers having responded that you would like to share?
Question 5.1.

A good practice noted by a data controller is that it also requires the external hosting providers to comply with ISO 27001 standards. Control 8.10 of this standard actually requires organisations to delete the data once it is no more needed.

Question 5.3.

A good practice noted by a data controller is when the technical deletion process is handled by the user management software that interacts with the user front ends (i.e. the website), the administration tool front-end used by the customer service agents and the actual databases.
Question 5.5.

A data controller explains that when being erased, the data stored in the database is replaced by random character strings so as not to destroy records in the database and avoid a structural impact on the database.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

Guidance "Le droit à l'effacement" can be found here after: https://cnpd.public.lu/fr/particuliers/vos-droits/droit-oubli.html (FR).
In July 2024 the CNPD published a general guidance on the right to erasure. This guidance, made of a written description and a video aimed at a large public, focuses on the essential points of the right to erasure (situations when the data subject can request the erasure of his data with examples, limitations of the right to erasure, how to send a request, the time limits to respect and the costs of such requests). It also explains that the data subjects also have the right to send an access request to the Police, the State Intelligence Service, the National Security Authority, the Army, the Financial Intelligence Unit and the Customs and Excise Administration (which is regulated by a specific national Act that transposes the « law enforcement directive » (EU directive 2016/680)).

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.

Apart from the element described under point 29, the CNPD has been taking action to prompt data controllers to respect the right to erasure through different levers:

- The handling of complaints filed with the CNPD and the request to follow remedial actions
- The answering to questions data controllers / data subjects may have with the department in charge in the CNPD
- The promotion of compliance with the issuance of the CNPD own certification scheme ((GDPR-CARPA) that encompasses the right to erasure (https://cnpd.public.lu/en/professionnels/outils-conformite/certification.html)) and the accreditation of certification bodies (that are in charge of reviewing the implementation of the criteria of the CNPD's and other certification schemes that include the right to erasure by the data controllers and processors).
- The training of personal involved or interested in data protection through regular training and online training platform (an interactive tool named DAAZ, aimed at a broad public, was created by the CNPD (see the dedicated website here after: https://cnpd.public.lu/en/professionnels/outils-conformite/daaz.html)).

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?

Since 2018, we have recorded annual complaints, among which a relatively important proportion related to the right to erasure (Article 17 GDPR). The figures are as follows:

	Number of complaints	Percentage compared to the total of complaints
2018	68	15%
2019	125	20%
2020	121	25%
2021	118	23%
2022	96	20%
2023	65	11%
2024	88	17%

Over the 2018–2024 period, we can notice:

- around 681 complaints related to the right to erasure (19% of all the complaints received);
- the highest percentage related to the right to erasure in 2020 (25%), and the lowest in 2023 (11%).

1. Evolution

- Between 2018 and 2020, there was a clear increase of complaints related to the right to erasure received per year (from 68 to 121 cases). The initial increase (2018–2020) probably reflects growing awareness of GDPR rights, in particular the right to erasure, shortly after its entry into force.
- From 2021 onwards, the percentage of complaints decreased before slightly increasing again in 2024. The decline may indicate either better compliance by controllers or improved internal handling of erasure requests.

2. Handling of complaints by the "Complaints" Department

Most complaints regarding Article 17 concern delays or refusals by controllers to erase personal data.

In many cases, the intervention of the CNPD consisted in reminding controllers of their obligations and ordering erasure where justified.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).
The respondents will be informed when the European report will be published to prompt them to follow the recommendations of the CEF.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes:

If "Yes", please specify: *(please select one or more answers)*

a. More online guidance: No (not planned at this stage)
b. Online or remote training sessions: Yes. Integration of the feedback of the CEF in the coming training sessions provided by the CNPD.
c. Conferences organised: Communication of the results of the CEF when the European report will be published (on the CNPD website, through conferences…)
d. Others: please specify: Reuse of the results/lessons learned of the CEF during the next CNPD's workshops (Daprolab - CNPD's Open Data Protection Laboratory). These are workshops for the exchange of ideas, interpretations, points of view on a specific subject between data protection professionals. The subject of the workshop is defined in advance and discussed between the participants. The participants compare their decisions, positions, points of view, ideas with other participants in order to obtain feedback on the choices they made. The CNPD acts as moderator and mediator of these meetings.

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

b. Yes: Yes

Some respondents explain that they would like to get new guidelines clarifying the expectations and opinions of the CNPD and/or the EDPB at organizational and technical levels (e.g. how certain procedures are expected to work, what aspects to pay attention to when implementing them, etc.).

Some data controllers explained that they wanted further explanations on Article 17 (2) GDPR (for example on how to inform the other data controllers and processors taking account of available technology and implementation costs with "reasonable efforts") and more detailed guidelines on the exemptions established by Article 17 (3) GDPR.

In our opinion, awareness raising could also be focused on persons who have no / limited knowledge about data protection. To this purpose, the CNPD already launched an interactive tool named DAAZ (see point 30 here above) that uses easily understandable language and practical cases and is aimed at small/medium sized organisations but also at individuals.

35. Are there any other observations that you would like to share?

No additional observations to be shared.

LV SA

Name of Supervisory Authority: Data State Inspectorate of Latvia (DSI)

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding: DSI answer: fact finding only.
b. Fact finding + determining follow-up action based on the results:
c. New formal investigation[39]:
d. Ongoing investigation:

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? DSI answer: No
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. DSI answer: No
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? DSI answer: No. Information will be used only for educational (for example, prepare some explanation to controllers) purposes.

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
DSI answer: yes.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
DSI answer: we used all questions and options of the consolidated questionnaire.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?
DSI answer: N/A

Part I - Information about the controllers addressed

6. How many controllers did you contact?
DSI answer: anonymous questionnaire were sent out to ministries and different associations (private sector) to share information to other authorities and companies that are members of those associations.

[39] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

7. Out of the contacted controllers, how many controllers responded?

*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

DSI answer: 155

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

DSI answer: based on our experience public sector are more open to participate on anonymized questionnaires than private sector.

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 148
b. Private sector: 7
c. Other:

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector: 27 responding controllers
b. Health sector: 4 responding controllers
c. Social sector: 7 responding controllers
d. Insurance sector: 0 responding controllers
e. Finance sector: 2 responding controllers
f. IT sector: 2 responding controllers
g. Retail sector: 0 responding controllers
h. Logistics sector: 0 responding controllers
i. Public transportation: 0 responding controllers
j. Telecommunications: 3 responding controllers
k. Postal services: 0 responding controllers
l. Advertising sector: 0 responding controllers
m. Entertainment sector: 7 responding controllers
n. Information / journalism sector: 1 responding controllers
o. Scientific / historical research: 2 responding controllers
p. Credit scoring agency: 0 responding controllers
q. Public utility/infrastructure provider (e.g. energy): 0 responding controllers
r. Housing industry: 2 responding controllers
s. Manufacturing: 0 responding controllers
t. Consulting: 0 responding controllers
u. Public administration: 129 responding controllers
v. Other (please specify):

11. Please specify the category in which the responding controllers fall[40]:

a. Micro enterprise: 0 responding controllers

[40] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

b. Small enterprise: 0 responding controllers
c. Medium-size enterprise: 7 responding controllers
d. Large enterprise (more than 250 employees): 0 responding controllers
e. Non-profit organisation: 1 responding controllers
f. Ministry: 13 responding controllers
g. Local authority: 70 responding controllers
h. Administrative authority/agency/office (e.g. job center): 47 responding controllers
i. School/university/educational institution: 17 responding controllers
j. Other (please specify):

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers: 19
b. Customers: 89
c. Contractors: 51
d. Job applicants: 115
e. Employees: 80
f. Applicants (for public services): 115
g. Citizens (for public sector): 115
h. Patients: 4
i. Other (please specify): [*to be completed*]

12.b. According to the responding controllers, are those data subjects also:

a. Children: 99
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 73
c. Non applicable: 45

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: 17
b. 101 – 1 000: 43
c. 1 001 – 10 000: 29
d. 10 001 – 100 000: 40
e. 100 001 – 500 000: 10
f. 500 001 – 1 000 000: 6
g. > 1 000 000: 10

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 144
b. Payment data: 73
c. Identification data: 140
d. Marketing data: 11
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 64

f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 57
g. Other, please specify: 8

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years - Yes

☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	126	132	129
1 – 10	27	20	23
11 – 50	1	2	2
51 – 100	0	0	0
101 – 500	1	1	1
more than 500	0	0	0

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0			

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

DSI answer: all controllers provided figures for this question

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years- Yes

☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding*

controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).

	2024*	2023	2022
0%	142	141	139
10%	3	5	4
20%	0	0	0
30%	0	0	0
40%	0	0	1
more than 50%	10	9	11

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?

☐ Yes

☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
DSI answer: all controllers provided figures for this question

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years - Yes

☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	2023	2022
0%	146	147	144
10%	4	3	6
20%	0	1	1
30%	0	0	0
40%	1	0	0
more than 50%	4	4	4

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
DSI answer: all controllers provided figures for this question

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 4
b. Customers: 21
c. Contractors: 8

d. Job applicants: 8
e. Employees: 11
f. Applicants (for public services): 0
g. Citizens (for public sector): 36
h. Patients: 2
i. Other:

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): Yes
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: Yes

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
DSI answer: Yes, considering that 93% of the controllers responding to this questionnaire are from public sector, in our opinion, the results are consistent.

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
c. Average Yes
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?
DSI answer: considering that 93% of the controllers responding to this questionnaire are from public sector, we didn't identify any significant differences.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it. **Lack of knowledge of the internal procedure for handling requests under Article 17 GDPR**; in some cases, respondents were unaware of such a procedure. Additional challenge: many respondents were from the public sector,

where requests under Article 17 GDPR are often not applicable due to legal obligations to process data for specific public purposes.

b. Which provision(s) of the GDPR (or national laws) does this concern? Article 17 GDPR – Right to erasure, in conjunction with relevant national laws providing exemptions for public authorities when processing data for statutory tasks.
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers? Lack of awareness/training on the procedure for handling Article 17 GDPR requests; legal restrictions in the public sector limit applicability, making controllers less familiar with practical implementation.
d. What are differences that you have encountered between controllers in your Member State? Considering that 93% of the controllers responding to this questionnaire are from public sector, we didn't identify any differences.
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)? Awareness campaigns that includes training and guidance on Article 17 procedures for controllers, including clear explanation of exemptions and legal limitations.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?
DSI answer: N/A

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).
DSI answer: N/A

24. Are there any leading or best practices of the controllers having responded that you would like to share?
DSI answer: N/A

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.
DSI answer: N/A

26. Are there any leading or best practices of the controllers having responded that you would like to share?
DSI answer: N/A

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers
DSI answer: N/A

28. Are there any leading or best practices of the controllers having responded that you would like to share?
DSI answer: N/A

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?
DSI answer: We have published general guidance for data subjects how they can exercise their right according to Article 17) GDPR (1) and the right to erasure when using online platforms (including social media) (2). (1) https://www.dvi.gov.lv/lv/jaunums/dviskaidro-vai-man-ir-tiesibas-lugt-dzest-datus-tikt-aizmirstam-ja-personas-dati-vairs-nav-nepieciesami and (2) https://www.dvi.gov.lv/lv/jaunums/dviskaidro-tiesibas-uz-savu-personas-datu-dzesanu-no-publiskas-vides . Available only in Latvian.
The DSI have issued general guidance for controllers what they need to take into account when reviewing data subject request (including according to article 17 GDPR) Available only in Latvian: https://www.dvi.gov.lv/lv/jaunums/dviskaidro-kas-jaievero-parzinim-izskatot-datu-subjekta-pieprasijumu

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.
DSI answer: N/A

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?
DSI answer: Since the entry into force of the GDPR, the DSI has received complaints and questions from data subjects relating to the right to erasure, for example concerning marketing emails, social media content and other online platforms. We don't maintain statistics on the number or proportion of such complaints compared to other complains received.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).
DSI answer: In 2026 we plan to issue more targeted guidance on Article 17 procedures for controllers, including clear explanation of exemptions and legal limitations.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes: Yes
If "Yes", please specify: *(please select one or more answers)*
   a. More online guidance: Yes
   b. Online or remote training sessions: Yes
   c. Conferences organised:
   d. Others: please specify:

b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

c. Yes: It would be useful to develop additional materials on the right to erasure, for example, a dedicated Q&A document addressing common scenarios, short guidance notes with practical use cases and clear infographics to help both controllers and data subjects understand the scope, limitations and procedures under Article 17 GDPR. Such resources would support consistent interpretation and application across sectors, especially in areas where exemptions apply.
d. No:

35. Are there any other observations that you would like to share?
DSI answer: N/A

MT SA

Name of Supervisory Authority: Maltese SA

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding: Yes
b. Fact finding + determining follow-up action based on the results
c. New formal investigation[41]
d. Ongoing investigation

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? no
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. no

- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how?

Rather than having an impact on our enforcement activities, this Office is using the results as a gauge on how organisations comply with the right of erasure in practice.

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.

The same questionnaire for all controllers was used.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.

a) The following questions were not included:
1.1 asking for the identification details of the controller,

3.4 and 3.8 from the 'Case Scenarios' section where detailed information was specifically requested, in order to keep the questionnaire as user friendly as possible and thus encourage a good number of responses.
b) No changes in wording which may have a significant effect on the results obtained were effected.

[41] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?

No other comments/remarks

Part I - Information about the controllers addressed

6. How many controllers did you contact?

100

7. Out of the contacted controllers, how many controllers responded?

*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*

14

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

The main reason is possibly lack of resources

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector
b. Private sector: Yes
c. Other:
    h. If so, what were the other sectors?

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector
b. Health sector: 2 responding controllers
c. Social sector
d. Insurance sector: 1 responding controller
e. Finance sector: 5 responding controllers
f. IT sector: 1 responding controller
g. Retail sector: 1 responding controller
h. Logistics sector
i. Public transportation
j. Telecommunications
k. Postal services
l. Advertising sector
m. Marketing services
n. Entertainment sector
o. Information / journalism sector
p. Scientific / historical research
q. Credit scoring agency
r. Public utility/infrastructure provider (e.g. energy)

s. Housing industry
t. Manufacturing: 1 responding controller
u. Consulting: 1 responding controller
v. Public administration
w. Other (please specify): Hospitality: 1 responding controller

Wide ranging across different sectors: 1 responding controller

11. Please specify the category in which the responding controllers fall[42]:

a. Micro enterprise
b. Small enterprise: 2 responding controllers
c. Medium-size enterprise: 7 responding controllers
d. Large enterprise (more than 250 employees): 5 responding controllers
e. Non-profit organisation
f. Ministry]
g. Local authority
h. Administrative authority/agency/office (e.g. job centre)
i. School/university/educational institution
j. Other (please specify)

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers
b. Customers: 11 responding controllers
c. Contractors
d. Job applicants
e. Employees: 2 responding controllers
f. Applicants (for public services)
g. Citizens (for public sector)
h. Patients: 1 responding controller
i. Other (please specify)

12.b. According to the responding controllers, are those data subjects also:

a. Children: 2 responding controllers
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 7 responding controllers
c. Non applicable

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100
b. 101 – 1 000: 3 responding controllers
c. 1 001 – 10 000: 4 responding controllers
d. 10 001 – 100 000: [2 responding controllers]
e. 100 001 – 500 000: 5 responding controllers
f. 500 001 – 1 000 000
g. > 1 000 000

[42] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 14 responding controllers
b. Payment data: 12 responding controllers
c. Identification data: 12 responding controllers
d. Marketing data: 4 responding controllers
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 6 responding controllers
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 1 responding controller
g. Other, please specify: [Occupation and Income: 1 responding controller

a. Domicile and residency: 1 responding controller
Due Diligence: 1 responding controller

a. Financial Information: 1 responding controller
Transaction Data: 1 responding controller
Data on personal possessions linked to insured persons: 1 responding controller]

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☒ 1 year Yes
☐ 3 years
☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	9 responding controllers	6 responding controllers	5 responding controllers
1 – 10	5 responding controllers		
11 – 50			
51 – 100			
101 – 500			
more than 500			

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0	NA	NA	NA

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
Nil, all controllers provided figures

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☒ 1 year- Yes
☐ 3 years
☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	**2023**	**2022**
0%	14 responding controllers	7 responding controllers	7 responding controllers
10%			
20%			
30%			
40%			
more than 50%			

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?
☐ Yes
☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
Nil, all controllers provided figures.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☒ 1 year - Yes
☐ 3 years
☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	14 responding controllers	7 responding controllers	7 responding controllers
10%			
20%			
30%			
40%			
more than 50%			

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
Nil, all controllers provided figures

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: [2 responding controllers]
b. Customers: [5 responding controllers]
c. Contractors
d. Job applicants
e. Employees: [1 responding controller]
f. Applicants (for public services)
g. Citizens (for public sector)
h. Patients
i. Other: [Former employees: 1 responding controller]

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: Yes

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
It is difficult to give a definite answer considering that the responding controllers were not clearly identified and the SA opted for anonymous responses.

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High ☒

b. High
c. Average
d. Low
e. Very low
f. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

No such difference was identified.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

No such issues or challenges were identified.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

Yes, a best practice worth sharing is in relation to the development of specific internal guidelines regarding the right to erasure. Whilst all the responding controllers have issued internal guidelines on the matter and how to deal with such a request, one of the responding controllers goes a step further. Apart from providing its employees with thorough documentation in the company's internal 'Data Protection Policy' it also provides a checklist to be followed which includes exceptions and timeframes.

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).
No such issues or challenges were identified.

24. Are there any leading or best practices of the controllers having responded that you would like to share?
Yes, a best practice worth mentioning concerns the implementation of article 17(2) if the personal data was made public. Whilst all responding controllers take all the necessary steps to inform controllers that a data subject has requested the erasure of his/her personal data, one of the controllers has specific processes in place in this regard which ensures that all such actions are properly documented and traceable.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.
No such issues or challenges were identified.

26. Are there any leading or best practices of the controllers having responded that you would like to share?
All practices indicated by the responding controllers are very similar in nature and method and as such there is no particular practice which stands out.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers
A possible issue which was identified in the evaluation of this section on the questionnaire is that out of all the responding controllers only one complies and adheres with technical standards when it comes to erasing personal data. The same controller is also the only responding controller which uses technical tools to process Art 17 GDPR requests

28. Are there any leading or best practices of the controllers having responded that you would like to share?
In general, all practices indicated by the responding controllers are very similar in nature and method and as such there is no particular practice which stands out.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

Yes, IDPC has published such guidance on its website in the form of a fact sheet. It is generic in nature and targeted towards data subjects. It explains that the 'Right to

erasure' is one of the rights found in 'Chapter III' of the GDPR and provides a brief explanation and insight by enlisting the instances when it can be exercised. It also enlists the instances when the data controller can legitimately refuse to comply with a 'Right to erasure' request. This was published prior to the launch of the CEF and can be found via this link:

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

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.

Yes, actions towards controllers specifically concerning the right to erasure prior to the launch of CEF 2025 were taken. They take the form of an investigation following the lodging of a complaint by a data subject alleging a breach of article 17 by the controller. When these investigations indeed establish a breach of article 17 the Commissioner exercises his corrective powers in terms of article 58(2) of the GDPR to ensure that the complainant's data protection rights are fully safeguarded. If a controller fails to demonstrate to the satisfaction of the Commissioner that the exceptions raised in his refusal to erase the personal data of the complainant are justified, he is ordered to comply with the request of the complainant and permanently erase all personal data relating to the data subject in terms of article 58(2)(c).

The below link is an example of action taken towards a particular controller concerning the right of erasure and the outcome of such action:

https://idpc.org.mt/wp-content/uploads/2024/01/CDP_COMP_84_2023.pdf

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?

The number of complaints received regarding Art. 17 GDPR since the entry into force of the regulation amounts to 49. The number of complaints on this right is a growing number, year after year, however when compared to other complaints received by the SA the volume is much less.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).

Taking into account the results of this CEF and the fact that no significant problems could be identified together with the fact that the SA opted for anonymous responses, there isn't any specific action towards the controllers contacted currently being planned. However more information targeted towards controllers in general on our portal and possibly through other communication methods is considered.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes: ☒ - Yes

   If "Yes", please specify: *(please select one or more answers)*
   a. More online guidance: Yes
   b. Online or remote training sessions
   c. Conferences organised
   d. Others: please specify
   b.

b. No

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes
b. No: Yes

35. Are there any other observations that you would like to share?
No such other observations.

NL SA

Name of Supervisory Authority: Autoriteit Persoonsgegevens (AP)

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding:
b. Fact finding + determining follow-up action based on the results: Yes
c. New formal investigation[43]:
d. Ongoing investigation:

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? Partially. As the option for anonymous participation was provided, it was only possible to identify a portion of the responding controllers.
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. No, there are currently no plans to launch a formal investigation based on the results of the fact finding exercise.
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? No, it will not impact the enforcement activities of Autoriteit Persoonsgegevens (AP), the Dutch Data Protection Authority (DPA).

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
Yes, the same questionnaire was used for all controllers. There were no differences in the content of the questions.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
The same questionnaire was used in its entirety; no questions were omitted. The only difference was the inclusion of an option for respondents to complete the questionnaire anonymously, which did not affect the content of the questions themselves.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?
As a general remark, the AP received a significant number out-of-office-replies during the response period, which may have impacted its ability to reach certain individuals. AP also notes that, in several cases, the data protection officer (DPO) listed in the national register was no longer employed by the controller. In such instances, the

[43] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

contact details had not been updated, although it is the responsibility of the organisation to notify any changes to ensure that the register remains accurate and up to date.

Part I - Information about the controllers addressed

6. How many controllers did you contact?
A total of 286 controllers were contacted as part of this fact finding activity. This number does not include controllers whose contact details resulted in an error.

7. Out of the contacted controllers, how many controllers responded?
*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*
A total of 35 controllers responded effectively to the questionnaire.

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?
One possible explanation for the gap in the amount of responses is the timing of when the questionnaire was sent, which coincided with a holiday period. The AP received a substantial number of out-of-office replies, which may have contributed to the low response rate. Additionally, some organisations or data protection officers may have been reluctant to participate due to concerns about potential follow-up or enforcement actions. The AP also received feedback indicating that, in certain cases, individuals declined to complete the questionnaire on principle, citing previous negative experiences with government led surveys. Furthermore, it is possible that some controllers did not complete the questionnaire due to the length and/or complexity of the questionnaire.

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 17 responding controllers
b. Private sector: 18 responding controllers
c. Other: N/A
    i. If so, what were the other sectors?

Of the responding controllers, approximately 49% were from the public sector and 51% from the private sector.

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector: 1 responding controller
b. Health sector: 9 responding controllers
c. Social sector: 4 responding controllers
d. Insurance sector: 0 responding controllers
e. Finance sector: 3 responding controllers
f. IT sector: 1 responding controller
g. Retail sector: 0 responding controllers
h. Logistics sector: 0 responding controllers
i. Public transportation: 0 responding controllers

j. Telecommunications: 1 responding controller
k. Postal services: 0 responding controllers
l. Advertising sector: 0 responding controllers
m. Marketing services: 0 responding controllers
n. Entertainment sector: 0 responding controllers
o. Information / journalism sector: 0 responding controllers
p. Scientific / historical research: 1 responding controller
q. Credit scoring agency: 0 responding controllers
r. Public utility/infrastructure provider (e.g. energy): 2 responding controllers
s. Housing industry: 0 responding controllers
t. Manufacturing: 0 responding controllers
u. Consulting: 1 responding controller
v. Public administration: 4 responding controllers
w. Other (please specify): 8 responding controllers

11. Please specify the category in which the responding controllers fall[44]:

a. Micro enterprise: 3 responding controllers
b. Small enterprise: 5 responding controllers
c. Medium-size enterprise: 6 responding controllers
d. Large enterprise (more than 250 employees): 9 responding controllers
e. Non-profit organisation: 4 responding controllers
f. Ministry: 0 responding controllers
g. Local authority: 6 responding controllers
h. Administrative authority/agency/office (e.g. job center): 0 responding controllers
i. School/university/educational institution: 0 responding controllers
j. Other (please specify): 2 responding controllers

12.a. Which category of data subjects is <u>mainly</u> concerned by the processing activities of the responding controllers?

a. Potential customers: 0 responding controllers
b. Customers: 10 responding controllers
c. Contractors: 0 responding controllers
d. Job applicants: 1 responding controller
e. Employees: 7 responding controllers
f. Applicants (for public services): 0 responding controllers
g. Citizens (for public sector): 7 responding controllers
h. Patients: 5 responding controllers
i. Other (please specify): 5 responding controllers

12.b. According to the responding controllers, are those data subjects also:

a. Children: 12 responding controllers

[44] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en?prefLang=nl

b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 16 responding controllers
c. Non applicable: 18 responding controllers

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: 3 responding controllers
b. 101 – 1 000: 5 responding controllers
c. 1 001 – 10 000: 6 responding controllers
d. 10 001 – 100 000: 14 responding controllers
e. 100 001 – 500 000: 3 responding controllers
f. 500 001 – 1 000 000: 0 responding controllers
g. > 1 000 000: 4 responding controllers

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 31 responding controllers
b. Payment data: 16 responding controllers
c. Identification data: 21 responding controllers
d. Marketing data: 5 responding controllers
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 16 responding controllers
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 4 responding controllers
g. Other, please specify: 4 responding controllers

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years

☐ other, specify: Controllers were asked to provide figures for three years: 2022, 2023 and 2024. Providing data for 2024 was mandatory while figures for 2022 and 2023 were optional.

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	17	16	16

1 – 10	14	6	5
11 – 50	2	0	0
51 – 100	1	0	0
101 – 500	0	0	0
more than 500	1	0	0

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0			

Please see answer to the question above.

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
For the year 2023, a total of 13 controllers did not provide any figures. For the year 2022, 14 controllers did not provide any figures.

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 1 year
☐ 3 years
☐ other, specify: Controllers were asked to provide figures for three years: 2022, 2023 and 2024. Providing data for 2024 was mandatory while figures for 2022 and 2023 were optional.

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*
The AP notes that while the responses indicate that most erasure requests are not rejected and thus granted, more research is needed, such as follow-up questions to controllers who participated in the questionnaire, to properly understand these figures. In addition, the question arises whether it was necessary for organisations to retain data for a certain period until removal is requested by a data subject if erasure requests are generally granted by the responding controllers. However, the topic of retention falls outside the scope of this activity and requires further investigation before any conclusions can be drawn.

	2024*	2023	2022
0%	28	16	17
10%	3	1	0
20%	0	0	0
30%	0	0	0
40%	0	0	0
more than 50%	4	3	3

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?

☐ Yes

☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

This question is not applicable for the AP, as the AP did not carry out any enforcement actions.

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

15 controllers did not provide any figures for 2022 and 2023. For the year 2024, all controllers provided figures.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years

☐ other, specify: Controllers were asked to provide figures for three years: 2022, 2023 and 2024. Providing data for 2024 was mandatory while figures for 2022 and 2023 were optional.

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

The AP notes that a possible explanation for the low percentage of erasure requests that were linked to Article 21 GDPR is that data subjects may generally be unfamiliar with the right to object under Article 21 GDPR and therefore do not submit a request related thereto.

	2024	2023	2022
0%	27	18	16
10%	4	0	0
20%	0	0	0
30%	0	0	0
40%	1	0	0
more than 50%	3	1	2

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

For the year 2022, 17 controllers did not provide any figures. For the year 2023, 16 controllers did not provide any figures. For the year 2024, all controllers provided figures.

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 1 responding controller
b. Customers: 8 responding controllers
c. Contractors: 1 responding controller
d. Job applicants: 7 responding controllers
e. Employees: 4 responding controllers
f. Applicants (for public services): 1 responding controller
g. Citizens (for public sector): 5 responding controllers
h. Patients: 3 responding controllers
i. Other: 16 responding controllers

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): Yes
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: Yes

Both groups are overrepresented: Parents or guardians on behalf of children accounted for approximately 40% of the requests. Vulnerable subjects accounted for approximately 60% of the requests.

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?

The majority of responses were received from the health sector, which aligns with the overrepresentation of requests made by parents or guardians on behalf of children (40%) and vulnerable subjects (60%). These groups are commonly encountered in healthcare settings, where the nature of the services often involves the processing of personal data relating to children and vulnerable individuals. This correlation is further reflected in the broader trends the AP observes in complaints. Nearly 30% of all complaints the AP receives relate to the exercise of data subject rights under the GDPR, with the right to erasure accounting for approximately 13% of those complaints. This supports the idea that these rights are particularly relevant in sectors such as health, where sensitive data and special categories of data are frequently processed. Additionally, the AP notes that a significant number of controllers did not provide figures for the years 2022, 2023, and/or 2024, which limits the completeness of the data over time. Regarding the outcomes of erasure requests, it appears that only a small number of requests were rejected, suggesting that the right to erasure is generally being granted. Interestingly, one controller reported receiving over 500 erasure requests, which is considerably higher than the majority, who reported receiving between 1 and 10 requests. While the specific sector of this outlier respondent is unknown, the volume further highlights the variability depending on processing activities. In conclusion, the data shows a consistent pattern when viewed in relation to the nature of the health sector and its data processing practices.

However, some inconsistencies in reporting and missing data across certain years limit the overall comparability.

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
c. Average
d. Low
e. Very low
f. Too diverse levels to qualify

The AP notes that due to the low number of respondents the outcome of the questionnaire is not representative of the general practice of erasure requests. Of the controllers who did participate in the survey, the general impression from their responses is that most responding controllers have an average to high level of compliance. This is because, for example, most have a process in place to handle erasure requests, with some being more extensive than others.

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

The number of respondents in the public and private sector is roughly the same (about 49% public, 51% private). The AP noticed a significant difference in the maturity in how procedures are arranged; some controllers have a comprehensive internal procedure for handling erasure requests, while some have less or none because, for example, such requests are less frequent. However, more research is needed to get a good understanding of the (different) types of controllers and sectors in which this occurs.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.

17% of respondents state that they do not have developed specific internal documents regarding the right to erasure or follow a defined process to handle such requests. The lack of such documents or process may lead to lack of communication with the data subject and/or delay in the processing of the requests.
About half of respondents indicate that they do not train their staff regarding erasure requests. This creates a risk that a request for erasure may not (quickly) be recognised as a request based on Art. 17 of the GDPR. For example, because the request was worded differently in an email that was initially about a different subject.

37% of respondents state that the procedure for implementing Art. 17 GDPR is not regularly reviewed and adjusted. If this is not reviewed/ evaluated regularly then the procedure may become outdated.

b. Which provision(s) of the GDPR (or national laws) does this concern?
Articles 12, 17, 19, 77 of the GDPR.

c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
A possible explanation is that some respondents receive few or no erasure requests, which means that they hardly come in contact with these requests.

d. What are differences that you have encountered between controllers in your Member State?
The AP notes a difference in maturity in process and experience with data subject rights between responding controllers. As previously stated, some controllers may receive less erasure requests. This may be because they are smaller, or it may depend on the sector in which they operate.

e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?
Based on the results of the questionnaire it is difficult to determine whether the issues identified are truly related to organisational size or linked to a specific sector due to the low responses. These findings could serve as a starting point for further research, for example into sector-specific differences or the impact of organizational size. Such follow-up research could, in turn, inform more targeted actions on our part, such as providing focused awareness and tailored guidance for particular sectors or types of organizations.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?
No

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).

The submitted responses show that not every controller receives a request containing both a request for access and a request for erasure. Generally, both requests are handled separately and in conjunction, with the request for access being processed first and the request for erasure being assessed subsequently before a decision is made.

24. Are there any leading or best practices of the controllers having responded that you would like to share?
No

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.
Erasure requests are sometimes submitted verbally or by phone. The questionnaire does not address how these verbal requests are documented, so no insight was obtained into this.

The AP notes that the majority of respondents send an acknowledgement of receipt of erasure request to the data subject containing information about (expected) processing time of the handling of the request.

26. Are there any leading or best practices of the controllers having responded that you would like to share?
No

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers
Although many controllers indicate that they comply with or adhere to technical standards when it comes to erasing personal data, a majority of the respondents do not use such standards.
In most cases, personal data is deleted. It happens to a lesser extent that a controller uses anonymization to comply with an erasure request. A respondent indicates that erasure requests generally involve actual removal from its systems. In certain cases, such as for internal quality analyses, policy development or scientific research, personal data is anonymised. In the event of anonymization, identifying data is structurally deleted or irreversibly modified, so that the data subject is no longer identifiable. The respondent indicates that this approach is only applied when the data is no longer needed for individual case handling, but is still valuable for aggregated use. In another case, a different respondent indicates that in some cases it is not possible to permanently delete personal data. Thus, an anonymization technique is used. This also applies if the data is part of a larger whole. Through anonymization, the context is preserved but the data cannot be traced back to an individual person.
Often controllers also remove personal data from backups or different data bases, but for some this is (technically) not possible with the software they use. However, it seems that controllers are generally aware that data is also stored in backups. If a recovery of the system is needed, this may have an effect on previously executed removal requests. For example, a respondent indicates that ICT is involved in erasure requests for this reason.

28. Are there any leading or best practices of the controllers having responded that you would like to share?

Below are some practices of respondents that may contribute to the handling of erasure requests.

- Deletion of data in production environment with a notification that if a backup needs to be restored, the specific data has to be removed again. Delete backup data permanently in accordance with a(n) (internal) backup retention policy.
- Involve ICT in erasure requests if a system restore affects previously executed erasure requests.
- When executing erasure requests, delete data from source systems and in addition consult with directly involved staff for, for example, deletion of relevant data from mailbox.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

The AP provides various forms of support and information related to the right to erasure:

• The website of AP contains accessible information about the different data subject rights under the GDPR, including the right to erasure, and how these rights can be invoked.
• The AP also offers model letters that individuals can use to exercise their rights.
• In addition, the AP holds consultation hours during which both individuals and organisations can contact us with questions or request advice regarding data protection and the application of GDPR rights, including the right to erasure.

Some guidance, such as factsheets and information on the website, is provided below with (if possible) a date when this information was published. In most cases, the information is also available in English.

General guidance

Right to erasure

General information on the right to erasure.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacyrechten-avg/recht-op-gegevens-verwijderen
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/privacy-rights-under-the-gdpr/right-to-erasure

Model letter to request controller to delete personal data, 14 June 2024

Data subjects can request controllers to delete their personal data with the help of a model letter provided by the AP.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/documenten/voorbeeldbrief-verwijdering

Question of the month regarding right to erasure

URL (NL): https://www.autoriteitpersoonsgegevens.nl/vraag-van-de-maand/ik-wil-dat-een-organisatie-mijn-gegevens-verwijdert-wat-kan-ik-doen

Information on having data removed
URL (NL): https://www.autoriteitpersoonsgegevens.nl/jij-en-jouw-online-gegevens/jouw-privacyrechten/jouw-gegevens-laten-verwijderen
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/you-and-your-online-data/your-privacy-rights/having-your-data-removed

Overview of GDPR guidelines
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/internationaal/internationale-samenwerking/overzicht-van-avg-guidelines
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/international/international-cooperation/overview-of-gdpr-guidelines

Targeted guidance

Regarding health data
Information on exercising data subject rights regarding health data that care providers include in a (medical) file.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/gezondheid/gezondheidsgegevens-in-een-dossier/rechten-bij-het-dossier-met-gezondheidsgegevens
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/health/health-data-in-a-file/rights-regarding-the-health-data-file

Regarding law enforcement, border control
Data subject rights with police, special investigation services and judicial authorities
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/politie-en-justitie/politie-bijzondere-opsporing-en-justitie/uw-privacyrechten-bij-politie-bijzondere-opsporing-en-justitie
URL (EN): 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

Europol
Information on Europol including information about exercising data subject rights, such as the right to erasure.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/politie-en-justitie/europol-eurojust-en-eom/europol#uw-rechten-bij-europol
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/police-and-judicial-authorities/europol-eurojust-and-eppo/europol

Model letter to request Europol to correct or delete personal data, 4 August 2024
Model letter data subjects can use to request Europol to correct or delete personal data.

URL (NL): https://www.autoriteitpersoonsgegevens.nl/documenten/voorbeeldbrief-correctie-of-verwijdering-europol

Europol, guide for exercising data subjects rights, 8 August 2024
Guide describing modalities for exercising privacy rights regarding personal data collected, held or otherwise processed by Europol.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/documenten/europol-guide-for-exercising-data-subjects-rights
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/documents/europol-guide-for-exercising-data-subjects-rights

Schengen Information System (SIS)
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/politie-en-justitie/europese-informatiesystemen/schengen-informatiesysteem-sis
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/police-and-judicial-authorities/european-information-systems/schengen-information-system-sis#your-rights-if-you-are-in-sis

Model letter correction or deletion Schengen Information System (SIS), 12 February 2024
URL (NL): https://www.autoriteitpersoonsgegevens.nl/documenten/voorbeeldbrief-correctie-of-verwijdering-sis
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/documents/model-letter-correction-or-deletion-sis

Model letter mediation SIS, 12 February 2024
Data subjects can use a model letter to ask the AP to mediate in case they are not satisfied with the decision (response) to their (erasure) request regarding SIS.
URL(NL): https://www.autoriteitpersoonsgegevens.nl/documenten/voorbeeldbrief-bemiddeling-sis
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/documents/model-letter-mediation-sis

Exercising data subject rights Schengen Information System II, Visa Information System (VIS)
URL (EN): https://www.autoriteitpersoonsgegevens.nl/exercising-your-rights-sis-ii-vis

Eurodac
This page contains information on exercising privacy rights regarding Eurodac, a central database with fingerprints of asylum seekers and persons who have crossed the external borders of the Schengen area without a legal basis.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/politie-en-justitie/europese-informatiesystemen/eurodac
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/police-and-judicial-authorities/european-information-systems/eurodac

API data
Information on exercising privacy rights regarding API data (identity and flight data of passengers on board an aircraft).

URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/vervoer/reisgegevens/api-gegevens
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/transport/travel-data/api-data

Regarding passport and identity card

Rules for organisations for establishing identity
Rules for organisations for establishing identity including information about the possibility to establish identity without an identity document in the case a data subject wants to delete its account.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/voor-organisaties-regels-voor-vaststellen-identiteit
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/identification/passport-and-identity-card/for-organisations-rules-for-establishing-identity

Question of the month about whether it is allowed for hotels to make a copy of the passport of a data subject
URL (NL): https://www.autoriteitpersoonsgegevens.nl/vraag-van-de-maand/mag-een-hotel-een-kopie-maken-van-mijn-paspoort
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/question-of-the-month/is-a-hotel-allowed-to-make-a-copy-of-my-passport

Regarding social media, cookies, internet of things:

Publishing and removing personal data on the internet
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme-apparaten/persoonsgegevens-op-internet/persoonsgegevens-publiceren-en-verwijderen-internet
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/internet-and-smart-devices/personal-data-on-the-internet/publishing-and-removing-personal-data-on-the-internet

Question of the month regarding how data subjects can completely remove their data from social media
URL (NL): https://www.autoriteitpersoonsgegevens.nl/vraag-van-de-maand/hoe-kan-ik-mijn-gegevens-op-sociale-media-helemaal-verwijderen
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/question-of-the-month/how-can-i-completely-remove-my-data-from-social-media

Cookies
Information on protecting privacy against cookies, including (automatically) erasing cookies and right to erasure of data.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme-apparaten/cookies/privacyrisicos-en-het-beschermen-van-uw-privacy-bij-cookies
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/internet-and-smart-devices/cookies/privacy-risks-and-protecting-your-privacy-when-accepting-cookies

Smart devices
Information on setting a smart device and how to remove data in case of replacement.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme-apparaten/internet-of-things/een-slim-apparaat-instellen
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/internet-and-smart-devices/internet-of-things/setting-a-smart-device

Connected vehicles
Information on privacy rights in case of connected vehicles.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/vervoer/connected-vehicles/connected-vehicles-en-privacy
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/transport/connected-vehicles/connected-vehicles-and-privacy

Regarding biometrics:

Biometrics
Rules for the use of biometrics, including information on the right to erasure.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/biometrie/regels-voor-gebruik-biometrie
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/identification/biometrics/rules-for-the-use-of-biometrics

Use of facial recognition (organisations)
Information on when facial recognition is allowed and what rules apply for organisations that want to use cameras with facial recognition.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/biometrie/gezichtsherkenning
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/identification/biometrics/facial-recognition

Facial recognition (data subjects)
Information for data subjects that have to deal with facial recognition, including privacy rights regarding this use.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/biometrie/krijgt-u-te-maken-met-gezichtsherkenning-dit-moet-u-weten
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/identification/biometrics/do-you-have-to-deal-with-facial-recognition-this-is-what-you-need-to-know

Facial recognition, legal framework (in Dutch)

The AP answers several frequently asked legal questions about the use of facial recognition.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/documenten/juridisch-kader-gezichtsherkenning

Camera use in and around the house
Information on camera use in and around the house. The page also mentions that people that are being filmed have privacy rights.
URL (NL): https://www.autoriteitpersoonsgegevens.nl/themas/cameratoezicht/cameragebruik-in-en-om-het-huis/cameras-bij-het-eigen-huis
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/themes/camera-surveillance/camera-use-in-and-around-the-home/cameras-in-your-own-home

Question of the month about whether it is allowed that the camera of the neighbours is filming a data subject, page last edited on 30 August 2024
URL (NL): https://www.autoriteitpersoonsgegevens.nl/vraag-van-de-maand/de-camera-van-mijn-buren-filmt-mij-als-ik-door-mijn-straat-loop-mag-dat
URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/question-of-the-month/the-camera-of-my-neighbours-is-filming-me-when-i-walk-the-street-is-that-allowed

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.
The AP has taken such actions. Often these are based on complaints that the AP receives, which may lead to the launch of a formal investigation. Below are some examples of actions that are published on AP's website that resulted in a fine for the controller. In other cases, the AP engages in fact-finding or informal interventions aimed at encouraging the controller to remove personal data. In this way, the AP ensures that individuals' rights are respected and that their data is deleted when appropriate.

(1) URL (NL): https://www.autoriteitpersoonsgegevens.nl/actueel/boete-voor-recruitmentbedrijf-om-negeren-verwijderverzoeken

URL (EN): https://www.autoriteitpersoonsgegevens.nl/en/current/fine-for-recruitment-company-for-ignoring-requests-for-removal

(2) URL (NL): https://www.autoriteitpersoonsgegevens.nl/actueel/boete-van-525000-euro-voor-locatefamilycom

URL (EN): https://www.autoriteitpersoonsgegevens.nl/actueel/boete-van-525000-euro-voor-locatefamilycom

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in

comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?
The AP has concrete figures available for the year 2024. In that year, the AP received a total of approximately 3,122 complaints. Of these, 954 complaints (around 30.6%) concerned data subject rights under the GDPR. This makes them the largest category of complaints the AP receives as a data protection authority. Specifically, 580 complaints (about 18.6% of the total, and 60.8% of complaints concerning data subject rights) relate to the right to erasure. The largest category within these complaints involves recurring issues in the context of business services. In many of these cases, there appears to be an overlap with the right to object under Article 21 of the GDPR, which allows individuals to object to the use of their personal data for direct marketing purposes. Another significant portion of the complaints the AP received concerns matters of an international nature. These often relate to business services and typically involve large online platforms or companies established in other EU Member States or outside the EU. These complaints may concern, for example, social media services or other digital service providers that operate across borders within or outside the EU.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).
The AP is not planning to take any action based on the results of this exercise other than reviewing the findings and check whether awareness about, or (additional) guidance on, the right to erasure is needed.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes:

If “Yes”, please specify: *(please select one or more answers)*

e. More online guidance:
f. Online or remote training sessions:
g. Conferences organised:
h. Others: please specify: Based on the results of this inquiry and the nature of the complaints received, the AP believes it would be beneficial to take further steps to raise awareness around the right of erasure. This could include providing more online guidance and potentially engaging more directly with organisations to increase understanding of the importance of this right. It may also be helpful to offer practical support to organizations on how to properly handle erasure requests. More consistent data collection on how the right of erasure is used, so it could help identify patterns and gaps. However, before doing so, a logical first step would be to potentially conduct a follow-up research to determine whether the issues are linked to organizational size or to a specific sectors. Should this follow-up research provide clear insights, the AP, and perhaps other SA’s as well, would then be in a position

to develop a more targeted awareness and tailored guidance for the relevant organisations and or sectors.

b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes: Yes, sector specific guidance with examples of typical scenarios. Case studies showing when erasure request should be honoured, when it can be rejected and how to communicate that clearly. EU-wide awareness campaigns. More coordinated positions or interpretative notes from the EDPB to support consistent application across the EU.
b. No:

35. Are there any other observations that you would like to share?

As mentioned earlier and in general, the AP notes that due to the low response, no conclusions can be drawn from this fact finding activity as, for example, further research is needed on some aspects. In addition, it is important to consider the possibility that organisations that comply less or not at all with the right to erasure did not participate in the questionnaire due to fear of possible enforcement action or other follow-up actions.

PL SA

Name of Supervisory Authority: The Personal Data Protection Office in Poland

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding + determining follow-up action based on the results:

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? Yes
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. No
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? Yes

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
We used the same questionnaire for all controllers.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
No changes.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?
No.

Part I - Information about the controllers addressed

6. How many controllers did you contact?2847

7. Out of the contacted controllers, how many controllers responded?
*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*
101

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

Yes. The main reasons for the discrepancy between the number of contacts and the number of responses received appear to be due to, among other things, limited organizational resources on the part of smaller public administration units and businesses, which lack dedicated data protection officers, as well as incorrect or outdated contact information (especially in the case of smaller local government units and private entities). The resulting response rate was approximately 3.5%, which is comparable to similar consultations conducted in previous years at the national level.

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 98
b. Private sector: 3
c.

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector 2
b. Social sector 1
c. Retail sector 1
d. Public administration: 90
e. Other (please specify): Institution/community center - 2 Social organization/non-governmental organization - 2 Social integration center/social assistance - 1 State archives/archival institution - 1 Sports and recreation center/local government auxiliary unit - 1

11. Please specify the category in which the responding controllers fall[45]:

a. Small enterprise: 3
b. Medium-size enterprise: 1
c. Large enterprise (more than 250 employees): 2
d. Non-profit organisation: 2
e. Local authority: 73
f. Administrative authority/agency/office (e.g. job center): 15
g. School/university/educational institution: 1
h. Other (please specify): Cultural institution - 2 Social integration center/assistance center - 1 Local government auxiliary unit - 1

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Customers: 5
b. Contractors: 1
c. Employees: 1
d. Applicants (for public services): 16
e. Citizens (for public sector): 73
f. Other (please specify): Beneficiares of social projects or programs - 2 Participants in cultural/sporting events - 1 Applicants/bidders in

[45] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

administrative proceedings - 1 Participants in competitions, training courses, or public consultations – 1

12.b. According to the responding controllers, are those data subjects also:

a. Children 71
b. Vulnerable subjects 74
c. Non applicable – marked in 22 replies.

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: 4
b. 101 – 1 000: 11
c. 1 001 – 10 000: 41
d. 10 001 – 100 000: 34
e. 100 001 – 500 000: 7
f. 500 001 – 1 000 000: 1
g. > 1 000 000: 3

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 95
b. Payment data: 80
c. Identification data: 88
d. Marketing data: 5
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 35
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 30
g. Other, please specify: Data on beneficiaries' activities - 2 Data on participation in events/recruitment - 1 Data on property status or financial situation in the context of social assistance - 1

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ other, specify: 1 year, but additionally 2023/2022 was requested only when the value "0" was reported for 2024.

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	2023	2022
0	82	82	79
1 – 10	8	3	5
11 – 50	0	0	0
51 – 100	0	0	0
101 – 500	2	2	2
more than 500	0	0	0

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	2024-2023	2024-2022
0	82	82	79

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
9 controllers.

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ other, specify: 1 year, but additionally 2023/2022 was requested only when the value "0" was reported for 2024.

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	2023	2022
0%	85	83	81
10%	0	0	0
20%	2	1	1
30%	0	0	0
40%	0	0	0
more than 50%	3	1	2

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?
☐ Yes
☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
11 controllers.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 1 year, but additionally 2023/2022 was requested only when the value "0" was reported for 2024.

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	85	83	83
10%	3	1	1
20%	0	0	0
30%	0	0	0
40%	2	0	0
more than 50%	0	0	0

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
11 controlers.

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 3
b. Customers: 3
c. Contractors: 3
d. Employees: 2
e. Applicants (for public services): 4
f. Citizens (for public sector): 7
g. Other: Beneficiaries of publicly funded projects - 1 Participants in local programs or activities - 1 Parties or participants in administrative proceedings - 1

18.b. Were the following groups over-represented in the requests received?

a. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: Yes

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Average

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).
24. Are there any leading or best practices of the controllers having responded that you would like to share?

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.
26. Are there any leading or best practices of the controllers having responded that you would like to share?

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers

28. Are there any leading or best practices of the controllers having responded that you would like to share?

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?
No

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.
No

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. No

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. No

35. Are there any other observations that you would like to share?

PT SA

Name of Supervisory Authority: Comissão Nacional de Proteção de Dados

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

Fact finding + determining follow-up action based on the results: Most cases
New formal investigation[46]: (for non-cooperating controllers)

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? Yes. All responding controllers were clearly identified, except in two cases where the entities attempted to remain anonymous in the form. However, due to the individualised survey links, identification was possible.
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. Yes. For non-cooperating controllers or those who submitted incomplete replies, cases were referred to inspection.
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? Yes. The results highlighted structural weaknesses:
  - lack of technical means for systematic deletion;
  - reliance on anonymisation instead of proper erasure;
  - incomplete records of requests;
  - absence of internal monitoring systems.

These findings will guide sectoral inspections and enforcement priorities.

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
Yes, the same EDPB questionnaire (translated into Portuguese) was used for all entities.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
No content changes. Only linguistic adaptation (translation).

[46] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?
Some controllers exploited technical flaws in the form (e.g. leaving mandatory identification fields blank). Reminder letters were sent; in some cases, letters were returned unopened.

Part I - Information about the controllers addressed

6. How many controllers did you contact?
15

7. Out of the contacted controllers, how many controllers responded?
*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*
12

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?
Three entities did not reply

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 2
b. Private sector: 10

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Health sector: 5
b. Insurance sector: 3
c. Marketing services: 2
d. Consulting: 2

11. Please specify the category in which the responding controllers fall[47]:

a. Micro enterprise: 1
b. Small enterprise: 1
c. Medium-size enterprise: 1
d. Large enterprise (more than 250 employees): 9

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers: 3
b. Customers: 6
c. Contractors: 3
d. Job applicants: 4
e. Employees: 2

[47] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

f. Applicants (for public services): 0
g. Citizens (for public sector): 2
h. Patients: 4
i. Other (please specify): 1

12.b. According to the responding controllers, are those data subjects also:

a. Children: 7 controllers
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 6 controllers

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: 1
b. 101 – 1 000:
c. 1 001 – 10 000:
d. 10 001 – 100 000: 1
e. 100 001 – 500 000:
f. 500 001 – 1 000 000: 2
g. > 1 000 000: 8

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 12
b. Payment data: 8
c. Identification data: 12
d. Marketing data: 5
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 6
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 1
g. Other, please specify: 1

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 3 years - Yes

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	2023	2022
0	1	1	1
1 – 10	6	6	7
11 – 50	3	3	3
51 – 100	1	1	1
101 – 500	1	1	0
more than 500	0	0	0

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	2024-2023	2024-2022
0	1	1	1

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
0

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 3 years- Yes

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	2023	2022
0%	2	2	3
10%	3	3	2
20%	0	0	0
30%	1	1	1
40%	0	0	0
more than 50%	5	5	5

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?
☐ Yes
☐ No, if so: Mixed. Health and insurance sectors often rely on legal retention/defence; nonetheless, consistently high or consistently zero rejection rates warrant scrutiny to ensure case-by-case assessment.

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
0

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 3 years

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	4	5	5
10%	3	3	3
20%	1	0	0
30%	0	0	0
40%	1	1	1
more than 50%	2	2	2

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
0

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 3
b. Customers: 5
c. Contractors:
d. Job applicants:
e. Employees:
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients: 5
i. Other: 1

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): Yes
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: Yes

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
Yes (health: low volume/complex grounds; insurance: higher volume with exceptions; marketing: objection-linked).

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Average
b. Too diverse levels to qualify

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?
Health: low volumes, refusals due to legal retention; technical challenges (backups, anonymisation).

Insurance: higher volumes; 20-year retention; refusals frequent.
Marketing: inconsistencies in declared scope; requests often linked to Art. 21.
Credit/collection: reliance on public data; refusals based on legitimate interest.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

Lack of acknowledgment of receipt.
Incomplete procedures, not regularly reviewed.
Prorogations not communicated to data subjects.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?
Platforms.
Registers of requests.
Written Standard Operating Procedure (SOPs).

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).
High or zero rejection rates not credible.
Confusion between erasure and objection.
Blanket 20-year retention in insurance.

24. Are there any leading or best practices of the controllers having responded that you would like to share?

De-indexation.

Legal review of each case.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.
No receipt acknowledgments.
No indication of time limits.
Limited accessibility.

26. Are there any leading or best practices of the controllers having responded that you would like to share?
Systematic receipts.
Dedicated portals.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers
No deletion in backups.
Anonymisation instead of deletion.
Contradictions in reporting.

28. Are there any leading or best practices of the controllers having responded that you would like to share?
Hard delete with proof.
Use of enterprise platforms.
Secure destruction methods

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

Yes – general guidance on data subject rights (no sector-specific Art. 17).

https://www.cnpd.pt/organizacoes/orientacoes-e-recomendacoes/

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.
Yes – complaint-based (mainly in health and marketing).

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?
Low but rising; mostly refusals (health) and marketing communications.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).

5 controllers referred directly to inspection.
Others subject to further documentary investigation and possible on-site checks.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes:
   If "Yes", please specify: *(please select one or more answers)*
   a. More online guidance: In progress
   b. Online or remote training sessions: In progress
   c. Conferences organised: In progress
   d. Others: please specify:
b. No:

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes: Guidance on erasure in backups; distinction between erasure/restriction/anonymisation; clarification on exceptions in health/insurance.
b. No:

35. Are there any other observations that you would like to share?

- Large disparities in maturity;

- micro-entity with >1M data subjects;
- large hospitals still without robust deletion means.

SE SA

Name of Supervisory Authority: Swedish Authority for Privacy Protection (IMY)

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding: No
b. Fact finding + determining follow-up action based on the results: Yes
c. New formal investigation[48]: No
d. Ongoing investigation: No

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

- **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? Yes
- **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. No
- **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? Yes. The outcome of this fact-finding exercise will be taken into account in IMY's annual supervisory planning for the year 2026.

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.
The outcome of this fact-finding exercise will be taken into account in IMY's annual supervisory planning for the year 2026.

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
In principle, all questions were used in the common questionnaire. However, we amended two of the questions concerning case descriptions (questions 3.4 and 3.8), so that no detailed description of cases encountered by respondents and the analysis carried out at that time needed to be submitted. Finally, question 2.1 was formulated in such a way that it was mandatory for the respondent to submit such established documents and process descriptions.

5. Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?
No.

[48] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

Part I - Information about the controllers addressed

6. How many controllers did you contact?
20.

7. Out of the contacted controllers, how many controllers responded?
*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*
20.

8. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?
Not applicable.

9. Please specify the sectors of activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable.*

a. Public sector: 7
b. Private sector: 13
c. Other: 0

If so, what were the other sectors? Not applicable.

10. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector: 0
b. Health sector: 5
c. Social sector: 0
d. Insurance sector: 2
e. Finance sector: 2
f. IT sector: 1
g. Retail sector: 1
h. Logistics sector: 0
i. Public transportation: 3
j. Telecommunications: 2
k. Postal services: 0
l. Advertising sector: 0
m. Marketing services: 0
n. Entertainment sector: 1
o. Information / journalism sector: 1
p. Scientific / historical research: 0
q. Credit scoring agency: 0
r. Public utility/infrastructure provider (e.g. energy): 0
s. Housing industry: 0
t. Manufacturing: 0
u. Consulting: 0
v. Public administration: 4
w. Other (please specify): 1 Regional development and culture

11. Please specify the category in which the responding controllers fall[49]:

a. Micro enterprise: 0
b. Small enterprise: 0
c. Medium-size enterprise: 1
d. Large enterprise (more than 250 employees): 12
e. Non-profit organisation: 0
f. Ministry: 3
g. Local authority: 3
h. Administrative authority/agency/office (e.g. job center): 0
i. School/university/educational institution: 0
j. Other (please specify): 1 Regionally owned limited liability company (companies owned by the public authorities)

12.a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers: 0
b. Customers: 13
c. Contractors: 0
d. Job applicants: 0
e. Employees: 0
f. Applicants (for public services): 0
g. Citizens (for public sector): 4
h. Patients: 3
i. Other (please specify): 0

12.b. According to the responding controllers, are those data subjects also:

a. Children: 14
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people): 13
c. Non applicable: 5

13. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

a. < 100: 0
b. 101 – 1 000: 0
c. 1 001 – 10 000: 0
d. 10 001 – 100 000: 0
e. 100 001 – 500 000: 1
f. 500 001 – 1 000 000: 0
g. > 1 000 000: 19

14. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 19
b. Payment data: 12
c. Identification data: 17
d. Marketing data: 7

[49] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data: 11
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences: 2
g. Other, please specify: 2 e.g. traffic data, location data and internet access data. 1 Details of the customers' insurance contracts, the insured items, the damage and the event of damage. 1 User data such as listening history.

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year- Yes

☐ 3 years

☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0	1	Not applicable	Not applicable
1 – 10	5	Not applicable	Not applicable
11 – 50	4	Not applicable	Not applicable
51 – 100	0	Not applicable	Not applicable
101 – 500	2	Not applicable	Not applicable
more than 500	6	Not applicable	Not applicable

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (*we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s)*)

	2024*	**2024-2023**	**2024-2022**
0	Not applicable	Not applicable	Not applicable

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

0.

16.a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐1 year- Yes

☐ 3 years
☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).*

	2024*	**2023**	**2022**
0%	4	Not applicable	Not applicable
10%	6	Not applicable	Not applicable
20%	1	Not applicable	Not applicable
30%	0	Not applicable	Not applicable
40%	1	Not applicable	Not applicable
more than 50%	7	Not applicable	Not applicable

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?
☐ Yes
☐ No, if so: Not applicable please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
1.

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):
☐ 1 year- Yes
☐ 3 years
☐ other, specify: Not applicable.

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	**2023**	**2022**
0%	10	Not applicable	Not applicable
10%	6	Not applicable	Not applicable
20%	0	Not applicable	Not applicable
30%	0	Not applicable	Not applicable
40%	1	Not applicable	Not applicable
more than 50%	2	Not applicable	Not applicable

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
1.

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 4
b. Customers: 13
c. Contractors: 1
d. Job applicants: 7
e. Employees: 5
f. Applicants (for public services): 0
g. Citizens (for public sector): 4
h. Patients: 2
i. Other: 1 Politicians. 1 Unknown category.

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): 6 yes.
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: 4 yes.

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?

The results we have obtained on this issue are partly inconsistent given the sectors and processing activities of the respondents.

An inconsistency concerns the overall number of requests received, which appears to be too low, in light of the size of the organizations and the number of data subjects concerned by their processing operations. This is especially true for respondents who are large companies. One possible acceptable explanation for the low number of requests is that several of the respondents are subject to legal documentation requirements, for example under the Swedish Archives Act, the Patient Data Act or the Pharmacy Data Act. It is conceivable that data subjects are aware of these requirements and therefore refrain from requesting erasure. An alternative explanation is that actual requests for erasure are not handled and/or recorded correctly. Another explanation is that data subjects have not received sufficient information about their rights.

Another observation pointing to an inconsistency is that several respondents state that they only received requests from categories of data subjects in the form of customers, patients and citizens, but not employees or job seekers. This is despite the fact that they are big employers.

The result shows that there is variation in how many requests are rejected. The majority of respondents in the public sector report that more than half of the requests are rejected, which seems reasonable as these activities are subject to documentation requirements that prevent erasure. At the same time, two healthcare activities have reported a low level of refusal despite being subject to documentation requirements. This creates an inconsistency in the outcome in terms of the sector and processing activities of the controllers. Among the organizations that reported a low level of refusal are those that operate public transport. For these respondents, it can be assumed that they support their personal data processing on legal grounds that give the right to erasure, which makes the result more consistent in this context. Two healthcare activities have reported low refusal rates despite being subject to documentation

requirements, these results appear inconsistent from the point of view of the controllers' sector and processing activities.
Several respondents state that no request received has concerned the right to object under Article 21. This is consistent for organizations that largely base their personal data processing on legal obligations based on legal documentation requirements. In other cases, however, this may indicate that the organisation lacks procedures for categorizing requests or that relevant statistics are not available. Another explanation is that data subjects have not received sufficient information about their rights.

Part II – Substantive issues regarding controllers' level of compliance

19. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

c. Very High
a. High
b. Average
c. Low
d. Very low
e. Too diverse levels to qualify - Yes

20. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?
No.

Workflow of responding controllers

21. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

Challenge: The lack of or insufficient internal procedures and processes
A key challenge is that many controllers appear to lack sufficiently developed and documented internal procedures to handle a request for erasure. Many have not submitted any documentation at all, or only an incomplete materials, although this was mandatory if such materials existed. Oftentimes cases are handled manually and on a case-by-case basis, making the process dependent on certain individuals and inconsistent. There are also ambiguities in the division of responsibilities, where, for

example, data protection officers incorrectly make decisions, which is in breach of their independent role. Overall, this suggests that procedures are not sufficiently clear or consistent to ensure proper and effective handling.
The provisions concerned in the GDPR are Articles 5(1)(e), 5(1)(f), 5(2), 12(3), 17 and 24.
One **possible explanation** is a combination of lack of prioritization and mainly manual handling. When set routines and supporting systems are missing, the process becomes inefficient, dependent on certain individuals and difficult to monitor, especially in case of a larger number of requests.
Differences that have been identified are that some businesses have well-functioning processes where lawyers and data protection officers are involved, while others have ambiguous procedures and division of responsibilities. There are also differences in how an individual's identify is verified, and in some instances clear processes are completely missing in this regard.
Possible solutions could be guidance and recommendations from the EDPB. Such guidance should describe, from a practical perspective, how internal processes could be designed, for example by mapping out systems and data flows, clarifying roles and responsibilities, and what documentation is needed to demonstrate compliance.

Challenge: Difficulty identifying which information should be erased
Another challenge is that controllers seem to have difficulties in technically identifying and locating all personal data subject to a request for erasure. The responses are often vague and do not describe how it is ensured that all relevant information is identified in different systems. Some refer only to the information provided by the individual, without an explanation of their own search process. This indicates that technical tools and systematic methods are often missing in order to carry out a complete erasure.
The provisions concerned in the GDPR are Articles 5(1)(e), 5(1)(f), 12(3), 17 and 32.
One **possible explanation** is that these issues are not given sufficient priority within the organizations. Thus, it does not allow for allocation of sufficient amount of time and resources in order to develop technical solutions or necessary policy documents and training that is required.
There are significant differences that have been identified, in particular between the organization that are subject to legal requirements to retain information (such as the Swedish Archives Act) and those who are not. The former often have to adhere more complex conditions, which places higher demands on technical support and legal expertise.
Possible solutions could be technical solutions that facilitate the identification of personal data in different systems. Guidance is also needed from IMY or the EDPB, on the one hand on how national retention laws relate to the right to erasure and on the other hand on how technical solutions can be used to comply with the requirements.

22. Are there any **leading or best practices** of the controllers having responded that you would like to share?
Despite a limited scope of material, the following are examples of best practices that have been identified in relation to handling erasure requests:

- Create clear and up-to-date procedures, policy documents and checklists that specify who does what, how the assessment should be carried out and what criteria apply for erasure pursuant to both Article 17(1) and 17(3).
- Ensure that all staff receive basic and recurrent training in data protection according to their role and needs, starting from the start of their employment.
- Ensure that employees who handle erasures have access to and, if necessary, seek support from experts, such as data protection officers.
- Use a case management system to record and monitor all requests, and automate the process where appropriate.
- Let a central function coordinate the handling when a case affects several departments in the organization.
- Offer multiple channels for submitting a request, such as email, phone, web forms, or physical visits.
- Always confirm the receipt of a request and ask for additional information if it is unclear.
- Only verify the identity of the applicant in case of reasonable uncertainty. In such cases, use methods that are proportionate to the characteristics of the information and the situation (such as e-ID (including services that require such login and verification), registered letters, letters to the officially registered address, physical ID checks on site or verifying questions).
- On average, handle cases well within the outer deadline of one month, such as two weeks, and proactively inform about any delays.
- Always provide a clear justification with reference to the relevant provisions in case of a refusal to comply with a request.
- Inform, on your own accord, other recipients of the personal data that an erasure has been carried out.
- Ensure that personal data processing agreements stipulate how erasure should take place and provide clear instructions to the processor when an erasure is to be carried out.

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

23. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).

Challenge: Incorrect handling when a request for erasure is denied

One challenge is that several controllers do not take sufficient action when they deny a request for erasure. Many report that they often refuse erasure on the basis of exceptions in the GDPR, for example to comply with a legal obligation or to establish, exercise or defend legal claims. Despite this, they rarely implement any other protective measures, such as restricting the processing of personal data. This indicates a lack of understanding of the need to proactively protect the rights of individuals, even when a request for erasure cannot be granted directly.

The provisions concerned in the GDPR are Articles 5(1)(a), 5(1)(e), 5(2), 17(3), 18 and 24.

One **possible explanation** for this issue is a lack of understanding of how the right to erasure relates to other rights, such as the right to restriction of processing. There is uncertainty about how to practically protect the rights of the data subject when immediate erasure is not an option.

No clear **differences** have been identified between the controllers in this regard.

Possible solutions could include guidance and recommendations from the European Data Protection Board (EDPB). Such guidance should provide practical explanations, of how the right to erasure interacts with the right to restriction and how controllers can design their procedures to address these situations.

Challenge: Misunderstandings concerning the notification obligation

Another challenge is that many controllers do not seem to understand their obligation to notify recipients of personal data that the data has been erased. The responses reveal several misunderstandings. Some argue that the obligation is applicable, while others believe that it only applies if the data subject explicitly requests it. Some only notify internal recipients, while others notify only certain external recipients. This indicates that a majority does not understand that they are required to notify all recipients, both internal and external, regardless of whether the data subject has made a specific request.

The provisions concerned in the GDPR are Articles 5(2), 17, 19 and 24.

One **possible explanation** for this issue is a lack of understanding of the scope and purpose of the notification obligation under Article 19. The controllers seem uncertain as to how the obligation is to be applied in practice.

No clear **differences** have been identified between the controllers.

Possible solutions could include guidance and recommendations from the EDPB. Such guidance should clarify how controllers should practically design their processes to comply with the notification obligation and how they should inform the data subject thereof.

Challenge: Ignorance regarding erasure when balancing interests

An additional challenge is that few controllers appear to have ever denied a request for erasure on the grounds that their legitimate interests outweigh those of the individual. This may indicate that the original basis for the processing, i.e. the balancing of interests, was not sufficiently strong from the outset to constitute a valid legal basis. If there are rarely reasons that outweigh the data subject's interest in erasure, it raised question of whether a legitimate interest strong enough to justify the processing existed from the outset.

The provisions concerned in the GDPR are Articles 5(1)(a), 5(2), 6(1)(f), 17(1)(c) and 24.

One **possible explanation** is a lack of understanding of how the right to erasure and objection interact with the legal basis legitimate interest.
No clear **differences** have been identified between the controllers.
Possible solutions could include guidance and recommendations from the EDPB on the right to erasure and how it relates to the balancing of interests under Article 6(1)(f).

Challenge: Perceived complexity and uncertainty in the public sector
A particular challenge for the public sector is that the right to erasure rarely becomes applicable. A large part of the personal data processing in this sector is regulated by other legislation, such as archival laws, which means that exceptions to the right of erasure often apply. The legal landscape is perceived as complicated and there is uncertainty about how the GDPR and national legislation relate to each other. Since the decisions of public authorities can be appealed, there are high demands for legal justification, which in turn requires a level of certainty in the application of the law that many respondents appear to lack.
The provisions concerned in the GDPR and national legislation are Articles 6(1), 17(3), 19 and Chapter 7, Section 2 of the Data Protection Act.
One **possible explanation** is that since erasure is rarely relevant on the public sector, these organizations do not build up knowledge or experience regarding the right to erasure. This in turn makes it difficult to justify allocating resources to competence development in this area.
Differences that have been identified include that some organizations have an active involvement of data protection officers and legal experts, while others give vague or unclear responses regarding how assessments are made. There are also variations in how combined request for access and erasure are handled.
Possible solutions could be guidance and recommendations from the EDPB that clarify how the right to erasure should be handled in the public sector, taking national legislation into account.

24. Are there any leading or best practices of the controllers having responded that you would like to share?
Although few respondents provided detailed answers, the following good examples and recommendations for the handling of erasure cases have been identified:

- Manage requests in the correct order. When someone requests both access to and erasure of their data at the same time, handle the request for access first and then the request for erasure.
- Always carry out an individual assessment. Assess each request for erasure individually, even if the organization is generally subject to exceptions that limit the right to erasure.
- Establish procedures to inform recipients. Make sure to notify other recipients (as referred to in Article 19) on your own initiative when personal data has been erased, even if this may be technically challenging.
- Restrict access when erasure is not possible. If personal data cannot be erased immediately, access to it should be restricted while awaiting erasure.

- Document and seek assistance if necessary. Document all decisions and consult the Data Protection Officer or other expert when facing difficult or complex assessments.

Communication with Data Subjects

25. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.

Challenge: Insufficient adaptation of the response channel to the sensitivity of the information
Another challenge is that controllers do not always adapt the response channel to the sensitivity of the personal data. Some use more secure methods such as registered mail or secure digital healthcare services, but this is not a self-evident matter for all. This indicates a lack of awareness about information security and a possible lack of risk assessment procedures.
The provisions concerned by the GDPR are Articles 5(1)(f), 12, 17, 24 and 32.
One **possible explanation** is a general lack of awareness about information security. It may also be due to the fact that clear internal procedures for assessing risks and selecting an appropriate and secure communication channel in each case are missing.
The differences that have been identified are that the routines vary greatly. Some businesses adapt the response channel to the sensitivity of the information, while others do not seem to make that assessment.
Possible solutions could be guidance and recommendations from the EDPB. The guidance should clarify the importance of conducting a risk assessment and choosing a response channel that adequately protects the personal data of the individual.

Challenge: Insufficient information about the length of the processing time
Another challenge is that most controllers do not inform about the expected processing time when they receive a request for erasure. Although many controllers send an acknowledgement of receipt, few indicate how long the processing may take. This can negatively affect transparency and the individual's expectations.
The provisions concerned by the GDPR are Articles 5(1)(a), 12, 17 and 24.
One **possible explanation** is that there is no explicit legal requirement to inform about processing time. Therefore, this is not a priority for the organizations.
Differences that have been identified are small, as almost none of the respondents state that they regularly inform about the processing time.
Possible solutions could be guidance from the EDPB. The guidance could highlight the importance of communicating processing times as part of good practices to maintain transparency towards the data subject.

Challenge: Lack of flexibility in relation to communication channels
One challenge seems to be that although a request for erasure is often received through several different channels, they are only answered through one or a few of those channels. This may indicate that the data subject's preferences regarding a communication channel are not always taken into account. There is a risk that communication is not sufficiently clear and easily accessible, and that it is not easy enough for individuals to exercise their rights.

The provisions concerned by the GDPR are Articles 12, 17 and 24.
One **possible explanation** is that resources and priorities to coordinate communication channels are missing. It may also be due to missing technical systems, such as a privacy portal, which can handle both receiving and responding to a request in a flexible manner that suits the needs of the individual while ensuring an appropriate level of security.
No clear **differences** have been identified between the controllers.
Possible solutions could be guidance and recommendations from the EDPB. Such guidance should explain, from a practical perspective, how controllers can create effective and flexible channels for receiving and responding to a request for erasure that can, on the one hand, take into account the needs of the individual and, on the other hand, ensure an appropriate level of security and how such an assessment can be performed.

26. Are there any leading or best practices of the controllers having responded that you would like to share?
Based on the responses received, the following good examples and recommendations in relation to information and communication regarding erasure have been identified:

- Be clear in the privacy policy. Specify both the criteria that determine how long personal data is stored and, if possible, the exact retention period.
- Provide clear information and multiple means of contact. Provide information in an easily accessible manner, for example on the website, about how to request erasure. Enable submission of requests through multiple channels, such as email, phone, web form or physical visit.
- Be flexible and proportionate regarding identity verification. Use methods to verify an individual's identity that are proportionate to the characteristics of the information and the situation (e.g. e-ID, on-site ID check or a letter to the officially registered address).
- Always confirm that the request has been received. Send an acknowledgement of receipt and at the same time provide information about the expected processing time, if possible.
- Choose a secure response channel. Adapt the response channel based on how the request was received and what information the response contains, taking information security into account.

Technical aspects

27. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers

Challenge: Uncertainty about erasure in backups
According to many data controllers, the erasure of personal data in backups is performed according to separate procedures where data is erased, but over a longer period of time. This creates a challenge in the form of uncertainty as to whether the deletion in accordance with such separate procedures in the case of an individual

request actually takes place immediately and ‘without undue delay’ as required by the GDPR.
The provisions concerned in the GDPR are Articles 5(1)(f), 17 and 24, 32(1)(c) and 32(2).
One **possible explanation** is that while controllers shall comply with the requirements of Article 17 on erasure, they shall also consider the security of processing personal data in Article 32. This is so that the data is protected from destruction, loss or alteration while being processed, and that availability and access can be restored in a reasonable time after a physical or technical incident.
A general challenge for controllers and processors when it comes to backups is to technically not be able to use them for restoring data them back when necessary after a physical or technical incident.
At the next step, in order to ensure, that the erasure remains after restoring data from the backups into the operational information systems, it is important to have internal procedures to flag erased records of personal data in the backups.
No clear **differences** have been identified between the controllers.
Possible solutions could be guidance and recommendations from the EDPB. The guidance should explain how controllers should practically deal with erasure in backups and what is meant by "without undue delay" in this context.

Challenge: Use of data anonymisation instead of erasure
Another challenge is that several controllers fulfil a request for erasure by anonymisation instead, for example in order to continue to use it for analysis. This creates a risk that the actual erasure of the personal data is not carried out in full according to the requirements of the law.
The provisions concerned in the GDPR are Articles 6, 7 and 17.
One **possible explanation** is a desire to retain data for other purposes, such as statistics or analysis, combined with an uncertainty about what legally and technically constitutes erasure compared to an effective anonymisation.
For anonymisation, there is an additional challenge in managing the risk of personal data processing if it has not been carried out in such a way that the data subject is no longer identifiable.
No clear **differences** have been identified between the controllers.
Possible solutions could be guidance and recommendations from the EDPB. The guidance should clarify the difference between erasure and anonymisation and under what conditions anonymisation can be considered as fulfilling the erasure requirement. This could be done, for example, in the planned future guidelines on anonymisation from the EDPB.

Challenge: Absence of internal processes and guidelines
A further challenge is that many organizations lack clear internal instructions and established processes to handle a request for deletion. As a result, the work becomes inefficient and the handling may differ within the same organisation. Without a systematic approach, it is difficult to ensure that all data to be deleted are actually found and deleted. However, respondents refer to international standards in their responses, such as those within the ISO/IEC 27000 series.
The provisions concerned in the GDPR are Articles 5(2), 17, 24 and 32.
One **possible explanation** is that the issue has not been prioritised enough to have allocated resources to create clear policies, procedures and training efforts.

Differences that have been identified are that organisations that handle many erasure requests have more often developed an automated and unified process. It also appears that the responsibility for handling requests may lie with different departments, which contributes to inconsistent practices.
Possible solutions could be for regulators to offer support and advice, for example by referring to international information security standards (such as ISO/IEC).[50] To this can also be added a reference to practical national frameworks, such as the Swedish Civil Contingencies Agency's (MSB) methodological support for information and cybersecurity. This is to provide guidance in support of a risk-based and systematic information security work that supports all information management, as well as erasure.

Challenge: Difficulties in verifying the identity of the data subject
A specific challenge raised is the difficulty of identifying with certainty that the person requesting the erasure is indeed the data subject, and not an unauthorised person pretending to be the data subject. This creates a security risk and a difficult balance for the controller.
The provisions concerned in the GDPR are Article 12.
One **possible explanation** is the inherent conflict between making it easy for individuals to exercise their rights and the need to protect personal data from unauthorized access, loss, destruction or alteration.
No clear **differences** have been identified between the controllers.
Possible solutions could be guidance from the EDPB on practical and proportionate methods to verify a person's identity. The guidance should help controllers to find a balance that is secure but not unreasonably burdensome for the individual.

28. Are there any leading or best practices of the controllers having responded that you would like to share?
Although the evidence on the technical aspects is limited, the following good examples and recommendations for implementing deletion have been identified:

- Create clear internal governance documents. Document the erasure process and the legal bases governing the retention of different data. Clear, internal rules and processes create a more uniform management.
- Automate where possible. Use centralized systems and technical tools to automate both the handling of a request and the deletion itself. This reduces the risk of manual errors and makes the process more efficient.
- Provide a digital portal for case management. A portal, "my pages" or similar enhances the security of identification and allows individuals to track the status of their cases.

[50] The ISO/IEC 27000 series is a collection of standards for information security, cybersecurity and privacy management systems. The collection consists of two types of standards – one for management systems aimed at supporting a systematic approach and one for guidance focusing on security measures aimed at protecting the information. The series also includes, among other things, standards for guidance on information security risk management and security techniques for handling personal data.

- Verify that the erasure has been carried out. Implement procedures and technical checks to test and verify that the data that should be erased is permanently gone.
- Consider anonymisation as a method. By removing all identifiers, data can be used for statistics and analysis without any longer being classified as personal data. This can be an effective way to fulfill a request while retaining valuable information that is not personal data.
- Follow established standards. Use frameworks such as the ISO 27000 series, as a guidance to identify, erase and destroy information in a secure and structured manner.

Part III – Actions by participating SAs

29. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?
We have general information on our website (in Swedish) about what the right to erasure means: Right to erasure of your personal data | IMY: https://www.imy.se/privatperson/dataskydd/dina-rattigheter/radering/.

30. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.
In 2020, after investigating Google, IMY issued a fine of SEK 75 million for Google's mishandling of data subjects' rights to have search results delisted pursuant to the right to erasure (in Swedish): https://www.imy.se/tillsyner/google/. The Administrative Court of Appeal reduced the fine to SEK 50 million.

31. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?
We do not keep precise statistics on which articles are the subject of complaints. On the other hand, a large number of complaints are deemed to have concerned Article 17, particularly with regard to so-called search services.

32. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).

No specific measures against those contacted are currently under consideration.

33. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

a. Yes:

If "Yes", please specify: *(please select one or more answers)*

e. More online guidance: Yes
f. Online or remote training sessions: No.
g. Conferences organised: No.
h. Others: please specify: Yes. In the light of the findings of the EDPB report, IMY will consider developing guidance and recommendations tailored to national circumstances.

b. No: Not applicable.

34. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes: Yes. Guidance and recommendations. Especially from a more proactive and practical perspective. The following should be addressed:
   i. How controllers can map out their systems and data flows, which can facilitate the handling of erasure requests.
   ii. What supporting system, tools and other automation as well as internal role allocation that could facilitate the handling of erasure requests.
   iii. How the right to erasure relates to, for example, predetermined retention periods.
   iv. What documentation and information that should be provided to data subjects, in particular in the case of more automated processes.
   v. More information on how the right to erasure should be understood and implemented, in particular on how the restrictions and exceptions should be interpreted.
   vi. How the right to erasure relates to the other rights in Articles 18 to 19, in particular from a more practical perspective with recommendations on how controllers should design their procedures/processes, systems and information provided to the data subject.
   vii. How controllers are expected to design their erasure processes, in particular regarding backups.
   viii. How anonymisation could be considered as fulfilling the erasure requirement.
   ix. How to erasure 'without undue delay' in Article 17 should be interpreted.

b. No: Not applicable

35. Are there any other observations that you would like to share?

IMY would like to note that as part of the inquiry questions were also directed to respondents affected by certain national legislation that supplements the GDPR

provisions on the right to erasure. Sweden has introduced supplementary national legislation to the GDPR, stipulating that decisions pursuant to Articles 12(5) and 15–21 of the GDPR issued by a public authority acting as a data controller, may be appealed to a general administrative court.[51] Public authorities are also required by national law to provide reasons for such decisions.[52]
Within the scope of this inquiry, IMY has collected information to assess compliance with these rules, particularly in relation to the right to receive justification and the possibility to appeal. The results show that most of the concerned respondents are well aware of their obligations. Many have also developed concrete tools, such as decision templates, to ensure that the individual receives clear justification and information on how to appeal a rejection.

At the same time, there appears to be considerable uncertainty in organizations with more complex organisational forms. When an organization has elements of both private and public governance (for example, a limited liability company managed by a public board), it is unclear how the requirement for appealable decisions should be applied. The result shows that very few rejection decisions are appealed to the administrative courts. This may be interpreted in two ways: either the decisions of the public authorities are so well-reasoned that the individuals understand and accepts the outcome, or it could indicate that individuals have low awareness of their right to appeal, and the potential outcomes of doing so.
Overall, the results show that there is a good awareness among the relevant respondents of their obligations under national law. At the same time, some challenges remain and IMY sees a continued need for guidance specifically targeted at public authorities.
Furthermore, IMY would like to highlight the experiences related to challenges and requests for guidance that have been raised directly by the respondents themselves cited below.
The respondents subject to the survey have identified several legal, technical and organizational challenges in relation to implementing the right to erasure.
In particular, with regard to **legal and communicative challenges:**

- To balance the right to erasure with other laws, such as the Swedish Accounting Act, which require that information is retained.
- To determine the exact time when personal data may be erased, for example after a legal process has concluded.
- To explain to individuals in a simple manner why the right to erasure is not absolute and why a request can be refused.
- To deal with confusion around certain terms that arises when the right to erasure is confused with other rights, such as access to public documents.

In particular, in the case of **technical challenges:**

- Locating all information related to an individual when it is spread out over many different IT systems that lack central search functions.

[51] Chapter 7, Section 2 of the Act containing Supplementary Provisions to the EU General Data Protection Regulation (2018:218)
[52] Section 32 of the Administrative Procedure Act (2017:900)

- The complexity and cost of developing and maintaining automated processes for erasure, especially if the number of cases is low.

In particular, in the case of **organisational challenges**:

- That the process of erasure often requires a lot of time and manual handling, from identifying an individual to verifying that all information is erased.
- To coordinate the erasure within large organizations with several different responsible parties, to ensure that all information is identified and erased.
- To ensure that external providers also erase the information that they handle, which requires clear agreements and monitoring.

To facilitate the handling of erasure requests, respondents are calling for clearer guidance and practical support, better technical tools and increased opportunities for training and knowledge sharing.

- In terms of **guidance and practical support,** this should be easily accessible and include concrete examples of how the right to erasure should be handled in practice, the following would be particularly desirable:
- Clearer information on which types of personal data are exempt from the right to erasure, for example when other legislation requires data to be retained.
- Recommendations on how long different types of commonly processed personal data should be retained.
- Concrete advice on how anonymisation can be used to meet the requirement for erasure.
- Standardized templates for decisions and checklists that can be used in the handling of cases.
- Guidance tailored for both the private and public sectors, as well as for specific industries.
- Regarding **technical tools,** the following would be particularly desirable:
- Tools that can automate more parts of the process, reducing the need for manual work and improving traceability. AI could be used to streamline, secure and document the process.
- Better tools to search for and identify an individual's data across the various systems where it may be stored.
- Clearer requirements for external service providers to offer systems and tools with built-in functionality that make it easy to fulfill data subjects' rights.
- When it comes to **training and knowledge sharing,** the following would be particularly desirable:
- More training activities, especially those aimed at staff who are not legal professionals.

- Creating forums for the knowledge exchange between different organizations and industries, to enable mutual learning and the development of shared solutions.

SI SA

Introduction

1. What was the initial procedural framework of your action? *Please select one or more answers.*

a. Fact finding:
b. Fact finding + determining follow-up action based on the results:
c. New formal investigation[53]: - Yes
d. Ongoing investigation: - Yes

In our case, this year CEF action was conducted as a formal investigation of three controllers; two of which in a new formal investigation and one as an expansion of an ongoing investigation. One supervisor was designated for all cases with support of one other supervisor. The initiation of the new investigation was on 27. 1. 2025. In all investigations onsite visits were performed. Internally, three organisational meetings were held regarding this year CEF action.

2. If your action is oriented towards "Fact Finding" (i.e. the first two responses in the previous question),

a. **2.a**. Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? [yes / partially / no]
b. **2.b**. Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right to erasure in the near future? If so, please provide more detail if available. [no / yes; if yes: free text]
c. **2.c**. If not, will this fact finding activity impact your enforcement activities and if yes, how? [no / yes; if yes: free text]

3. Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers? If so, please indicate the differences.

For the new investigations, we initially used the same questionnaire for all three controllers. This was later complemented with a more detailed examination during the onsite visits. In the case of the ongoing investigation, the scope was expanded to include questions related to the CEF topic, which were addressed exclusively during the onsite visit. In this context, the questions were not structured in the same way as in the standard questionnaire (see also the explanation provided under question 1).

4. If applicable, please provide a general explanation as to a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) the changes in wording which may have a significant effect on the results obtained.
The information presented in this report was collected through various methods, namely written questionnaires and onsite visits. In the new investigations, all questions from the consolidated questionnaire were included in the written requests submitted

[53] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

prior to the onsite visits. In the ongoing investigation, however, all information was obtained exclusively during the onsite visit, where the questions were not structured in the same manner as in the consolidated questionnaire, while its substance was still followed

Do you have other general comments/remarks you would like to indicate (e.g. with regard to your use of the questionnaire, the procedural framework selected, the specificities of your CEF action, etc.)?

Please see explanations to questions 3. and 4.

Part I - Information about the controllers addressed

5. How many controllers did you contact?

3.

6. Out of the contacted controllers, how many controllers responded?

*Please note that we would ask you to provide all of the following responses based on the number of the controllers that **effectively responded** to the survey/your questions.*
All.

7. In case of a gap between the answers to the two questions above, have you have identified the main reason(s) of the gap?

Not relevant to our exercise.

8. Please specify the sectors of activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable.

a. Public sector: 1
b. Private sector: 2
c. Other: /
    j. If so, what were the other sectors? /

9. Please specify the sector ("core business") in which the responding controllers mainly operate:

a. Education sector:
b. Health sector:
c. Social sector:
d. Insurance sector:
e. Finance sector:
f. IT sector:
g. Retail sector:
h. Logistics sector:
i. Public transportation: 1
j. Telecommunications:
k. Postal services:
l. Advertising sector:
m. Marketing services:

n. Entertainment sector:
o. Information / journalism sector:
p. Scientific / historical research:
q. Credit scoring agency:
r. Public utility/infrastructure provider (e.g. energy):
s. Housing industry:
t. Manufacturing:
u. Consulting:
v. Public administration:
w. Other (please specify): Shared mobility 2
d.

10. Please specify the category in which the responding controllers fall[54]:

a. Micro enterprise:
b. Small enterprise:
c. Medium-size enterprise: 2 controllers
d. Large enterprise (more than 250 employees): 1 controller
e. Non-profit organisation:
f. Ministry:
g. Local authority:
h. Administrative authority/agency/office (e.g. job center):
i. School/university/educational institution:
j. Other (please specify):

11. a. Which category of data subjects is mainly concerned by the processing activities of the responding controllers?

a. Potential customers:
b. Customers: 3 controllers
c. Contractors:
d. Job applicants:
e. Employees:
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients:
i. Other (please specify):

12.b. According to the responding controllers, are those data subjects also:

a. Children: Some children are included, especially in public transport services (bus services), but they do not represent a majority of data subjects processed
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people):
c. Non applicable:

12. Please provide an approximate number of all the data subjects concerned by the processing activities of the responding controllers:

[54] Information on the enterprise categories can be found at https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de

a. < 100:
b. 101 – 1 000:
c. 1 001 – 10 000:
d. 10 001 – 100 000: 1 controllers
e. 100 001 – 500 000: 2 controller
f. 500 001 – 1 000 000:
g. > 1 000 000:

13. Which types of personal data are mainly concerned by the processing activities of the responding controllers?

a. Contact data: 3 controllers
b. Payment data: 3 controllers
c. Identification data: 3 controllers
d. Marketing data:
e. Sensitive data within the meaning of Art. 9 GDPR, e.g. data concerning health; sex life or sexual orientation; racial or ethnic origin; political opinions, religious beliefs; biometric and genetic data:
f. Data of a highly personal nature within the meaning of Art. 10 GDPR, e.g. data relating to criminal convictions and offences:
g. Other, please specify:

15.a. For question 1.8 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year
☐ 3 years Yes
☐ other, specify:

15.b. How many requests for erasure in accordance with Art. 17 GDPR did the responding controllers received during the timeframe specified below (approximately)?

Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers received between 11-50 requests in 2023 but 0 in 2024). As a reminder, figures should be provided at least for 2024 (and for 2023, if 2024 figures are equal to 0; and 2022 if 2024 and 2023 figures are equal to 0). Please also indicate when figures are equal to 0.

	2024*	**2023**	**2022**
0			
1 – 10		1 controller	
11 – 50			
51 – 100	1 controller	1 controller	1 controller
101 – 500	2 controllers	1 controller	1 controller
more than 500			

15.c. For the SAs which asked figures relating to several years, could you please complete this table? (we are particularly interested in knowing whether responding controllers who reported having received 0 request in 2024 also had the same the previous year(s))

	2024*	2024-2023	2024-2022
0			

15.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

We gathered information for this question from all the controllers.

16. a. For question 1.9 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years - Yes

☐ other, specify:

16.b. Out of these requests, what was the percentage of requests that the responding controllers rejected (approximately)? Please specify the number of responding controllers in the relevant rows based on the figures that you collected (e.g. 10 responding controllers rejected 40% of the requests in 2023 but 0% in 2024).

	2024*	2023	2022
0%	2 controllers	2 controllers	2 controllers
10%	1 controller		
20%		1 controller	
30%			1 controller
40%			
more than 50%			

16.c. For the SAs who carried out an enforcement action, do you have the impression that the rejection of the requests by responding controllers was overall justified?

☐ **Yes**

☐ No, if so: please explain the reasons (e.g. responding controllers over-rejected requests).

16.d. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).

0

17.a. For question 1.10 in the questionnaire for controllers, for how many years were you asking controllers to provide figures (*please select one*):

☐ 1 year

☐ 3 years- Yes

☐ other, specify:

17.b. Out of the requests for erasure received, what was the percentage of the requests that was linked to the exercise of the right to object under Art. 21 GDPR by the same data subject (including objection to marketing)? *Please specify the number of responding controllers in the relevant rows based on the figures that you collected*

	2024	2023	2022
0%	2 controllers	2 controllers	2 controllers
10%	1 controller (2,28 %)	1 controller (7,9%)	1 controller (6,33%)
20%			
30%			
40%			
more than 50%			

17.c. Please specify the number of controllers who did not provide **any** figures for this question (but who responded to the questionnaire and the other questions).
Two out of three claimed that they did not process any such requests.

18.a. During the time period for which you provided information in Questions 15-17 above, which categories of data subjects were the most active groups who submitted the requests for erasure to responding controllers?

a. Potential customers: 1
b. Customers: 3
c. Contractors:
d. Job applicants:
e. Employees:
f. Applicants (for public services):
g. Citizens (for public sector):
h. Patients:
i. Other:

18.b. Were the following groups over-represented in the requests received?

a. Parents or guardians on behalf of (a) child(ren): No
b. Vulnerable subjects (e.g. elderly people, asylum seekers, ethnic minorities, disabled people) or guardians on behalf of a vulnerable subject: No

18.c. In your opinion, are the results that you obtained for this question consistent, considering the sector and processing activities of the responding controllers?
All responding controllers provide transport services (car-sharing, bike-sharing, and public bus services). In this context, it is consistent that customers or potential customers (e.g. users of the application without completing a purchase) represent the most active group submitting erasure requests. The controllers also noted that the majority of such requests originated from foreign tourists who used the services only for a short period of time. By contrast, domestic users, who typically rely on the services over a longer period, rarely submit requests for erasure of their data.

Part II - Substantive issues regarding controller's level of compliance

14. What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right to erasure? *(one answer possible)*

a. Very High
b. High
c. Average Yes
d. Low
e. Very low
f. Too diverse levels to qualify

15. Did you identify any significant differences regarding different types of controllers (such as between public and private sectors, size, etc.), and if so which ones?

A notable difference was observed between public and private sector controllers. The public sector controller (bus service) provides access to its services both via a mobile application and through a city card system, which is also used for other municipal services (e.g. library, public parking). The erasure requests received by this controller related exclusively to app users, while no requests were submitted by city card users. In contrast, the private companies provide their services solely through mobile applications. This indicates that customers using digital platforms are generally more aware of their data protection rights and act more cautiously when it comes to leaving their personal data behind.

Workflow of responding controllers

16. Please explain **the main issue(s) or challenge(s)** (e.g. from one to three issue(s)) that you have identified (if any) in your evaluations/actions with respect to **Questions 2.1 and 2.9** (relating to internal procedures, internal organisation and training, request handling, etc.) in the questionnaire for controllers:

a. Name the issue(s) identified and briefly describe it.
b. Which provision(s) of the GDPR (or national laws) does this concern?
c. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
d. What are differences that you have encountered between controllers in your Member State?
e. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

a. **Issues identified:**

- **Transparency with automatic erasure procedure:** in some instances data subjects are not properly informed about the result of their automatic erasure request; car-sharing company offers an option to "delete account" within an app, although choosing this option does not result in deletion of the profile data in the controller's database, but merely to delete an app from the user's mobile device, while for controller this request serves as basis for restriction of processing untill expiry of retention period and data subjects are not informed of this result; the public bus service offers an option that

the holder of a city card can virtualise it in an app, but after sending a request for erasure of the app profile, personal data affiliated to the city card remain stored separately even though the virtual profile of a user is deleted and data subject is also not informed of this;

- **No organised documentation or keeping records of erasure requests;** in several instances the controllers receive erasure requests via email, but they do not have an organised way for keeping records of the erasure request procedures. Often they only hold the correspondence within the mailbox of the employee who deals with data subject's requests. In cases with automatic erasure procedures, the controllers often do not keep any record of erasures and had to perform an analysis of their database for the sole purpose of the formal procedures. This affects the controller's possibility to demonstrate compliance according to Article 24 GDPR.

b. **Relevant provisions:**

These issues primarily concern Article 17 GDPR (Right to erasure), Article 12(4) GDPR (obligation to inform he data subject without undue delay that it shall not take action on the request and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy), and Article 24 GDPR (responsibility of the controller to implement appropriate measures).

c. Possible explanations:

The main reasons identified are insufficient internal procedures, limited resources allocated to data protection, and a lack of staff training on handling erasure requests.

d. Differences between controllers:

The car-sharing company holds higher risk from inadequate use of the service (traffic penalties, car accidents etc.) than public bus service and bike-sharing service, which, understandably, results in different retention periods. This affects also the results of the erasure requests procedure.

e. Possible solutions:

Adoption of internal guidelines establishing clear deadlines and responsibilities for handling and recording erasure requests.

Improvement of automated systems for processing requests.

Enhanced training of staff responsible for data protection tasks.

Supervisory authority may consider issuing further guidance and, where necessary, corrective measures to ensure consistency and compliance.

17. Are there any **leading or best practices** of the controllers having responded that you would like to share?

/

Questions 21 and 22 are relevant for the following sections. Please make sure to respond to subquestions 21.a) to e) below.

Conditions applicable to the exercise of the right to erasure and exceptions to the right to erasure

18. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 3.1 to 3.11** in the questionnaire addressed to controllers (relating to different case scenarios).

In evaluating and taking actions related to Questions 3.1 to 3.11 in the questionnaire addressed to controllers (regarding different case scenarios), the following issues and challenges have been identified:

In the case of the public bus and bike-sharing services, where the stakes for the controller in relation to service usage are low, the controller generally grants all erasure requests, provided that all dues have been settled. In this context, the process is straightforward, as the risk of misuse of services is minimal.

In contrast, in the case of the car-sharing company, the stakes for the controller are higher due to the potential for improper use of the services (e.g., traffic violations, accidents, etc.). As a result, the controller typically refuses the erasure request based on Article 17(3)(e) of the GDPR – for the establishment, exercise, or defense of legal claims. Additionally, the erasure deadlines are significantly longer, and the process is subject to further investigation and potential corrective actions to ensure compliance with legal obligations.

19. Are there any leading or best practices of the controllers having responded that you- would like to share?

/

Communication with Data Subjects

20. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 4.1 to 4.5.1** in the questionnaire addressed to controllers.

Specific retention periods were provided in the privacy notices 2 out of three controllers. One was instructed to make an update of the privacy notice.

The instructions for submitting a request for erasure were not specifically put down in the privacy policy, although the procedure inferred from the privacy policy (contact details of the controller, description of each data protection right, including the right to erasure and the possibility to file a request with the controller). In practice all controllers receive requests received via email or via app when the erasure is done automatically.

21. Are there any leading or best practices of the controllers having responded that you would like to share?

No best practice.

Technical aspects

22. Please explain the main issue(s) or challenge(s) that you have identified (if any) in your evaluations/actions with respect to **Questions 5.1 to 5.6.1** in the questionnaire addressed to controllers

On the question how the erasure is technically performed (with reference to question 5.2 of the questionnaire) it was established that all controllers store personal data (contact details, payment details) in a profile of a user. Separately they store data about services provided (drives, transactions etc.). Each profile is linked to the services through its own IT solution. Each controller uses their own service provider as a processor (some controllers are more/some less involved in the processing itself). The right to erasure is always applied to the profile information. All controllers consider that by deleting the profile, the data about services provided are anonymised. In review of each controller it was found that after deletion of an account, the controller has no information about the user and cannot link it to an identifiable person.

Regarding technical tools used to process Art 17 GDPR requests (with reference to question **5.3** of the questionnaire) we noted that all controllers have established a possibility for the data subject to request deletion of their account inside the application using a special button: "delete account". The app automatically prevents deletion of an account only when there was a payment due to settle. In cases with two controllers, after using the erase option, the system would delete data subject's profile data automatically and the data would be anonymized (by the processor supported system) and the controllers would have no direct influence in the process. The data subject would be informed that his account would be irreversibly deleted. In case with one controller, if the user used the button "delete account" inside the app, this would only cause the removal of the app from user's mobile device, but his data would remain in the controller' database until the storage period would expire. In such case, the request for erasure would in fact be denied due to the reason from 17(3) GDPR, although the data subject would not be properly informed of that fact. **It follows that in case of technical solutions for data deletion, the controllers should pay much attention about the transparency of processing, so that they do not violate ART 12(3) GDPR obligation regarding providing adequate information to the data subject, including the right to file a complaint against a decision of a controller.**

Regarding service provider used (with reference to question **5.4** of the questionnaire), we found that all controllers rely on their service provider for the functioning of their apps. Different controllers demonstrated a different level of influence on their service provider. The bike-sharing company has no influence on the service provider – they merely use the system developed and sustained by the service provider. On the other hand public bus service has been actively involved in development of the app and IT systems behind and thus has more influence on the controller.

Regarding anonymization technique (with reference to question **5.5** of the questionnaire), we found that all controllers perform erasure through anonymisation technique by deleting all directly identifiable data from the data subject' profile (name, surname, contact details etc.) and the data about services provided remain as anonymised data for further statistical analysis (drives performed, bus entry time and place etc.). For example, public bus services use the

anonymised data for planning of additional busses for a certain lane for a certain time period, car-sharing and bike-sharing use the data for planning of new stations etc.

23. Are there any leading or best practices of the controllers having responded that you would like to share?

/

Part III - Actions by participating SAs

24. Have you already published **guidance** (e.g. factsheets, guidelines, Q&A, training) on the implementation of the right to erasure? Please include any **general or targeted guidance you have adopted** (e.g. children's right to erasure; right to erasure in specific contexts such as online or for credit scoring, etc.), including *before* launching the CEF?

TITLE: **Guidelines for individuals regarding their right to data protection;**
DATE: February 2021;
LINK: 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 ;
DESCRIPTION: The guidelines are intended for individuals and explain their data protection rights and legislative requirements in various situations in which an individual finds himself - as a consumer, as an employee, as a user of public sector services etc.

TITLE: **You decide; I wish to erase my data;**
DATE: 2018;
LINK: https://tiodlocas.si/zelim-izbrisati-svoje-podatke/;
DESCRIPTION: Project webpage intended for awareness raising about data subject's rights.

25. Have you taken any actions (i.e., fact finding exercises, informal contacts, prior consultations, *ex officio* or complaint-based investigations and enforcement actions such as cases where your SA issued an order to erase personal data or restrict of processing and notify actions to recipients (art. 58.2(g) GDPR)) towards controllers concerning the right to erasure ***prior to*** launching the CEF 2025? Please provide a brief overview of the actions you have taken and the outcome of these actions.

No action was taken towards corresponding controllers prior to CEF 2025 regarding the right to erasure.

26. Are you able to provide some information on the **complaints that you have received regarding the right to erasure** since the entry into force of GDPR? (e.g. number of complaints regarding Art. 17 GDPR, volume of complaints on this matter in comparison with the rest of the complaints, growing number of complaints, handling of these complaints, etc.)?

Since the entry into force of the GDPR and until the end of 2024, we have received a total of 126 complaints under Article 17, representing approximately 10% of all complaints submitted during this period. While the absolute number of such complaints has not shown a consistent growth trend over the years, we have observed a steady increase in their relative share. For

instance, complaints concerning the right to erasure accounted for 4% of all complaints in 2020, rising to 19% in 2024.

27. What action(s) are you considering to undertake based on the results of this CEF towards controllers contacted, if any? (e.g. letter, recommendations to the controller, further guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the **timeline** for these actions (also in case formal investigations are still ongoing).

Against the corresponding controllers actions will be taken within 1 year from the start of the investigations. We foresee corrective measures will be necessary, namely to update the privacy policies, limit the storage deadlines and delete overdue data. Additionally, individuals must be notified in writing when their request for data erasure, submitted through the in-app option designed to initiate account deletion, is denied. Possible sanctions/penalty procedures will be started, taking into account the level of investment of controllers to implement corrective measures.

28. In light of your findings in this CEF, do you consider carrying out, **at the level of your SA**, actions to communicate and raise awareness with respect to the right to erasure and if yes, which actions do you consider to be preferable?

c. Yes:
   If "Yes", please specify: *(please select one or more answers)*
   a. More online guidance: Updating the existent publications with additional guidelines on the transparency of processing within the app services
   b. Online or remote training sessions: /
   c. Conferences organised: /
   d. Others: please specify: /
d. No: /

29. In your opinion, should more actions be carried out **at the level of the EDPB** on the right to erasure and if yes, which actions would be preferable. If needed, please specify the aspects of the right to erasure that could be developed)?

a. Yes: Guidelines on the right to erasure with particular focus on apps
b. No: /

30. Are there any other observations that you would like to share?