

## **Annex 1**

National Reports for the CEF action on the Right of  
access

## **Table of content**

Introduction.....	3
Commonly-built questionnaire to be addressed to controllers .....	4
AT SA.....	13
BG SA.....	23
CZ SA .....	38
DE SAs.....	51
DK SA.....	80
EDPS.....	89
EE SA.....	103
EL SA.....	113
ES SA.....	126
FI SA.....	136
FR SA.....	147
HU SA.....	157
HR SA.....	169
IE SA.....	181
IT SA.....	200
LI SA.....	215
LT SA.....	229
LU SA.....	234
MT SA .....	249
PL SA.....	261
PT SA.....	268
NL SA.....	281
SI SA.....	296

## Introduction

This Annex includes the national reports completed by participating SAs during the CEF action on the right of access, which were taken into account to draft the main EDPB report.

For the sake of transparency the questionnaire that participating SAs built together in the first half of 2024 to contact and obtain insights from controllers is included below. National reports refer to this questionnaire at times.

The methodology used by participating SAs to draft the questionnaire, send it to controllers at national level and to draft the national report is described in Section 2.2 of the main report. In particular, the questionnaire was drafted without focus on a specific sector or type of controllers and had a modular design so that SAs could use it in full or in part or supplement it with sector or national specific questions.

# Commonly-built questionnaire to be addressed to controllers

## **Instructions for controllers to complete this questionnaire**

*Throughout this questionnaire, where applicable, please differentiate your responses with regard to different groups of data subjects (e.g. where there are different communication channels with your customers than with your employees).*

### **1 Information about the controller**

1.1 Name, address, contact information

1.2 Please provide information on

1. the company turnover in 2023 (if applicable)
2. the number of employees/staff members
3. the legal structure.

1.3 Sector specific information:

1. Please describe the sector of your activity:

public sector

private sector

2. Do you qualify as:

micro enterprise

small enterprise

medium-sized enterprise

large enterprise (bigger than 250 employees)

*Information on these categories can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de)*

non-profit organisation

ministry

local authority

administrative authority/agency/office (e.g. job center)

school / university / educational institution

other (please specify)

3. Please describe the nature of your (business) activity:

education sector

health sector

social sector

insurance sector

finance sector

IT sector

retail sector

logistics sector

public transportation

telecommunications

postal services

advertising sector

marketing services

entertainment sector

- information / journalism sector
- scientific / historical research
- credit scoring agency
- public utility/infrastructure provider (e.g. energy)
- housing industry
- manufacturing
- other (please specify)

1.4 Main processing activities:  
Which categories of data subjects are mainly concerned by your processing activities?

- customers
- potential customers
- employees
- job applicants
- children
- vulnerable adults
- patients
- citizens (for public sector; please specify)
- applicants (for public services; please specify)
- recipients (for postal services)
- other (please specify)

Please provide an approximate number of data subjects concerned by your processing activities (e.g. 100, 100.000, 2.000.000): \_\_\_\_\_

Which types of personal data are mainly concerned by your processing activities?

- contact data
- payment data
- identification data
- sensitive data within the meaning of Art. 9 GDPR (please specify)
- data of a highly personal nature within the meaning of Art. 10 GDPR (please specify)
- other (please specify)

1.5 How many requests for access in accordance with Art. 15 GDPR did you receive in 2023 (approximately)?

What percentage do these access requests represent in regards to the rest of the data protection requests received?

Out of the access requests received in 2023, what percentage included a request to receive an insight into and inspection of and/or a copy of the personal data, and what percentage included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)?

## 2 Documentation of compliance with requests for access

2.1 Do you document compliance with requests for access in accordance with Art. 15 GDPR? If so, please explain your process for documenting compliance with requests for access.

Please also address your access and role management with regard to this documentation. Where applicable, please differentiate your response with regard to different groups of data subjects.

- 2.2 How long do you store information on access requests from data subjects and associated correspondence, including the response? If applicable, please cite any regulation you base this retention period on. If relevant, please distinguish between requests that have been complied with and requests that have been rejected, as well as between different groups of data subjects.

### 3 Process-related questions

- 3.1 Do you have a pre-defined process for handling requests for access in accordance with Art. 15 GDPR?

If so, please describe your general process from the receipt of the data subject's request until you provide the access and information. If available, please provide internal process descriptions or instructions (e.g. organizational charts, any templates used like request or reply templates, excerpts from your records of processing activities, excerpts from your data breach documentation). Please address in particular the following aspects in your description:

1. The respective input channel(s) for access requests (e-mail, telephone, online form, letter, etc.),
  2. organizational units involved, including the role of the appointed Data Protection Officer (if any) in this process and external entities/persons involved in the process (if any), such as lawyers, consultants, etc.,
  3. centralized/decentralized data storage and processing of requests for access,
  4. in case of several establishments in the EEA Member States, the centralized/decentralized handling of access requests,
  5. the use of software to support the processing of requests for access, e.g. for pre-sorting requests from data subjects, for internal coordination, for fully automated provision of access (if any),
  6. the use of self-service tools, for example enabling data subjects to download their personal data themselves at any time (if any),
  7. and the respective output channel(s) for answering the request (e-mail, letter, etc.).
- 3.2 Do you consider the implementation of data subjects' rights, in particular the right of access in accordance with Art. 15 GDPR, when digitizing your processes or when onboarding or integrating new digital tools (e.g. new software)? If so, please elaborate in particular:
1. (when and how) do you involve your DPO when digitizing processes,
  2. do you update your record of processing activities accordingly,
  3. (how) do you connect new tools or services with existing proceedings to collect information to be provided in case of access requests,
  4. (how) do you verify and ensure the assistance required by any processor engaged in responding to access requests?
- 3.3 Do you monitor or systematically control the handling of requests for access under Art. 15 GDPR (i.e. the number of access requests received, the date of receipt, the respective status of processing the requests)? If applicable, please describe the type of monitoring and who within your organisational structure implements it.
- 3.4 Do you send confirmations of receipt of access requests to the data subject? If so, do you include a note about the processing time/end of the deadline? Where applicable, please differentiate your response with regard to different groups of data subjects.

#### 4 Questions about the implementation of general requirements from Art. 12 GDPR

##### 4.1 Via which communication channels can requests for access in accordance with Art. 15 GDPR be made to you?

Please describe where and how exactly data subjects can find information on the relevant communication channel, as well as the precise pathway from the starting point until the request can actually be sent to you (e.g. from the start page of your website, how many clicks are required until the respective communication channel can be found and the request can be sent).

Where applicable, please differentiate your response with regard to different groups of data subjects and the different communication channels used.

##### 4.2 In case a data subject addresses an access request to you via a channel that you have not specifically provided for receiving such requests, do you refer such request to the correct unit within your organisation to process it? Please elaborate.

##### 4.3 Do you have certain requirements as to the form of the requests for access as a condition for these requests to be handled by you (e.g. requirement for requests to be in writing / provided through a specific communication channel)? If so, please describe these requirements.

In case you have such requirements, do you consider compliance with these requirements a condition for the start of the one-month-deadline in which access requests should be handled? If so, please explain why this is the case.

##### 4.4 In what form – and, if electronically, in which (file) format (xls, pdf, docx, zip, other) – do you provide information in accordance with Art. 15 GDPR? What are the situations where you provide access in a different format than requested? Do you explain the reasons why you provide access in a different format to the data subject?

Please also take the respective input channel (e.g. electronic) and group of data subjects into account when answering.

##### 4.5 Which data security measures do you have in place when providing access in accordance with Art. 15 GDPR?

information regarding access requests is provided on a webpage whose authenticity is verifiable (i.e. https)

digital access request can be filled on a dedicated webpage accessible via https

digital access request can be filled by e-mail protected by end to end encryption

digital access request can be filled by other means protected by end to end encryption

individuals are identified through a known and up to date eID system

individuals are identified through a scan of identity credentials collected via a secure channel (e.g. an authenticated and encrypted webpage, an encrypted e-mail, etc.)

scan of identity credentials are stored encrypted

individuals are identified through an existing account with their usual means of authentication or identification to the service

a specific account is created for the request

authentication to the account use for the request is password protected

authentication to the account use for the request is password protected following the better practice of the industry, including brute force attacks protection  
 authentication to the account use for the request is protected by two-factor authentication

information regarding request are stored encrypted

individual is authenticated to access the answer to his or her request  
 access to the request is provided through a link in an e-mail  
 answers to request are made available on a website protected with https  
 answers are sent by encrypted e-mail

an information security management system including this procedure exists  
 the corresponding part of the system (i.e. webpage, file management, etc.) has been fully or partially audited

role based access control is in place

access are logged

website and application used in the process are protected against main known attacks:

- protection against DDoS attacks
- protection against cross-site scripting
- protection against SQL injection

server and software (incl. CMS and plugins) are up to date

default credential have been changed

other security measures in place (please specify)

- 4.6 When responding to access request, do you take into account any special characteristics of data subjects (e.g. age of data subjects, visual impairment of data subject etc.) in light of the transparency requirements in Art. 12 (1) 1 GDPR? If so, please elaborate on these specific measures taken.

#### **Identification and authentication**

- 4.7 In 2023, have you received access requests for oral information (e.g. requests to provide information via phone)?

Do you respond to access requests for oral information?  
If so, do you have specific mechanisms in place to verify the identity of data subjects in case of access requests for oral information? Please elaborate.

- 4.8 How do you ensure the definitive identification of the data subject exercising the right of access under Art. 15 GDPR? Please describe the concrete process and any minimum identifiers you usually require (e.g. two-factor authentication, user account, (digital) ID); if necessary, please differentiate in relation to different categories of data subjects.

- 4.9 Do you respond to access requests according to Art. 15 GDPR submitted via third parties (e.g. portals for exercising data protection rights) or by someone acting on behalf of the data subject?  
Do you verify that such third parties act legitimately on behalf of the data subject? If so, please describe the process used.  
To whom do you send the information to be provided (directly to the data subject or to the third party)?



- 4.10 What are the most frequent circumstances in your practice (if any) in which you assume reasonable doubts about the identity of the data subject requesting access? In how many cases out of the total number of access requests received in 2023 did you conclude that there were reasonable doubts about the identity of the data subject?
- 4.11 What information do you request from the data subject requesting access if you have reasonable doubts about the data subject's identity? Do you request data subjects to login to an existing account? Do you request ID documents or copies thereof? Do you accept other methods for authentication than ID documents? If so, which methods? Do you impose a deadline on the data subject to provide such additional information? If so, how long is this deadline?

### ***Deadlines***

- 4.12 What measures do you take to ensure that requests for access in accordance with Art. 15 GDPR are answered immediately, but in any case within one month of receipt?
- 4.13 What are the most frequent circumstances/cases in which you extend the one-month deadline for processing access rights in accordance with Art. 15 GDPR? In how many cases out of the total number of data subject access request received in 2023 did you extend the one-month deadline?
- 4.14 At which point during the process of handling an access request do you inform a data subject about any delays in processing their individual request?
- 4.15 What was the average time (in calendar days) required to answer individual access requests in 2023 (or in the last 10 cases if you have not received at least 10 access requests in 2023)?

## **5 Questions regarding the content of access requests and respective responses according to Art. 15 GDPR**

### ***General***

- 5.1 How do you identify which data you need to select in the context of an access request in accordance with Art. 15 GDPR?
- 5.2 Do you process pseudonymised data? If so, how do you identify which pseudonymised data is related to the data subject requesting access to include them in your response?
- 5.3 What are the circumstances in which you ask the data subject to specify their request for access in accordance with Art. 15 GDPR? Do you inform the data subject of the (possibly) relevant processing operations when you ask for such specification?
- 5.4 Out of the total number of access requests received in 2023, how often did you ask data subjects to clarify their request for information?

### ***Layered approach***

5.5 When responding to a request in accordance with Art. 15 GDPR, do you make sure that the data subject is not overloaded with the information provided and can understand it with reasonable effort? How do you ensure this (e.g. layered approach for providing information, for example providing a list of the concrete personal data processed by category as a first layer, then providing data excerpts from your system in a second layer)?

How do you provide access to the data processed (e.g. bulk or single file download, electronic or postal mail)? Please describe the according procedure.

**Catalogue according to Art. 15 (1) 1 lit. a – h), Art. 15 (2) GDPR**

5.6 When providing the information in accordance with Art. 15 (1) lit. a - h), Art. 15 (2) GDPR, do you:

Refer to or use text modules of your privacy notice

Update the information on the concrete purposes pursued with the processing of the specific data subject's data

Narrow down the information provided to processing actually applying to the data subject (e.g. remove information on customer data processing if data subject is not a customer)

Tailor the information to the concrete access request in another way (please specify)?  
Where applicable, please differentiate your response with regard to different groups of data subjects.

5.7 With regard to information on recipients of personal data (Art. 15 (1) lit. c) GDPR), when do you provide concrete recipients and when do you provide categories of recipients? What criteria do you base your decision on?

5.8 With regard to the storage period in accordance with Art. 15 (1) lit. d) GDPR:  
Do you provide  
 concrete deletion dates  
 the duration of the retention period  
 the event triggering a specific retention period/the moment of deletion?  
Do you provide this information separately for each processing operation or data category?

5.9 Out of the total number of access requests received in 2023, how often have data subjects objected to the content of the information provided in accordance with Art. 15 (1) 1 lit. a – h), Art. 15 (2) GDPR / criticised its incompleteness?

**Copy**

5.10 If a data subject requests a copy of the personal data processed in accordance with Art. 15 (3) GDPR, do you provide:

File compilations specifically produced for the respective access request

Extracts from databases

Transcripts

Communication between you and the data subject

Full or partial documents containing the personal data

Other (please specify)

5.11 If you do provide access to documents containing the personal data:  
(a) how do you select which documents you provide access to?

(b) in which circumstances do you include the entire document, in which circumstances do you only include parts of such documents? On which criteria do you base your decision (e.g. business secrets contained in such documents)?

- 5.12 When you provide extracts or full or partial documents containing personal data, how do you ensure that the personal data contained therein are understandable for the data subject within the meaning of Art. 12 (1) 1 GDPR (e.g. with an explanatory document)?
- 5.13 Do you provide the data subject with other ways of access in addition to providing him/her with a copy in accordance with Art. 15 (3) GDPR (e.g. oral information, on-site or remote access)? If so, please explain such other ways of access and elaborate on the conditions in which you provide them. Where applicable, please differentiate your response with regard to different groups of data subjects.

### ***Special forms of processing***

- 5.14 Do you grant access to non-textual personal data such as images, video (e.g. CCTV) or voice recordings? If so, please describe the communication channels via which you provide access, the format in which you provide access, and whether and how you modify or alter such non-textual personal data.

### ***Specifics and particularities***

- 5.15 Have you taken measures to provide access to personal data with short retention periods (for example in case the data are supposed to be deleted within 48 hours, but handling the access request takes longer than those 48 hours)? If yes, please describe these measures.
- 5.16 If there is a change in the personal data processed by you from the date of the request until the date you provide access to such data, do you provide:  
(a) the personal data at the time of the request  
(b) the personal data at the time of your decision to provide access  
(c) information that the data has changed in the meantime?
- 5.17 If a data subject only requests access to parts of the data processed about them, do you comply with such request ("partial access request")? In which circumstances do you consider a request to be a partial access request? When responding to a partial access request, do you include information in accordance with Art. 15 (1) lit. a – h), 15 (2) GDPR?
- 5.18 In case of repeated requests for access within a short period of time (but not excessive within the meaning of Art. 12 (5) GDPR), do you only provide information about changes that occurred since the last provision of information or do you provide complete information?

## **6 Limitations of access requests**

- 6.1 Please list the most frequent circumstances in which you refuse to comply with an access request, as well as the grounds you base your refusal on. Do you inform the data subject about your refusal and the reasons?

- 6.2 Which types of personal data or information on processing do you not provide in reaction to an access request (e.g. data in backups, in your accounting, in the online shop, in apps ...)?  
If you do not provide certain types of data: On what legal basis do you leave out the respective information?  
Do you inform the data subject about your decision to leave out personal data and about the legal basis for doing so?  
Where applicable, please differentiate your response with regard to different groups of data subjects.
- 6.3 In which circumstances do you provide information about the identity of individuals within your organisation processing the data subject's personal data?
- 6.4 To what extent do you check whether the rights and freedoms of other people are affected before providing access in accordance with Art. 15 GDPR and in particular before sending a copy? Describe the procedure used, also in relation to providing access to non-textual personal data such as images, video or voice recordings (e.g. do you provide partial access in such cases).
- 6.5 Out of the total number of access requests received in 2023, how often did you limit the information provided to the data subject due to the rights of third parties (non-disclosure, redaction, etc.)?
- 6.6 Under which circumstances do you consider an access request to be manifestly unfounded or excessive within the meaning of Art. 12 (5) GDPR? In these cases, based on which criteria do you decide whether you should not respond to such a request at all or charge a reasonable fee? How do you calculate the reasonable fee and how do you inform the data subject about such fee?
- 6.7 How many requests out of the total number of access requests received in 2023 did you consider to be manifestly unfounded, how many to be excessive?
- 6.8 Please name the most frequent Union or Member States legal provisions you apply when refusing (entirely or in part) to comply with access requests, if any.

## 7 **Miscellaneous**

- 7.1 Are you aware of the European Data Protection Board Guidelines 01/2022 (Version 2.0 adopted on 28 March 2023) on data subjects rights – Right of access? If so, do you consult these Guidelines in practice?
- 7.2 After the publication of these guidelines, have you made any changes or additions to your practice of processing access requests?

Date

Contact person for further questions (name, e-mail/telephone number)

List of annexes

# AT SA

Österreichische Datenschutzbehörde

## 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<sup>1</sup>: **Yes**
  - d. Ongoing investigation:
  
- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),
  - Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? -
  - Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. -
  - If not, will this fact finding activity impact your enforcement activities and if yes, how? -
  
- 3) For all SAs: 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 for all controllers.**
  
- 4) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.  
**a) We included all of them**  
**b) No amendments other than obvious translation errors**
  
- 5) For all SAs: 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 etc.)?  
-

## Part I – Some numbers on the controllers addressed

- 6) How many controllers did you contact?  
**10**
  
- 7) Out of the contacted controllers, how many controllers responded?

---

<sup>1</sup> 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/to your questions.

10

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: Please select one or more answers.*

- a. Public sector:
- b. Private sector: 10

10) Please specify the category<sup>2</sup> of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers*

- a. Micro enterprise:
- b. Small enterprise: 2
- c. Medium-sized enterprise: 5
- d. Large enterprise (more than 250 employees): 3
- 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) Please specify the nature of the (business) activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. education sector:
- b. health sector:
- c. social sector:
- d. insurance sector:
- e. finance sector:
- f. IT sector: 2
- g. retail sector:
- h. logistics sector:
- i. public transportation:
- j. telecommunications: 10
- k. postal services:
- l. advertising sector:
- m. marketing services:
- n. entertainment sector:

---

<sup>2</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- 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. other (please specify):

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. customers: 10
- b. potential customers: 7
- c. employees: 6
- d. job applicants: 5
- e. children: 1
- f. vulnerable adults:
- g. patients:
- h. citizens (for public sector):
- i. applicants (for public services):
- j. recipients (for postal services):
- k. other (please specify):

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. Less than 100:
- b. 100 - 200:
- c. 201 - 500:
- d. 501 - 2,000: 1
- e. 2,001 - 10,000: 1
- f. 10,001 - 50,000: 1
- g. 50,001 - 100,000:
- h. 100,001 - 1,000,000: 3
- i. 1,000,001 - 10,000,000: 4
- j. More than 10,000,000:

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? *Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.*

- a. Contact data: 10
- b. Payment data: 9
- c. Identification data: 7
- d. Sensitive data within the meaning of Art. 9 GDPR:
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR:
- l. Other (please specify):

All in relation to telecommunication:

- Master data (4)
- Traffic data (6)
- Location data (3)
- Content data (4)
- Usage data (1)

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- 0 request: 4
- 1-10 requests: 4
- 11-25 requests:
- 26-50 requests: 1
- 51-100 requests: 1
- 101-150 requests:
- 151-200 requests:
- 201-500 requests:
- 501-10,000 requests:
- >10,000 requests:
- No information:

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

Size of the controller, importance on the market, number of customers seems to be quite indicative.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- None of the requests:
- >0–25%: 1
- 26–50% requests: 2
- 51–75% requests:
- 76–100% requests:
- No information:

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

Not every controller has data on this question; no big difference was noticed



17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 3
- b. >0–25%: 1
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests:
- f. No information:

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

-

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 3
- b. >0–25%: 1
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests:
- f. No information:

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

-

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 in the questionnaire for controllers:

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

No issues have been identified; several controllers have a more low-level process in place, since they very rarely, if ever, get access requests.

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

24(4) of the Austrian Data Protection Law includes a preclusion period of three years, after which a data subject may no longer have the right to lodge a complaint (e.g. because it thinks the right of access was infringed).

c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.

-

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

-

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

Several controllers have a more low-level process in place, since they very rarely, if ever, get access requests.

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

-

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

-

### **Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

21) 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 3.4 in the questionnaire addressed to controllers.

All controllers had a process for handling requests in place. Several controllers have a more low-level process (without extensive software-use) in place, since they very rarely, if ever, get access requests. Bigger controllers have very sophisticated processes and documentation in place. Only a few controllers send a confirmation of receipt regarding the access requests.

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

-

### **Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

23) 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 4.15 in the questionnaire addressed to controllers.

All controllers provided adequate contact options and did not exclude any specific modes of request. If a request is made by phone or in person (meaning not in writing), some controllers ask the data subject to provide the request in writing if possible, but will still handle the request, even if the data subject refuses to provide the request in writing. All controllers had adequate processes for identification in place.

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

-

### **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

25) 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 5.18 in the questionnaire addressed to controllers.

Some controllers ask data subjects to specify their request, mostly if some information is missing to attribute data from certain data bases to them. Almost all controllers provide details on specific recipients as mandated by the ECJ decision. Most controllers use a layered approach.

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

-

### **Section on “LIMITATIONS OF ACCESS REQUESTS”**

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

Controllers generally do not give information on the identity of individuals within the organisation processing the data subject's personal data. Controllers generally use the possibility of redacting certain information if needed and do not fully reject the request for access (but based on the numbers this rarely happened to the Controllers in question). Only one controller has rejected a request for access in 2023 based on Art 12(5) GDPR.

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

-

## Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

All controllers had a process for handling requests in place. Several controllers have a more low-level process (without extensive software-use) in place, since they very rarely, if ever, get access requests. Bigger controllers have very sophisticated processes and documentation in place.

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, “size” of the controller, etc.):

The three big controllers that were part of our investigation demonstrated deeper knowledge about the Guidelines, even though all controllers claimed to be aware of them.

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

Topics that are generally exceptions to the rule are naturally "lesser" known among smaller controllers who are rarely confronted with requests for access. These include:

Access to non-textual personal data

Requests via third parties

Restrictions and limitations

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance**

**you have adopted** (e.g. employees' right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF?  
If yes, please provide the date, link to the guidance, and a short description of the guidance.

The AT SA has published a Q&A that includes basic information on Article 15 (but also includes reference to the ECJ decision C-487/21): [https://www.dsb.gv.at/download-links/fragen-und-antworten.html#Art\\_15](https://www.dsb.gv.at/download-links/fragen-und-antworten.html#Art_15) (Website is in the process of being modernized, link could therefore change as well)

Information on Article 15 in some fashion has been up on the website of the AT SA since at least 2020.

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

The AT SA is often confronted with cases about Article 15. In many cases the controller will provide the information requested during the ongoing investigation and the case may be closed. However, the AT SA also has taken many decisions on Article 15 including enforcement action. Main topics of contention often included Article 15(3), Article 15(1)(c) and Article 15(1)(h). Several cases from Austria regarding Article 15 ended up at the ECJ.

34) **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 are still ongoing, however, in all likelihood the AT SA will have no enforcement action or will give recommendations to the controller. As of now, corrective measures are not planned.

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Often

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Sometimes

37) 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 content of EDPB Guidelines 01/2022 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:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

- a. Yes: [Yes](#)

The report [about this CEA with a reference to the guidelines will increase awareness.](#)

- b. No:

### **The reasoning behind conducting an anonymous fact-finding exercise for the CEF action.**

The Commission for Personal Data Protection of the Republic of Bulgaria (the CPDP) chose to undertake a comprehensive fact-finding exercise through this survey, with the aim of mapping the broader landscape surrounding data access rights. Rather than narrowing the focus to specific sectors or restricting the number of participants, the survey embraced a wide-reaching approach to capture a diverse array of perspectives. This inclusive strategy enables a more nuanced analysis of both citizens' awareness of their data rights across different sectors and demographics, and of companies' and data protection officers' adherence to their responsibilities under the GDPR.

By reaching a broad cross-section of participants, the survey offers insight into how data protection is understood and practiced across various fields. This approach not only helps identify patterns in citizens' knowledge and expectations regarding their data rights, but also sheds light on the effectiveness of GDPR compliance measures within organizations. In turn, this data offers invaluable input for constructing policies and educational initiatives that can strengthen data protection standards across the board, ensuring that practices are equitable, effective, and aligned with both legal obligations and public expectations. This approach aims to reveal whether identified issues with data protection are systemic or more prevalent in specific areas. Such insights can guide the development of more effective and inclusive strategies to enhance data protection awareness and practices across diverse sectors.

To facilitate honest and transparent responses, the survey was conducted anonymously. This anonymity encouraged participants to share their views openly, without the apprehension of oversight or regulatory consequences. With privacy assured, respondents were more likely to provide candid insights into their understanding and implementation of data protection laws, as well as their experiences interacting with data subjects. This approach effectively reduces concerns over potential repercussions or follow-up investigations, resulting in a more reliable data set.

The anonymous nature of the survey also underscores the value of collaboration between stakeholders and regulatory authorities. Rather than imposing pressure to comply, it shifts the focus toward shared, constructive efforts to improve data protection practices. By fostering cooperation, this approach emphasizes the collective responsibility of all parties to enhance transparency and uphold citizens' rights. In this way, it strengthens the foundation for a more resilient and informed data protection environment.

### **Identified problem area.**

Based on the responses gathered from the EU survey, it appears that some citizens have a misunderstanding regarding their personal interpretation of the right of access to personal data. When informed by a data controller that their data is being processed, individuals frequently interpret this notification as a signal that their data should be immediately deleted. This confusion may stem from a few factors. For one, data controllers often use complex legal jargon in their communications, which can leave citizens uncertain about their rights, leading them to assume that deletion is the most effective way to regain control. Additionally, the closely connected rights under the GDPR – such as rectification, erasure, objection, and withdrawal of consent – can create further confusion, causing citizens to believe mistakenly these rights are absolute and may be exercised unconditionally. As a result, for example, many assume deletion is a default entitlement upon request, overlooking that certain conditions may limit these rights. Heightened awareness around privacy risks and distrust in data processing may also prompt citizens to seek deletion prematurely as a protective measure against potential misuse. The complex nature of data processing – often involving multiple parties – can leave citizens feeling overwhelmed, leading them to view deletion as simpler and more secure. Finally, there is a psychological tendency to equate deletion with control, as individuals often feel that erasing data provides them with the highest level of privacy and security. Addressing these misunderstandings is essential to help citizens more fully understand and effectively exercise their data rights within the legal framework.

**Before engaging in the Coordinated Enforcement Framework**, constant proactive measures have been undertaken to educate citizens and stakeholders about their rights under the General Data Protection Regulation. One key initiative is the establishment of a dedicated telephone helpline staffed by knowledgeable experts who are available to provide information and guidance on a range of topics related to data protection and relevant national and European data protection frameworks. This service ensures that data subjects have direct access to professional support, allowing them to understand better their rights, navigate data protection policies, and receive assistance on securely managing their personal data. By offering this resource, the aim is to promote transparency and empower citizens to make well-informed decisions regarding their personal information.

Furthermore, the CPDP has provided an extensive range of informational resources on its website, including detailed information leaflets that guide data subjects on their rights. Links to these resources will be included to ensure easy access:

Links available here: [Data subject rights. \(BG\) \(EN\)](#)

Links available here (BG): [Advice when applying for a job \(BG\)](#).

Available links here (ENG): [Your personal data and the internet – advices for parents \(EN\)](#).

Moreover, the CPDP has developed a variety of educational materials specifically designed for children, such as publications, guidelines, leaflets, and informational videos. These resources aim to raise awareness about the significance of digital safety and privacy, fostering a culture of informed and responsible online behavior among younger audiences.



**Following the Coordinated Enforcement Action 2024** the CPDP aims to build positive trends at the national level, based on continuing the series of targeted initiatives on enhancing citizens' understanding of their rights and facilitating their ability to exercise the right of access to their personal data more effectively.

## 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<sup>3</sup>:
  - d. Ongoing investigation:
  
- 2) If your action is oriented toward "Fact Finding" (i.e. the first two responses in the previous question),
  - Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? **No**
  - Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. **No**
  - If not, will this fact finding activity impact your enforcement activities and if yes, how? **No**
  
- 3) For all SAs: 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) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.
  - a) **We have excluded only the questions regarding the information about the controllers to avoid identifying them.**
  - b) **We have not.**
  
- 5) For all SAs: 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 etc.)?  
**No**

## Part I – Some numbers on the controllers addressed

- 6) How many controllers did you contact?  
**4074**

---

<sup>3</sup> 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/to your questions.

51

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 response rate from controllers to the survey may be attributed to several factors. Firstly, the timing of the survey during the summer period (spring-summer), when many may be on vacation or less focused on work-related tasks, could also contribute to the reduced response. The optional nature of the survey might have also led to less engagement.

Additionally, there could be concerns about self-incrimination, which may have deterred participation despite that the CPDP took extra steps to publicly proclaim the lack of any follow-up actions including formal investigations based on the survey answers.

Finally, a general distrust in public administration based on the abovementioned reason may have played a role, with potential private respondents being hesitant to share their opinions.

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: Please select one or more answers.*

- a. Public sector: 38
- b. Private sector: 13

10) Please specify the category<sup>4</sup> of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers*

- a. Micro enterprise: 2
- b. Small enterprise: 3
- c. Medium-sized enterprise: 2
- d. Large enterprise (more than 250 employees): 8
- e. Non-profit organisation:
- f. Ministry: 2
- g. Local authority: 7
- h. Administrative authority/agency/office (e.g. job center): 13
- i. School / university / educational institution: 6
- j. Other (please specify): Judicial authority, state enterprise, district court, medical institution (hospital facility) and a banking authority (credit institution).

11) Please specify the nature of the (business) activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. education sector: 8
- b. health sector: 12
- c. social sector: 2
- d. insurance sector:

---

<sup>4</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- e. finance sector: 7
- f. IT sector:
- g. retail sector: 1
- h. logistics sector: 1
- 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): 1
- s. housing industry:
- t. manufacturing:
- u. other (please specify): 18 others.  
 Service provision and regulation; administrative services; administration of justice – authority of the judiciary; state administration with control activities; management of forest areas; territorial sole executive authority with general jurisdiction; representative of the government and the state authority.

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. customers: 23
- b. potential customers: 10
- c. employees: 40
- d. job applicants: 36
- e. children: 17
- f. vulnerable adults: 4
- g. patients: 4
- h. citizens (for public sector): 24
- i. applicants (for public services): 19
- j. recipients (for postal services): 2
- k. other (please specify): f 2 other.  
 Students, candidate-students  
 Employees of tenants and subcontractors.

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. Less than 100: 3
- b. 100 - 200: 2
- c. 201 - 500: 4
- d. 501 - 2,000: 4

- e. 2,001 - 10,000: 8
- f. 10,001 - 50,000: 7
- g. 50,001 - 100,000: 3
- h. 100,001 - 1,000,000: 5
- i. 1,000,001 - 10,000,000: 3
- j. More than 10,000,000:

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? *Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.*

- a. Contact data: 47
- b. Payment data: 27
- c. Identification data: 43
- d. Sensitive data within the meaning of Art. 9 GDPR: 21
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR: 8
- f. Other (please specify): 2 other.
- g. Students, candidate-students  
Employees of tenants and subcontractors.

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. 0 request: 29
- b. 1-10 requests: 6
- c. 11-25 requests: 2
- d. 26-50 requests:
- e. 51-100 requests:
- f. 101-150 requests:
- g. 151-200 requests:
- h. 201-500 requests: 3
- i. 501-10,000 requests: 1
- j. >10,000 requests: 1
- k. No information: 9

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

We believe we have a higher number of responding controllers from the public sector compared to private ones is due to the strong inter-institutional trust, partnership, and cooperation that characterize the public sector. Public entities often have established relationships and collaborative frameworks that facilitate more frequent and open communication.

Certain controllers are receiving a higher volume of access requests due to the nature of their sectors and the large number of data subjects they manage. The controllers experiencing the most access requests tend to be from the public education and health sectors. In the private sector, controllers from the financial industry also report a significant number of access requests.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 26
- b. >0–25%: 4
- c. 26–50% requests:
- d. 51–75% requests: 1
- e. 76–100% requests: 3
- f. No information: 17

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

*Due to the low general rate of access requests received by the controllers, it is impossible to summarise reasonable conclusions.*

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 3
- b. >0–25%: 1
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests: 12
- f. No information: 35

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

*Our findings indicate that the majority of data subjects request direct access to, or copies of, their personal data rather than information on the processing activities. The overall breakdown is around 90% requesting access to their data and 10% inquiring about processing details. We believe this is because people are generally more interested in knowing what information controllers hold about them, rather than the reasons behind the data collection.*

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 21
- b. >0–25%: 5
- c. 26–50% requests: 1
- d. 51–75% requests:
- e. 76–100% requests: 4
- f. No information: 35

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, "size" of the controller, sector)?

We believe this is because people are generally more interested in knowing what information controllers hold about them, rather than the reasons behind the data collection.

Our findings indicate that the majority of data subjects request direct access to, or copies of, their personal data rather than information on the processing activities. The overall breakdown is around 90% requesting access to their data and 10% inquiring about processing details. We believe this is because people are generally more interested in knowing what information controllers hold about them, rather than the reasons behind the data collection.

## Part II – Substantive issues regarding controllers' level of compliance

### Section on "DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS"

19) 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 2.2 in the questionnaire for controllers:

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

We found that in 72% of the responses, DPOs maintain a "Register of Data Subject Rights Management Requests." While 2% process requests on paper. Most of the replying controllers handle and store them on a secure server. Some of the controllers provided their contact forms, the contents vary depending on the sector of activity of the entity. Half of the forms require the person to specify the exact data they want to receive, while the other half use a general access to personal data form. Only one controller mentioned offering a self-service option, where the data subject can download their data independently. Larger controllers have an internal procedure for managing requests submitted by data subjects, following a specified and detailed process. In contrast, smaller controllers rely on their DPOs and have not shared detailed methodologies on how they process requests.

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

6 month storage period according to art. 25k of the Personal Data Protection Act (regarding storage period for candidate recruitment)

24 months storage period according to Art. 38 par.1 of the Personal Data Protection Act

5 year storage period according to art. 6, par. 1 c) and art. 67 par. 1 of the National law on measures against money laundering

5 year storage period according to art. 24, par. 3 of the Law on Payment Services and Payment Systems Article 9 of the Ordinance on the Procedure for the Organization, Processing, Expertise, Preservation and Use of Documents in the Institutional Archives of State and Municipal Institutions

5 year storage period according to the Special Educational Needs Ordinance

5 year storage period from internal rules and procedure for requesting the exercise of data subject rights Depending on the sector specific legislation, some respondents have mentioned also 50 years and 100 years.

- i. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.

Also

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

Storage periods are not strictly mentioned in the GDPR and national legislation gives general guidance depending on the sector or the need of the controller.

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

We observe that some controllers request data subjects to specify the categories of data they wish to access, while others provide all processed data without such distinction. Additionally, access to data may be facilitated through various channels: some controllers allow unofficial requests to be made directly to the DPOs, offer self-service options on their websites, less accept requests via phone or handwritten forms. Email or in-site requests remain the most common used method for registering requests. The duration for storing records of data access requests and related communications varies, largely due to different national regulations.

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

We believe a potential solution could involve both informal and formal campaigns led by the CPDP to raise awareness about the right to access to personal data. A campaign should inform citizens that they have the right to request personal information from both private and public institutions without fear of negative attitudes or repercussions against them. Educating the public on the deadlines for replies, cooperation, and the simplicity of the process could encourage more people to exercise their right to access their personal data.

Regardless of the active role of the CPDP the controllers should also pay special attention and implement further awareness measures in regard to inform data subjects about their rights. Thus, an entire environment (culture) for data protection can be established.

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

Our team has noticed that controllers adhere to strict processes when managing their access to information requests. They implement robust security and identification measures to ensure that requests are handled appropriately and that data protection is maintained. They also manage to reply within the set period in the GDPR. They have noted that they manage to reply within 3 to 5 business days and only one has mentioned a delay due to the volume of information. This controller mentioned they notified the data subject of the delay within 15 days of this request.

### **Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”**

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

- 21) 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 3.4 in the questionnaire addressed to controllers.



We have observed that some controllers either lack a formal procedure or tend to overlook notifying data subjects about the progress of their requests. Data subjects may not be informed about the receipt of their request, the anticipated processing time, or the completion of deadlines. This lack of communication can lead to the violation of the time specified in the GDPR if the data subject is unaware of the deadlines in the GDPR.

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

We have observed that almost all controllers have integrated a pre-defined process for handling access requests – including a monitored registry by the DPO's or have implemented a self-service tool. They have all noted that they perform due diligence and monitoring tasks on the requests for access which is completed by their DPO's, system administrators or a service team.

### **Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”**

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

23) 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 4.15 in the questionnaire addressed to controllers.

Our findings reveal that most responding controllers have indicated that their biggest challenge lies in accurately identifying the data subject. In some cases, the data subject has not properly identified themselves or refuses to give more personal information. Controllers noted that an e-signature (Qualified electronic signature) is often required to confirm identity when processing requests online, but many data subjects find obtaining an e-signature time-consuming and give up on the access request or they would instead prefer to visit the office in person to sign a paper form for access or get identified there. Additionally, 70% of respondents indicated that they do not provide verbal information due to the lack of proper identification of the data subject. However, 30% reported that they do offer verbal information when multiple identifiers, such as a client or ID number, are provided, or when working in sectors that process the data of vulnerable individuals, such as the elderly, the visually impaired, or persons with cognitive or other disabilities.

24) 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 access requests 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. 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.

The most common format for requests is .pdf or .doc and .xls for the data itself.



We found that controllers ensure the information they provide is concise, transparent, understandable, and accessible, using clear and plain language. They take an individualized approach in each case, tailoring the information to suit the specific needs of the person. Extra steps are taken when addressing vulnerable groups such as children, the elderly, the visually impaired, or persons with cognitive or other disabilities, proactively offering easily accessible resources to help these individuals exercise their rights effectively. We found that controllers consistently respond to requests within a maximum of 3-5 official working days.

Cases where responding controllers have noted that they experience delay to the data access request has been due to the volume of information and they note that the data subject is informed no longer than an average of 15 days. Delays are experienced also when further information is required in order to verify the identity of the data subject.

We believe controllers do a commendable job in identifying data subjects, with more than 90% mentioning the use of a combination of credentials such as name, ID number, personal identification number, client ID /number, or a specific document number. In cases where there is doubt about the identity of the individual (e. g., due to name or address coincidences), the responsible officer may request additional information to ensure undisputed identification. Additionally, 50% of responding controllers require an e-signature to verify the data subject's identity and process the request. The largest controller mentioned that if remote identification is not possible, the officer in the Regulatory Compliance and Control Department will invite the individual to visit the company's office for in-person identification and to sign the request, objection, or complaint.

### **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

25) 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 5.18 in the questionnaire addressed to controllers.

We found that only two of the largest responding controllers have indicated they use specialized internal software to pseudonymized data, and they process such pseudonymized data accordingly. Depending on the sector of activity of the responding controllers they provide back different types of information. It is noted that more than 87% of the responders have noted they only provide the predetermined requested type of data the data subject has requested and do not provide anything else on the side. Controllers don't tend to give out information about the process of relevant processing operations regarding their requests.

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

We found that controllers ensure the information they provide is concise, transparent, understandable, and accessible, using clear and plain language. They take an individualized approach in each case, tailoring the information to suit the specific needs of the person. Extra steps are taken when addressing vulnerable groups such as children, the elderly, the visually impaired, or persons with cognitive or other disabilities, proactively offering easily accessible resources to help these individuals exercise their rights effectively.

### **Section on “LIMITATIONS OF ACCESS REQUESTS”**

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

Our findings show that most of the responding controllers refuse to grant access to personal data only when the data subject is uncooperative in verifying their identity or has already received the requested information multiple times. Additionally, controllers only provide access to employee information when legally required to do so or when the employees are acting as representatives of the entity.

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

Our findings indicate that most of the responding controllers have not encountered situations where they declined to process an access request on the grounds of it being unfounded or excessive. Furthermore, they have not imposed fees related to administrative costs. Controllers also take steps to ensure that employee personal data is not disclosed without a valid legal basis. Additionally, four controllers mentioned they implement extra measures to protect and delete third-party data that might be inadvertently revealed, such as in video recordings or documents.

### **Part III – Impressions on the levels of awareness and compliance**

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

Our analysis shows that private controllers tend to have much stricter procedures in place, or at least were more willing to provide detailed information about their processes. The private sector has also received the most access requests. Additionally, private controllers typically have more staff, or even entire units, dedicated to overseeing personal data protection, alongside the Data Protection Officer. They also tend to implement more security measures beyond the responsibilities of the DPO.

We concluded that citizens request access to their rights less frequently in the private sector, likely due to the presence of various national regulations that authorize the processing of certain types of personal data. As a result, data subjects often find these practices reasonable and do not feel the need for further explanations or justification of the right to process.

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

- a. Very High
- b. High [Yes](#)
- c. Average
- d. Low
- e. Very low
- f. Too diverse levels to qualify

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, “size” of the controller, etc.):

The EDPB Guidelines 01/2022 are available both in Bulgarian and English on the institutional website of the CPDP and are announced via the informational bulletin. Our analysis indicates that out of the 24 responding controllers, 75% are familiar with the guidelines and actively use them as a reference in their work. However, the remaining 25% have not yet familiarized themselves with the guidelines

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

N/A

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees’ right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF? If yes, please provide the date, link to the guidance, and a short description of the guidance.

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 obtain access to their data from various entities. Our experts explain the process and assist data subjects on how to better understand and exercise their rights.

The CPDP has also published guidance on what personal information may be required when applying for a job. Link available [here](#) (BG).

We give out information that applicants should provide identification, contact details, and relevant qualifications. Unnecessary data or sensitive information like ID copies or bank details should not be requested. Employers must follow legal data protection rules and return original documents after six months if not hired.

We have also published guidance on which cases consent to the processing of personal data is not required. Link available [here](#) (BG)

We have explained that these bases include consent, necessity for contract performance, legal obligations, protection of vital interests, public interest tasks, or legitimate interests. Notably, consent is just one of several bases and is not hierarchically superior. Specific

scenarios where consent is not required include compliance with legal obligations, performance of public tasks, employment-related processing, and certain professional activities. Special categories of data, such as health information, have additional conditions for lawful processing.

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).

[“Your personal data and the internet – advices for children”](#)(EN)

[“GDPR and your rights. Data protection, a fundamental right for every EU data subject – EDPB brochure”](#) (EN).

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

No.

34) **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 launching an information campaign focused on the results of the coordinated enforcement on the right to access. The campaign will aim to raise public awareness about citizens' right to access personal data 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.

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Often

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Sometimes

37) 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 content of EDPB Guidelines 01/2022 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
  - ii. Online or remote training sessions: YES
  - iii. Conferences organised:
  - iv. Others: please specify:
- b. No:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

- a. Yes
- a. No: YES

# CZ SA

Office for Personal Data Protection

## 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<sup>5</sup>:
  - d. Ongoing investigation:

- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),

- Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? **Yes**
- Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. **No**
- If not, will this fact finding activity impact your enforcement activities and if yes, how? **We cannot completely exclude the possibility of us launching formal investigation(s), but we are not currently planning any. We are going to publish our findings from this action, and we are considering publishing some guidance material relating to this topic. We intend to follow up with relevant controllers on how (or whether) they implemented our recommendations.**

- 3) For all SAs: 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 every controller in the initial round of this action. The only major difference was made in the framing of question n. 3.1, where we allowed the respondents to address each of the aspects mentioned as separate points and we did not expect them to provide us with a continuous text.**

**We then concluded that it would be best to follow-up with the controllers as soon as possible and inquire about their responses to certain questions in the questionnaire that we felt were not answered fully. The biggest difference in the subsequent round of questioning laid in us either rephrasing the questions from the questionnaire or directly addressing some inconsistencies that we tried to resolve as soon as possible, since we currently are not planning any formal investigation(s) of the responding controllers relating to the right of access.**

**We made no changes to the questionnaire initially; different wording and additional elements were only added once we began with the second round of questioning.**

---

<sup>5</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

From this point onward we will use answers provided in the first round and the second round of questioning as a basis for our national report, as we feel the combined answers better reflect the circumstances of processing these controllers perform.

4) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.

a) We included all questions from the consolidated questionnaire.

b) We did not alter any questions in the initial round of questioning. We made additional inquiries in the second round mostly about the subject-matter of questions n. 1.4, 1.5, 2.2, 3.1, 3.2, 3.3, 4.1, 4.6, 4.7, 4.8, 4.13, 5.1, 5.14, 6.1, 6.4, 6.6, 6.7 from the original questionnaire. As we consider any other additional questions to be part of our own follow-up, we don't see a need to elaborate on the precise wording of all additional questions posed by us. Some of those questions were tailored specifically to the respondent and could therefore identify them.

The most relevant differences laid in us asking about whether they process biometric data and which biometric data they process, asking whether they process personal data of children when offering services for children, asking about their identification processes for communication via phone and their preparedness for phone number spoofing, what they would specifically do to anonymise or otherwise alter contents of their responses to protect rights and freedoms of third parties while providing access, and in us specifically asking whether they would limit access requests due to some relevant legal provisions with us making a direct reference to legal acts that could contain those relevant legal provisions.

Our questions occasionally featured amended wording of the original question or split the question into multiple parts. Some contained references to publicly available information about the controller, especially questions related to processing of biometric personal data. Other questions referenced standard threats known in the industry, such as phone number spoofing.

5) For all SAs: 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 etc.)?

Our method consisted of two fact-finding exercises. After we received the initial responses to the questionnaire, we decided to follow-up with the controllers immediately, so that there may be no confusion on the controllers' end later. It is too early to tell whether formal investigations or any other action are the right way of addressing the issues we identified or that we will identify, as we are still analysing the answers given in the second round of questioning. We therefore cannot rule out that formal investigation(s) will follow depending on our findings, but no formal investigations are currently planned.

## **Part I – Some numbers on the controllers addressed**

6) How many controllers did you contact?

22

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/to your questions.

22

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: Please select one or more answers.

- a. Public sector:
- b. Private sector: 22

10) Please specify the category<sup>6</sup> of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers

- a. Micro enterprise:
- b. Small enterprise:
- c. Medium-sized enterprise: 8
- d. Large enterprise (more than 250 employees): 14
- 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) Please specify the nature of the (business) activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. education sector:
- b. health sector:
- c. social sector:
- d. insurance sector:
- e. finance sector: 22
- 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:

---

<sup>6</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).



- 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. other (please specify):

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. customers: 22
- b. potential customers: 17
- c. employees: 22
- d. job applicants: 16
- e. children: 14
- f. vulnerable adults: 1
- g. patients:
- h. citizens (for public sector):
- i. applicants (for public services):
- j. recipients (for postal services):
- k. other (please specify):

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. Less than 100:
- b. 100 - 200:
- c. 201 - 500:
- d. 501 - 2,000:
- e. 2,001 - 10,000: 1
- f. 10,001 - 50,000: 3
- g. 50,001 - 100,000: 1
- h. 100,001 - 1,000,000: 10
- i. 1,000,001 - 10,000,000: 7
- j. More than 10,000,000:

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.

- a. Contact data: 22
- b. Payment data: 21
- c. Identification data: 22
- d. Sensitive data within the meaning of Art. 9 GDPR: 17
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR:
- l. Other (please specify):

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. 0 request: 8
- b. 1-10 requests: 9
- c. 11-25 requests:
- d. 26-50 requests: 4
- e. 51-100 requests:
- f. 101-150 requests: 1
- g. 151-200 requests:
- h. 201-500 requests:
- i. 501-10,000 requests:
- j. >10,000 requests:
- k. No information:

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

The singular outlier who stated that they received requests in amounts from 101 to 150 is not the controller processing the largest amount of personal data, which we were able to determine due to the number of concerned data subjects reported by the controllers. This might either indicate underreporting by other controllers or possibly a higher threshold for exercising data subjects' rights when it comes to controllers in question. By higher threshold, we mean that data subjects might have a hard time finding information about where or how they should request access etc. Conversely, it might indicate that the controller with the largest number of filed requests has lower threshold for exercising said right.

At the same time, we also cannot dismiss the possibility of this being a fluke and that 2023 was a statistical outlier.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 4
- b. >0–25%: 14
- c. 26–50% requests: 3
- d. 51–75% requests:
- e. 76–100% requests: 1
- f. No information:

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

There was only a singular outlier in the responses and due to the overall low number of any requests received by the controller in question nothing seems out of ordinary. Some controllers

chose to clarify that majority of requests received by them tend to be focused on exercising the right to be forgotten instead of right of access.

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 10
- b. >0–25%:
- c. 26–50% requests: 1
- d. 51–75% requests:
- e. 76–100% requests: 3
- f. No information: 8

- 17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

Controllers clearly had difficulties with this question. Sometimes this might be due to the fact that data subjects usually send a very general access requests without differentiating various options available to them. On some occasions this might be because they do not keep an evidence of access requests contents. In some cases, the controllers provided only a singular figure when the original question aimed to obtain two figures - one that would serve as basis for answer to question n. 17) in the national report and one that would serve as a basis for answer to question n. 18) in the national report. This made it impossible to tell which aspect the controllers wanted to address in their answers.

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 10
- b. >0–25%:
- c. 26–50% requests: 1
- d. 51–75% requests:
- e. 76–100% requests: 3
- f. No information: 8

- Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

Controllers clearly had difficulties with this question. Sometimes this might be due to the fact that data subjects usually send a very general access requests without differentiating various options available to them. On some occasions this might be because they do not keep an evidence of access requests contents. In some cases, the controllers provided only a singular figure when the original question aimed to obtain two figures - one that would serve as basis

for answer to question n. 17) in the national report and one that would serve as a basis for answer to question n. 18) in the national report. This made it impossible to tell which aspect the controllers wanted to address in their answers.

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 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. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.
- d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
- e. What are differences that you have encountered between controllers in your Member State?
- f. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

a) We identified some issues with respect to storage period of the information about access requests. In some cases, the controllers set an unjustifiably long storage periods which seem to have no (explicit) legal provision in EU law or national law as their bases, or where there was no logical reason for them to set the storage period for such a long time. While there might not be a specific legal provision mandating a set period of time for data storage, they might still choose a period of time using some logical (and possibly legal) criteria. For example, Czech national law sets a period of one or three years (depending on the severity of the possible sanction) for the public bodies to take punitive action towards an offender in the relevant statute of limitations. Violations of the GDPR are (standardly) subject to the three-year period. Therefore, some controllers chose to set a retention period which corresponds to this statute of limitations. On the other hand, some controllers chose seemingly arbitrarily, setting unnecessarily decades-long storage periods for information about access requests. Longer storage periods are of course justifiable and even required in the financial sector, but some answers make it clear that no legal provisions were relied on while choosing the period of time in question.

b) Art. 5(2) GDPR

Section 30 of Act. No. 250/2016 Coll., on Liability for and Proceedings on Administrative Offences

Section 16 of Act. No. 253/2008 Coll., on some Measures against Money Laundering and Financing of Terrorism

Act. No. 21/1992 Coll., Bank Act

c) Not applicable.

d) Currently, we have yet to find an explanation for the most extreme cases.

e) First difference arose from whether the controller chose to rely on any period of time referenced in relevant legislation. Second difference stems from whether the controller in question differentiated between different categories of data subjects.

f) Possible solution to the issue identified by us could lay in publishing some advisory material when we make our findings from this action known to the public. Alternatively, we could approach controllers individually and address them a letter pointing out the issue and advising them to amend the situation.]

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

Utilising software to oversee fulfilment status of the request can be useful for some controllers, especially if the program regularly reminds the assigned worker about fulfilling said request. Usage of these systems might in some cases also be connected to role management, which is also appropriate.

### **Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”**

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

21) 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 3.4 in the questionnaire addressed to controllers.

Vast majority of respondents are utilising services of processors for some of their processing operations. Presumably, their legal relationship is set up accordingly, fulfilling the requirements of Art. 28 GDPR. Yet a significant portion of controllers failed to account for these processors and the fact that they may play a role in obliging an access request.

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

Some controllers have implemented an audit procedure which leads to reassessment of the relationship between them and the processors. In some cases, this audit may include an on-site inspection. Others have implemented contractual penalties for breaching the contract, i.e. fines or even avenues for immediate termination of contract.

### **Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”**

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

23) 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 4.15 in the questionnaire addressed to controllers.

Initial round of this action revealed some potential issues when it comes to access requests made over phone. A significant portion of responders relied on some notorious identifiers or

similar information that could potentially be acquired by bad actors. This included using an already known phone number, social security number, name and surname, date of birth etc. With ever increasing data breach incidents it is not impossible to think that such measures could prove to be insufficient due to previously leaked information. Taking this to the extreme, it could lead to a possible data breach on the controllers' end.

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

Some controllers utilise their applications in ways that allow them to ascertain the identity of the caller using a higher factor authentication. The controllers' employee sends a push notification via their application while on a call with whoever is making the access request. Responding to this push notification proves in the very least that the person making the call also has access to a verified device, making this a 2FA.

Some applications are apparently written to allow calls made from the application directly, which serves as a higher factor authentication on its own. We cannot speak about the quality of this solution, since it was not the subject of our fact-finding exercise, but if the rights of data subjects are respected then it presents itself as another multi-factor authentication option.

If a relatively simple way of identification was employed by the controller, then some controllers also made sure that whoever made the request could only file the request. They would not receive a response over the phone. The response would be sent to a pre-agreed address.

### **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

25) 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 5.18 in the questionnaire addressed to controllers.

What could potentially pose an issue is the fact that vast majority of the controllers in question make use of a pre-defined set of information that they send out as a response to an access request. It is unlikely that this pre-defined set manages to encompass all of the personal data processed and therefore it could limit the exercise of the right pursuant to Art. 15 GDPR in its entirety. The controllers must understand that if a data subject that filed an access request is not satisfied with this pre-determined data set, then they will be obliged to attempt to fulfil the request using a different scope of data if the data subject's right of access prevails over rights and freedoms of others. Otherwise, they run afoul of the possibility of failing to uphold their obligations pursuant to Art. 15 GDPR.

Responses to the question related to clarifying data subjects' requests indicate that the question was usually understood only in context of ascertaining the identity of the person making the request. Most controllers did not address the possibility of asking the data subject to specify their request with regard to the type of personal data they are interested in. The controllers in question undoubtedly process vast amounts personal data and therefore asking for clarification as advised by the Guidelines in section 2.3.1. might be a useful approach to

some respondents as it might make the controllers' response to the request more comprehensible.

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

Not applicable.

### Section on “LIMITATIONS OF ACCESS REQUESTS”

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

Some respondents reductively stated that they give access to every information they have on the person requesting access. This obviously cannot be true, because besides the fact that GDPR itself accounts for possibility of situations when denying access is the correct approach, relevant provisions of legislation which detail AML measures or confidentiality occasionally explicitly forbid certain entities from providing access to certain information. Controllers we approached, banks, would certainly be obliged to deny access in cases falling within the scope of AML legislation, which makes this omission on the controllers' part odd.

Besides the abovementioned, vast majority of controllers stated that they would not provide data subjects with information about the identity of individuals within their organisation. While in general this approach is not incorrect, occasionally it might be necessary to share such information in cases where the information about identities of these individuals will be necessary for the data subject's ability to verify lawfulness pursuant to Art. 5(1) GDPR and provided that the rights and freedoms of the employees involved are taken into account. We make this comment with regard to recent case-law of the CJEU (see C-579/21, Pankki S). It is possible that the awareness concerning this possibility is not currently very high among the controllers.

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

Not applicable.

## Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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



29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

The biggest differences were observed between controllers that offered so-called 'retail' services and those that did not. We approached every bank in Czechia and therefore even entities offering their services primarily to businesses and entrepreneurs were included in the enforcement action. Controllers like that generally did not have a hands-on experience with data subjects exercising right of access but adopted internal procedures to fulfil their GDPR obligations. The controllers offering retail services had more specific experience and could reference previous events when relevant.

Other differences stemmed from the varying sizes of controllers. Some controllers process personal data of millions of data subjects and therefore have a larger amount of access requests to deal with.

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, "size" of the controller, etc.):

Most responding controllers have stated that they familiarized themselves with the Guidelines in question. However, the Guidelines were not available in Czech when the questionnaire was first sent out, which may have affected the level of understanding among the respondents and should be therefore taken into account. The controllers also may be affected by the lack of awareness of previous WP29 guidelines referenced, which would be able to further explain some related terms (such as 'layered approach') to them.

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

Some controllers exhibited lower understanding of layered approach, which played a significant part in the Guidelines on the right of access. While layered approach is not something that can play a role only in responding to the data subject in general and therefore exceeds the context of Art. 15 GDPR, it is nonetheless important enough to examine its usage in the context of providing access as well. Significant amount of the respondents already uses elements of the layered approach in their day-to-day practice, but they are not making full use of the concept. Oftentimes they present the pre-defined set of personal data provided in response to an access request as 'giving the data subject everything they have', when this is unlikely to be true. If they were to approach this pre-defined set as a first layer that can be supplied, then this could be a more suitable practice.



## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees' right of access; right of access exercised in the public sector, or regarding data concerning health, 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.

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

Right of access is something we focus on 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 regarding right of access is either a letter addressed to the controller concerned, 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 that controller needs to react to the right of access request accordingly (corrective measure) in certain time period and this decision can also impose a fine.

34) **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 going to publish our findings, which we intend to accompany with recommendations based on these findings. We then intend to follow up with relevant controllers on how (or whether) they implemented these recommendations.

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Very often.

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Very often.

37) 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 content of EDPB Guidelines 01/2022 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:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes:

b. No: **No**

## DE SAs

Consolidated report for all participating German SAs, i.e. SAs of Bavaria for the private sector (BayLDA), Brandenburg, Mecklenburg-Western Pomerania, Lower Saxony, Rhineland-Palatinate, Schleswig-Holstein, Saarland 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<sup>7</sup>: **Yes**
  - d. Ongoing investigation: **No**
  
- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),
  - Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? **Yes**
  - Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. **Yes. Partially, in particular on-site audit of one controller in 2024. Additionally, the new findings can be used to prioritise supervisory activities where necessary, and to better alert controllers to priorities/problematic topics as preventive measures.**
  - If not, will this fact finding activity impact your enforcement activities and if yes, how?
  
- 3) For all SAs: 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.

Slightly different versions used for:

  - 3 controllers in the (federal) economic administration sector (who all received the same questionnaire),
  - 4 controllers in the (federal) social sector (who all received the same questionnaire),
  - 15 controllers in Lower Saxony (who all received the same questionnaire).
  
- 4) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.
  - 3 controllers in the (federal) economic administration sector: the following questions have not been asked: Q 3.3, 4.3, 4.5, 4.6, 5.13, 5.15
  - 4 controllers in the (federal) social sector: the following questions have not been asked: Q 4.6, 5.15

---

<sup>7</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

- 15 controllers in Lower Saxony: the following questions have not been asked: 3.1, 3.2, 3.3, 3.4, 4.7, 4.13, 4.14, 5.5, 5.12, 5.15, 5.17, 6.3, 6.8, 7.1, 7.2.

5) For all SAs: 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 etc.)?

For clarification purposes, this is a consolidated National Report of all 8 German SAs participating in the CEF 2024 Action. The findings presented herein may not be valid for other German SAs which have not participated in this CEF.

Furthermore, not all participating German SAs contributing to this National Report have contacted the same number, types or sectors of controllers. Not all findings listed in Part II of this National Report apply to all responding controllers; and not all findings, impressions, possible explanations or solutions are valid or apply in full to each participating German SA. The issues presented are either the ones that the participating German SAs consider to be the most common or the most important. Where there is no response given to subquestions lit. e (“What are differences that you have encountered between controllers in your Member State?”), this should not be interpreted as stating that there are no differences. Rather, based on the CEF Action and the controllers contacted, a meaningful answer cannot be provided. Finally, not all options selected for answers in this National Report precisely reflect the practices of all participating German SAs. For example, in Q 35 and 36 below (reference to EDPB Guidelines) the responses of the participating German SAs vary.

As an overall remark, many of the controllers contacted, throughout all participating German SAs, have stated that they received a low to very low number of access requests during the time in question. This seems to be the case even for bigger controllers. Possibly, the right of access is either not sufficiently known to data subjects or is only used in very limited circumstances.

As an overall background information, in Germany, (most) public sector controllers cannot be fined in accordance with Art. 58(2)(i), 83 GDPR due to restrictions imposed by the legislator in national law.

Clarification on Q 13 below (approx. number of data subjects): Three of the responding controllers have not provided an answer to this question.

## Part I – Some numbers on the controllers addressed

6) How many controllers did you contact?

116

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/to your questions.

115

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?

In one case, extension of deadline to respond.

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: Please select one or more answers.

- a. Public sector: 25
- b. Private sector: 90

10) Please specify the category<sup>8</sup> of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers

- a. Micro enterprise: 6
- b. Small enterprise: 13
- c. Medium-sized enterprise: 25
- d. Large enterprise (more than 250 employees): 46
- e. Non-profit organisation: 0
- f. Ministry: 2
- g. Local authority: 3
- h. Administrative authority/agency/office (e.g. job center): 19
- i. School / university / educational institution: 1
- j. Other (please specify): 0

11) Please specify the nature of the (business) activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. education sector: 1
- b. health sector: 3
- c. social sector: 5
- d. insurance sector: 6
- e. finance sector: 24
- f. IT sector: 1
- g. retail sector: 5
- h. logistics sector: 1
- i. public transportation: 0
- j. telecommunications: 0
- k. postal services: 0
- l. advertising sector: 2
- m. marketing services: 3
- n. entertainment sector: 2
- o. information / journalism sector: 0
- p. scientific / historical research: 0
- q. credit scoring agency: 0
- r. public utility/infrastructure provider (e.g. energy): 22
- s. housing industry: 5
- t. manufacturing: 1
- u. other (please specify):

---

<sup>8</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- Administrative or local district administrative authority: 15 responding controllers,
- Economic administration: 3 responding controllers,
- Public employment / HR administration: 1 responding controller,
- Hotel and restaurant industry: 4 responding controllers,
- Tourism: 4 responding controllers,
- Car dealers: 3 responding controllers,
- Recruitment: 1 responding controller,
- Leisure sector: 2 responding controllers,
- Mobility: 1 responding controller.

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. customers: 89
  - b. potential customers: 54
  - c. employees: 91
  - d. job applicants: 60
  - e. children: 17
  - f. vulnerable adults: 7
  - g. patients: 3
  - h. citizens (for public sector): 22
  - i. applicants (for public services): 17
  - j. recipients (for postal services): 0
  - k. other (please specify):
- Debtors: 5 responding controllers,
  - Members of expert circles: 1 responding controller,
  - Claimant and damaged/injured third parties: 2 responding controller,
  - Policy holders/insured persons: 1 responding controller,
  - Internet users: 1 responding controller,
  - Brand ambassadors/influencers: 1 responding controller,
  - Shareholders: 1 responding controller,
  - Suppliers / contractual partners: 5 responding controllers,
  - Adolescents, persons responsible for paying alimonies/support, contractual partners of applicants (e.g. landlords, insurances, banks, other third parties): 4 responding controllers,
  - Other types of applicants, customers or participants: 1 responding controller,
  - Volunteers: 1 responding controller,
  - Representatives of companies and associations: 2 responding controllers,
  - Chosen "other" but not specified: 2 responding controllers.

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. Less than 100: 3
- b. 100 - 200: 0
- c. 201 - 500: 0
- d. 501 - 2,000: 1

- e. 2,001 - 10,000: 17
- f. 10,001 - 50,000: 18
- g. 50,001 - 100,000: 7
- h. 100,001 - 1,000,000: 39
- i. 1,000,001 - 10,000,000: 23
- j. More than 10,000,000: 4

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.

- a. Contact data: 109
- b. Payment data: 95
- c. Identification data: 75
- d. Sensitive data within the meaning of Art. 9 GDPR: 30
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR: 3
- l. Other (please specify):
  - Asset data: 2 responding controllers
  - Contract data: 2 responding controllers
  - Images: 1 responding controller
  - Appointment information (e.g. time, organisation unit): 1 responding controller
  - Claims and benefit data within the scope of insurance contracts: 1 responding controller
  - Information on consumption and meter readings: 10 responding controllers
  - Dates of birth: 2 responding controllers
  - Access data: 1 responding controller
  - Financing requests: 1 responding controller
  - Location information: 1 responding controller
  - Content of emails sent to the data subject: 1 responding controller
  - Device log files and configurations: 1 responding controller
  - Information about computers, devices and connections, such as Device application software, browser types and versions: 1 responding controller
  - Information about internet or platform accounts and account settings: 1 responding controller
  - Purchase or refund information: 1 responding controller
  - Information about the data subject's interactions with the services offered: 1 responding controller
  - Information about the data subject's subscriptions and personal preferences in relation to the services offered: 1 responding controller
  - Information about content interactions, such as content downloads, streams and playback details, including duration and number of simultaneous streams and downloads, and network details for streaming and download quality, including information about the data subject's internet service provider: 1 responding controller
  - Data on the granting of social benefits, career or job counselling and job placement: 4 responding controllers
  - Data related to decisions on the establishment, performance or ending of an employment relationship (e.g. personnel CV, personnel file, insurance status): 12 responding controllers
  - Other data on professional activities and relationships in terms of company law: 1 responding controller
  - Vehicle identification number, licence plate: 1 responding controller
  - Chosen "other" but not specified: 14 responding controllers.

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. 0 request: 39
- b. 1-10 requests: 40
- c. 11-25 requests: 13
- d. 26-50 requests: 7
- e. 51-100 requests: 5
- f. 101-150 requests: 2
- g. 151-200 requests: 1
- h. 201-500 requests: 1
- i. 501-10,000 requests: 2
- j. >10,000 requests: 1
- k. No information: 4

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

Certain controllers do not register access requests in a centralized manner, which is why they cannot provide the relevant numbers.

Overall, it seems (even though this is not true for all contacted controllers) that controllers responsible for the most data subjects also receive the most requests.

Based on the questionnaire it seems that data subjects are less likely to exercise their right of access when the controller is a public authority, but rather use it for commercial controllers / controllers in the private sector.

Low numbers of access requests in the private sector can otherwise possibly be explained in the B2B sector (considering these are mostly professional data used in business transactions) and in the employee context (which is a permanent relationship and access requests are probably only asserted in very specific cases).

However, considering the low number of access requests received even by bigger controllers, it seems that the right of access in general is quite unknown among data subjects. It seems that data subjects that exercise their right of access tend to have had some sort of conflict with the controller before exercising their data subject rights (e.g. where there is a high volume of customer complaints overall).

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 32
- b. >0–25%: 21
- c. 26–50% requests: 20



- d. 51–75% requests: 9
- e. 76–100% requests: 17
- f. No information: 16

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

The variation of percentages does not seem explicable with reference to the sectors or sizes of controllers. In some instances, it might be purely statistical. A considerable amount of responding controllers did not have statistics at hand, possibly due to either having no central registration of data subject rights / access requests, or due to the little amount of requests received in total.

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 39
- b. >0–25%: 14
- c. 26–50% requests: 14
- d. 51–75% requests: 5
- e. 76–100% requests: 25
- f. No information: 18

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

Certain controllers do not register requests in a centralized manner, which is why they cannot provide the relevant numbers. However, controllers with small numbers of access requests seem to have a higher percentage of specific requests to receive a copy. Also, data subjects seem to be more likely to request a copy of their personal data when there are special categories of personal data according to Art. 9 GDPR involved.

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 51
- b. >0–25%: 17
- c. 26–50% requests: 10
- d. 51–75% requests: 5
- e. 76–100% requests: 11
- f. No information: 21

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No explanation. However, certain controllers do not register requests in a centralized manner, which is why they cannot provide the relevant numbers.

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

- 19) 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 2.2 in the questionnaire for controllers:
- Name the issue(s) identified and briefly describe it.
  - Which provision(s) of the GDPR (or national laws) does this concern?
  - If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.
  - Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
  - What are differences that you have encountered between controllers in your Member State?
  - What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

#### Issue 1

##### a. Issue identified

There is a tension between the obligations of the controller to delete data and the need to prove fulfilment of access requests, e.g. in an audit or a legal dispute. In some cases, access-request related information is deleted immediately after the requests have been answered. In other cases, there is no separate storage of the documentation regarding access requests and associated correspondence, but the relevant documentation is stored in the productive system. The documentation in question is then (a) subject to the general access rights implemented by the controller for handling a data subject’s file, and (b) can be subject to the general retention periods corresponding to other types of information like business records or tax documentation, leading in some cases to particularly long retention, and differing even between similar controllers.

##### b. GDPR or national law provision

- Art. 5(1)(e), Art. 17 GDPR
- Art. 5(1)(f) GDPR
- Art. 5(2) GDPR
- Section 34(2)3 German Federal Data Protection Act (BDSG), Art. 18 GDPR on separate storage with restrictive access rights
- Section 35 BDSG on specifics regarding deletion (Art. 17 GDPR) and restriction of processing (Art. 18 GDPR)

##### c. CJEU caselaw / EDPB Guidelines 01/2022

N/A

##### d. Potential explanation

Both in the public and the private sector, controllers often formally handle access requests as regular business/administrative procedures connected to other procedures of the same data subject.

In the private sector, controllers state that most access requests are motivated by legal disputes, which is why they base retention periods e.g. on the (regular or maximum) civil limitation periods under German law for the purpose of potential legal justification.

e. Differences between controllers in your Member State

In particular in the private sector, controllers also take into account possible complaints of data subjects and subsequent investigations and administrative procedures of the supervisory authority. In this regard the documentation on access requests is stored for the purpose of potential legal justification. Different experiences in legal disputes, as well as taking into account the (regular or maximum) civil limitation periods under German law, probably led to setting different retention periods (e.g. between 3 and 10 years).

f. Possible solutions

- Requesting relevant controllers to ensure separate storage of access request documentation with corresponding limited access rights to such documentation.
- Awareness-raising and recommendations for an appropriate storage period and uniform and meaningful criteria for its determination, clarifying that general retention periods applicable to other types of information should not be used as a rule for access request documentation.

## **Issue 2**

a. Issue identified

For certain controllers, there is no centralized registration of access requests. Controllers handling access requests on a decentralised basis often store them exclusively in the electronic file of the respective data subject (see also issue no. 1 above). This leads to difficulties for such controllers, in particular in the public sector using specific IT systems, to comply with their accountability obligations.

b. GDPR or national law provision

Art. 5(2) GDPR

c. CJEU caselaw / EDPB Guidelines 01/2022

N/A

d. Potential explanation

In order to fulfil their tasks, certain controllers in the public sector use IT systems and procedures which are managed centrally by a separate entity responsible for such IT systems; and are obliged to access a common central database created on this basis. These IT systems currently do not provide for a separate documentation for data subjects' rights.

e. Differences between controllers in your Member State

At some controllers with central handling of access requests by (or information of) the data protection officer, the requests are also stored there

f. Possible solutions

The separate entity responsible for the respective IT systems has now announced that it will expand the electronic file system to include the section “Data subjects’ rights under the GDPR”. This should make it easier to monitor compliance with the GDPR.

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

- Access and role management concepts ensuring “need to know” restriction for access request related information, often linked to legal departments of controllers and DPO, and in particular once the access request has been answered
- Information and/or involvement of the DPO in supervising and documenting access requests
- Central registration of access requests by certain controllers
- Use of tools developed for data protection and data processing management, e.g. identification and documentation of personal data, assignment of data origin, consent and processing documentation, documentation of data subjects’ requests such as access requests, technical procedures to export data, ensure deletion or anonymization in certain periods etc.

### **Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”**

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

21) 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 3.4 in the questionnaire addressed to controllers.

#### **Issue 1**

a. Issue identified

Controllers especially in the public sector who have only received very few access requests in recent years have not developed a systematic process to handle and monitor the handling of access requests.

b. GDPR or national law provision

Art. 24, 25, 5(2), 15 GDPR

c. CJEU caselaw / EDPB Guidelines 01/2022

N/A

d. Potential explanation

The low number of access requests received by such controllers and therefore considered minor relevance, as well as the lack of experience with access requests might be a possible explanation.

e. Differences between controllers in your Member State

Controllers in the private sector or controllers having received a larger number of access requests were able to demonstrate far more detailed pre-defined procedures and internal guidance.

f. Possible solutions

Guidance and recommendations on how to pro-actively implement pre-defined procedures in light of the responsibility of the controllers according to Art. 24(1) and (2) GDPR

**Issue 2**

a. Issue identified

Not all controllers register and handle access requests in a centralized manner by a dedicated central unit. Rather, access requests are handled separately by the departments concerned, or by the specific department(s) responsible for handling the data subject's overall proceedings/files. This can lead i.a. to incorrect, incomplete or delayed responses to access requests, or to confirmations of receipt not being sent.

b. GDPR or national law provision

Art. 24(1), 25(1), 15, 12 GDPR

c. CJEU caselaw / EDPB Guidelines 01/2022

Para. 57 Guidelines 01/2022 on confirmation of receipt as best practice

d. Potential explanation

Missing centralized registration and handling of access requests is often due to the internal structure of responding controllers and sometimes the (mandatory) IT infrastructure used.

e. Differences between controllers in your Member State

Different internal structures between controllers, often grown over several years.

f. Possible solutions

Recommendation to revise existing procedures and possibly establish a central unit registering and handling all access requests (improvement / optimisation in some cases already announced by responding controllers / IT infrastructure providers)

**Issue 3**

a. Issue identified

Where processes for handling access requests are implemented in general, there is still room for improvement in detail, particularly when it comes to controllers in the public sector. In particular:

- central handling of access requests is recommended, but controllers must ensure that requests received are (a) identified as access requests under Art. 15 GDPR where applicable and (b) forwarded to this central unit, and that coordination and cooperation between this central unit and other units processing relevant personal data for each request is ensured, including by clearly defined and documented instructions on how to handle access requests and a clear assignment of roles,
- the process should include procedures for handling access requests submitted via authorised third parties,
- it should be clearly defined and documented which inventory, data pools and processes must be verified to determine the data to be included in a response to an access request; this requires a prior assessment of the scope of the access right under Art. 15 GDPR,
- there should be a structured and documented approach on the handling of possible rights and freedoms of third parties affected pursuant to Art. 15(4) GDPR,

- it should be clearly determined which person/unit is responsible for which assessment, and which person/unit takes the final decisions on any outstanding questions,
- the legal role of the DPO as an internal contact person and supervisor, but not as an executive body in place of the controller, should be clarified.

b. GDPR or national law provision

Art. 24(1), 25, 5(2), 15(4) GDPR

c. CJEU caselaw / EDPB Guidelines 01/2022

Sections 2.2.3, 6.2 Guidelines 01/2022 for Art. 15(4) GDPR

d. Potential explanation

Possibly due to sometimes rather low numbers of access requests (see above). Regarding the correct classification of communication as being access requests, they can be communicated informally via many channels and therefore do not always stand out from other requests.

e. Differences between controllers in your Member State

Shortcomings in the design of procedures for handling access requests almost exclusively concern the public sector.

f. Possible solutions

Corresponding recommendations and advice to relevant controllers; potentially separate investigations and, where necessary, exercising corrective powers

#### **Issue 4**

a. Issue identified

During the implementation of new tools and digitization of processes data subjects' rights are barely taken into account (apart of being considered within the record of processing activities and the involvement of processors). This also concerns the onboarding of new processors. This can also lead to processors, data bases or processes not being taken into account or verified when handling an access request.

b. GDPR or national law provision

Art. 24(1), 25 GDPR

c. CJEU caselaw / EDPB Guidelines 01/2022

Para. 137 Guidelines 01/2022

d. Potential explanation

For many public authorities, a possible explanation could be that personal data is still mostly being processed by other than automated means and the right of access is consequently interpreted with regards to documents and files.

e. Differences between controllers in your Member State

N/A

f. Possible solutions

- Corresponding recommendations and advice to relevant controllers regarding the onboarding of new tools or processors.
- Recommendation to implement tools to support the retrieval of personal data and of self-service tools which could facilitate the handling of access requests (para. 137, 138 Guidelines 01/2022), taking into account the principle of purpose limitation

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

- Implementing procedures facilitating the exercise of the right of access for data subjects (e.g. providing possibilities to automatically receive a copy of the data in a data subject's account and educating controller employees to inform data subjects about this).
- Extensive concepts for the protection of data subject rights developed by controllers and handed over to employees, awareness training for all employees to ensure that access requests are recognized and forwarded to the competent unit without any delay.
- Establishment of a specific organizational unit that is detached from day-to-day business which, if necessary using special software, collects the information on the data subject from the various specialist departments and their respective systems and compiles it into a report, supplements it with data restricted from processing, checks its completeness and makes it available to the data subject.
- Implementation of a process in which the department of compliance is mainly responsible for handling the requests for access and the data protection officer monitors the process and the compliance with the data protection provisions.
- In addition to the Data Protection Officer, Internal Audit also monitors the complaints processes (access requests are a subset of these).
- Annual report of the data protection officer is submitted to the Executive Board, containing information on monitoring and handling access requests.
- Early involvement of the data protection officer in new processes and processing activities.
- Confirmation of receipts are often sent automatically but at the latest when it is clear that the handling of the request cannot be completed immediately, and mostly including a note about the expected processing time/end of deadline.
- The German Saving Banks and Giro Association founded a working group to provide specific guidance as to the right of access and the necessary implementation of processes.

## **Section on "IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR"**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

23) 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 4.15 in the questionnaire addressed to controllers.

### **Issue 1**

#### a. Issue identified

Controllers condition the handling of access requests to the adherence to specific formal requirements (e.g. requiring requests to be in writing or text form), sometimes stating that only the receipt of a request in such a specific form would trigger the deadline in Art. 12(3) GDPR. In particular, many controllers do not accept oral access requests and/or requests for oral



information at all, without further examination of the specific request. This in practice means that certain controllers cannot accommodate certain requirements, in particular accessibility needs of data subjects.

b. GDPR or national law provision

Art. 12(1)1, 12(2)1, 12(2)3, 25(1) GDPR

c- CJEU caselaw / EDPB Guidelines 01/2022

Paras. 52, 128, 133, 142 Guidelines 01/2022

d. Potential explanation

A possible explanation could be that accepting oral access requests/providing access only orally is perceived as risky with regard to the identification of the data subject and the subsequent proof of the provision of access. Reasons provided by the controllers as to why they did not yet establish processes to provide access for certain accessibility needs is the genuinely low number of access request and no case where accommodating certain accessibility requirements was ever necessary.

e. Differences between controllers in your Member State

There is a higher focus in the need to identify data subjects and therefore more restrictions on e.g. providing access via telephone when the controllers process special categories of data acc. to Art. 9 GDPR.

f. Possible solutions

Awareness-raising measures and recommendations to relevant controllers, in particular informing about the legal situation and the circumstances in which the receipt of an oral request for information or an oral provision of information can and should take place, and further guidance on different / separate methods for authentication of the data subject in this context. At least where the level of compliance in combination with other requirements regarding the right of access is low, this issue will be included in follow-up investigations.

## **Issue 2**

a. Issue identified

In particular public sector controllers request further information to identify data subjects in an excessive manner: (a) even in cases where there aren't any reasonable doubts about the data subject's identity, or (b) the minimum information collected for identification is to be considered excessive for this purpose (e.g. partly anonymised ID cards, other additional information not required for identification).

b. GDPR or national law provision

Art. 12(6) GDPR

c. CJEU caselaw / EDPB Guidelines 01/2022

Section 3.2, in particular para. 65 Guidelines 01/2022

d. Potential explanation



Controllers often state that these measures are necessary to ensure confidentiality and to confirm the identity of the data subject, possibly considering risks of unauthorized disclosure. Furthermore, controllers seem to want to standardise identification processes for all cases.

e. Differences between controllers in your Member State

The issue seems to affect in particular public sector controllers. For example, controllers of the banking sector accept the authentication method of the bank account as valid additional information to confirm the identity of the data subject.

f. Possible solutions

Further recommendations and guidance to relevant controllers, in particular clarifying that requesting additional information for identifying the data subject requires a case-by-case assessment.

**Issue 3**

a. Issue identified

The (one-month and/or extended) deadline can pose a challenge for certain controllers, for example public agencies, due to the complexity of the requests or the complexity of the processing activities (e.g. large data volume stemming from several different administrative procedures including different units and departments, verification of third parties' rights, provision of copy from (outdated) IT systems).

b. GDPR or national law provision

Art. 12(3) GDPR)

c. CJEU caselaw / EDPB Guidelines 01/2022

Section 5.3, in particular para. 163 Guidelines 01/2022

d. Potential explanation

The processing activities of such controllers are very complex. For some requests the legal department must be consulted. In case of certain public agencies, a large amount of data can be processed in paper form or stored in IT systems which, due to their age, have not been designed to facilitate the handling of access requests.

e. Differences between controllers in your Member State

N/A

f. Possible solutions

Further recommendations to controllers on how to optimize their procedures.

**Issue 4**

a. Issue identified

Without login to an online-platform (e.g. online-banking, user portal) of controllers it can be challenging to get (secure) access to personal data in an electronic format. In some cases, the controller does not have sufficient security measures in place when providing access (e.g. passwords which are not sufficiently secure; providing access via postal services without taking sufficient measures to ensure that the information is provided to the correct recipient, end-to-end encrypted e-mail is rarely used).

b. GDPR or national law provision  
Art. 15(3), 25, 32 GDPR

c. CJEU caselaw / EDPB Guidelines 01/2022  
Para. 32, 40, 134 Guidelines 01/2022

d. Potential explanation

Where there are user portals or online platforms provided by the controller, most data subjects have a respective login; controllers therefore seem to wish to lead all data subjects there for efficiency reasons. It is also possible that data controllers see the advantage of using their own platform in the fact that it is easier to authenticate the person making the request and ensure sufficient security measures.

e. Differences between controllers in your Member State  
N/A

f. Possible solutions

Recommendations to relevant controllers on how to provide access, including copies, electronically and securely, also clarifying that selecting a format for the provision of access requires taking into account the corresponding risks for data subjects – also taking into account secure postal services like registered mail, pick-up of requested documents at controller's premises or sending electronic information on encrypted USB sticks.

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

- Access requests concerning employee data are being handled by the HR department due to the necessary higher level of confidentiality.
- Controllers take into account the wishes of data subjects concerning their format to provide access.
- To address special characteristics of data subjects, external service providers are involved, for example, to draft responses in plain language.

## **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

25) 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 5.18 in the questionnaire addressed to controllers.

### **Issue 1**

a. Issue identified

Controllers have difficulties grasping the scope of the access right and the scope of the term “personal data” in practice. Compiling personal data for an access request is only performed by searching the most common internal systems and not all data banks are verified for every

access request; controllers are not sufficiently aware that personal data can also be contained in non-textual files, in meta data or in back-up data.

b. GDPR or national law provision

Art. 4 no. 1, 15(1) GDPR

c. CJEU caselaw / EDPB Guidelines 01/2022

Paras 34, Section 2.3.1, paras. 35, 37, 91-122 Guidelines 01/2022

d. Potential explanation

Often, the controller does not have one individual system in which all data are processed. Instead, in the course of increasing and changing tasks, organizational peculiarities and technical progress, individual systems, databases and specific applications have gradually emerged or were added over years and decades. In addition, various service providers are used. This means that, in addition to the existing core system, a large number of other ancillary systems, alternative sources and, as the case may be, paper files, would have to be searched for each request for access. This involves a great deal of effort for the controller.

e. Differences between controllers in your Member State

This challenge mainly affects large controllers who process the personal data of a large number of data subjects in a wide range of tasks and processing activities and who have structures that have grown over many years.

f. Possible solutions

Recommendations to relevant controllers, possibly suggesting stronger referral to the record of processing activities to precisely identify possible storage locations of personal data, and recommendation / awareness-raising to take into account data subjects' rights already during the process of onboarding new IT systems or processors, enlarging the organisational structure of the controller and beginning new processing activities.

## **Issue 2**

a. Issue identified

Insofar as an assignment of personal data to a data subject, e.g. when using cookies, is only possible on the basis of a specific identifier, the necessary information was not pointed out to data subjects from the outset but only at a later point in time or not at all. E.g., a controller states that assigning data to an access request based on the commonly available data (e.g. name, e-mail address) is not possible. In such cases, the controller sends a negative confirmation to the data subject, but includes that a new request could be made for the receipt of further information and identity features to be checked, such as technical identification features or identifiers, can be provided for this purpose.

Insofar as a controller has to assume on the basis of its business model or its specific processing activities that personal data cannot be assigned to a name or an e-mail address, but requires a different identifier for the assignment, the controller should inform transparently about this in accordance with Art. 12(2) GDPR (facilitating the exercise of rights) at the latest when data subjects are exercising their rights.

b. GDPR or national law provision

Art. 12(2), 15(1), Art. 24(1), 25(1) GDPR

c. [CJEU caselaw/ EDPB Guidelines 01/2022](#)  
Para. 128 Guidelines 01/2022

d. [Potential explanation](#)  
N/A

e. [Differences between controllers in your Member State](#)  
N/A

f. [Possible solutions](#)

Awareness raising with the aim that controllers explain to data subjects, if possible at the time when they are requesting access, that a corresponding identifier may have to be communicated in order to receive comprehensive information.

### **Issue 3**

a. [Issue identified](#)

Some controllers ask data subjects to specify their request for information automatically in all cases, (1) without verifying whether the access request in question leaves any doubt about the scope of the request or (2) whether the controller processes a large amount of personal data concerning the concrete data subject, and (3) without any pre-check or plausibility check in the controller's system related to the specific access request, and (4) in some cases without informing data subjects about any processing operations that could concern them and (5) in some cases making the specification of the request a pre-condition for its further handling. For this purpose, in some cases access requests are answered with a general letter and only after further reaction from the data subject, the requested information is provided.

b. [GDPR or national law provision](#)  
Art. 15(1), Recital 63 sentence 7, Art. 24, 25 GDPR

c. [CJEU caselaw / EDPB Guidelines 01/2022](#)  
Section 2.3.1, in particular para 35(b) Guidelines 01/2022

d. [Potential explanation](#)

Especially regarding general access requests, controllers seem to consider the handling as being a high burden and severe interference with their usual tasks/duties/businesses. This seems to be the case in particular where the controller generally processes a large amount of personal data in different systems, departments and procedures, and by several service providers.

Also, the possibility to proceed in these two stages was considered admissible by some supervisory authorities immediately after the entry into force of the GDPR, so that the process may have continued unchanged.

e. [Differences between controllers in your Member State](#)

This challenge mainly affects large controllers who process the personal data of a large number of data subjects in a wide range of tasks and have structures that have grown over many years. On the other hand, controllers with more detailed internal processes and a higher level of digitalisation seem to rather not ask data subjects to specify their access requests.

#### f. Possible solutions

Recommendation to respective controllers regarding the scope of application of recital 63 sentence 7 and the use cases in which specification can be requested, clarifying that each access request must be assessed on a case-by-case basis with regard to its scope, and at least some kind of plausibility check with regard to the respective data subject should be performed before asking for a specification of their access request, information on the processing activities potentially concerning the data subject should be included, and that the specification by the data subject cannot be made a pre-condition for further handling of the request.

For supervisory authorities, revision of publications on the right of access where necessary and awareness raising about this fact.

### **Issue 4**

#### a. Issue identified

The information required according to Art. 15(1)(a)-(h) GDPR is not being tailored to the data subject, in particular regarding the relevant data categories, storage periods and recipients. In many cases the controllers refer to the general information according to Art. 13 GDPR. A number of controllers disclose the specific recipients in accordance with Art. 15(1)(c) GDPR only in cases of specific requests. The retention period is commonly only specified in general terms, without distinguishing between different processing operations or data categories.

#### b. GDPR or national law provision

Art. 12(1), 15(1), in particular lit. (c) and (d), Recital 63, Art. 24, 25 GDPR

#### c. CJEU caselaw / EDPB Guidelines 01/2022

Paras. 11, 112 et seq. Guidelines 01/2022

CJEU, 12.1.2023, C-154/21 (for Art. 15(1)(c) GDPR)

#### d. Potential explanation

The controllers often use a template to provide the information required according to Art. 15(1)(a)-(h) GDPR which seems to be similar to the general information provided in accordance with Art. 13 GDPR.

#### e. Differences between controllers in your Member State

N/A

#### f. Possible solutions

Guidance / awareness raising concerning the CJEU caselaw and clarifying the scope of Art. 15(1) GDPR, requesting the controllers to revise their templates accordingly.

For supervisory authorities, revision of publications on the right of access in light of recent CJEU caselaw where necessary and awareness raising about this fact.

### **Issue 5**

#### a. Issue identified

Provision of access via copy (Art. 15(3) GDPR) is not sufficiently implemented. Many controllers assume that the right to receive a copy is independent of the right to receive access, and thereby often require an explicit request from the data subject to provide document

excerpts or extracts from databases. Furthermore, for some controllers, entire or redacted documents are, as a principle, not part of the copy provided to data subjects; they will only send the compiled personal data contained in such documents.

b. GDPR or national law provision

Art. 15(1), (3), 25 GDPR

c. CJEU caselaw / EDPB Guidelines 01/2022

Para. 23 Guidelines 01/2022, CJEU, 4.5.2023 – C-487/21, CJEU, 26.10.2023 – C-307/22 on the right to receive a copy

CJEU, 4.5.2023 – C-487/21, CJEU, 22.6.2023 – C-579/21, CJEU, 26.10.2023 – C-307/22 on providing access to documents

d. Potential explanation

N/A

e. Differences between controllers in your Member State

N/A

f. Possible solutions

Recommendations to relevant controllers on the scope of the right of access with regard to documents and correspondence in light of the cited CJEU case-law.

For supervisory authorities, revision of publications on the right of access in light of recent CJEU caselaw where necessary and awareness raising about this fact.

**Issue 6**

a. Issue identified

Many controllers do not always provide full and complete access, but only inform the data subject about changes or engage individually to identify their interest, when they receive several request within a short period of time.

b. GDPR or national law provision

Art. 15(1), 25 GDPR

c. CJEU caselaw / EDPB Guidelines 01/2022

Para. 111 Guidelines 01/2022

d. Potential explanation

The relevant controllers process very large amount of data and seem to inform only about changes for capacity reasons, as providing a full copy for each request might take a considerable effort.

e. Differences between controllers in your Member State

N/A

f. Possible solutions

Recommendation / guidance for the relevant controllers clarifying that, for new general access requests received, controllers cannot narrow the scope of the request themselves (even though the relevant data subjects seem to be generally satisfied with this practice).

### Issue 7

#### a. Issue identified

Some controllers appear to be unaware of the correct timing for providing information and do not provide the personal data as it is at the time of the request. In particular, controllers have not taken measures to provide access to personal data with short retention periods and to store such data longer for the handling of access requests.

#### b. GDPR or national law provision

Art. 6(1), 15(1) GDPR

#### c. CJEU caselaw / EDPB Guidelines 01/2022

Paras. 38, 158 Guidelines 01/2022

#### d. Potential explanation

The controllers see a contradiction between keeping the data for information requests and erasure, but also seem to be unaware of the requirement to provide personal data as it is at the time of the request and the relevant paragraphs of the Guidelines 01/2022.

#### e. Differences between controllers in your Member State

N/A

#### f. Possible solutions

Recommendation to relevant controllers regarding the timing of providing access and the suspension of erasure of personal data once a request is received.

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

- Use of forms/templates by which the data subject can select the relevant departments/branches and processing information it seeks access to.
- Where the controller provides access via copy, the controller provides explanatory information to ensure intelligibility of the access.
- Due to the complexity of the processing, controllers use different layered approaches (2 and 3 layers). To keep the information manageable, the first layer usually contains general information (such as general deletion periods) and personal data. The first layer information also points out that more specific information can be provided in second layer.

### Section on “LIMITATIONS OF ACCESS REQUESTS”

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

### **Issue 1**

#### a. Issue identified

Controllers seem to not have a sufficiently differentiated understanding of the scope and extent of certain (Union law or national) provisions limiting the right of access, and sometimes extend their application to cases where access would have to be provided. Also, controllers rely on Art. 13, 14 and Art. 17 GDPR to limit the right of access despite the fact that these provisions are not applicable.

#### b. GDPR or national law provision

Art. 12(5), 15(4), Art. 23 GDPR, national legislation providing for exceptions/restrictions to the right of access

#### c. CJEU caselaw / EDPB Guidelines 01/2022

Section 6 Guidelines 01/2022

#### d. Potential explanation

N/A

#### e. Differences between controllers in your Member State

N/A

#### f. Possible solutions

Recommendations and further guidance to relevant controllers, using specific scenarios (use-cases) resulting into a limitation of access, in particular with regard to national provisions implemented in accordance with Art. 23 GDPR.

### **Issue 2**

#### a. Issue identified

Different application and interpretation of requests being manifestly unfounded or excessive within the meaning of Art. 12(5) GDPR. In some cases, the requirements are being set too low, e.g. due to the lack of precision of the request. Also, some controllers consider that the data subject's intention to pursue objectives unrelated to data protection with the access request should trigger the exception under Art. 12(5) GDPR.

#### b. GDPR or national law provision

Art. 12(5) GDPR

#### c. CJEU caselaw / EDPB Guidelines 01/2022

Para. 13, 177 Guidelines 01/2022

CJEU, 26.10.2023, C-307/22

#### d. Potential explanation

Especially regarding general requests for access the controllers seem to consider the handling as being a high burden and severe interference with their usual tasks/duties/businesses. As



many requests against controllers are not motivated by data protection law (but legal disputes), conflicts concerning the data subject's objective arise more frequently.

e. Differences between controllers in your Member State

N/A

f. Possible solutions

Controllers should implement processes and tools to grant access even in cases of general, non-specific access requests.

Further guidance for controllers on the legal situation, in particular the CJEU caselaw.

### Issue 3

a. Issue identified

Controllers face challenges where data subjects request information about employee access to their personal data, in particular how, when and which employee has processed the data subject's data. Controllers often or always (sometimes incorrectly) do not provide such information.

b. GDPR or national law provision

Art. 15(1), 15(4) GDPR, Section 26 BDSG on the processing of employee data

c. CJEU caselaw / EDPB Guidelines 01/2022

CJEU, 22.6.2023, C-579/21 ("unless that information is essential in order to enable the data subject effectively to exercise the rights conferred on him or her by that regulation and provided that the rights and freedoms of those employees are taken into account").

d. Potential explanation

Balancing the personal rights of the data subject and the employee is not easy in these cases. Due to uncertainty and duty of care for employees, decisions are often made in favour of the employee's personal rights. Also, the CJEU caselaw may not be known by all controllers.

e. Differences between controllers in your Member State

Some controllers disclose data of employees in cases of uninstructed processing activities performed by such employees on the requesting data subject's personal data.

f. Possible solutions

Awareness raising regarding CJEU caselaw. Also, further guidance for controllers with clear criteria (use-cases) to determine when employee access must be disclosed to data subjects could be useful.

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

N/A

## Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

The level of compliance is too diverse to qualify, in light of the different (types of) controllers contacted by different participating German SAs, see also explanation in Q 5 above.

The overall impression is that the level of compliance in the private sector is high or very high and tends to be (slightly) lower in the public sector. However, there are also significant differences with regard to controllers in the public sector. The level of compliance of Ministries, other higher administrative bodies or specialised agencies tends to be higher than the level of compliance of lower public bodies or public agencies processing personal data of a large number of data subjects (mostly due to their size and diverse tasks, procedures and processing activities).

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, “size” of the controller, etc.):

The level of compliance is too diverse to qualify, in light of the different (types of) controllers contacted by different participating German SAs, see also explanation in Q 5 above.

The level of awareness of certain public bodies contacted (e.g. Ministries or specialised, smaller agencies) can be considered high; however overall and in particular with regard to larger public agencies, the level of awareness should rather be considered low to average.

A higher awareness for and use of the Guidelines 01/2022 can be noticed in bigger controllers with many concerned data subjects, both in the public and non-public sector.

Very few controllers are unaware of the guidelines. However, some stated that while they are aware of the guidelines, they do not use them.

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

(1) The understanding of the scope / extent of the access right in general (Section 2.2.1.2 Guidelines 01/2022) as well as the fact that when identifying the data that must be included in the response to an access request, all data banks, all file types, documents, and also non-textual data must be taken into account (Section 4, in particular 4.1, para. 98, and para. 152 Guidelines 01/2022).

(2) Defining the content of the catalogue information on the processing in accordance with Art. 15(1)(a)-(h), 15(2) GDPR which can be based on the text of the controller's privacy notice as a starting point, as opposed to access to the specific personal data processed (Section 2.2.1.3 Guidelines 01/2022).

(3) Providing a copy (Section 2.2.2.1 Guidelines 01/2022), in particular as one method of providing access.

(4) Facilitating the exercise of rights by providing sufficient information about the need for special knowledge - especially where an assignment is only possible with the knowledge of an identifier (e.g. Cookie-ID) (Art. 12(2) GDPR)

(5) The possibility to receive oral requests and to provide information orally (paras 133, 142 Guidelines 01/2022).

(6) The circumstances in which a request for specification of a data subject's request for access may be addressed to the data subject (para 35 (b) Guidelines 01/2022).

(7) The topic of suspension of erasure of personal data for the handling of access requests to ensure inclusion of personal data with short retention periods (para. 38, 158 Guidelines 01/2022).

(8) The (restricted) possibilities of limiting provision of access, in particular regarding the interpretation of "manifestly unfounded and excessive", due to a lack of concrete criteria (Section 6 Guidelines 01/2022).

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees' right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF? If yes, please provide the date, link to the guidance, and a short description of the guidance.

### Bavaria (BayLDA):

- "Auskunft gem. Art. 15 DS-GVO" (Access according to Art. 15 GDPR), general information provided on SA's website, including links to further fact sheets for data subjects and controllers, templates and to the EDPB Guidelines 01/2022,

[https://www.lida.bayern.de/de/thema\\_auskunft.html](https://www.lida.bayern.de/de/thema_auskunft.html), regularly updated

#### Brandenburg:

- "Meine Daten, meine Rechte" ("My data, my rights", information material on general data subject rights, including Art. 15 GDPR, and primarily aimed at data subjects, [https://www.lda.brandenburg.de/sixcms/media.php/9/Brosch%C3%BCre\\_Meine\\_Daten\\_Meine\\_Rechte14ua.4269840.pdf](https://www.lda.brandenburg.de/sixcms/media.php/9/Brosch%C3%BCre_Meine_Daten_Meine_Rechte14ua.4269840.pdf), dated 1 November 2018

#### Lower Saxony:

- "Data subject rights", general information on data subject rights including the right of access, aimed primarily at data subjects, [https://www.lfd.niedersachsen.de/startseite/datenschutzrecht/ds\\_gvo/betroffenenrechte/](https://www.lfd.niedersachsen.de/startseite/datenschutzrecht/ds_gvo/betroffenenrechte/), regularly updated

#### Rhineland-Palatinate:

- Data subject rights", general information on data subject rights including the right of access, aimed primarily at data subjects, <https://www.datenschutz.rlp.de/buergerinnen-/buerger/ihre-rechte> , regularly updated

- Anonymized case register for the public sector, containing also cases concerning Art. 15 GDPR, <https://www.datenschutz.rlp.de/themen/fallboerse/organisation-zentrale-dienste-finanzen-datenschutz-allgemein>, regularly updated

> Right of access regarding data processing in medical treatments: <https://www.datenschutz.rlp.de/themen/auskunftsanspruch-in-der-heilbehandlung>, regularly updated

#### Federal/BfDI:

- "The Right of Access (Art. 15 GDPR)", general information for data subjects on DE\_Federal website,

[https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Betroffenenrechte/Betroffenenrechte\\_Auskunftsrecht.html](https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Betroffenenrechte/Betroffenenrechte_Auskunftsrecht.html) ; as well as several further articles on DE\_Federal website relating to different areas of competence, regularly updated

- „Info 1: GDPR and German Federal Data Protection Act – Texts and explanations”, general information for data subjects and other interested persons including an overview and explanation of the structure of Art. 13, 14 and 15 GDPR and exceptions deriving from national legislation,

[https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO1.pdf?\\_\\_blob=publicationFile&v=16](https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO1.pdf?__blob=publicationFile&v=16) , dated May 2022

- „Info 06: GDPR in the Federal Administration”, general information for data subjects and Federal public bodies, including information on the right of access and exceptions deriving from national legislation,

[https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO6.pdf?\\_\\_blob=publicationFile&v=9](https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO6.pdf?__blob=publicationFile&v=9) , dated December 2020

- „The Right of Access under Art. 15 GDPR”, slides for a presentation on the “Ecumenical Data Protection Day”, with comparison to specific provisions in the data protection legislation for churches,

[https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/AccessForAll/2023/2022-Vortrag-Recht-auf-Auskunft.pdf?\\_\\_blob=publicationFile&v=2](https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/AccessForAll/2023/2022-Vortrag-Recht-auf-Auskunft.pdf?__blob=publicationFile&v=2) , dated 29 April 2022

- General explanations on the applicability of Art. 15 GDPR towards fiscal authorities, including in particular specific exceptions stipulated in the German fiscal regulation,

[https://www.bfdi.bund.de/DE/Buerger/Inhalte/Finanzen-Steuern/ABC\\_Auskunftsrecht.html?nn=335688](https://www.bfdi.bund.de/DE/Buerger/Inhalte/Finanzen-Steuern/ABC_Auskunftsrecht.html?nn=335688)

- „Guidance for Jobcenters to provide access in accordance with Art. 15 GDPR”, providing jobcenters (which are organised as joint institutions) with recommendations to handle access requests under Art. 15 GDPR, <https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/AccessForAll/2020/20-Arbeitshilfe-Artikel-15-Jobcenter.html?nn=340784>, dated 15 April 2020

- Several times per year: Circular letters to Jobcenters, in which the right of access under Art. 15 GDPR has been mentioned several times (Circular letter no. 1 dated 30 September 2019 referring to the above-mentioned Guidance for Jobcenters; Circular letter no. 10 dated 9 May 2023 including a reminder of said guidance and requests to verify whether general procedures can be optimised and awareness of the staff for the deadline for handling requests can be raised;

<https://www.bfdi.bund.de/DE/DerBfDI/Dokumente/Rundschreiben/Jobcenter/Rundschreiben-Jobcenter-node.html>.

- Booklet „Archive law and data protection”, containing information on the interplay of data protection and archive legislation, data subjects’ rights under GDPR and specific exceptions under Federal archive legislation, [https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/Archivrecht.pdf?\\_\\_blob=publicationFile&v=9](https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/Archivrecht.pdf?__blob=publicationFile&v=9), dated 2023

- Booklet “Data Protection rights for refugees and asylum seekers”, providing an overview over data processing in the asylum and residence procedure, [https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Flyer/Datenschutz-Asyl.pdf?\\_\\_blob=publicationFile&v=9](https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Flyer/Datenschutz-Asyl.pdf?__blob=publicationFile&v=9), dated July 2023

- Recommendation to Federal public bodies concerning access requests in staff and employee data protection, [https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2020/Auskunftsersuchen\\_Beschäftigtendatenschutz.html](https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2020/Auskunftsersuchen_Beschäftigtendatenschutz.html) , dated 24 June 2020

- “Position paper on access requests towards telecommunications providers”, Working paper concerning the right of access directed at telecommunications providers containing guidance on recurring practical questions concerning the application of Art. 15 GDPR and the EDPB Guidelines on Art. 15 GDPR, [https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Datenschutzpraxis/Auskunftsrecht\\_Telekommunikationsanbieter.html](https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Datenschutzpraxis/Auskunftsrecht_Telekommunikationsanbieter.html) , dated 21 March 2024

For all German SAs:

- “DSK Fact Sheet no. 6” on the right of access, containing a short guidance on the exercise and granting of the right of access, <https://www.datenschutzkonferenz-online.de/kurzpapiere.html>, dated December 2018, currently under revision.

**33) Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

- Actions resulting from data subjects’ complaints, in particular in the financial and in the public sector (often leading to enforcement actions like reprimands or orders, most relevant issues concerning the form of providing access, deadlines, the scope of the access request, naming

(categories of) recipients, restrictions of the right of access, lack of action by controllers on access requests).

- General unspecific audits of controllers, but which include investigating the audited controllers' handling of access requests.
- One specific questionnaire audit of a specific private sector focussing on the handling of data subjects' rights by controllers, resulting in practical advice.
- Consultations upon requests of controllers or controllers' DPOs.

34) **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:

- Various practical recommendations / information letters / further guidance for the controllers contacted in the CEF 2024 Action.
- Launch of formal investigations where this has not already been part of the CEF 2024 Action, and consideration of corrective measures in individual cases by the end of 2024 or in beginning of 2025 (possibly warnings or other measures).
- On-site audit of one controller to be performed in 2024.
- Information events and training sessions with controllers.
- General Information for controllers and data subjects.

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Often.

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Sometimes.

37) 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 content of EDPB Guidelines 01/2022 and if yes, which actions do you consider to be preferable?

a. Yes: Yes

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

- More online guidance: Yes
- Online or remote training sessions: Yes
- Conferences organised: Yes
- Others: please specify: Yes

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

- Best practices and use cases for SMEs.
- Information events and training sessions with controllers.

- General consulting/advisory practice, e.g. during regular exchanges with stakeholders (e.g. controllers of different sectors or DPOs, industry or sectoral associations).
- Networking conferences or regular counselling meetings.
- Updating guidance already issued in light of findings of the CEF 2024 action.

b. No: No

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes: Yes

- Raising awareness regarding the flowcharts in the annex of the EDPB Guidelines 01/2022.
- Conducting a “Frequently Asked Questions”-Paper in addition to the guidelines.
- Development of further information on individual chapters of the guidelines, possibly collected outside of the immediate text of the guidelines as separate resources of information (e.g. on chapter 6.4 at national level of the member states, a list of existing regulations on limitations of the right of access).
- As a general remark with regard to guidelines, more timely translations into the languages of the member states, as well as communication and awareness-raising once these translations are made available, could be helpful.

b. No: No



## 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<sup>9</sup>: **No**
  - d. Ongoing investigation: **No**
- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),
- Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? **Yes**
  - Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. **No**
  - If not, will this fact finding activity impact your enforcement activities and if yes, how?  
**The fact finding activity will impact the supervision’s day-to-day work to ensure that the data protection rules are complied with, including consideration of which cases the supervisory authority should address on its own initiative.**
- 3) For all SAs: 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 SA used the same questionnaire for all controllers.**
- 4) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.  
**The Danish SA included all the questions in the questionnaire. The Danish SA did not amend any questions, but did however make minor changes in the translation of the questionnaire.**
- 5) For all SAs: 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 etc.)?  
**No.**

## Part I – Some numbers on the controllers addressed

- 6) How many controllers did you contact? **11**
- 7) Out of the contacted controllers, how many controllers responded? **3**

---

<sup>9</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.



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 Danish SA has identified two main reasons for the gap; the questionnaire was voluntary and comprehensive.

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: Please select one or more answers.

- a. Public sector: 0
- b. Private sector: 3

10) Please specify the category<sup>10</sup> of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers

- a. Micro enterprise: 0
- b. Small enterprise: 1
- c. Medium-sized enterprise: 0
- d. Large enterprise (more than 250 employees): 2
- 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) Please specify the nature of the (business) activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. education sector: 0
- b. health sector: 0
- c. social sector: 0
- d. insurance sector: 0
- e. finance sector: 0
- f. IT sector: 0
- g. retail sector: 3
- h. logistics sector: 0
- i. public transportation: 0
- j. telecommunications: 0
- k. postal services: 0
- l. advertising sector: 0
- m. marketing services: 0
- n. entertainment sector: 0
- o. information / journalism sector: 0
- p. scientific / historical research: 0
- q. credit scoring agency: 0
- r. public utility/infrastructure provider (e.g. energy): 0

---

<sup>10</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- s. housing industry: 0
- t. manufacturing: 0
- u. other (please specify): 0

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. customers: 3
- b. potential customers: 1
- c. employees: 0
- d. job applicants: 0
- e. children: 1
- f. vulnerable adults: 1
- g. patients: 0
- h. citizens (for public sector): -
- i. applicants (for public services): -
- j. recipients (for postal services): -
- k. other (please specify): 0

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. Less than 100: 0
- b. 100 - 200: 0
- c. 201 - 500: 0
- d. 501 - 2,000: 0
- e. 2,001 - 10,000: 0
- f. 10,001 - 50,000: 0
- g. 50,001 - 100,000: 1
- h. 100,001 - 1,000,000: 0
- i. 1,000,001 - 10,000,000: 2
- j. More than 10,000,000: 0

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.

- a. Contact data: 3
- b. Payment data: 1
- c. Identification data: 1
- d. Sensitive data within the meaning of Art. 9 GDPR: 1
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR: 1
- l. Other (please specify): 0

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. 0 request: 1
- b. 1-10 requests: 1
- c. 11-25 requests: 1
- d. 26-50 requests: 0
- e. 51-100 requests: 0
- f. 101-150 requests: 0
- g. 151-200 requests: 0
- h. 201-500 requests: 0
- i. 501-10,000 requests: 0
- j. >10,000 requests: 0
- k. No information: 0

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

The Danish SA has not identified any significant differences.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 1
- b. >0–25%: 2
- c. 26–50% requests: 0
- d. 51–75% requests: 0
- e. 76–100% requests: 0
- f. No information: 0

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

The Danish SA has not identified any significant differences.

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 1
- b. >0–25%: 0
- c. 26–50% requests: 0
- d. 51–75% requests: 0
- e. 76–100% requests: 2
- f. No information: 0

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

The Danish SA has not identified any significant differences.

- 18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.
- a. None of the requests: 3
  - b. >0–25%: 0
  - c. 26–50% requests: 0
  - d. 51–75% requests: 0
  - e. 76–100% requests: 0
  - f. No information: 0

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

The Danish SA has not identified any significant differences.

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

- 19) 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 2.2 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. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.
  - d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
  - e. What are differences that you have encountered between controllers in your Member State?
  - f. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

The Danish SA has not identified any issues regarding the documentation of compliance with requests for access.

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

### Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

21) 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 3.4 in the questionnaire addressed to controllers.

The Danish SA has not identified any issues regarding the process for handling requests for access.

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

### **Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”**

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

23) 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 4.15 in the questionnaire addressed to controllers.

The Danish SA has not identified any issues regarding implementation of general requirements from article 12 GDPR.

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

### **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

25) 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 5.18 in the questionnaire addressed to controllers.

The Danish SA has not identified any issues regarding content of access requests and respective responses according to GDPR article 15.

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

### **Section on “LIMITATIONS OF ACCESS REQUESTS”**

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

The Danish SA has not identified any issues regarding limitations of access requests.

28) Are there any **leading or best practices** of the controllers having responded that you would like to share? [No](#).

### Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

[Due to the low number of responses, the Danish SA cannot comment on the general level of compliance of the controllers.](#)

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, “size” of the controller, etc.):

[Due to the low number of responses, the Danish SA cannot comment on the general level of compliance of the controllers.](#)

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

[Due to the low number of responses, the Danish SA cannot comment on the general level of compliance of the controllers.](#)

### Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees’ right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF?

If yes, please provide the date, link to the guidance, and a short description of the guidance.

Vejledning om de registreredes rettigheder (Guidance on the rights of the data subject)

- Published: July 2018

The guidance gives a general overview of the rights of the data subject including the right of access. The guidance includes a template for response to a request of access. The Danish SA has furthermore guidance on specific topics, e.g. video surveillance and employment law, which contains sections on the right of access.

[Registreredes rettigheder.pdf \(datatilsynet.dk\)](#)

**33) Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

In 2019, the SA carried out six own-volition investigations, three concerning private companies and three concerning public authorities, focusing on their compliance with the right of access.

On the basis of the investigations carried out, the Danish SA issued reprimands in four of the six cases. In two of the cases, the Danish SA made a statement without a reprimand.

The Danish SA has in 2022 completed investigations of the handling of requests of access from customers by five selected banks. The investigations focused on the process for handling requests for access.

The Danish SA issued one reprimand and four statements.

**34) 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 fact finding activity will impact the supervision's day-to-day work to ensure that the data protection rules are complied with, including consideration of which cases the supervisory authority should address on its own initiative.

**35) In general** (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

The Danish SA refers mainly to our own guidance on the right of access. Where appropriate, the Danish SA also refers to the EDPB Guidelines.

**36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?**

The Danish SA does not have an overview of the extent to which the EDPB Guidelines has been referred to in decisions related to the exercise of other data protection rights than the right of access.

37) 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 content of EDPB Guidelines 01/2022 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](#)

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes:

b. No: [Yes](#)



# EDPS

European Data Protection Supervisor

## Introduction

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

b. **Fact finding + determining follow-up action based on the results**

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

- Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? **Yes**
- Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. **No**
- If not, will this fact finding activity impact your enforcement activities and if yes, how? **Yes. The results of the survey will enable the EDPS to identify the EUIs that deal with the highest number of data subject access requests (DSAR) and, where appropriate, to target enforcement activities accordingly.**

3) For all SAs: 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) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.

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:

- the experience gained from its recent complaint handling practice (01/01/2023-30/06/2024);
- the output of a workshop on the implementation of the right of access that took place on 19 June 2024 at the bi-annual EDPS-EUI DPOs meeting,
- a number of DPO annual activity reports (for year 2023) sent to the EDPS;
- 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 DSARs they received in 2023 and calculate the percentage of DSARs in comparison to the total number of data subject requests. Thus, the EDPS used question 1.5. from the EDPB questionnaire, which corresponds to sections 1.10 (How many data subject access requests received in 2023) and 1.12 (What percentage of the data subject requests received in 2023 were data subject access requests) of this report.

b) The processing of personal data by EUIs do 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 (approximate) percentage of data subject access requests (Article 17 EUDPR) received in the period 1.1.2023 to 31.12.2023 originated from staff members from your EUI, i.e. officials and other servants employed by your EUI? (Former staff members are included)'. 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) For all SAs: 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 etc.)?

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 0.4);

- for the sake of selectiveness, the EDPS picked one relevant issue for each of the five sections.

## Part I – Some numbers on the controllers addressed

6) How many controllers did you contact?

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](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/to your questions.

63

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?

Certain EUIs encountered issues gathering the requested statistics because they do not keep centralised information of DSARs.

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: Please select one or more answers.*

a. Public sector: All 75 surveyed EUIs belong to the public sector

b. Private sector: N/A

10) Please specify the category<sup>11</sup> of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers*

---

<sup>11</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

All respondents are EUIs, i.e. EU institutions, bodies, offices and agencies

11) Please specify the nature of the (business) activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

EUIs' activities cover all areas of EU competence.

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

The data subjects concerned by the EUIs' processing activities are EUI staff members, as well as any individual interacting with EUIs (for example, if they register to an EUI newsletter).

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. Less than 100:
- b. 100 - 200:
- c. 201 - 500:
- d. 501 - 2,000:
- e. 2,001 - 10,000:
- f. 10,001 - 50,000:
- g. 50,001 - 100,000:

All EUIs process personal data of their staff members, amounting to approximately 60.000 staff members in total.

- h. 100,001 - 1,000,000:
- i. 1,000,001 - 10,000,000:
- j. More than 10,000,000:

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.

As indicated above (section 4.b), the EDPS added a specific question to the questionnaire about the approximate percentage of DSARs received from EUI staff members between 1.1.2023 and 31.12.2023.

The replies are as follows:

% of DSARs originating from staff members :

- 0-25%:	46
- 26-50%:	4
- >50%:	13

The results show that a high staff headcount does not automatically result in a higher amount of DSARs submitted by staff members. Several reasons may explain this. First, EUI staff members can directly access HR data (evaluation, promotion, family allowances, etc.) that are available in their so-called 'personnel file', saving them from submitting DSARs on these matters. Second, not all EUIs keep information on DSARs that enable them to extract statistics on/identify the quality of the requesting persons. Third, requesting persons do not necessarily identify themselves as staff members, using for example a personal address as contact detail.

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? *Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.*

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. Sensitive data within the meaning of Art. 9 GDPR:

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.

e. Data of a highly personal nature within the meaning of Art. 10 GDPR:

(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.

f. Other (please specify):

N/A

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- |                         |    |
|-------------------------|----|
| a. 0 request:           | 25 |
| b. 1-10 requests:       | 27 |
| c. 11-25 requests:      | 6  |
| d. 26-50 requests:      | 2  |
| e. 51-100 requests:     | 1  |
| f. 101-150 requests:    | 0  |
| g. 151-200 requests:    | 1  |
| h. 201-500 requests:    | 1  |
| i. 501-10,000 requests: | 0  |
| j. >10,000 requests:    | 0  |
| k. No information:      | 0  |

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, "size" of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

Overall, the numbers are relatively low.

The EUI that reported the highest number of DSARs is a large one in terms of staff headcount and also has significant public exposure, which could provide an explanation.

That being said, it is not clear that there is a correlation. Other prominent EUIs (in terms of staff headcount or exposure), did not report a high number of DSARs.

Finally, one large EUI, which dealt with >500 data subject requests (including DSARs) in 2023, did not report in detail about the numbers on DSARs; their input is therefore not included in the above statistics, which could also affect this year's result.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 25
- b. >0–25%: 10
- c. 26–50% requests: 11
- d. 51–75% requests: 4
- e. 76–100% requests: 12
- f. No information: 1

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

The survey results do not allow to identify patterns neither to draw significant conclusions.

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

f. No information.

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

N/A

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

f. No information.

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

N/A

## **Part II – Substantive issues regarding controllers’ level of compliance**

## Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 in the questionnaire for controllers:

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

Accountability. Not all EUIs, including certain big EUIs, keep centralised information on DSARs. This may result in inconsistent implementation of DSARs, 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.

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

Article 4(2) EUDPR - Accountability

Article 26 EUDPR - Responsibility of the controller

Article 32 EUDPR - Cooperation with the EDPS

c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.

EDPB Guidelines, paragraphs 123 and fol. (section 5. How can a controller provide access?)

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

The absence of centralised information seems to be prevalent in EUIs where the DPO (or the Data Protection Coordinator - DPC - in big EUIs) is not involved in the DSARs (if only as adviser to the entity in charge) or not involved in all cases (only in the most complicated/sensitive ones).\*

\*According to the results of the EDPS survey on the designation and position of the DPO in EUIs (18 January 2024), 41 DPOs (out of 69 respondents) indicated that they were in charge of handling DSARs (see p. 5).

e. What are differences that you have encountered between controllers?

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

f. 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 DSARs, having a central register of DSARs, which the DPOs maintain or at least have access to (even if they are not responsible for handling the DSARs\*) could provide an appropriate solution. This register would help monitor DSARs and ensure that DSAR rules (such as, deadlines, ID authentication of the requester, access rights to the DSAR files and storage duration) 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).

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

Having a central register of DSARs seems to be key factor in enabling controllers to demonstrate compliance, including by being able to provide easily accurate statistics on the matter.

## Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

21) 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 3.4 in the questionnaire addressed to controllers.

a) Issue

One issue often raised by EUIs concerns the filtering of the requests they receive on a daily basis. EUIs receive individual requests that vary in nature, including:

- DSAR under the EUDPR;
- public access to document requests under Regulation (EC) 1049/2001 (ATDR);
- access to file in administrative procedures handled by EUIs, which is part of the right to good administration enshrined in Article 41(2)(b) of the Charter of Fundamental Rights of the EU;
- requests that boil down to complaints against the EUI;
- requests for information.

b) Relevant provisions

- Article 17 EUDPR - Right of access
- Articles 15-16 EUDPR - Information to data subjects
- Article 27(1) EUDPR - Data protection by design and by default
- Article 57(1)(e) EUDPR - Complaints
- Article 9 EUDPR - Transmission of personal data to recipients established in the Union other than EUIs; in particular, Article 9(3) provides that EUIs shall reconcile the right to the protection of personal data with the right of access to documents in accordance with Union law. (No equivalent in GDPR)

c) Relevant case law or EDPB Guidelines 02/2021

EDPB Guidelines, paragraph 10 and fol. (section 2.1. Aim of the right of access).

d) Potential explanation why this has been an issue for EUIs

Requesters are not always clear as to what they are actually seeking, or they file mixed requests.

Moreover, several organisational entities can theoretically be involved, depending on the requests (DPO, Transparency Officer for ATDR, entity in charge of the administrative procedure, Information and Communications service for requests for information, etc.).

e) Differences between EUIs

The situation depends on the volume of nature of the requests. ‘Big’ EUIs, with a significant amount of staff, will logically receive more DSARs than the smaller ones and more ATDRs due to their public exposure. Other EUIs, regardless of their size, will receive more ATDRs because of the nature of their activities, notably those that are involved in scientific research.

These factors influence the diversity of the requests received by EUIs and the corresponding



need to have a filtering tool in place to classify the request from the outset, especially for DSARs and ATDRs that are subject to strict deadlines.

As to the role of the DPO in this context, in some EUIs, the DPO is involved in the handling of the request following its reception by the front office and participates in the classification of the request. In other EUIs, the DPO is involved in the handling of the merits of the DSAR, while the sorting and classification of the request is done by legal or other colleagues. In EUIs with higher volume of requests, the DPO is consulted only in difficult/sensitive DSARs.

f) Possible solutions

The EDPS has encountered complaint cases where a deadline was missed because of a requestors lack of clarity but has also faced cases where the missed deadline was because of the lack of communication between the DPO and relevant actors as to whom should take care of the DSAR. Therefore, it is key that EUIs set up an efficient and centralised filtering process, which involves all relevant actors (including the DPO) from the beginning. Furthermore, the filtering should take place at an early stage, to avoid missing deadlines.

In addition, EUIs should provide detailed information on their website to explain the scope of DSARs and clarify the differences vis-à-vis other individual requests. A good practice could be to set up a web form to file DSAR. The form would guide the requester to a series of preliminary questions aiming to help the person identify whether they chose the right channel to obtain what they look for. It could also allow filters to be applied from the out-set allowing for a more streamlined process.

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

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

## **Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”**

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

23) 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 4.15 in the questionnaire addressed to controllers.

a) Issue(s)

Verification of the identity of the persons requesting access when they are not EUI staff members. Such verification may sometimes lead to processing an excessive amount of personal data and/or to unnecessary processing of sensitive data.

b) Relevant provisions

Article 12 EUDPR - Processing which does not require identification

Article 14(6) EUDPR - Transparency and modalities

c) Relevant case law or EDPB Guidelines 01/2022



EDPB Guidelines, paragraphs 58 and fol. (sections 3.2. Identification and authentication and 3.3. Proportionality assessment regarding authentication of the requesting person)

d) Potential explanation why this has been an issue for EUIs

Where the requesting person is among their staff members, EUIs have generally the means for authenticating them, notably thanks to the credentials already used by the staff member to log in to the online environment offered by the EUI. Moreover, it is common practice in EUIs staff members can have direct access to a broad range of HR data (personnel file, annual appraisal, career path, etc.) thanks to a HR-dedicated portal.

For requesters other than their own staff members, EUIs must regularly ask for additional proof of identification of the person to ensure that the latter is entitled to have access to the personal data at stake and avoid unauthorised disclosure. At the same time, EUIs must facilitate the exercise of data subject rights (Recital 34 EUDPR). This can lead to excessive data collection and processing.

e) Differences between EUIs

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

f) Possible solutions

To avoid excessive data collection in accordance with the data minimisation principle, certain EUIs instruct proactively the requester about the elements needed for authentication purposes and ask them to refrain from providing any additional information. Other EUIs reported that they conduct a proportionality assessment, taking into account the type of personal data at stake, the nature of the request, its context, etc., the extent of which may vary depending on the EUI's business area.

In certain cases, EUIs use credentials already available (for example: email address and other identification data provided by job applicants while enrolling for the selection process). In other cases, EUIs cannot lift 'reasonable doubts' about the identity of the requesting person without requesting a copy of an identity document (ID card, passport, driving licence). In such circumstance, EUIs reported that only the relevant elements are collected, which may vary depending on the processing at stake and its sensitivity. If irrelevant elements are provided, they are redacted. Some EUIs reported that once the identity of the requesting person is checked, they record the identity check in the DSAR file and delete the ID document provided.

The EDPS has recently dealt with a complaint case in which an EUI had doubts about the identity of the person making the DSAR. The EUI informed the person about the pieces of information required for authentication purposes and explained why they were necessary. The EUI indicated that any other elements appearing on the ID document should be redacted by the requesting person and that the copy of the ID document would in any case be destroyed as soon as no longer needed. The person nevertheless persisted in refusing to provide additional information enabling their identification. The EDPS considered that the EUI request for additional information was proportionate in the case at stake and that the EUI was entitled not to act on the DSAR in the absence of authentication of the requester.

To summarise, the key element here is pedagogical, i.e. data subjects should be informed about the 'personal data processing within the personal data processing', i.e. (i) the reason why they need to show credentials to be entitled to having access to their personal data and (ii) the identification data necessary for the controller to authenticate them. In accordance with Articles 15(2)(b) and 16(2)(b) EUDPR, information on the exercise of DSAR in the EUI in the respective data protection notices. If strengthened authentication procedures apply to get access to specific (sensitive) data processing operations, a good practice would be to include the additional requirements in the respective data protection notices, or in the DSAR

acknowledgement of receipt, or in the online form dedicated to data subject requests, if applicable. Another good practice could be to make available general information on how to submit a DSAR on the EUI website, separated from the respective data protection notices.

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

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

## **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

25) 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 5.18 in the questionnaire addressed to controllers.

a) Issue(s)

The modalities of the reply to DSARs and in particular the interpretation of the notion of ‘copy of the data undergoing processing’ under Article 17(3) EUDPR.

To the knowledge of the EDPS, there is no significant issue as to the means of replying (Article 14(1) EUDPR (The EDPB Guidelines refer to the ‘format’ of the reply - see section 5.2.5). In the EUI context, most data subjects file their request by electronic means. Therefore, EUIs generally reply by electronic means, unless otherwise requested by the data subject.

The issues the EDPS would like to highlight pertain to the modalities of replying to DSARs.

Under Article 17 EUDPR, the right of access includes three components, i.e. (i) obtain confirmation as to whether or not personal data concerning them are being processed, (ii) where that is the case, obtain access to the personal data and (iii) obtain information on the processing. Article 17(3) EUDPR supplements the modalities laid down in Article 12 EUDPR with specifications pertaining to DSARs, i.e. the obligation to provide a ‘copy of the personal data undergoing processing’. The obligation to provide a copy is not an additional right of the data subject but a modality of providing access to the data, which refers only to the second component of the right of access.

b) Relevant provisions

Article 14(1) EUDPR - Transparency and modalities

Articles 17(1)-(3) EUDPR - Right of access

c) Relevant case law or EDPB Guidelines 01/2022

EDPB Guidelines, sections 2.2.1. (Defining the contents of the right of access), 2.2.2. (Provisions on modalities - providing a ‘copy’) and 5.2.5. (Format)

Recent case law (judgments from the Court of Justice of the European Union rendered after the adoption of the EDPB Guidelines):

CJEU, 27 May 2024, Addiko Bank, C-312/23

CJEU, 26 Oct 2023, FT, C-307/22

CJEU 22 June 2023, Pankki C-579/21

d) Potential explanation why this has been an issue for EUIs

The issue revolves around the interpretation of the concept of 'copy of the personal data undergoing processing' under Article 17(3) EUDPR.

The EDPS has identified two main practices among EUIs in this respect.

According to a literal interpretation of Article 17(3) EUDPR, the right to obtain a copy 'of the data undergoing processing' does not amount to receiving a copy of the document(s) that contain(s) their personal data. Under this approach, data subjects are generally provided with a table that lists the personal data being processed, by category.

Another approach consists of providing a copy of the documents that contain personal data relating to the requesting person, after redacting the elements that would not be 'personal data relating to the person' (for example a legal analysis included in the document - cf. CJEU, 17 July 2014, YS, C-141/12), as well as any elements that would fall within the limitation of Article 17(4) EUDPR (rights and freedoms of others - see below) or a restriction provided in the EUI's internal rules on restrictions under Article 25 EUDPR. Providing a copy of the document seems to be the rule for documents that were originally submitted to the EUI by the data subject. This approach seems to provide more contextual information to data subjects. However, in situations where the document is heavily redacted, the information may end up being unintelligible in the end.

The Court of Justice has recently provided some legal clarifications on the matter (see section f) below).

e) Differences between EUIs

EUIs with investigative powers may be more reluctant to share copies of documents, even redacted, with data subjects, as this could infringe their legal obligation of confidentiality and/or affect rights and freedoms of others (for ex.: victims and witnesses in harassment investigations; whistle blowers in fraud investigations, etc.).

f) Possible solutions

According to recent decisions of the Court (CJEU, 27 May 2024, Addiko Bank, C-312/23; CJEU, 26 Oct 2023, FT, C-307/22; CJEU, 4 May 2023, Österreichische Datenschutzbehörde, C-487/21), the right to obtain a copy of the personal data undergoing processing (i) means the provision of 'a faithful and intelligible reproduction' of those data; (ii) can entail the right to obtain copies of extracts from documents or even entire documents which contain those data, if the provision of such a copy is essential in order to enable data subjects to exercise effectively their rights; and (iii) must take the rights and freedoms of others into account. Thus, the Court, while not disregarding the literal interpretation, stressed that the second approach has to be followed in certain circumstances.

Thus, there is no one-size-fits-all solution. EUIs should conduct an assessment on a case-by-case basis to balance the conflicting rights/interests in presence and keep in mind the rationale behind the right of access.

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

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

### Section on “LIMITATIONS OF ACCESS REQUESTS”

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

a) Issue(s)

Implementation of the limitation of the right of access that results from the need to protect rights and freedoms of others than the data subject.

b) Relevant provisions

Article 17(4) EUDPR - Right of access

Recital 37 EUDPR

c) Relevant case law or EDPB Guidelines 01/2022

EDPB Guidelines, section 6.2. (Article 15(4) GDPR)

Recent case law

AG Opinion, 12 September 2024, Dun & Bradstreet Asutria, C-203/22

CJEU 22 June 2023, Pankki C-579/21

CJEU, 27 May 2024, Addiko Bank, C-312/23

CJEU 4 May 2023, Österreichische Datenschutzbehörde, C-487/2021

d) Potential explanation why this has been an issue for EUIs

The implementation of Article 17(4) EUDPR implies a delicate balancing exercise between conflicting rights and interests.

Examples in EUI context include: selection/evaluation procedures (secrecy of jury deliberations), administrative inquiries and disciplinary proceedings (protection of victims, witnesses and accused person), whistleblowing procedures (protection of informants).

e) Differences between EUIs

All EUIs can be confronted with most of the above situations. However, certain EUIs have investigations or selections as their core business and are, therefore, more exposed to these issues.

f) Possible solutions

Have clear procedures in place to ensure a harmonised and fair application of the rules to individual cases.

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

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

## Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

b. High

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

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

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

b. High

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, “size” of the controller, etc.):

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

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

The Guidelines should be updated taking into account the most recent decisions of the Court of Justice of the European Union on the right of access (C-487/21; C-579/21; C-307/22, C-312/23), which clarified notably the following:

- the concept of ‘copy’ under article 15(3), 1st sentence GDPR (section 2.2.2.1. of the EDPB Guidelines);
- the concept of ‘information’ under Article 15(3), third sentence GDPR section 2.2.2.3. of the EDPB Guidelines);
- the scope of the right of access (i.e. information to log data) (section 4.1. of the EDPS Guidelines); - the definition of ‘recipients’ under Article 15(1)(C) GDPR (section 4.3. of the EDPB Guidelines).

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees’ right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF?

If yes, please provide the date, link to the guidance, and a short description of the guidance.

The EDPS published a Factsheet on data subject rights, including the right of access, in 2022: ([https://www.edps.europa.eu/system/files/2022-01/22-01-21\\_infographic\\_dataproday22\\_en.pdf](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 of access ([https://www.edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines\\_en](https://www.edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en))

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? 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.

34) **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.

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Very often

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Very often

37) 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 content of EDPB Guidelines 01/2022 and if yes, which actions do you consider to be preferable?

Yes: Online or remote training sessions

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

No

# EE SA

Estonian Data Protection Inspectorate (Andmekaitse Inspeksioon)

## Introduction

- 1) What was the initial procedural framework of your action? Please select one or more answers.
- Fact finding: **Yes**
  - Fact finding + determining follow-up action based on the results:
  - New formal investigation<sup>12</sup>:
  - Ongoing investigation:

- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),

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

**As we will give feedback to the controllers where we will point out in which areas their practice could be improved, in the case of future complaint we will take into account if we have requested improvement of practice and if it is implemented by the controller or not.**

- 3) For all SAs: 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) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.

**Did not include question 1.2.**

**Amended questions: 1.3 (as directed to a specific sector, removed all that was not needed or we knew the answer ourselves), 1.4 (as directed to a specific sector, removed all that was not needed), 3.1 did not ask to provide documentation.**

- 5) For all SAs: 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 etc.)?

**No**

---

<sup>12</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.



## Part I – Some numbers on the controllers addressed

6) How many controllers did you contact?

9

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/to your questions.

9

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: Please select one or more answers.

- a. Public sector: 0 responding controller
- b. Private sector: 9 responding controllers

10) Please specify the category<sup>13</sup> of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers

- a. Micro enterprise:
- b. Small enterprise: 3 responding controllers
- c. Medium-sized enterprise: 4 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):

11) Please specify the nature of the (business) activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. education sector:
- b. health sector:
- c. social sector:
- d. insurance sector: 9 responding controllers
- e. finance sector:
- f. IT sector:
- g. retail sector:
- h. logistics sector:

---

<sup>13</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).



- 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. other (please specify):

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. customers: 8 responding controllers
- b. potential customers: 7 responding controllers
- c. employees: 8 responding controllers
- d. job applicants: 7 responding controllers
- e. children: 5 responding controllers
- f. vulnerable adults: 3 responding controllers
- g. patients:
- h. citizens (for public sector):
- i. applicants (for public services):
- j. recipients (for postal services):
- k. other (please specify): 4 responding controllers

For example, data of insurance policyholders, insured persons, beneficiaries, traffic damage victims and in some cases their family members and/or legal representatives.

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. Less than 100: 1 responding controller
- b. 100 - 200:
- c. 201 - 500:
- d. 501 - 2,000:
- e. 2,001 - 10,000:
- f. 10,001 - 50,000:
- g. 50,001 - 100,000: 1 responding controllers
- h. 100,001 - 1,000,000: 7 responding controllers
- i. 1,000,001 - 10,000,000:
- j. More than 10,000,000:

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.

- a. Contact data: 9 responding controllers
- b. Payment data: 6 responding controllers
- c. Identification data: 8 responding controllers
- d. Sensitive data within the meaning of Art. 9 GDPR: 8 responding controllers
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR: 4 responding controllers
- f. Other (please specify): 6 responding controllers  
For example, data related to processing damage claims under insurance policy, demographical data, CV data for the job applicants (e.g. education, former employment history), employment data for the employees (e.g. salaries, data on missions and trainings), data on damages caused to the victim.

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. 0 request: 3 responding controllers
- b. 1-10 requests: 6 responding controllers
- c. 11-25 requests:
- d. 26-50 requests:
- e. 51-100 requests:
- f. 101-150 requests:
- g. 151-200 requests:
- h. 201-500 requests:
- i. 501-10,000 requests:
- j. >10,000 requests:
- k. No information:

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, "size" of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

No

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 3 responding controllers
- b. >0–25%: 1 responding controllers
- c. 26–50% requests:
- d. 51–75% requests: 1 responding controllers
- e. 76–100% requests: 4 responding controllers
- f. No information:

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 6 responding controllers
- b. >0–25%:
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests: 3 responding controllers
- f. No information:

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 5 responding controllers
- b. >0–25%:
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests: 4 responding controllers
- f. No information:

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 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. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.
- d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
- e. What are differences that you have encountered between controllers in your Member State?
- f. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

The main issue identified was the difference in retention periods of data subjects access requests and associated correspondence which seems to stem from different interpretation of the Estonian national law [related to GDPR art 5 (1) (e)]. Different approaches are:

- 4 responding controllers: retention period of 3 years - limitation period for a claim arising from a transaction under An Act on the General Part of the Civil Code art 146 (1).
- 1 responding controller: retention period of the same length as data is processed for - expiry of claims arising from insurance contract under Law of Obligations Act art 475.
- 1 responding controller: retention period of the same length as data is processed for, but not less than 3 years to ensure effective answering to the recurrent access requests.
- 2 responding controllers: retention period of 10 years from the date data subject received the last answer – one controller based it on their internal order and one controller on their legitimate interest to defend against legal claims.

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

No

### **Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”**

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

21) 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 3.4 in the questionnaire addressed to controllers.

We did not identify any considerable shortcomings in established processes of handling GDPR art 15 access requests.

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

From answers of 5 responding controllers emerged a practice that there is a unit that deals with the requests, among others requests by data subjects. In case specific, more complex issues arise when answering, these units consult with legal departments and/or DPOs. We would like to point out that practices of the companies that are not delegating the responsibility

of answering to data subjects only to DPOs are in our view more in line with the essence of the GDPR as controller is the one to ensure that data processing is in compliance with GDPR while DPO has more of an advisory and monitoring role. In addition, larger team of people handling requests is more likely to ensure the continuity if for some reason the numbers of requests should grow significantly.

In one case DPO also carried out an inspection at the beginning of 2024 of how the data subjects' requests were handled in 2023 which is a good example of the DPO role in the process.

All responding controllers answered that they send confirmation of receipt of the request, and it was clear in 8 cases that confirmation includes information on when data subject can expect an answer.

### **Section on "IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR"**

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

23) 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 4.15 in the questionnaire addressed to controllers.

The main issue identified was that in 2 cases the data security measures either are not adequate [raises questions of compliance with of art 5 (1) (f)] or the respondents have misread the question 4.5. Additional clarification is needed from the respondents to reach informed conclusions.

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

There are enough channels to submit access requests, in most cases there are self-service portals, possibility to send requests via e-mail, make an appointment in the service office or send the request in handwritten form via regular mail service. In the case of 2 responding controllers, oral requests are also possible as they have the possibility to identify the data subject in a phone call in most cases.

It is also worth noting, that many service providers (including some of the respondents) in Estonia also offer the possibility to access the data subject's personal data being processed through service provider's self-service portals and this also has an impact on how many requests are submitted as data subjects can access all relevant data directly without requesting it.

### **Section on "CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR"**

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

25) 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 5.18 in the questionnaire addressed to controllers.

The main issue identified is that in relation to providing data subjects with information about the recipients or categories of recipient to whom the personal data have been or will be disclosed [obligation under GDPR art 15 (1) (c)], most of the respondents give the data subjects information only about the categories of recipients. Issuing a list of concrete recipients to data subjects seems to be subject to some additional requirements by the controllers, e.g. when data subject specifically requires the list of concrete recipients (if general request, provide categories); when the list is relevant for the interests of the data subjects; depends on the volume of the answer etc. Our understanding of para 117 EDPB guidelines 01/2022 (... Under Article 15, if the data subject has not chosen otherwise, the controller is obliged to name the actual recipients, unless it is impossible to identify those recipients...) and ECJ case C-154/21 RW v Österreichische Post AG para 36 (... Article 15 of the GDPR lays down a genuine right of access for the data subject, with the result that the data subject must have the option of obtaining either information about the specific recipients to whom the data have been or will be disclosed, where possible, or information about the categories of recipient...) is that if the information is available, concrete recipients have to be presented to the data subject, if data subject so wishes, without any additional conditions.

In the cases of 2 responding controllers, the practice is questionable regarding granting access to non-textual personal data. One controller referred to the need to ask permission from the owner of e.g. the video recording to give access to the personal data, while another controller claimed to evaluate on the case-by-case basis if the access request is grounded enough. Both approaches are not compatible with the art 15 (3) which grants data subject a right to get a copy of the personal data undergoing processing.

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

Two responding controllers use pseudonymisation of the personal data in their internal processing activities where personalisation of data is not important.

### Section on “LIMITATIONS OF ACCESS REQUESTS”

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

We did not identify any considerable shortcomings in limitations of access requests.

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

No

## Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

a. Very High

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.): [No](#)

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

- a. **Very High**
- g. High
- h. Average
- i. Low
- j. Very low
- k. Too diverse levels to qualify

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, “size” of the controller, etc.): [No](#)

31) In your opinion, which **topics concerning the right of access** or which parts of **the EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

[Where available issuing a list of concrete recipients to data subjects, instead of categories of the recipients.](#)

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees’ right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF? If yes, please provide the date, link to the guidance, and a short description of the guidance.

[We have published special section dedicated to data subjects’ rights, including access requests, on our website.](#)

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

[No](#)

34) **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 plan to send a letter of summarising our findings and making recommendations for improvements to the controllers.

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Often

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Sometimes

37) 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 content of EDPB Guidelines 01/2022 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: Video and podcast on data subjects' rights directed to the data subjects

b. No:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes:

b. No: No



# EL SA

Hellenic Data Protection Authority

## 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<sup>14</sup>:
  - d. Ongoing investigation:
  
- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),
  - Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? **Yes**
  - Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. **No**
  - If not, will this fact finding activity impact your enforcement activities and if yes, how? **The Authority will examine whether further enforcement activities are required.**
  
- 3) For all SAs: 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 version was used for all controllers.**
  
- 4) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.  
**All questions were applied.**
  
- 5) For all SAs: 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 etc.)?  
**Yes. We had further categorized the questions to facilitate the gathering of the feedback from the controllers to achieve a more uniform and harmonized analysis approach.**

## Part I – Some numbers on the controllers addressed

- 6) How many controllers did you contact?  
**36**
  
- 7) Out of the contacted controllers, how many controllers responded?

---

<sup>14</sup> 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/to your questions.

27

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?

Some organizations are no longer operating and some are in the process of being liquidated.

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: Please select one or more answers.

- a. Public sector: 1
- b. Private sector: 26

10) Please specify the category<sup>15</sup> of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers

- a. Micro enterprise: 6
- b. Small enterprise: 5
- c. Medium-sized enterprise: 4
- d. Large enterprise (more than 250 employees): 12
- 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) Please specify the nature of the (business) activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. education sector:
- b. health sector:
- c. social sector:
- d. insurance sector:
- e. finance sector: 27 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:

---

<sup>15</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- 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. other (please specify):

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. customers: 25 responding controllers
- b. potential customers: 19 responding controllers
- c. employees: 26 responding controllers
- d. job applicants: 23 responding controllers
- e. children: 4 responding controllers
- f. vulnerable adults: 6 responding controllers
- g. patients:
- h. citizens (for public sector):
- i. applicants (for public services):
- j. recipients (for postal services): 2 responding controllers
- k. other (please specify): 8 responding controllers

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. Less than 100: 7 responding controllers
- b. 100 - 200: 3 responding controllers
- c. 201 - 500: 8 responding controllers
- d. 501 - 2,000: 8 responding controllers
- e. 2,001 - 10,000: 2 responding controllers
- f. 10,001 - 50,000:
- g. 50,001 - 100,000: 1 responding controller
- h. 100,001 - 1,000,000:
- i. 1,000,001 - 10,000,000: 5 responding controllers

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.

- a. Contact data: 27 responding controllers
- b. Payment data: 26 responding controllers
- c. Identification data: 26 responding controllers
- d. Sensitive data within the meaning of Art. 9 GDPR: 10 responding controllers
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR: 13 responding controllers
- f. Other (please specify): 11 responding controllers

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. 0 request: 1 responding controller
- b. 1-10 requests: 6 responding controllers
- c. 11-25 requests: 6 responding controllers
- d. 26-50 requests: 6 responding controllers
- e. 51-100 requests: 1 responding controller
- f. 101-150 requests: 1 responding controller
- g. 151-200 requests: 1 responding controller
- h. 201-500 requests: 1 responding controller
- i. 501-10,000 requests: 4 responding controllers
- j. >10,000 requests:
- k. No information:

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

Significant differences identified may be linked to:

- the sector/ purpose of processing, as claim management companies receive in general more access requests,
- the number of data subjects concerned, as the systemic banks receive a large number of access requests.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 1 responding controller
- b. >0–25%: 7 responding controllers
- c. 26–50% requests: 5 responding controllers
- d. 51–75% requests: 2 responding controllers
- e. 76–100% requests: 12 responding controllers
- f. No information:

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

Significant differences identified may be linked to the sector/ purpose of processing, as claim management companies receive a high number of access requests compared to other data protection access requests.

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 1 responding controller
- b. >0–25%: 13 responding controllers
- c. 26–50% requests: 2 responding controllers
- d. 51–75% requests: 1 responding controller
- e. 76–100% requests: 10 responding controllers
- f. No information:

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

In this case, it would be challenging to state the potential explanation, as significant differences occur between controllers of the same size or the same sector.

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 1 responding controller
- b. >0–25%: 21 responding controllers
- c. 26–50% requests: 3 responding controllers
- d. 51–75% requests: 1 responding controller
- e. 76–100% requests: 1 responding controller
- f. No information:

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No significant difference between controllers is identified as the majority falls under (b) above; 2 controllers with a higher percentage are “large” systemic banks.

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 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. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.
- d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?

- e. What are differences that you have encountered between controllers in your Member State?
  - f. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?
- a. Most controllers document the procedure of handling and complying with Art. 15 GDPR requests.  
 Most controllers store Art. 15 GDPR requests along with other GDPR requests in a common registry. A few do not have a special registry for GDPR or Art. 15 GRDP requests.  
 2 controllers do not keep a record of Art. 15 GDPR requests.  
 Almost all controllers mentioned that access to Art.15 GDPR requests is limited to the minimum necessary departments, as these requests are handled by the Customer Service/ Complaints Department/ DPO. Most controllers designate their DPO as the main or sole responsible department to handle access requests, therefore in this case, access to Art.15 GDPR requests is limited to the DPO and is shared only with the department involved, if necessary.  
 Only 2 controllers explicitly included log files in the description of the documentation procedure regarding access requests.  
 Most controllers store Art. 15 GDPR request for 5 or 20 years. These time-limits are provided by national law (Articles 249-250 of the Civil Code) regarding the limitation of rights and actions.
- b. GDPR Art. 5 (2), 12 (5), 24, 31.  
 Greek National Law: Articles 249-250 of the Civil Code.
  - c. EDPB Guidelines 01/2022 par. 108, 193.  
 CJEU (C-579/21)
  - d. This may be a matter of structure and/ or the “size” of the controller, in general largest controllers have in place extended documentation of processes and procedures.
  - e. Results vary as to the documentation procedures, as well as access rights within the controller (both as described above).
  - f. A possible solution for ensuring harmonisation and effective implementation of GDPR would be the issuance of guidance and / or recommendations regarding best practices for documenting compliance with Art. 15 requests, including detailed documentation, minimum access within the controller, and the storage of log files regarding access.

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

No.

### **Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”**

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

21) 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 3.4 in the questionnaire addressed to controllers.

- a. Only one controller hasn't applied a (specific) procedure for handling requests for access under article 15 GDPR.
- b. GDPR articles 12, 15, Greek law 4624/2019 article 33
- c. EDPB Guidelines 01/2022, para. 123-124, 127-138
- d. This may be a matter of structure and/ or the "size" of the controller.
- e. There are differences related to the structure and the competent offices within the controller (ex. DPO, customer service department, legal department, compliance department), the related procedures applied (ex. different communication channels, email, paper documents)
- f. SAs should conduct more audits and provide guidance, in particular, towards the SMEs.

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

One controller has put in place a special platform for the handling of such requests.

### **Section on "IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR"**

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

23) 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 4.15 in the questionnaire addressed to controllers.

a. Most controllers apply certain general procedures to facilitate communication. No particular procedures or information documents for vulnerable persons (ex. braille documents or websites accessible to persons with disabilities), but in most cases there is a cooperation with the DPO to find the best solution to facilitate the exercise of the right (ad hoc examination of each case).

In 2023 only 4 controllers received oral access request and only the two of them replied.

None of the participants have issued or apply specific id verification procedures. In each case, the id verification depends on the communication channel selected by the applicant/data subject.

Only in one case there is a deadline of 3 days for the data subject to provide additional information in case there are doubts about the identity of the applicant. After this time period the request is cancelled and the data subject has to make again the request with the additional information.

b. GDPR articles 12, art 15, 32

Greek Law 4624/2019 article 33

c. EDPB Guidelines 01/2022 on the right of access, para. 139-164

d. This may be a matter of structure and/ or the "size" of the controller. In general, largest controllers have in place policies and procedures not precisely relating to the right of access, but they facilitate its exercise.

e. No significant differences encountered.



f. Data controllers should design and apply concrete, transparent and clear policies and best practices on issues relating to technical and organizational measures facilitating the right of access.

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

One controller has put in place deadline tracking process (ex. alerts, reports) in order to ensure that access requests pursuant to Article 15 of the GDPR are responded to promptly, and in any event within one month of receipt

### **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

25) 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 5.18 in the questionnaire addressed to controllers.

The main issues that we have identified are the following:

i) While all controllers provide information to data subjects regarding the duration of data retention, only 25% of them provide information on the specific retention period as well as the exact deletion time

ii) 55% of the controllers have not taken steps to provide access to personal data with short retention periods

iii) If there is a change in the personal data processed since the date of making the request by the date the controllers provide access to that data, only 48 % of the controllers provide the updated personal data, thus the personal data that exist at the time of their decision to provide access

iv) In case of repeated access requests within a short period of time (but not excessive within the meaning of Article 12(5) GDPR), 52% of the controllers provide to data subjects only information about changes that occurred after the last provision of information, while 48% provide full and complete access to all their personal data.

v) 45% of the controllers have taken action to provide access to personal data with short retention periods, while 55 % have not taken any such steps.

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

The controllers provide the data subjects with all the information provided for in article 15 of the GDPR, namely, the purposes of the processing, the categories of personal data concerned, the recipients or categories of recipient to whom the personal data have been or will be disclosed, the period for which the personal data will be stored, or, if not possible, the criteria used to determine that period. They do not process pseudonymized data. If a data subject requests a copy of personal data in accordance with Article 15(3) of the GDPR, the controllers provide data from various files they have produced specifically for the respective request access, data exports from databases, copies of requested information (Transcripts), information about their contact, and complete documents or part of documents that contain



the personal data. They also provide the data subject with other means of access beyond the provision of copies of the information requested, such as oral information, on-site or remote access. Moreover, the controllers grant access to personal data such as images, video or voice registrations, and if a data subject requests access to only parts of his/her data, they comply with that request ("partial access request").

### Section on “LIMITATIONS OF ACCESS REQUESTS”

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

70 % of the respondents do not provide information to their data subjects about the identity of the persons within their organization that process their personal data.

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

The restrictions provided for in the legal/regulatory framework are taken into account, e.g. in article 23 of the GDPR and in the guidelines of the EDPB. More specifically, the controllers do not grant the access request when requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, or when access is prohibited by law (tax or bank secrecy). In these cases the controllers inform the data subjects accordingly. Moreover, the controllers check whether the rights and freedoms of others are affected before providing access in accordance with Article 15 of the GDPR and in particular before sending a copy of their data.

In relation to the provision of access to personal data, such as images, videos or voice recordings, it is ensured in any case that the information provided does not contain personal data of third parties (e.g. when providing a copy of video material, if required, the data is hidden of third-party depicted persons (blurring)).

### Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

**No noticeably significant differences were observed between the participants on the levels of compliance and awareness concerning the GDPR provisions relating to the right of access.**

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, “size” of the controller, etc.):

Only 2 out of the 27 respondents indicated that they are not aware of the European Data Protection Board Guidelines 01/2022 on data subjects' rights. Both of these organizations operate in the finance sector. Specifically, the first is a microenterprise offering receivables management services from loans and credit facilities. The second organization is a public law entity that provides deposit and loan services.

It should be noted that 2 out of the 25 respondents who are aware of these guidelines mentioned that they have launched targeted training and awareness activities for their employees based on these guidelines to ensure full compliance with the new requirements

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

According to the responses of the participating controllers there is a problem on how the controllers provide access and comply with an access request. More specifically while all controllers provide information to data subjects regarding the duration of data retention, only 25% of them provide information on the specific retention period as well as the exact deletion time, and half of them have not taken steps to provide access to personal data with short retention periods. Moreover, if there is a change in the personal data processed since the date of making the request by the date the controllers provide access to that data, only 48 % of the controllers provide the updated personal data, thus the personal data that exist at the time of their decision to provide access. In case of repeated access requests within a short period of time (but not excessive within the meaning of Article 12(5) GDPR), 52% of the controllers provide to data subjects only information about changes that occurred after the last provision of information, while 48% provide full and complete access to all their personal data. Regarding access to personal data with short retention periods, 45% of the controllers have taken action to provide access to the information, while 55 % have not taken any such steps.

## **Part IV – Actions by participating SAs**

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees' right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF?

If yes, please provide the date, link to the guidance, and a short description of the guidance.

- An online platform has been created and is accessible through this link (<https://awareness.dpa.gr/>). The goal of this platform is to inform and raise awareness among young citizens about the protection of their personal data and privacy issues
- As part of the **byDesign** project, 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.
- As part of the **byDefault** project, the following activities were carried out:
  - An e-platform and digital library has been created for DPOs and privacy professionals and is available at "<https://collab.dpa.gr>
  - the educational programme and physical game on data protection, which was created for primary and secondary school students, and its supporting material for teachers
- 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

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

- The **Hellenic Supervisory Authority**, coordinated the following initiatives:
  - A two-year project entitled "**byDesign**" funded by the European Union's Citizens, Equality, Rights and Values (CERV) Programme. 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) Programme. 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 specialised 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 24<sup>th</sup> 2024
- **18th Data Protection Day, the Hellenic SA** organised 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.

34) **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 available to the Collegial body of the Hellenic SA, who will decide if further actions are required and determine a potential timeline for these actions

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Very often

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Often

37) 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 content of EDPB Guidelines 01/2022 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
- ii. Online or remote training sessions: Yes
- iii. Conferences organised: Yes
- iv. Others: please specify:

b. No:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

- a. Yes: awareness activities (e.g. seminars, events, workshops) should be carried out at EU level with the involvement of broader audience, training seminars, asynchronous online toolkits ...

In order to communicate and raise awareness regarding the EDPB Guidelines, a number of relevant activities should be initiated, including:

- Public consultation and policy events involving policymakers, European, regional, and local authorities, and other relevant stakeholders and working groups (identified through, e.g., policy fellowship schemes). The goal is to present the main aspects of the EDPB Guidelines and to demonstrate best practices and successful use cases.
- Open national and international networking events and training seminars to boost relationships among researchers, industry, and policymakers, focusing on right of access issues.
- Development of asynchronous online toolkits and platforms to foster discussions about regulations, contributing to other relevant EU policies and directives, e.g., eIDAS, NIS 2 Directive, Digital Services Act (DSA), Digital Market Act (DMA), Data Governance Act (DGA), and EU initiatives such as the EU Digital Identity Wallet, the Regulation on a European approach for Artificial Intelligence (AIR), and the EU Data Spaces.
- Creation of synergies with other Horizon Europe programs and standardization activities to further position these guidelines as a valuable asset in advancing GDPR-compliant solutions.
- Participation in clustering activities at the EU level to exchange knowledge, results, and experiences with other relevant initiatives, creating strong links between them.

# ES SA

Agencia Española de Protección de Datos (AEPD)

## Introduction

- 1) What was the initial procedural framework of your action? Please select one or more answers.
- Fact finding: **Yes**
  - Fact finding + determining follow-up action based on the results:
  - New formal investigation<sup>16</sup>:
  - Ongoing investigation:

- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),

- Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? **Yes**
- Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. **No**
- If not, will this fact finding activity impact your enforcement activities and if yes, how? **There are no provisions for this activity to impact 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 for all controllers.**

- 4) If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.

**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 etc.)?

## Part I – Some numbers on the controllers addressed

- 6) How many controllers did you contact?

**20 were contacted.**

- 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/to your questions.

---

<sup>16</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

39 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?

Two public regional bodies spread the invitation among the controllers invited to participate in several health departments and hospitals under its jurisdiction completing several questionnaires.

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: Please select one or more answers.

a. Public sector: 23 responding controllers

b. Private sector: 16 responding controllers

10) Please specify the category<sup>17</sup> of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers

a. Micro enterprise:

b. Small enterprise:

c. Medium-sized enterprise:

d. Large enterprise (more than 250 employees): 16 responding controllers

e. Non-profit organisation:

f. Ministry: 1 responding controller

g. Local authority: 22 responding controllers

h. Administrative authority/agency/office (e.g. job center):

i. School / university / educational institution:

j. Other (please specify):

11) Please specify the nature of the (business) activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

a. education sector:

b. health sector: 24 responding controllers

c. social sector: 2 responding controllers

d. insurance sector: 1 responding controller

e. finance sector: 2 responding controllers

f. IT sector: 1 responding controller

g. retail sector: 2 responding controllers

h. logistics sector:

i. public transportation: 1 responding controller

j. telecommunications: 2 responding controllers

k. postal services: 1 responding controller

l. advertising sector:

m. marketing services:

n. entertainment sector:

o. information / journalism sector:

---

<sup>17</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).



- p. scientific / historical research: 1 responding controller
- q. credit scoring agency:
- r. public utility/infrastructure provider (e.g. energy): 3 responding controllers
- s. housing industry:
- t. manufacturing:
- u. other (please specify): A relevant company in the tourism sector also participated.

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. customers: 16 responding controllers
- b. potential customers: 17 responding controllers
- c. employees: 25 responding controllers
- d. job applicants: 19 responding controllers
- e. children: 5 responding controllers
- f. vulnerable adults: 5 responding controllers
- g. patients: 2 responding controllers
- h. citizens (for public sector): 4 responding controllers
- i. applicants (for public services): 4 responding controllers
- j. recipients (for postal services): 1 responding controller
- k. other (please specify):

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. Less than 100: 2 responding controllers
- b. 100 - 200:
- c. 201 - 500:
- d. 501 - 2,000: 2 responding controllers
- e. 2,001 - 10,000:
- f. 10,001 - 50,000:
- g. 50,001 - 100,000: 7 responding controllers
- h. 100,001 - 1,000,000: 12 responding controllers
- i. 1,000,001 - 10,000,000: 9 responding controllers
- j. More than 10,000,000: 10 responding controllers

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.

- a. Contact data: 39 responding controllers
- b. Payment data: 19 responding controllers
- c. Identification data: 19 responding controllers
- d. Sensitive data within the meaning of Art. 9 GDPR: 24 responding controllers
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR: 4
- f. Other (please specify):



15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. 0 request: 3 responding controllers
- b. 1-10 requests: 1 responding controller
- c. 11-25 requests: 10 responding controllers
- d. 26-50 requests: 5 responding controllers
- e. 51-100 requests: 2 responding controllers
- f. 101-150 requests:
- g. 151-200 requests:
- h. 201-500 requests:
- i. 501-10,000 requests: 16 responding controllers
- j. >10,000 requests:
- k. No information:

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

One possible explanation for the difference between the data subjects concerned and the number of access requests may be that for a great number of data subjects whose data are processed, as employees or patients, do not generate doubts about the purposes for which the data is processed, resulting in a lower number of access requests since the data subjects have been duly informed of these purposes.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 4 responding controllers
- b. >0–25%: 17 responding controllers
- c. 26–50% requests: 5 responding controllers
- d. 51–75% requests: 4 responding controllers
- e. 76–100% requests: 9 responding controllers
- f. No information:

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No significant differences in the percentages of the responding controllers have been detected.

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 6 responding controllers

- b. >0–25%: 3 responding controllers
- c. 26–50% requests: 6 responding controllers
- d. 51–75% requests: 6 responding controllers
- e. 76–100% requests: 15 responding controllers
- f. No information: 3 responding controllers

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No significant differences in the percentages of the responding controllers have been detected.

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 6 responding controllers
- b. >0–25%: 3 responding controllers
- c. 26–50% requests: 6 responding controllers
- d. 51–75% requests: 6 responding controllers
- e. 76–100% requests: 11 responding controllers
- f. No information: 7 responding controllers

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No significant differences in the percentages of the responding controllers have been detected.

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 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. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.
- d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
- e. What are differences that you have encountered between controllers in your Member State?

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

Most companies and bodies answering the questionnaire reported adopting a defined procedure to deal with privacy rights in order for the requests to be tracked and documented.

Some of them use specific privacy management software. The interviewers informed that trained staff, assisted by the DPO are in charge of dealing with the data subject requests.

As for the time that information on access requests is stored it will depend on the legislation applied to the controller (health, commercial regulation, contractual relationship, etc). In some case, the respondents refer to the applicable Global Privacy Policy.

In general terms, large companies and public bodies can deploy more resources (e.g. trained staff, privacy software) regarding privacy management to review, accept, or deny, as well as track the requests.

At the same time, small institutions in the field of the public health sector, despite having fewer resources can deal with the requests for access received efficiently.

Continue to raise awareness among controllers and data protection officers about their obligations as well as among data subjects about their rights.

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

Implementing appropriate resources regarding privacy management to review, accept or deny, as well as to track the requests is considered a best practice to be recommended.

### **Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”**

- 21) 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 3.4 in the questionnaire addressed to controllers.

The main challenge would be to spread the necessity to carry out a Privacy Assessment for new services or solutions where the data subjects' can be taken into consideration by the organization.

At the same time, it would be advisable to adopt procedures to systematically track the requests.

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

Monitoring access requests displaying deadlines for answering to the data subjects as well as the confirmation of the request reception can be considered as a best practice.

### **Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”**

23) 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 4.15 in the questionnaire addressed to controllers.

In general, data controllers encourage data subjects to use specific channels implemented to submit a request although requests received outside these formal channels are also attended. Regarding identification and authentication respondents manage the requests in writing and use reasonable and proportionate measures to verify the requestors' identity,

Regarding the most frequent circumstances to extend the one-month deadline for processing access rights, It might be relevant to highlight the requests that involve copies of email conversations that have to be reviewed manually and redacted.

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

Permanent training of employees in charge of dealing with data subjects' requests together with defined and reviewed procedures seems to be one of the best practices to ensure the proper management of these requests.

### **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

25) 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 5.18 in the questionnaire addressed to controllers.

In some cases, the data controller must send a communication to ask data subjects to clarify their request to avoid overloading with the information provided. The information offered to the data subjects refers or uses text modules of controllers' privacy notice as well as tailored for specific requests (e.g. recipients of personal data).

Concerning information on recipients of personal data categories of recipients are usually provided unless the requestor asks for any particular recipient.

Regarding data subjects' objection to the information provided by controllers no significant claims figures have been reported.

Some controllers reported that if a data subject requests a copy of the personal data processed file compilations specifically produced for the respective access request, extracts from a database, communication between the controller and the data subject as well as full or partial documents containing the personal data are provided.]

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

A trained team and updated procedures are of capital importance when it comes to appropriately addressing data subjects' requests.

### **Section on “LIMITATIONS OF ACCESS REQUESTS”**

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

As regards of the limitations of access requests, only when the requests are manifestly unfounded or excessive.

After assessing the request by the expert, only information including the requestor's data is provided.

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

A trained team is of capital importance when it comes to assessing on a case-by-case basis data subjects' requests asking for clarification if needed.

### Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

In general terms, large companies and institutions can deploy more resources (e.g. trained staff, privacy management software) regarding privacy management to review, accept, or deny, as well as track the requests.

At the same time, small institutions in the field of the public health sector, despite having fewer resources can deal with the requests for access received efficiently.

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, "size" of the controller, etc.):

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

All the controllers consulted are aware of the [EDPB Guidelines 1/2022 on data subject rights](#).

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees' right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF?

If yes, please provide the date, link to the guidance, and a short description of the guidance.

[Spanish Data Protection Agency website](#) has published several sections in its website dedicated to the rights of data subjects as well as the obligations of controllers in the various topics addressed by the GDPR. It also has a series of specific sections for various sectors and topics where the most relevant issues for controllers and their DPOs are addressed.

It also has a Q@A section grouped by relevant topics, including those related to the exercise of rights, which includes an online assistant to answer questions addressed by data subjects.

The links to the relevant documents can be found as follows:

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 the first level of AEPD's web (<https://www.aepd.es/>), includes your rights section providing practical forms for exercising rights.]

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

[For now, no actions have been considered to be undertaken.](#)

34) **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).

[For now, no actions have been considered to be undertaken.](#)

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on**

**or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

We often rely on or refer to the EDPB Guidelines on the right of access in our outgoing decisions or guidance to the right of access.

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

We often rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access.

37) 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 content of EDPB Guidelines 01/2022 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:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes: **Yes. Continue to clarify aspects that may arise when exercising the right of access.**

b. No:

# FI SA

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:
  - b. Fact finding + determining follow-up action based on the results: [Yes](#)
  - c. New formal investigation<sup>18</sup>:
  - d. Ongoing investigation:
- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),
  - Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? [Yes](#)
  - Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. [Yes; the Office of the Data Protection Ombudsman has launched formal investigations based on the results of the survey. The Office of the Data Protection Ombudsman has sent requests of clarification to some of the controllers to investigate their practices further.](#)
  - If not, will this fact finding activity impact your enforcement activities and if yes, how? -
- 3) For all SAs: 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 was used for all controllers.](#)
- 4) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.

-
- 5) For all SAs: 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 etc.)?

-

## Part I – Some numbers on the controllers addressed

- 6) How many controllers did you contact?  
[15](#)
- 7) Out of the contacted controllers, how many controllers responded?

---

<sup>18</sup> 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/to your questions.

15

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: Please select one or more answers.

- a. Public sector: 6
- b. Private sector: 9

10) Please specify the category<sup>19</sup> of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers

- a. Micro enterprise: -
- b. Small enterprise: 1
- c. Medium-sized enterprise: 3
- d. Large enterprise (more than 250 employees): 4
- e. Non-profit organisation: 1
- f. Ministry: -
- g. Local authority: -
- h. Administrative authority/agency/office (e.g. job center): 5
- i. School / university / educational institution: -
- j. Other (please specify): Public healthcare provider

11) Please specify the nature of the (business) activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. education sector:
- b. health sector: 3
- c. social sector: 2
- d. insurance sector:
- e. finance sector: 1
- f. IT sector:
- g. retail sector: 1
- h. logistics sector: 1
- i. public transportation: 1
- j. telecommunications:
- k. postal services:
- l. advertising sector:
- m. marketing services:
- n. entertainment sector:

---

<sup>19</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- o. information / journalism sector:
- p. scientific / historical research:
- q. credit scoring agency:
- r. public utility/infrastructure provider (e.g. energy):
- s. housing industry: 1
- t. manufacturing:
- u. other (please specify): Housing management, real estate, rental agency, fire and rescue services, invoicing, debt collection, agriculture and forestry, parking services, municipality, compilation of statistics, trade union

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. customers: 15
- b. potential customers: 4
- c. employees: 14
- d. job applicants: 11
- e. children: 5
- f. vulnerable adults: 4
- g. patients: 3
- h. citizens (for public sector): 5
- i. applicants (for public services): 4
- j. recipients (for postal services): 3
- k. other (please specify):

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. Less than 100:
- b. 100 - 200:
- c. 201 - 500:
- d. 501 - 2,000:
- e. 2,001 - 10,000:
- f. 10,001 - 50,000:
- g. 50,001 - 100,000: 1
- h. 100,001 - 1,000,000: 8
- i. 1,000,001 - 10,000,000: 6
- j. More than 10,000,000:

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.

- a. Contact data: 14
- b. Payment data: 12
- c. Identification data: 13
- d. Sensitive data within the meaning of Art. 9 GDPR: 8

- e. Data of a highly personal nature within the meaning of Art. 10 GDPR: 2
- l. Other (please specify): Information on transport tickets, information concerning employment, information concerning parking and vehicles, teaching, land use planning, environmental health care, information based on national data protection legislation

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. 0 request: 1
- b. 1-10 requests: 6
- c. 11-25 requests: 2
- d. 26-50 requests: 3
- e. 51-100 requests: 2
- f. 101-150 requests: 1
- g. 151-200 requests: -
- h. 201-500 requests: -
- i. 501-10,000 requests: -
- j. >10,000 requests: -
- k. No information: 1

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, "size" of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

The size and sector of the controller affected the number of requests of access. In health and social care sectors it is more common to request access to data than in many other sectors. Data subjects may be more aware of their rights within the health and social care sectors. In health and social care sectors, controllers process sensitive information, that might have a significant effect on the freedoms and rights of the data subjects (for example what kind of care or social services the data subject can have access to), which might increase the number of requests.

The number of requests of access is higher also in the sector concerning parking services and debt collection. One contributing factor in the amount of access requests may be that the national supervisory authority has released decisions concerning right of access in the parking services sector and the data subjects might be aware of these decisions and their rights. In addition, parking and debt collection might have significant effect on the freedoms and rights of the data subjects (for example effects on financial status), which might increase the number of requests.

The nature and amount of data processed, and the nature of processing might impact the number of requests. Data subjects might not be aware of how some of the controllers process their information or on the other hand the processing might not have a significant effect on their rights and freedoms. Some controllers process very limited amount of data (for example no sensitive data) of the data subject, which might not be of concern for the data subjects. The processing might also be passive. On the other hand, in sectors such as health and social care, finance, debt collection or parking the amount of data processed might be larger, more

actively processed, more sensitive and affect the rights and freedoms of data subjects more considerably.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 1
- b. >0–25%: 4
- c. 26–50% requests: 1
- d. 51–75% requests: 2
- e. 76–100% requests: 5
- f. No information: 2

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

There were significant differences between controllers in the percentages of access requests in regard to the rest of the data protection requests received. For four controllers 100 percent of data protection requests were requests of access. These four controllers operate in different sectors and process different type of data.

Two controllers did not have precise information on the percentages of data protection requests. One controller had not received requests of access in 2023. For many controllers the number of access requests in comparison to other data protection requests was quite low. There were also significant differences within specific sectors. For example, in health and social care sector, the percentage of requests of access was 70 percent for one controller and only 0,05 for another controller. However, the number of requests affected this percentage. If the overall number of access requests was low, their percentage of all of the data protection requests was lower.

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: -
- b. >0–25%: -
- c. 26–50% requests: -
- d. 51–75% requests: 1
- e. 76–100% requests: 9
- f. No information: 5

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

There were no significant differences in the percentages. For most controllers 100 percent of the access requests included a request to receive an insight into and inspection of and/or a copy of the personal data.

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 6
- b. >0–25%: 3
- c. 26–50% requests: 1
- d. 51–75% requests: 1
- e. 76–100% requests: -
- f. No information: 4

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

Many controllers did not receive requests that included a specific request to receive information on the underlying processing activities. For a couple of controllers, the percentage of requests to receive information on processing activities was 50 percent of the requests. The fields these controllers operate in (trade union and debt collection) might affect the number of requests to receive information on processing activities.

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 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. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.
- d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
- e. What are differences that you have encountered between controllers in your Member State?
- f. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

In general, the controllers had implemented processes to handle the requests and document them. Some controllers had not clearly stated the storage periods for the requests. One explanation for this might be that the number of requests received is quite low and therefore some controllers have not implemented clear processes on how to handle access requests.

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

Many controllers had well documented practices on how to document and handle the requests and which personnel had right to process the requests.

### Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

21) 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 3.4 in the questionnaire addressed to controllers.

Most controllers have established clear processes for handling access requests. For some controllers the number of requests has been low and therefore the processes were not as precise. Overall there were no major issues or challenges identified.

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

Many controllers had established clear processes for handling access requests. Many controllers had established written instructions on the processes and had instructions on which personnel have right to handle the requests and what their responsibilities are in the process of answering the requests.

### Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

23) 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 4.15 in the questionnaire addressed to controllers.

Some controllers require excessive information in order to identify the data subject. According to Article 12 (6) without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject. As a rule, the controller cannot request more personal data than is necessary to enable authentication, and that the use of such information should be strictly limited to fulfilling the data subjects' request.

Some controllers require data subjects to request access via a specific channel for example by using a form or by logging in to a portal by using the Finnish strong identification (proving the identity online with e.g. online banking credentials or mobile certificate). Some controllers require data subjects to sign specific forms in order to process the request. Some controllers do not accept non-written requests such as request made by phone.

Most of the issues relate to controller's responsibility to facilitate exercise of data subject rights under Article 12 (2). The GDPR does not set requirements for the form in which the request

of access can be made. Therefore, the controller should facilitate the exercise of right of access and handle requests that are not made via official channels or by using signed forms.

Some controllers do not accept requests made by proxy. In general requests made by proxy should be processed.

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

Some controllers handled access requests even when the data subject did not contact the controller via the official contact channel. In these situations, some controllers forwarded the requests to the appropriate person to handle and did not insist on data subjects to use the official contact channels in order to handle the request.

### **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

25) 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 5.18 in the questionnaire addressed to controllers.

When providing the information in accordance with Article 15 (1) lit. a) - h) and Article 15 (2) GDPR, some controllers only refer to their privacy notice and do not update the information on the concrete purposes pursued with the processing of the specific data subject's data. The controller should provide the data subject concrete information tailored to the data subject and specific access request.

Some controllers state that they process pseudonymised data but did not state clearly if they provide access to such data. As a rule, data subjects have right of access to all data relating to them.

Some controllers do not provide access to non-textual information such as video or phone call recordings. Some controllers provide access to non-textual information but do not provide a copy. As a rule, data subjects have right of access to all data relating to them including to video or phone call recordings unless it adversely affects the rights and freedoms of others.

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

-

### **Section on “LIMITATIONS OF ACCESS REQUESTS”**

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.



Some controllers charge a fee if a data subject request access more than once a year. Before GDPR the Personal Data Act was in force in Finland. According to Personal Data Act section 26, the controller may charge for the provision of access to the data only if less than one year has passed since the previous instance of providing the data subject with access to data. The Personal Data Act was revoked once GDPR took effect. According to article 12 (5) GDPR where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may charge a reasonable fee. The GDPR does not specify when request is repetitive. As a rule, controller cannot define access request repetitive just because less than one year has passed since the previous instance of providing the data subject with access to data.

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

-

### Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.): -

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, “size” of the controller, etc.): -

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

Identification of the data subject: Some controllers require excessive information in order to identify the data subject. This relates to controllers’ responsibility to facilitate exercise of data subject rights under Article 12 (2).



Access to non-textual information: Some controllers do not provide access to non-textual information such as video or phone call recordings. Some controllers provide access to non-textual information but do not provide a copy. As a rule, data subjects have right of access to all data relating to them including to video or phone call recordings unless it adversely affects the rights and freedoms of others.

Information provided in accordance with Article 15 (1) lit. a) - h) and Article 15 (2) GDPR: Some controllers only refer to their privacy notice and do not update the information on the concrete purposes pursued with the processing of the specific data subject's data. The controller should provide the data subject concrete information tailored to the data subject and specific access request.

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees' right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF? If yes, please provide the date, link to the guidance, and a short description of the guidance.

Not yet.

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

No.

34) **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 Office of the Data Protection Ombudsman has sent requests for clarification to some of the controllers. Based on the controllers' responses, the Office of the Data Protection Ombudsman will consider whether further guidance will be needed. The Office of the Data Protection Ombudsman will send guidance to some of the controllers who replied to the survey. The actions will be decided later this year or in the beginning of next year.

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Often.

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Sometimes.

37) 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 content of EDPB Guidelines 01/2022 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:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

c. Yes **Yes**

a. No

# FR SA

Commission Nationale de l'Informatique et des Libertés - CNIL

## 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<sup>20</sup>: **Yes**
  - d. Ongoing investigation:
- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),
  - Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)?
  - Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available.
  - If not, will this fact finding activity impact your enforcement activities and if yes, how?
- 3) For all SAs: 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 a common template of the questionnaire that was adapted by each investigation team during the onsite investigations

- 4) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.

Most of the questions were asked. However, due to the type of investigation chosen, each investigation team had to adapt the questionnaire in order for it to suit the course of the onsite investigation.

- 5) For all SAs: 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 etc.)?

No

## Part I – Some numbers on the controllers addressed

- 6) How many controllers did you contact?  
9 onsite investigations were conducted at this stage. 3 more will be conducted in the upcoming weeks.

---

<sup>20</sup> 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/to your questions.

9

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: Please select one or more answers.*

- a. Public sector: 2
- b. Private sector: 7

10) Please specify the category<sup>21</sup> of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers*

- a. Micro enterprise:
- b. Small enterprise:
- c. Medium-sized enterprise: 1
- d. Large enterprise (more than 250 employees): 6
- e. Non-profit organisation:
- f. Ministry: 1
- g. Local authority:
- h. Administrative authority/agency/office (e.g. job center):
- i. School / university / educational institution:
- j. Other (please specify):  
1 (public hospital)

11) Please specify the nature of the (business) activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. education sector: 1
- b. health sector: 1
- c. social sector:
- d. insurance sector: 1
- e. finance sector: 2
- f. IT sector:
- g. retail sector:
- h. logistics sector:
- i. public transportation: 1
- j. telecommunications: 1
- k. postal services:
- l. advertising sector:

---

<sup>21</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- m. marketing services:
- n. entertainment sector: 1
- 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. other (please specify): 1(social media)

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. customers: 7
- b. potential customers: 3
- c. employees: 9
- d. job applicants:
- e. children: 1
- f. vulnerable adults:
- g. patients: 1
- h. citizens (for public sector): 1
- i. applicants (for public services):
- j. recipients (for postal services):
- k. other (please specify):

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. Less than 100:
- b. 100 - 200:
- c. 201 - 500:
- d. 501 - 2,000:
- e. 2,001 - 10,000:
- f. 10,001 - 50,000: 1
- g. 50,001 - 100,000:
- h. 100,001 - 1,000,000: 1
- i. 1,000,001 - 10,000,000: 4
- j. More than 10,000,000: 3

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? *Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.*

- a. Contact data: 9
- b. Payment data: 9
- c. Identification data: 9
- d. Sensitive data within the meaning of Art. 9 GDPR: 4

- e. Data of a highly personal nature within the meaning of Art. 10 GDPR:
  - l. Other (please specify): [geolocation and biometric data](#)

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. 0 request:
- b. 1-10 requests: [1](#)
- c. 11-25 requests: [2](#)
- d. 26-50 requests: [2](#)
- e. 51-100 requests:
- f. 101-150 requests: [1](#)
- g. 151-200 requests: [1](#)
- h. 201-500 requests:
- i. 501-10,000 requests: [2](#)
- j. >10,000 requests:
- k. No information:

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

[The significant difference in the numbers of the responding controllers can be explained by the “size” of the controller \(in public transportation or telecommunications especially\), its sector \(in the public sector, requests for access can be based on other legal grounds\) or the fact that some categories of data controllers and/or lack knowledge regarding GDPR right of access.](#)

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests:
- b. >0–25%: [3](#)
- c. 26–50% requests: [1](#)
- d. 51–75% requests: [2](#)
- e. 76–100% requests: [2](#)
- f. No information: [1](#)

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

[The significant difference in the numbers of the responding controllers can be explained by the sector of the controller \(in the health sector, requests for access can be based on other legal grounds\).](#)

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a

copy of the personal data? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests:
- b. >0–25%:
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests: 6
- f. No information: 3

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 3
- b. >0–25%: 4
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests:
- f. No information: 2

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No significant difference was identified. However, specific request to receive information on the underlying processing activities are probably due to a lack of knowledge of the controllers and/or data subjects regarding this specific aspect of the art. 15.

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 in the questionnaire for controllers:

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

- No automatic process has been implemented by the data controller to ensure his obligation to inform the data subject within a delay of one month.

- Data retention. Some access requests and their responses were kept indefinitely.

- No automatic process has been implemented by the data controller to ensure his obligation to inform the data subject within a delay of one month.
- The company set retention period of two years for the exchanges related to access requests. The company does not respect this retention period and also stores the ID's of data subject collected to verify the identity of the data subject.

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

- Art.12.3.
- Art. 5.1.e.

c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.

N/A

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

- No nationwide coordination tool.
- Insufficient auditing processes.
- Technical reasons as the requests are transferred on a mailbox.

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

N/A

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

- Implement a common process and monitoring tool
- Set up the mailbox to receive alerts

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

N/A

## Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

21) 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 3.4 in the questionnaire addressed to controllers.

- No nationwide process for all data processing;
- The main challenge has been the sudden skyrocketing of the number of requests. This led the company to mobilize an unusual number of employees on these requests.
- No confirmation of receipt of access requests are sent by the controller to the data subject.

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

- The whole administrative file of an employee is accessible on site following a specific process. The employee is allowed to come with an advisor;



- Faced with the massive amount of requests, the company chose to alert the SA about it, explaining the difficulties it encountered and how it was attempting to manage it.
- Confirmations of receipt of access requests including the processing time

### **Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

23) 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 4.15 in the questionnaire addressed to controllers.

- Answers to access request are sometimes insufficiently secured (unprotected archive file sent by email);
- Responses to requests for access are sent by e-mail, including attachments, without any particular security measures.

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

- A tool allows the data subject to access some of his data directly;
- The company uses specialized management software to process rights requests. Depending on the information contained in the form and the source of the request, applications are processed by the appropriate department. This tool makes it possible to monitor processing times, trace reasons for rejection, and track all actions taken on processed requests.
- The company has set up a tool to exercise access request for individuals logged in to their account on the company's website. This tool allows for very quick and precise automated answers to access requests;
- An automatic receipt is sent to the data subject as soon as his request is received. Controller has put in place an automated alert system in order to monitor the deadline for processing access requests

### **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

25) 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 5.18 in the questionnaire addressed to controllers.

- The difficulty of granting access requests relating to a very large number of professional emails because of the rights of third parties, secrecy of correspondence and banking secrecy;
- Difficulty in qualifying and processing many complex or cross-functional requests sent to the DPO's e- mail address, which were not submitted via the dedicated form.
- Communications between the controller and the data subject are not provided. The controller has chosen to limit the information disclosed to the data subject in the first instance because

of the large number of information systems and applications that host customers' personal data.

- Communications between the controller and the data subject are not provided. The IT tools used by the controller do not allow automated extraction of the history of communications between the customer and the customer service department.

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

N/A

### Section on “LIMITATIONS OF ACCESS REQUESTS”

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

- Conflicting national and European legislation regarding the scope of the data that can be accessed;
- Systematic use of the limits to the right of access (rights of third parties, confidentiality of correspondence, business confidentiality) to refuse to grant employees' requests for access to professional emails and telephone recordings.
- The data controller may refuse to comply with an exercise of the right of access for the following reasons:
  - failure to respond to a request for clarification,
  - excessive request,
  - unfounded request,
  - requests from outside the European Union,
  - repetitive requests,
  - incomplete or partial data,
  - request not related to privacy protection.

This particular entity chooses to grant access to only some of the data it processes, unless specifically required to provide more. This stems from the vast amount of data it processes

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

N/A

## Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

- a. Very High
- b. High Yes
- c. Average
- d. Low

- e. Very low
- f. Too diverse levels to qualify

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

N/A

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, “size” of the controller, etc.):

We noticed that in the public sector, the level of awareness and understanding of the controllers was rather low (regarding the 2 controllers investigated by the CNIL). The level of awareness and understanding of the large companies was rather high.

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

- The content of access request (lack of information regarding the processing, misuse of limits to access request...)

- Obligation stemming from the French law to deliver a receipt when the individual makes a right of access in person.

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees’ right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF? If yes, please provide the date, link to the guidance, and a short description of the guidance.

No, the CNIL did not publish any guidelines regarding the right of access. However, the CNIL has published factsheets and Q&As on its website (<https://www.cnil.fr/fr/mots-cles/droit-dacces>) for the data subject and controllers.

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

- Informal contact
- Investigations
- Enforcement actions (order to comply, administrative fine)

34) **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).

Since the investigations are still ongoing, we cannot confirm the actions that will be undertaken based on the result of this CEF but Closing letters, corrective measures (reprimands) and recommendations to the controller are considered.

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Very often

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Never

37) 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 content of EDPB Guidelines 01/2022 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: At the stage, we can't confirm any action at the level of the SA.

b. No:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes:

b. No: Yes

# HU SA

## Hungarian 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.
- Fact finding:
  - Fact finding + determining follow-up action based on the results: **Yes**
  - New formal investigation<sup>22</sup>:
  - Ongoing investigation:

- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),

- Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? **Yes**
- Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access 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. Also, the Hungarian SA plans to carry out some corrective measures regarding one or two respondents.**
- If not, will this fact finding activity impact your enforcement activities and if yes, how?  
**Yes, it will, the Hungarian SA can refer to the findings of the CEF report in its procedures and use them to support its decisions too.**

- 3) For all SAs: 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) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.

**The Hungarian SA used the consolidated questionnaire and only amended the question 1.3.3. The Hungarian SA added a further activity: property protection services.**

- 5) For all SAs: 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 etc.)?

**The Hungarian SA targeted 3 sectors and received quite sector-specific responses. The three sectors were: property protection services, public utility/infrastructure provider (e.g. energy) and telecommunications.**

**The previous national legislation did not allow access to camera footage, only in administrative or judicial proceedings, so the examination of companies providing property protection services was important for the Hungarian SA in this year's CEF action.**

---

<sup>22</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

Please note that the responses processed were given in April 2024.

## Part I – Some numbers on the controllers addressed

6) How many controllers did you contact?

14 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/to your questions.

12 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?

One data controller was contacted twice by the Hungarian SA but the controller did not respond at all, although this controller is under inquiry procedure by the Hungarian SA. During the inquiry procedure the controller was cooperative so far. This inquiry procedure was opened in April, prior to sending out the questionnaires.

Another controller claimed that due to the fact that it merged into another company, the legal successor will be in charge of responding to the Hungarian SA. Fortunately, the legal successor has been previously contacted by the Hungarian SA.

One controller claimed that it is rather a data processor than a data controller.

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: Please select one or more answers.

- a. Public sector: 3 responding controllers
- b. Private sector: 9 responding controllers

10) Please specify the category<sup>23</sup> of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers

- a. Micro enterprise: 1 responding controller
- b. Small enterprise: 3 responding controllers
- c. Medium-sized enterprise:
- d. Large enterprise (more than 250 employees): 8 responding controllers
- e. Non-profit organisation: 1 responding controller, which is also a large enterprise
- f. Ministry:
- g. Local authority:
- h. Administrative authority/agency/office (e.g. job center):
- i. School / university / educational institution:
- j. Other (please specify):

---

<sup>23</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

11) Please specify the nature of the (business) activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- 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: 3
- 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. other (please specify): 6 – from which 5 are engaged with property protection services and one has marked other additional business services, as their company - typically for public utility companies - provides meter reading, billing, metering, billing, tariff collection and customer service on the basis of contracts.

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. customers: 11
- b. potential customers: 5
- c. employees: 11
- d. job applicants: 6
- e. children:
- f. vulnerable adults:
- g. patients:
- h. citizens (for public sector):
- i. applicants (for public services):
- j. recipients (for postal services):
- k. other (please specify): 1: notifiable persons provided by customers, 2. information on the clients or customers of the principals as data processor

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. Please indicate the number of (responding)

controllers to whom the respective option is applicable: Please select one or more answers.

- a. Less than 100:
- b. 100 - 200:
- c. 201 - 500: 2
- d. 501 - 2,000: 1
- e. 2,001 - 10,000: 2
- f. 10,001 - 50,000:
- g. 50,001 - 100,000:
- h. 100,001 - 1,000,000: 3
- i. 1,000,001 - 10,000,000: 4
- j. More than 10,000,000:

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.

- a. Contact data: 11
- b. Payment data: 10
- c. Identification data: 11
- d. Sensitive data within the meaning of Art. 9 GDPR: 1: trade union membership, loss of working capacity 2: data of consumers with disabilities to be protected
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR: 1
- f. Other (please specify): 1: data processed in a data-processing capacity in connection with property protection services 2. one data controller manages the data in accordance with Chapter XVII of Act C of 2003 on Electronic Communications and the categories of personal data relating to the employment 3: personal data necessary for the provision of energy services, personal data relating to the employment of employees 4: mandatory data generated in connection with the provision of communications services pursuant to the Communications Act and its implementing regulations, in particular traffic data

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. 0 request: 6
- b. 1-10 requests: 1
- c. 11-25 requests: 2
- d. 26-50 requests: 1
- e. 51-100 requests:
- f. 101-150 requests:
- g. 151-200 requests:
- h. 201-500 requests:
- i. 501-10,000 requests: 1
- j. >10,000 requests: 1
- k. No information:

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g.



number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

It is important to note that half of the respondents (6 respondents) did not receive an access request at all in 2023. The data controllers that did not receive access requests were mostly companies providing property protection, small enterprises. The two others are from different sectors, but are considered large enterprises.

The most access requests were received by a public utility provider. The other four were from the telecommunications sector and one from the sector of the public utility providers.

As the response was voluntary, in several cases the answers were not sufficiently detailed. Three data controllers' responses were not detailed and complete, these three provide property protection services.

Two controllers claimed that they do not keep separate records of access requests. This is the explanation why one of them had no information of the number of the requests, but claimed that it had received some. The Authority has contacted this controller to clarify its response. The controller replied that they had received 2 access requests in 2023, both via e-mail, attaching a copy of the requests and their reply. The other controller did not keep any records but also did not receive an access request.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 6
- b. >0–25%: 3
- c. 26–50% requests: 2
- d. 51–75% requests:
- e. 76–100% requests:
- f. No information: 1

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 6
- b. >0–25%: 3
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests: 3
- f. No information:

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 7
- b. >0–25%: 4
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests: 1
- f. No information:

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 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. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.
- d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
- e. What are differences that you have encountered between controllers in your Member State?
- f. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

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

## Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

21) 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 3.4 in the questionnaire addressed to controllers.

- a) Question 3.4: Confirming receipt of requests (an issue concerning four respondents)
  - confirmation is given verbally in the case of personal customer service or employee requests; no separate confirmation is sent for other channels in principle
  - automatic confirmation for requests sent to an e-mail address only
  - there is a confirmation but it does not contain information on the deadline for response, as it is not inconsistent due to different types of cases.
  - if the data subject requests, the controller sends a confirmation to the data subject
- b) Art. 12. (3) GDPR
- c) Point 57. of EDPB Guidelines 01/2022 on the right of access
- d) The potential explanation could be that the practice has not been fully developed by some controllers.
- e) The practices mentioned above were mainly from the public utility provider sector.
- f) To raise awareness to the fact that the EDPB considers as good practice for the controllers to confirm receipt of requests in writing, for example by sending e-mails (or information by post, if applicable) to the requesting persons confirming that their requests have been received and that the one-month period runs from day X to day Y.

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

Concerning Points 3.1 and 3.3 of the questionnaire it is best practice that some of the controllers have created a response template for personal data processing request, and a process description, furthermore their colleagues receive regular information and training, including on the enforcement of data subjects' rights, to ensure that requests for access from data subjects are correctly identified and handled. (These concerns four respondents.)

Concerning Point 3.2 of the questionnaire one respondent plans to introduce software applications for data protection, and is currently assessing the options.

## Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

23) 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 4.15 in the questionnaire addressed to controllers.

- a) Questions 4.8 and 4.11: one respondent claimed that it also identifies persons by requesting a copy of identity documents
- b) Art. 87. GDPR, Art. 5. (1) b) and c)
- c) Points 61., 63., 64., 65., 76., 77., 78., 79. of [EDPB Guidelines 01/2022](#) on the right of access.
- d) The potential explanation could be that the respondent is not fully aware of the [EDPB Guidelines 01/2022](#) on the right of access and the provisions of the GDPR.
- e) Only one data controller claimed that it had such a practice.
- f) A possible solution to this issue is a follow-up action (launching a procedure against the data controller) by the Hungarian SA.

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

Concerning Point 4.5 of the questionnaire one data controller stated that due to its practice, large amounts of data (e.g. a lot of paper, giga files) or responses containing sensitive or special category data should preferably be given to the data subject in person.

Concerning Point 4.9 of the questionnaire one respondent marked that in a reply, the third party is invited to provide evidence of procedural eligibility, while informing the data subject.

### **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

25) 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 5.18](#) in the questionnaire addressed to controllers.

- a) Question 5.18: According to Point 111. of [EDPB Guidelines 01/2022](#) on the right of access the controller should not inform the data subject only about the mere changes in the personal data processed or the processing itself since the last request, unless the data subject expressly agrees to this. Three of the respondents claimed that they only give information about the mere changes in the personal data processed.
- b) Recital 63 GDPR
- c) Point 111. of [EDPB Guidelines 01/2022](#) on the right of access
- d) The potential explanation could be that some of the controllers try to simplify the procedure or are not aware of the expectation of the EDPB.
- e) This issue is not limited to a single sector and involves data controllers of different sizes.
- f) The EDPB CEF 2024 report may draw attention to certain points in the [EDPB Guidelines 01/2022](#) on the right of access.

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

### **Section on “LIMITATIONS OF ACCESS REQUESTS”**

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

- a) Question 6.7: One respondent stated that since the burden of proving that a request is unfounded or excessive lies with the controller, they will respond to the data subject's requests even if they feel that they are unfounded or excessive. The Hungarian SA found that none of the respondents has ever had an excessive or unfounded request.
- b) Art. 12 (5) GDPR
- c) Point 175., 177., 181., 185., 190. of EDPB Guidelines 01/2022 on the right of access
- d) The potential explanation could be Art. 12 (5) GDPR
- e) There are no differences between the controllers regarding this issue.
- f) No solution is needed concerning this issue.

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

### Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, "size" of the controller, etc.):

Two data controllers stated that they were not aware or not fully aware of the EDPB Guidelines 01/2022 on the right of access. Three controllers plan to review their procedures on the right of access. The other nine have already done so.

One data controller noted that the EDPB Guidelines 01/2022 on the right of access are only available in English. The Hungarian SA would like to point out that the Guidelines are available on the website of the Hungarian SA. <https://naih.hu/europai-adatvedelmi-testulet-edpb/edpb-iranymutatasai>

Where there has been no precedent or practice, it can be observed that, for understandable reasons, the regulations have not been detailed or developed, therefore there are only general rules.

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

The topics concerning the right of access or the parts of the EDPB Guidelines 01/2022 on the right of access which are the least-known or the least implemented by controllers are set out in the points above. (see: main issue(s) or challenge(s))

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees' right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF? If yes, please provide the date, link to the guidance, and a short description of the guidance.

At the annual conference of data protection officers in December 2023 the main guidelines of the EDPB were presented, of which Dr Júlia Sziklay PhD, International Vice President focused on the main content of the Guidelines 01/2022 on the right of access, and then summarized the most important data protection decisions of the Court of Justice of the European Union, highlighting the decision C-307/22 on the disclosure of copies of medical records. The tutorial videos have been published on the Hungarian SA's website as part of the DPO conference, and are accessible to anyone.

Prior to the publication of the Guidelines 01/2022 on the right of access, in 2020 the Hungarian SA has issued a STAR II Guidance for SAs on setting up hotlines for SMEs, in which the right of access is also mentioned (page 62.):

<https://naih.hu/star-ii/starii-eredmenyek/kkv-kezikonyv-es-dpa-guidance>

[https://naih.hu/files/STAR%20II\\_Guidance%20for%20Data%20Protection%20Authorities%20on%20setting%20up%20hotlines%20for%20SMEs.pdf](https://naih.hu/files/STAR%20II_Guidance%20for%20Data%20Protection%20Authorities%20on%20setting%20up%20hotlines%20for%20SMEs.pdf)

The Hungarian SA publishes its decisions on its website at the following link:

<https://naih.hu/hatarozatok-vegzesek>

There can be found decisions published in individual cases for example regarding the right of access for separated parents, the right of access to lawyers' privilege and the exercise of the right of access to data obtained in the course of proceedings by a forensic expert.

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

The Hungarian SA publishes its decisions on its website, also the annual reports of the Hungarian SA can be found online (<https://naih.hu/about-the-authority/annual-reports>).

The Hungarian SA has carried out numerous consultations, one of them is an impact assessment preliminary consultation procedure for applying body cameras in the course of loading luggage at an airport. The Hungarian SA launched a preliminary consultation procedure in accordance with Article 36 of the GDPR concerning the risk assessment of the proposed processing (Annual report 2023, II.5.2.).

The Hungarian SA has opened inquiry procedures against four companies providing property protection services prior to sending out the questionnaires of the CEF 2024, in April 2024. Three of these five companies were also asked to complete the questionnaire, but out of these three data controllers, one did not send its response to the Hungarian SA. The reasons for initiating proceedings were typically: did not have a DPO, cookie management not appropriate, gaps in the/or lack of Privacy Notice. It can be concluded that no access request has been received by these companies. The procedures are still in progress. In summary, the Hungarian SA concludes that the level of compliance of the controllers mentioned above concerning the GDPR provisions is very low.

34) **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 Hungarian SA intends to take corrective measures against a number of data controllers [for example see Question 23)], where significant deficiencies are found. In its measures the Hungarian SA will draw the controller's attention to the provisions of the EDPB Guidelines 01/2022, and it will call the controller to change its practices.

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Very often. The Hungarian SA relies on and refers very often to the EDPB Guidelines in general in its decisions, and sometimes it may occur that the EDPB Guidelines on the right of access appears in the Hungarian SA's outgoing decisions.

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Very often. The EDPB Guidelines on the right of access are very often cited (where relevant) by the Hungarian SA in decisions related to the exercise of other data protection rights than the right of access after the publication of the EDPB Guidelines on the right of access in Hungarian.



37) 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 content of EDPB Guidelines 01/2022 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: [The main findings of the CEF will be published by the Hungarian SA on its website in Hungarian.](#)
- ii. Online or remote training sessions:
- iii. Conferences organised: [The Hungarian SA organizes a DPO conference every December, this year it will discuss this issue too.](#)
- iv. Others: please specify:

b. No:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes: [Yes. The publication of a sum-up poster, which is editable \(in order to translate it into other languages\) and based on the EDPB Guidelines 01/2022 and addressed to SMEs and individuals, would be ideal. Also, an editable flyer for the individuals would be preferable.](#)

b. No:



# HR SA

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<sup>24</sup>:
- d. Ongoing investigation:

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

- Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? **Yes**
- Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. **No**
- If not, will this fact finding activity impact your enforcement activities and if yes, how? **Yes it will.** After this fact finding activity we have detected shortcomings related to internal procedures regulating access rights and in the future we will put more focus on this.

3) For all SAs: 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**

4) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.

**We have included all questions of the consolidated questionnaire.**

5) For all SAs: 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 etc.)?

**No**

## Part I – Some numbers on the controllers addressed

6) How many controllers did you contact?

**40 (19 banks, 15 insurance companies, 6 hotels)**

---

<sup>24</sup> 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/to your questions.

40

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

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: Please select one or more answers.*

c. Private sector: 19 banks, 15 insurance companies, 6 hotels

10) Please specify the category<sup>25</sup> of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers*

a. Micro enterprise: 0

b. Small enterprise: 3

c. Medium-sized enterprise: 8

d. Large enterprise (more than 250 employees): 29

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

11) Please specify the nature of the (business) activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

a. education sector: 0

b. health sector: 0

c. social sector: 0

d. insurance sector: 15

e. finance sector: 19

f. IT sector: 0

g. retail sector: 0

h. logistics sector: 0

i. public transportation: 0

j. telecommunications: 0

k. postal services: 0

l. advertising sector: 0

---

<sup>25</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- m. marketing services: 0
- n. entertainment sector: 0
- 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. other (please specify): hospitality sector (hotels), 6

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. customers: 38
- b. potential customers: 20
- c. employees: 40
- d. job applicants: 31
- e. children: 9
- f. vulnerable adults: 3
- g. patients: 0
- h. citizens (for public sector): 0
- i. applicants (for public services): 0
- j. recipients (for postal services): 0
- k. other (please specify): Guests of hotels (6 data controllers)

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. Less than 100: 0
- b. 100 - 200: 2
- c. 201 - 500: 1
- d. 501 - 2,000: 3
- e. 2,001 - 10,000: 4
- f. 10,001 - 50,000: 12
- g. 50,001 - 100,000: 5
- h. 100,001 - 1,000,000: 12
- i. 1,000,001 - 10,000,000: 1
- j. More than 10,000,000: 0

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? *Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.*

- a. Contact data: 40
- b. Payment data: 39
- c. Identification data: 40
- d. Sensitive data within the meaning of Art. 9 GDPR: 19
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR: 12

I. Other (please specify): [sociodemographic data \(2 controllers\)](#)

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. 0 request: [15](#)
- b. 1-10 requests: [13](#)
- c. 11-25 requests: [4](#)
- d. 26-50 requests: [2](#)
- e. 51-100 requests: [0](#)
- f. 101-150 requests: [0](#)
- g. 151-200 requests: [0](#)
- h. 201-500 requests: [2](#)
- i. 501-10,000 requests: [2](#)
- j. >10,000 requests: [2](#)
- k. No information: [0](#)

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

[It is notable that hotels with a large number of data subjects \(over one million in 2023\) received a surprisingly low number of access requests. Out of six hotels, three did not receive a single access request, while the others reported receiving up to five requests. Another surprising observation is that the largest insurance company, with approximately 1.5 million users, received only 10 access requests. Moreover, 7 out of 14 insurance companies received no access requests at all in 2023.](#)

[This is not in line with AZOP expectations because we often receive questions from citizens about processing of personal data by hotels and insurance companies.](#)

[Overall, the number of access requests received by data controllers in the insurance and hotel sectors is unexpectedly low, given the large number of data subjects. In contrast, the volume of access requests in some banks aligns more closely with expectations. One insurance company reported receiving 30,000 access requests, but from their explanation, it’s clear they misunderstood the nature of an access request, categorizing every client inquiry—such as ‘How many installments do I have left on my insurance premium?’—as an access request. Other insurance companies received between 1 and 15 requests, with one exception where 27 access requests were reported.](#)

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: [15](#)
- b. >0–25%: [2](#)
- c. 26–50% requests: [14](#)
- d. 51–75% requests: [6](#)
- e. 76–100% requests: [3](#)

- f. No information: 0

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

It is surprising that 15 out of 40 data controllers did not receive a single access request, especially considering they process personal data of a large number of data subjects. The high proportion of access requests compared to other types of requests aligns with AZOP expectations. Notably, three data controllers—two hotels and one insurance company—reported that they have never received an access request. Additionally, insurance companies with large number of data subjects received very few access requests overall.

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 0
- b. >0–25%: 2
- c. 26–50% requests: 3
- d. 51–75% requests: 2
- e. 76–100% requests: 18
- f. No information: 0

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No. In all sectors data subjects requested mainly insight into their data and copy of their data.

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 15
- b. >0–25%: 20
- c. 26–50% requests: 4
- d. 51–75% requests: 0
- e. 76–100% requests: 1
- f. No information: 0

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No. What did not meet our expectations was the surprisingly low number of data subjects requesting information about the underlying processing activities. However, the Agency frequently receives similar inquiries, such as, 'Why is the bank making a copy of my ID?' This

suggests that many citizens may not be sufficiently aware that they should be directing these questions to data controllers.

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 in the questionnaire for controllers:

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

1. Many data controllers lack documented internal procedures for handling access requests. Out of 40 data controllers, only 6 provided internal documentation related to managing access requests.

2. Some of these internal procedures are not sufficiently detailed, consisting mostly of "copy-paste" excerpts from relevant GDPR Articles and EDPB guidelines, without offering practical instructions for employees on how to properly handle access requests. This suggests a focus on "paper compliance" rather than providing real operational guidance.

3. The internal documents lack specific deadlines or timeframes for how long data related to access requests should be retained.

4. Some data controllers do not fully understand what constitutes an access request, treating any inquiry from a data subject about their products or services as an access request. Some answers may indicate that data controllers might not comply with the access requests because they don't consider it as an access request.

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

Article 15 (1) (3) and Article 5. 1(c)

o. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.

C-312/23 Addiko Bank v Agencija za zaštitu osobnih podataka

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

Data controllers receive very small number of access requests so they don't consider relevant to have internal procedures and to give detailed instruction to employees on how to handle access requests.

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

Banks with higher incomes and a large number of data subjects, which receive the most access requests, have detailed procedures in place and utilize software or online applications to efficiently manage these requests.

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

There should be increased enforcement activities by AZOP, along with greater awareness campaigns aimed at citizens. Data controllers currently receive very few access requests, leading them to view this area as less relevant. Additionally, citizens are not adequately informed about their rights. As citizens begin to exercise their access rights and AZOP starts inquiring about internal procedures, data controllers will be prompted to develop more detailed and practical procedures. These will include all necessary information for employees handling access requests.

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

One bank provided a detailed description of the software/online application they use to facilitate the exercise of data subjects' rights. They also shared comprehensive instructions for their employees on how to navigate the system. The platform appears to be highly user-friendly, making it easier for data subjects to exercise their right of access, as well as for employees who are handling requests.

### **Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”**

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

21) 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 3.4 in the questionnaire addressed to controllers.

There were no specific issues or challenges identified. However, one data controller responded NO to all questions and we are planning enforcement actions in this case. The other data controllers provided standard descriptions of procedures for handling requests.

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

Several data controllers highlighted that access requests can be difficult to identify, as they are often submitted through channels not designated for that purpose (e.g., sent to the contact center instead of the DPO). To address this, all employees are trained to recognize such requests and promptly forward them to the data protection officer.

### **Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”**

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

23) 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 4.15 in the questionnaire addressed to controllers.

There are significant challenges with the authentication and identification of data subjects. Most data controllers did not provide detailed descriptions of how they verify the identity of individuals requesting access rights. Some are collecting copies of IDs, which may result in the excessive collection of personal data.

Most of them don't have procedures in case when third person acts on behalf of a data subject.

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

Most data controllers have established a special protocol has been for verifying the identity of data subjects.



It is necessary to confirm at least three identifiers, such as personal data recorded in the data controller's business system, email address, contract number, or other processing-related information. They don't collect unnecessary additional personal data (i.e. copies of IDs).

#### Description of procedure-bank1

When a data subject submits a request via email, the request must be sent from an address that is recorded in the Bank's system. A Bank employee checks whether the request was received from an email address that is registered in the Bank's system.

If the request is sent by post, the Bank employee verifies the information provided in the request (by checking the personal identification number (OIB), correspondence address, and other available data in the received request). Postal responses to the data subjects are always sent by registered mail.

Online banking users can submit a request through that channel by using the mToken.

In relation to requests from employees as data subjects, the employee is considered identified if the request is sent from their official Bank email address. For job candidates and former employees, the match between the email address from which the request was sent and the email address listed in the résumé and/or the data the Bank has stored in its system is verified.

Additionally, it is prescribed that when a request is received electronically, identification is also carried out by verifying at least two or more different pieces of personal data or data segments and their combinations. This is done by sending a corresponding query to the data subject at the email address from which the request was sent, asking them to return the correct data or combination of data. This applies in situations where we cannot establish a match between email addresses.

#### Description of procedure-bank2

For individual clients who submit a request for access to personal data, the requests are received through a special interface of the EMA application, where the subject's identifier, name, surname, and country are entered, along with one contact detail—either an email address or a phone number. The data subject may choose not to provide a contact detail, and their choice will determine how they are notified about the completion of the request, as further explained below. After entering this information, the category of the data subject and the type of request being submitted are selected. Once the request type is marked as requested, a request form is generated, which the client then signs.

The generated form for the specific submitted request also includes an individually created link to a special/non-public webpage of the Bank. Data subjects who provided an email address or mobile number when submitting the request will receive a notification of the completion of the request processing at that contact, along with a password to retrieve the response to their request. Upon receiving the notification and password, the data subject enters the received password into the individually created link and downloads the response to their request.

Data subjects who did not provide a contact detail must visit a branch, where bankers will print the response to their request. These data subjects are guaranteed access to retrieve the response to their request for an additional three months from the notification of the request's completion.

Requests are received through branches and e-branches, and the 'response' to the request is also largely supported by the application. The created IT procedure processes through the applications, retrieves the data subject's information, and prints it in the response.



## Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

25) 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 5.18 in the questionnaire addressed to controllers.

No issues or challenges identified.

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

-

## Section on “LIMITATIONS OF ACCESS REQUESTS”

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

No issues or challenges.

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

-

## Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

- g. Very High
- h. High
- i. Average Yes
- j. Low
- k. Very low
- l. Too diverse levels to qualify

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

Large banks receive the highest number of access requests, and most have detailed procedures in place to manage them. In contrast, five smaller banks reported no access requests at all, while larger banks, categorized as big enterprises, received between 802 and 3,010 requests. Notably, Addiko Bank reported the most access requests; however, in 2019, it refused to comply with a data subject's request, leading to a fine issued by the Croatian Supervisory Authority (C-312/23 Addiko Bank v Agencija za zaštitu osobnih podataka).

Insurance companies receive very few access requests, ranging from 0 to 27, while hotels report even lower numbers, from 0 to 3. It is particularly surprising that a small number of these

requests relate to requests about information specified in Article 15(1). Most requests consist solely of demands for copies of personal data/insight into personal data. This finding was unexpected, as the Croatian Data Authority frequently receives inquiries from citizens regarding the processing of personal data by banks and hotels—typically questions like "Why are they making a copy of my ID?" and inquiries related to in-depth analyses of bank clients.

The expectations were that data controllers in this three industries receives the largest number of access requests.

This suggests that while data subjects have questions about their personal data processing, they may not be sufficiently aware that they should direct these questions to data controllers. As a result, data controllers may not prioritize establishing robust procedures for handling access requests. This situation serves as a clear indicator for the Croatian Data Protection Agency (AZOP) to enhance public awareness of these rights.

When citizens begin to ask questions, data controllers are likely to view this issue as more relevant and take necessary action.

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

- g. Very High
- h. High
- i. Average **Yes**
- j. Low
- k. Very low
- l. Too diverse levels to qualify

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, "size" of the controller, etc.): [In 3.1.](#)

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

[2.3.1 Completeness of the information](#)

[3.3 Proportionality assessment regarding authentication of the requesting person](#)

[3.4 Requests made via third parties / proxies](#)

[4 SCOPE OF THE RIGHT OF ACCESS AND THE PERSONAL DATA AND INFORMATION TO WHICH IT REFERS](#)

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees' right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF?

If yes, please provide the date, link to the guidance, and a short description of the guidance.

NO, we didn't consider it necessary since the EDPB guidelines on this topic are very comprehensive. According to our opinion, the EDPB guidelines provide all the necessary information to data controllers, but data controllers simply don't read and implement in practice. Croatian SA will organize educational activities aimed at specifically to promoting EDPB guidelines on right to access.

**33) Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

Yes, as mentioned above, the most relevant case is C-312/23 Addiko Bank v Agencija za zaštitu osobnih podataka.

Between May 2018 and April 2019, several customers of a bank ('controller') asked it to provide them with a copy of documents containing their personal data, including loan contracts they had concluded, repayment plans, documents relating to changes in interest rates and account statements. Some of these requests were explicitly motivated by the data subjects' desire to bring a claim or legal action against the controller.

The controller refused to give access to these documents. The data subjects lodged complaints with the Croatian SA claiming that this rejection constituted a violation of Article 15(3) GDPR. As the controller did not comply with the injunctions issued by the SA in 26 specific cases, the SA ordered it to pay a HRK 1,100,000 (€146,667) fine.

The controller considered that Article 15(3) GDPR confers only a right to a copy of the personal data being processed, to the exclusion of the documents containing them. Therefore, the controller brought an action before the Administrative Court of Zagreb against the administrative fine imposed by the SA.

During this period, three other banks also refused to comply with data subjects' access requests. In response, the Agency ordered these data controllers to comply, and they adhered to our order.

**34) 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).

1. Recommendations to data controllers

2. Informal investigation for two insurance companies

**35) In general** (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Very often

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Very often

37) 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 content of EDPB Guidelines 01/2022 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:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes

b. No: **Yes**

# IE SA

Data Protection Commission

## 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<sup>26</sup>:
- d. Ongoing investigation:

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

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

**No**

3) For all SAs: 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.

**All questionnaires issued to controllers were the same version.**

4) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.

**N/A**

5) For all SAs: 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 etc.)?

**The questionnaire was issued via the EU Survey Portal. To gain as broad a view as possible, we selected controllers from various sectors and industries which may have dealt with large volumes of subject access requests in 2023.**

## Part I – Some numbers on the controllers addressed

6) How many controllers did you contact?

**30**

---

<sup>26</sup> 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/to 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?

We did not identify the main reason. As it was a fact-finding exercise, we did not make it mandatory to respond.

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: Please select one or more answers.*

- a. Public sector: 9
- b. Private sector: 11

10) Please specify the category<sup>27</sup> of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers*

- a. Micro enterprise:
- b. Small enterprise:
- c. Medium-sized enterprise: 2
- d. Large enterprise (more than 250 employees): 7
- e. Non-profit organisation:
- f. Ministry: 4
- g. Local authority: 2
- h. Administrative authority/agency/office (e.g. job center):
- i. School / university / educational institution: 4
- j. Other (please specify): 1 Public Body Transport

11) Please specify the nature of the (business) activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. education sector: 4
- b. health sector:
- c. social sector:
- d. insurance sector: 2
- e. finance sector:
- f. IT sector:
- g. retail sector:
- h. logistics sector:
- i. public transportation: 1
- j. telecommunications: 2
- k. postal services:
- l. advertising sector:

---

<sup>27</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- 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): 2
- s. housing industry:
- t. manufacturing:
- u. other (please specify):
- 4 Government Departments
- 2 Local Authorities
- 1 Agribusiness Sector

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. customers: 16
- b. potential customers: 13
- c. employees: 20
- d. job applicants: 20
- e. children: 2
- f. vulnerable adults: 5
- g. patients:
- h. citizens (for public sector): 5
- i. applicants (for public services): 5
- j. recipients (for postal services): 1
- k. other (please specify):
- Primary Students
- Post Primary Students
- Adult Student
- Learners
- Special needs students
- Parents
- Third Party Companies
- Suppliers
- Shareholders

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. Less than 100:
- b. 100 - 200:
- c. 201 - 500:
- d. 501 - 2,000:
- e. 2,001 - 10,000:
- f. 10,001 - 50,000: 3

- g. 50,001 - 100,000: 3
- h. 100,001 - 1,000,000: 7
- i. 1,000,001 - 10,000,000: 7
- j. More than 10,000,000:

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? *Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.*

- a. Contact data: 20
- b. Payment data: 18
- c. Identification data: 19
- d. Sensitive data within the meaning of Art. 9 GDPR: 11
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR: 3
- f. Other (please specify):  
  - Demographic data
  - Financial Data
  - HR data,
  - Research-related data,
  - Alumni-related data
  - Claims related information
  - Examination scripts
  - Network Traffic Data,
  - Device Data,
  - Energy Consumption Data

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. 0 request:
- b. 1-10 requests: 4
- c. 11-25 requests: 2
- d. 26-50 requests: 5
- e. 51-100 requests: 1
- f. 101-150 requests: 2
- g. 151-200 requests: 1
- h. 201-500 requests: 3
- i. 501-10,000 requests: 2
- j. >10,000 requests:
- k. No information:

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

The banking, insurance, and telecommunications sectors generally received the highest number of Subject Access Requests. This is unsurprising, considering they have the most extensive customer base and, accordingly, customer data that these controllers process. We



also noticed that some Government Departments or local councils had received quite a low number of Subject Access Requests, considering the amount of individual data they process.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests:
- b. >0–25%: 2
- c. 26–50% requests: 1
- d. 51–75% requests: 7
- e. 76–100% requests: 10
- f. No information:

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

The responses clearly show that the majority stated that Subject Access Requests account for the majority of data protection requests they received in 2023, mostly 90% of requests and upwards. Only three respondents stated that they accounted for less than 50% of their data protection requests.

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests:
- b. >0–25%:
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests: 100
- f. No information:

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

We noticed no significant differences in responding controllers.

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 13
- b. >0–25%: 4
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests:
- f. No information: 4

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

We noticed no significant difference in replies to this question. The majority received no requests for the underlying purposes of processing. Only four respondents stated that very rarely, or less than 10% of requests were for information on the underlying processing activities.

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 in the questionnaire for controllers:

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

Overall, this section was answered very well, noting there is no specific requirement obliging data controllers to adopt a specific procedure for handling access requests, provided that they can comply with the time limits and produce a response compliant with the other requirements necessitated by data protection law. Generally, the controllers who responded demonstrated commendable compliance, with very few instances of non-compliance reported.

We identified one controller who did not have a defined retention policy and kept access requests indefinitely. However, it was stated they were reviewing their SAR processes, and the retention policy was to be a part of this review.

The DPC's position on retention is that if the purpose for which the information was obtained has ceased and personal information is no longer required, the data must be deleted or disposed of in a secure manner. However, the General Data Protection Regulation (GDPR) does not stipulate specific retention periods for different types of data, and so organisations must have regard to any statutory obligations imposed on them as data controllers when determining appropriate retention periods. The retention period could be legitimately longer if the request is in the context of preparing a legal claim.

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

Article 5 (2) GDPR

Article 24 GDPR

Statute of Limitations Act 1957

Central Bank of Ireland Consumer Protection Code Rule 11.5

National Archives Act 1986

i. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.

N/A

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

N/A

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

N/A

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

The DPC will contact the respondent to offer guidance on this issue or any other issues noted throughout our findings. This will not be an enforcement exercise but will be conducted on an informal basis under our tasks under Article 57 GDPR.

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

We noticed several good practices, including automated workflow systems, that have proven to be valuable assets. These systems, with their ability to record the date of receipt of a SAR and highlight cases in order of their due date, significantly enhance the efficiency of the process.

In addition, the specific data protection SAR team's human oversight ensures that cases progress to the next stage of the SAR completion, thereby, further reinforcing the efficiency of the process.

Similarly, we noticed a good use of a ticketing system assigned to each request, which is tracked from beginning to end, ensuring a thorough and reliable process.

In relation to internal access to requests, we noted good examples of corporate policies of strictly limited access to SARs to Units on a need-to-know basis to folders containing SARs. This also included more enhanced restrictions in place for employee SARs due to their increased sensitivity and strict access to SAR logs for the relevant Units.

We also noted a good practice of separate complaints and escalations trackers. This feature helped one controller in identifying any increases in areas of complaints associated with the data provided, ensuring they could investigate and improve on any such areas.

### **Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

21) 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 3.4 in the questionnaire addressed to controllers.

As in Section Two, we found that the respondents answered this section's questions quite well overall. Again, we note there is no specific requirement obliging data controllers to adopt a particular procedure or pre-defined process for handling access requests, provided that they can comply with the time limits and produce a response compliant with the other requirements necessitated by data protection law. The process will also largely depend on the nature and

size of the organisation, the complexity of the data processed, and the amount of SARs received.

One notable issue we observed is that some controllers do not acknowledge SARs when they are received through channels other than the Compliance Department or Access Request Unit. This lack of acknowledgement, coupled with the immediate forwarding of the request to the Data Protection Office Unit, could lead to potential delays or even the risk of missing an acknowledgement when the request is passed to other Units. This is a concern, as the DPC often receives complaints when no acknowledgement of the SAR is issued to the data subject.

Another observation we made was that some controllers rely solely on a fully automated process to handle data access requests, without any human oversight. While the use of specialist software, as mentioned in Question 2, is indeed beneficial, it should always be complemented by human review. This human review is not just a good practice, but a necessary one to ensure data protection compliance.

Which provision(s) of the GDPR (or national laws) does this concern?: N/A

If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access:  
EDPB Guidelines para. 57

Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?: No

What are the differences that you have encountered between controllers in your Member State?: None

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

As in the EDPB Guidelines 01/2022, the DPC considers good practice by confirming with the requestor that their requests have been received and that the one-month period runs from day X to day Y. The official acknowledgement may come from the administration department, responsible for acknowledging receipts of such requests, but the DPC recommends good practice that whoever receives the initial request, for example, a customer service department, notify the requestor of this in case there is a delay. The DPC will contact the relevant respondents to offer guidance on this. This will not be an enforcement exercise but will be conducted on an informal basis under our tasks under Article 57 GDPR

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

While the majority of the respondents have dedicated email channels for SARs, it's crucial to note that requests can be accepted through any business channel. Most controllers have this practice in place. A standout practice we observed is the Subject Access Unit, which plays a vital role in training staff across the organisation to recognise access requests, even when they come in through informal or ad-hoc channels or as part of other customer interactions.

We've observed effective processes in place, such as appointing data protection liaison officers in each department or each department within the organisation has a designated decision maker for data access requests, and these designated people have received training in handling data access requests.

Another positive observation was the use of digital tools to assist in the SAR process. New digital tools that process personal data undergo a screening process, and a DPIA is carried out in appropriate circumstances. The business owner, who has the necessary expertise, completes any DPIAs when any process changes or new products and services are developed and implemented. However, it's important to note that the DPO is actively involved in the Privacy Risk Assessment and DPIA process, providing reviews and guidance on privacy risks and issues arising, and incorporating Privacy by Design (Article 25 GDPR).

Another positive practice we noticed was that new tools used for assessments also feed into the ROPA once an assessment is completed and a process is live. This means that any new data types or data sources are added to the ROPA. The ROPA is updated whenever new measures are implemented around security, changes to storage, changes to technical measures, or if a DPIA is updated or has to take place. This ensures that the ROPA is always reflective of the current data processing activities.

We noticed good use of management workflow tools tracking the number of access requests received and any SARs that exceeded the one-month time limit and regular reporting volume of requests, numbers completed, etc.) Are reported monthly to management. This practice was standard amongst most respondents.

We noticed good use of a second-line quality audit process completed quarterly that samples and checks the compliance with the defined processes.

All respondents have shown they acknowledge receipt of SAR, and most have good practices in sending out acknowledgements of the receipt of SAR with an expected time to complete upon receipt of their request via any medium. They have also demonstrated a proactive approach to potential delays, promptly notifying the data subject as soon as they are identified. If the request requires more time, a second letter explaining the situation and providing a new completion date is sent. We saw no differentiation in the response regarding different groups of data subjects.

## **Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”**

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

23) 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 4.15 in the questionnaire addressed to controllers.

The DPC noted a controller's practice that is not in line with the EDPB guidelines and the GDPR. This controller mandates that all requests be submitted in writing with proof of ID, a practice that is not in line with the recommendations in the EDPB guidelines. These guidelines, which are in line with Art. 12(2) and Art. 25 GDPR, encourage controllers to provide the most appropriate and user-friendly communication channels to enable the data subject to make an

effective request (para. 53). The controller's indiscriminate requesting of ID for all SARs, without considering the relationship with the requestor, may constitute excessive processing of personal data and create unnecessary obstacles to the data subject's rights.

We also noted one controller refusing subject access requests in electronic form and stating that they can only collect their data on-site. This is contrary to the provisions in Article 12 (3) and (4) GDPR, Article 15 (3) GDPR, and the EDPB Guidelines that "if the data subject submits the request for access by electronic means, all information must be provided in a commonly used electronic form" (para 32).

This is creating unnecessary barriers for an individual exercising their data protection rights, such as the need to physically visit the controller's premises to access their data, which can be time-consuming and inconvenient.

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

Article 5 GDPR

Article 12 (2) (3) (4) GDPR

Article 15 (3) GDPR

If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access:

EDPB Guidelines para. 53

EDPB Guidelines para. 32

Did you identify a potential explanation why this has been an issue for some or all of the responding controllers? No

What are the differences that you have encountered between controllers in your Member State? None

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

The general rule is that a controller should respond to an individual's access request in the same way the request was made, or in the way in which the requester specifically asked for a response. Where a request is made electronically, controllers should provide the required information in a commonly used electronic format, unless the individual requests otherwise. We will be writing to the respondent who advised they stated data subjects must collect their data on-site. This will not be an enforcement exercise but will be conducted on an informal basis under our tasks under Article 57 GDPR.

Requesting ID to be included with every subject access request is not a reasonable or proportionate approach. Seeking proof of identity would be less likely to be appropriate where there was no real doubt about identity; but, where there are doubts, or the information sought is of a particularly sensitive nature, then it may be appropriate to request proof. Controllers should only request the minimum amount of further information necessary and proportionate in order to prove the requester's identity. The DPC will contact the respondent who advised they request ID with every subject access request. This will not be an enforcement exercise



but will be conducted on an informal basis under our but will be conducted on an informal basis under our tasks under Article 57 GDPR.

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

Nearly all respondents advised on an easy one or two-click process from the Data Privacy Notice or Privacy Policy to exercise their data subject rights and they accept requests through a variety of channels, including telephone, letter, email, and in-person requests/ social media platforms.

We also noticed the excellent practice of a controller who directed customers on telephone voice messaging services to data subjects to exercise their data protection rights, including a SAR.

We noticed positives such as all staff receiving data protection training that includes a piece about data subject requests and informing staff what to do with them. We noticed a positive in that if a customer makes a SAR through social media channels, they are immediately directed to the correct channel to raise the request officially, and in general, we noticed no obstacles created for data subjects in exercising their data subject rights except for one or two controllers (noted above).

One respondent, in alignment with its sustainability goals, has a policy of issuing SARs in a paperless format, in line with its commitment to reducing paper and plastic use (but will accommodate paper requests if specifically sought).

We found most controllers are cognisant of their security obligations and have good security practices. For example, files are encrypted, and the password is sent to the customer under separate cover, using multifactor authentication or secure platforms or requesting a verification ID if collected in person.

We found that most controllers were cognisant of their obligations under Article 12(1) GDPR regarding communication with the data subject and taking appropriate measures. We noticed some excellent examples of dealing with customers who may need assistance due to a vulnerability or otherwise. For example, dealing with SARs on a case-by-case basis and engaging with vulnerable customer support teams were necessary, as well as seeking the assistance of appropriate external support agencies. Other examples are providing SARs in braille or large font or audio recordings as a written transcript where audio is unsuitable for someone with hearing difficulties. We also noticed good practices in accommodating customers who are not technically proficient by providing data in print if specifically requested.

Finally, in this section, considering the volumes of SARs that respondents receive in some cases, we notice proportionately every request to extend the one-month deadline. Some reasons for extending the deadline included:

- The request is excessive
- The volume of search areas in a complex organisation can be challenging to resource.
- Some technical reasons may delay the completion of the request, or a requestor may have interacted with the organisation for many years or with a long-standing employee
- Or they may be complex legal matters.

We noticed that nearly all controllers stated they notify the data subject as soon as possible if a request an extension is required. A good practice we noticed is getting an early estimation of the data that will be needed to be collected, the complexity of the request, and the departments to be involved so that if a delay is possible, it will be noted early. We noted that regularly updating the data subject on the process of their request was also a good practice.

### **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

*The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

25) 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 5.18 in the questionnaire addressed to controllers.

We found that quite a few controllers did not understand the questions about the categories of recipients or replied that they did not provide any information about recipients in the data when responding to a SAR.

It's important to note that the ECJ decision, *W v Österreichische Post AG*, Case C 154/21C-154/21, mandates the controller to provide information about specific recipients. This is unless it's impossible to provide or the request is manifestly unfounded or excessive under Art. 12 (5) GDPR. In such cases, the controller is allowed to provide only categories of recipients. Refusing to acknowledge the request or simply referring a requestor to a privacy or data protection notice is not compliant with Articles 13,14 and 15 of the GDPR.

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

Article 5 GDPR

Article 13 (1) (e) GDPR

Article 14 (1) (e) GDPR

Article 15 (1) (c) GDPR

If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access:

EDPB Guidelines para .116-118

C -154/21 Österreichische Post

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

No

What are the differences that you have encountered between controllers in your Member State?:

The requirement appears to be better understood at a private sector level . What are the possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?



As per Case C-154/21, data subjects have the right to know who has received their personal data unless it is impossible to identify those recipients or the request is manifestly unfounded or excessive. The controller must demonstrate that it is impossible to identify the recipients or prove that the data subject's request is manifestly unfounded or excessive.

Controllers are responsible for accurately recording where their data is going and where recipients are located. A comprehensive updated Record of Processing Activities is a powerful tool in this regard, helping to fulfil this responsibility.

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

We noticed many positive examples in this section regarding the content of access requests and respective responses according to Article 15 GDPR.

In determining the scope of personal data in replying to a SAR, we noticed good practices in some respondents who follow a checklist of where personal data is held, including good use of Record of Processing Activities (ROPAs) and Privacy Impact Assessments which will identify if any new data is being processed.

It appears quite common for controllers to ask the data subject to specify the request as is recommended in Recital 63 GDPR. By way of assistance, examples are provided of the units of the organisation within which their data may be processed, and, where that is the case, detail is provided on the types of information they may hold so that the data subject can give clarity on the types of data required. In the case of 'all' data being requested, a full template listing what 'all' might entail is provided to the data subject. The aim being not to overload the data subject with information.

In providing the responses and the data in a concise, transparent, intelligible, and easily accessible form (Art 12.1 GDPR), we found good examples such as releasing the requested data and listing it on the schedule with a description of the record and the decision made in relation to each record, for example, if any third party was redacted. We also noted good examples, including a glossary of terms and any acronyms used. We found good examples in which documents are redacted or a partial request is issued respondents included an explanatory note in our covering communication explaining why this is.

No respondents mentioned they used a layered approach as outlined in EDPB guidelines EDPB para 145- 147. Indeed, one respondent stated "Requesters want copies of material, they're not interested in 'layered approaches' or 'excerpts'."

In selecting what documents to include in a SAR, we noticed that most responded that the entire document would be provided unless an exemption exists. Some exemptions quoted were:

- Legal Advice/Legal Privilege (Section 162 of the Data Protection Act 2018 - Ireland),
- Relating to potential or ongoing civil or legal cases to which the respondent will be subject (Section 60 (3(iv) of the Data Protection Act 2018 - Ireland).

- Article 15 (4) GDPR, and we noticed good examples of the use of 'balancing tests' in this regard and also

- Data Protection Act 2018 (Access Modification) (Health) Regulations 2022. Some controllers advised that if they receive a confirmed opinion that there are reasonable grounds to believe that granting access to certain health or medical information is likely to cause serious physical or mental harm, they inform the data subject of this and ask for a medical practitioner of their choosing with whom they can share the information. Data will only be shared with the medical practitioner with the data subject's consent.

Concerning non-textual data, e.g. CCTV, we found all controllers redact footage pixelating images of third parties were necessary or is sent to external companies for editing. In rare cases, for example, when an employee has consented to be included in CCTV footage, we noted good practices that the controller makes the data subject aware that on receipt of unedited footage, they become a data controller and are responsible for protecting the rights of any individuals contained in the footage.

Similar practices were noted in relation to voice recordings, which may also need to be redacted, and actual transcripts of the call are issued for ease of redaction for the controller.

We noticed that all respondents replied they did not differentiate between partial and full access requests and had no metrics on this.

With regard to repeated requests, respondents advised that they would provide information on changes that have occurred since the last provision of information and refer to the previous set of information provided. However, some controllers provide complete information unless made clear by the data subject that only the subsequent data is being requested, but this is dependent on the amount or volume of data in the original request.

Finally, we noticed good practices that respondents consider the data subject and any special characteristics they may have. Respondents advised they would endeavour to facilitate the data subject's request, such as braille/large text/oral or providing data on-site if this was necessary.

## **Section on “LIMITATIONS OF ACCESS REQUESTS”**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

In our analysis, we found that Limitations of the Right of Access were often narrowly interpreted or required a very high threshold to be met. However, we identified some reasons for refusals or restrictions or considerations of restrictions due to the request being manifestly unfounded or excessive that did not align with the GDPR or the EDPB Guidelines.

In one case, a respondent advised that they refused a SAR for CCTV footage due to the high cost of pixilation. Our analysis also showed a case where a controller, faced with a large amount of data to be retrieved, which would take an excessive amount of time and put a burden on the systems, would ask the requester to narrow the scope or be charged a reasonable fee.

These refusals or restrictions are not compatible with the EDPB guidelines (para 22) and para (175) and recent ECJ case-law Case C-307/22 (FT v DW)

"Article 12(5) and Article 15(1) and (3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) must be interpreted as meaning that the controller is under an obligation to provide the data subject, free of charge, with a first copy of his or her personal data undergoing processing, even where the reason for that request is not related to those referred to in the first sentence of recital 63 of that regulation."

Art. 12(5) GDPR enables controllers to override requests for the right of access that are manifestly unfounded or excessive. These concepts have to be interpreted narrowly, as the principles of transparency and cost-free data subjects' rights must not be undermined. A data subject should not be burdened financially to exercise their data subject rights just because a controller does not have an appropriate system in place to deal with their request.

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

Article 12 (5) GDPR

If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access:

EDPB Guidelines 01/2022. para 22

EDPB Guidelines 01/2022. para 175

Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?: No

What are the differences that you have encountered between controllers in your Member State?:

Article 12(5) GDPR appears to be better understood at a private sector level as we noted no restrictions applied due to cost or excessive amount of time and burden used as a refusal or a restriction.

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

The provisions in Article 12(5) GDPR 'manifestly unfounded' or 'excessive' can only be availed of in exceptional circumstances, where evidence demonstrates that the requests are excessive or some improper purpose is in play. There are many ways controllers can reduce

the burden of large data requests, such as narrowing the scope of the request, having a well-structured updated data map or Record of Processing Activities in place. Equally important is training staff across the organisations to assist the unit in dealing with subject access requests and using platforms to assist in managing subject access requests.

The DPC will contact the respondent with guidance in this regard. This will not be an enforcement exercise but will be conducted on an informal basis under our tasks under Article 57 GDPR.

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

We noticed good practices that, in the main, the bar for any restrictions to the right of access for manifestly unfounded or excessive requests was set very high by respondents or only applied in exceptional circumstances, and this appeared to happen on very few occasions. We found good practices that any refusals or restrictions would only be done following a detailed assessment of the request involving the advice of the data protection officer or, in some instances, with external legal counsel. Any refusal would be communicated to the data subject, outlining the reasons for the refusal and providing information on the subject's right to lodge a complaint with the supervisory authority.

We noticed that most respondents stated that nearly all replies to SARs involved some form of redaction of third-party data. The process of redaction is assessed on a case-by-case basis, ensuring a fair and balanced approach. A balancing test is used to weigh up the competing rights, including whether the data is already known to the requester, whether it is a public record, and the potential impact on the rights and freedoms of the third party.

If it is decided it could cause a detriment to the third party, respondents advised they would redact the data or, in the case of call recordings, provide a redacted transcript of the call to protect the privacy of the third party.

It's notable that most respondents relied on similar restrictions citing a relevant GDPR or Irish legal provision, which were only applied to the extent they were necessary and proportionate. The following were the GDPR and legal provisions relied upon by respondents for the restrictions of rights.

Legal Advice/Legal Privilege (Section 162 of the Data Protection Act 2018 - Ireland), Relating to potential or ongoing civil or legal cases to which the respondent will be subject (Section 60(3)(iv) of the Data Protection Act 2018 - Ireland).

Data Protection Act 2018 (Access Modification) (Health) Regulations 2022 Section 60(3) (b)  
Data Protection Act 2018' expression of opinions'

Article 4(1) GDPR

Article 15 (4) GDPR

Recital 27 GDPR

### **Part III – Impressions on the levels of awareness and compliance**

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

In general, we noticed high levels of compliance with the GDPR provisions in relation to subject access requests from all the questionnaire respondents. However, in particular, we noted that organisations in the private sector such as the banking, insurance, and telecommunications sectors which receive considerably more subject access requests compared to other sectors, have established well-structured practices and compliance teams to deal with SARs, demonstrating a high level of compliance and awareness of GDPR provisions.

This was reflected in the few requests for time extensions and reduced average response times to subject access requests in those sectors, despite the high levels of subject access requests received.

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, "size" of the controller, etc.):

Again, similar to the controller's compliance level with the GDPR provisions, we found mainly a high level of awareness and understanding of the EDPB Guidelines 01/2022 on the right of access. However, this was not across the board, and some respondents' level of awareness and understanding could have been better. Respondents who identified that they had proper data protection and governance units and teams across all organisation channels showed a better understanding of the EDPB Guidelines 01 /2022.

We noted that a number of respondents advised they changed some procedures following the introduction of the guidelines, such as enhancing cover letters for responses and providing context to the data subject to have "meaningful interaction" with the data.

We noticed some respondents' data protection units ensured that all business units in the organisation were aware of the EDPB Guidelines 01/2022 and reviewed them against their current practices. The EDPB Guidelines 01/2022 have been helpful as a reference for

respondents in applying exemptions and obligations as data controllers when considering aspects of more complex requests on a case-by-case basis.

The EDPB Guidelines 01/2022 have been a valuable resource for one respondent, who advised that they have proved extremely valuable in training staff on the proper identification and processing of Art 15 access requests.

31) In your opinion, which **topics concerning the right of access** or which parts of **the EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

Recipients or categories of recipients.

See Answer 2.7

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees' right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF? If yes, please provide the date, link to the guidance, and a short description of the guidance:

[Data Subject Access Requests - FAQ General for all data controllers.](#)

[Full Guidance to controllers October 2022](#)

[General website introduction guidance on data subject access requests](#)

[General website guidance on the Right of Access and the Right to Data Portability.](#)

[FAQ for data subject on making a data access request on some ones behalf.](#)

[FAQ on how long an organisation have to respond to an access request.](#)

[FAQ for individuals having difficulties with their Subject Access Request.](#)

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

[Ryanair published decision 2020.](#)

The investigation found that the data controller failed to provide the complainant's personal data within one month of their request. Further, the data controller failed to notify the complainant of any extension to the statutory timeframe allowed for under

Article 12(3) of the GDPR and a reprimand was issued.

The DPC Access Unit issued 3 enforcement notices in 2023. Page 22 DPC Annual Report 2023

[And Page 110 DPC Annual Report](#)

34) **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).

After analysing the responses received, the DPC intends to write informally to a few respondents, offering them general guidance on compliance with Article 15 GDPR Subject Access Requests in some areas. The DPC does not intend to carry out any formal investigations.

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Very often

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Very often

37) 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 content of EDPB Guidelines 01/2022 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: **Check**

b. No:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes:

b. No: **No**



# IT SA

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<sup>28</sup>:
  - d. Ongoing investigation:
- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),
  - Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? [No](#)
  - Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. [No](#)
  - If not, will this fact finding activity impact your enforcement activities and if yes, how? [Generally speaking, the impact of this fact finding activity will be in relation to the carrying out, also by the Authority, of greater awareness activities, as better indicated in the following sections of this report \(e.g. Responses no. 2.3, 2.5 and 2.7\).](#)
- 3) For all SAs: 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](#)
- 4) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.  
[The Authority deleted the following questions: Questions n. 1.1, 3.1.a, 4.5, 4.5bis, 4.5.b](#)
- 5) For all SAs: 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 etc.)? [NO](#)

## Part I – Some numbers on the controllers addressed

- 6) How many controllers did you contact?  
[63](#)
- 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/to your questions.  
[49](#)

---

<sup>28</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.



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?

Participation in the fact finding was not mandatory and identification of the responding controller was not required

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: Please select one or more answers.

a. Public sector: 20 responding controllers

b. Private sector: 31 responding controllers

Number of responses is greater than the total number of responding controllers because two of them indicated that they work in both the public and private sectors.

10) Please specify the category<sup>29</sup> of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers

a. Micro enterprise: 1 responding controller

b. Small enterprise: 2 responding controllers

c. Medium-sized enterprise: 14 responding controllers

d. Large enterprise (more than 250 employees): 13 responding controllers

e. Non-profit organisation:

f. Ministry:

g. Local authority: 11 responding controllers

h. Administrative authority/agency/office (e.g. job center):

i. School / university / educational institution:

j. Other (please specify): 8 responding controllers, all from the health sector

11) Please specify the nature of the (business) activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

a. education sector:

b. health sector: 15 responding controllers

c. social sector:

d. insurance sector:

e. finance sector:

f. IT sector:

g. retail sector:

h. logistics sector:

i. public transportation:

j. telecommunications: 5 responding controllers

k. postal services:

l. advertising sector:

m. marketing services:

n. entertainment sector:

o. information / journalism sector: 5 responding controllers

---

<sup>29</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- p. scientific / historical research:
- q. credit scoring agency:
- r. public utility/infrastructure provider (e.g. energy): 6 responding controllers
- s. housing industry:
- t. manufacturing:
- u. other (please specify): 18 responding controllers, including 10 Local Authorities who carry out data processing activities in multiple sectors and 6 controllers related to the energy sector.

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. customers: 25 responding controllers
- b. potential customers: 20 responding controllers
- c. employees: 40 responding controllers
- d. job applicants: 22 responding controllers
- e. children: 15 responding controllers
- f. vulnerable adults: 16 responding controllers
- g. patients: 15 responding controllers
- h. citizens (for public sector): 16 responding controllers
- i. applicants (for public services): 8 responding controllers
- j. recipients (for postal services): 1 responding controller
- k. other (please specify): 8 responding controllers

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. Less than 100:
- b. 100 - 200:
- c. 201 - 500:
- d. 501 - 2,000:
- e. 2,001 - 10,000: 5 responding controllers
- f. 10,001 - 50,000: 4 responding controllers
- g. 50,001 - 100,000: 3 responding controllers
- h. 100,001 - 1,000,000: 23 responding controllers
- i. 1,000,001 - 10,000,000: 9 responding controllers
- j. More than 10,000,000: 4 responding controllers

Disclaimer: responding controller did not provide any indications of the approximate volume of data subjects concerned by the processing activities

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.

- a. Contact data: 43 responding controllers
- b. Payment data: 38 responding controllers
- c. Identification data: 46 responding controllers

- d. Sensitive data within the meaning of Art. 9 GDPR: 31 responding controllers
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR: 9 responding controllers
- f. Other (please specify): 9 responding controllers

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. 0 request: 20 responding controllers
- b. 1-10 requests: 15 responding controllers
- c. 11-25 requests: 3 responding controllers
- d. 26-50 requests: 2 responding controllers
- e. 51-100 requests:
- f. 101-150 requests: 3 responding controllers
- g. 151-200 requests:
- h. 201-500 requests: 1 responding controller
- i. 501-10,000 requests: 5 responding controllers
- j. >10,000 requests:
- k. No information:

15.1) Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

Access requests received by responding controllers in 2023 appear to be rather circumscribed. 41% of controllers received no requests at all, and 31% of controllers received no more than 10 requests during the year.

The sector and nature of the activity carried out by the data controller may be a relevant factor in relation to the number of requests received.

It was noted that both 83% of responding controllers who said they working in the information sector and 87% of responding controllers who said they operate in the health care sector are included in the aforementioned categories (a) and (b) of Question 1.10. In contrast, responding controllers working in the telecommunications sector are more likely to be subject to access requests.

The size of the data controller may also be relevant in relation to the volume of requests received, and in particular, it was noted that all responding micro and small businesses reported that they had not received any access requests during 2023.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 20 responding controllers
- b. >0–25%: 15 responding controllers
- c. 26–50% requests: 3 responding controllers
- d. 51–75% requests: 2 responding controllers
- e. 76–100% requests: 6 responding controllers
- f. No information: 3 responding controllers

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

Basically access requests account for a minority share of the overall requests made by data subjects to data controllers. In fact, more than one-third of the responding controllers fall within categories (a) and (b) of Question 1.12.

The nature of the activity carried out by the data controller appears to have an impact on the percentage of access requests received in relation to the total requests submitted under Articles 15-22 of the EU Regulation 2016/679. In this sense, it is noted that for entities working in the telecommunications sector, the percentage of access requests appear rather small (almost all respondents are in category b). In contrast, for those who carry out activities in the health care sector access requests tend to account for almost all of the requests received (83% of responding controllers are in category e). Such a finding, although it may appear contradictory to the findings in Section 1.11 with regard to the health care sector, nevertheless suggests that, in this sector, the number of requests submitted under the EU Regulation 2016/679 is on the whole limited and that those received by data controllers mostly qualify as access requests.

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 24 responding controllers
- b. >0–25%: 2 responding controllers
- c. 26–50% requests: 1 responding controller
- d. 51–75% requests: 2 responding controllers
- e. 76–100% requests: 17 responding controllers
- f. No information: 3 responding controllers

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

N/A

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 27 responding controllers
- b. >0–25%: 3 responding controllers
- c. 26–50% requests: 5 responding controllers
- d. 51–75% requests:
- e. 76–100% requests: 12 responding controllers
- f. No information: 2 responding controllers

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

N/A

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 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. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.
- d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
- e. What are differences that you have encountered between controllers in your Member State?
- f. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

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

Lack of documentation and role identification: some responding controllers did not provide any information on how they document compliance with access requests. Other controllers, while providing generic information, did not provide details with respect to did not provide details with respect to the actors involved in dealing with access requests, the related functions performed, and their authorization/permission. These findings suggest that appropriate measures to demonstrate how access requests are fulfilled and to ensure that the requests are handled by the appropriately authorized actors are not always adopted.

Furthermore, indefinite data retention period: ¼ of the data controllers indicated no data retention period or indicated that data retention is perpetual. Other data controllers indicate very general criteria for data retention period. These findings suggest that an appropriate deletion routine is not always established, and this approach does not appear to be compliant with the storage limitation principle.

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

Articles 5, paragraph 1, letter e) and f), 5, paragraph 2, 24, 25 and 32 of the GDPR.

c) If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.

Paragraphs 40, 41 and 42 of the EDPB Guidelines 01/2022. Reference could be made also to paragraphs 37 and 118 of such Guidelines: notwithstanding that these paragraphs refer to data processing for which the right of access is exercised, the same principles and provisions

regarding data retention should also apply to data processing carried out to comply with access requests.

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

Failure to receive access requests or receipt of a small number of requests may result in the data controller not establishing methods and procedures for adequate handling of access requests. In this sense, almost all of those who did not provide information are responding controllers who received no access requests in 2023, or at least no more than 10. About the issue concerning the retention period, with specific reference to the public sector, a potential explanation could be the use of protocol registry by the greater part of the data controllers.

- e) What are differences that you have encountered between controllers in your Member State?

Regarding Question 2.2. of the questionnaire, data controllers operating in the public sector, compared with those operating in the private sector, tend to provide less precise information regarding data retention periods.

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

Encourage data controllers to more carefully design activities and roles for handling access requests, such as by promoting the adoption of dedicated internal procedures. Moreover, the data controllers should limit their data retention period. In the public sector, the data controllers should specify the storage period or the criteria used to determine that period in their own Conservation plan and Discard ceiling to which the protocol registry generally refers to identify its data retention time.

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

In addition to adopting a specific internal procedure for the exercise of data subjects' rights, some responding controllers have also published this procedure on their institutional website. This practice can foster a greater level of transparency between the data controller and data subjects and also facilitate the exercise of the data subjects' rights.

## Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

- 21) 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 3.4 in the questionnaire addressed to controllers.

In light of the answers provided, three relevant issues arise for data controllers in handling access requests received under Article 15 of the GDPR.

The first relates to being able to ensure transparency and awareness to the data subject regarding the handling of the request and, in particular, the timing for processing the access



request. In fact, on the basis of the responses provided, it emerges that only the 50% of the responding data controllers send a confirmation that the request made by the data subject has been taken care of. Furthermore, only a few controllers (about 10), even when sending a preliminary communication to the data subject, indicate to the data subject the processing time.

The second issue concerns the absence, in some cases, of a formalized procedure - even included in a broader procedure regarding the handling of requests for the exercise of rights by data subjects under the GDPR - as the aforementioned access requests are handled in light of corporate practices. In the answers provided in the questionnaire, about 50% of the data controllers explicitly indicated the existence of a specific procedure for access or for handling requests for the exercise of rights by data subjects, while others described only the internal process applied, not specifying whether it is implemented by practice or on the basis of a specific formalized procedure. In limited cases it was specified that there is no procedure nor were the steps of any internally applied process described.

Lastly, the third issue relates to the lack of inclusion of the handling of requests for the exercise of rights in the assessments carried out by the relevant data controller when digitizing processes or integrating new digital tools, which could lead to problems in relation to the timing and manner in which requests are processed. This is because, only 40% of data controllers indicated such inclusion in their digitization processes, specifying, in some cases, that this process is being implemented or indicating in a more generic way the involvement of the DPO in the digitization of processes.

It should also be noted that, in two cases, there does not seem to be a proper distinction between the management of requests for access to administrative documents provided for by national legislation (e.g., Law no. 241/1990, Legislative Decree no. 33/2013) and requests for access to personal data under Article 15 of the GDPR, considering that the management of such requests is regulated in the same procedure or the management of requests for access under Article 15 of the GDPR is carried out according to the methods and terms provided for access to administrative documents.

Relevant legislation relates to compliance with the principle of transparency in art. 5, paragraph 1, letter a) as well as art. 12, paragraphs 1 and 3, of the GDPR, with regard to the issue concerning communications to data subjects. Generally speaking, the abovementioned issues relate to the broader principle of accountability set forth in articles 5, paragraph 2 and 24 of the GDPR.

Furthermore, the issues described concern the following paragraphs of the Guidelines: 6, 57, 137 and 164.

With regard to the reasons on which the occurrence of such issues depends, it should be noted that, in many cases, the lack of communication of the timing of the handling of requests has been motivated by the fact that they are handled within the month of receipt of such requests. With respect to procedures, in some cases it has not been implemented because the relevant data controller has not received requests for access under Article 15 of the GDPR. Regarding the failure to include requests to exercise rights in digitization processes, this could depend on the number of requests received.

No significant differences have been found among the various data controllers.

Possible solutions for the aforementioned issues could be:

- to foster the knowledge of the Guidelines among controllers, for instance through the Authority's website, together with the release of the report results, both at national and EU level, at the end of the CEF 2024 project;
- to promote the adoption of Codes of Conduct, pursuant to Article 40 of the GDPR, in order to identify standardized procedures for the effective application of the right of access, also in view of the different categories of data controllers.

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

Some possible best practices to highlight, based on the answers received, are the use of online forms to facilitate data subjects in submitting access requests under Article 15 of the GDPR, in accordance with the provisions of the Guidelines (paragraph 53), as well as the use of self-service access systems to allow data subjects to independently download their personal data at any time, in accordance with the provisions of paragraphs 137 and 138 of the aforementioned Guidelines. More than half of data controllers have, moreover, indicated that there is systematic monitoring or control of the handling of access requests - which in most cases is done by or with the involvement of the DPO - including through the maintenance of a special record concerning requests received from data subjects regarding their rights under the GDPR.

### **Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”**

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

23) 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 4.15 in the questionnaire addressed to controllers.

As a main issue worth mentioning that some controllers have not implemented specific measures and procedures to respond to requests of access, as required by the EDPB in the Guidelines 01/2022 on data subject rights - Right of access (below/hereafter, “Guidelines”). In particular, critical issues have emerged with reference to the following aspects:

- many controllers require the access request to be in written form, as opposed to the Guidelines; (questionnaire: 4.3)
- lack of appropriate and specific measures to ensure access to data in relation to different categories of data subjects, as suggested in the Guidelines; (questionnaire: 4.5).

The article 12(2) GDPR is the only relevant in the context of the questions considered (4.3 and 4.5).

The critical issues underlined above can be referred respectively the first to par. 52 and the second to par. 128 of the Guidelines.

The reason of those issues may be found, in the first case, in the need to ensure legal certainty concerning the definition of the time to respond to requests of access, in the second case, in the noted absence of a high level of accuracy in the handling of requests, such as that required by the Guidelines.



No differences were found among controllers.

Valid solutions for the critical issues arisen could be:

- to foster the knowledge of the Guidelines among controllers, for instance through the Authority's websites, together with the release of the report results, both at national and EU level, at the end of the CEF 2024 project;
- to promote the adoption, of Codes of Conduct, according to Article 40 of the GDPR, in order to identify standardized procedures for the effective application of the right of access, also taking into account the different nature of the data subjects involved.

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

The best practices emerge among those controllers who have better defined the procedures, also in terms of timing, to facilitate data subjects in exercising their right of access (e.g. delegation in case of requests received from third parties, measures or alerts to provide timely feedback).

## **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

25) 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 5.18 in the questionnaire addressed to controllers.

The main issues noted concern the following aspects:

- only a very small percentage of controllers adapt the information, taking into account different categories of data subjects (minors, elders, etc.); (questionnaire: 5.6)
- most controllers, with regard to the information related to the Article 15(1)(c) GDPR, merely indicate the categories of recipients without specifying, if possible, the individual recipients. The controllers hardly know the differences between what required for in art. 13 GDPR, concerning the information, and the obligations related to the right of access (questionnaire: 5.7)
- Approximately half of the controllers do not provide for alternative forms of data release than the handing over of a copy of them; (questionnaire: 5.13)
- if the data request change in the period between the date of the request and the date of the reply, approximately half of the controllers do not refer to the time of receipt of the request to provide the reply; (questionnaire: 5.16)

The relevant GDPR article in the context of the questions considered (4.3 and 4.5) are, respectively:

- Art. 12(1) and (2) (referring to the first point listed above)
- Art. 15(1)(c) (referring to the second point above)
- Art. 12(1) (referring to the third point above)

The critical issues underlined can be traceable to the following points of the Guidelines and the decisions of the CJEU, respectively:

- Point 113 of the Guidelines
- Point 117 of the Guidelines and CJEU judgment C-154/21

- Point 133 of the Guidelines
- Point 34 and 37 of the Guidelines.

A possible explanation in relation to the problems highlighted above may be that it has not been reached yet a level of accuracy such as that required in the Guidelines, despite the good intentions of the controllers.

No differences were found among controllers.

Valid solutions for the critical issues arisen could be:

- to foster the knowledge of the Guidelines among controllers, for instance through the Authority's websites, together with the release of the report results, both at national and EU level, at the end of the CEF 2024 project;
- to promote the adoption, of Codes of Conduct, according to Article 40 of the GDPR, especially in order to identify standardized procedures for the effective application of the right of access, also taking into account the different nature of the subjects involved.

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

The best practice identified is that almost all controllers when providing full or partial extracts or documents also furnish an explanatory note to ensure the comprehensibility of the data content.

### **Section on “LIMITATIONS OF ACCESS REQUESTS”**

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

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

- Few requests for access to data and even more limited cases of subsequent denial.

Almost half of the respondents stated that they had not received access requests at all. Those who have received access requests have declared that they refuse the request in cases where they are not able to identify the interested party or if this request does not come directly from the interested party but from a third party who claims to act on their behalf; Furthermore, refusal is possible if the requests are manifestly unfounded or excessive. The interested party is however informed of the reasons for the refusal.

- Reasons for refusal or partial response.

In general, no particular examples of types of data excluded a priori from access and different from what is already indicated in the rules are highlighted. One controller specified that he considered traffic data (telephone and electronic) excluded from access. In general it was stated that no information is provided on the identity of the persons processing personal data. Only in cases where such information falls within that which must be communicated by law, pursuant to national administrative law, will it be disclosed. In some cases, the information is still provided if deemed necessary by the interested party for his protection or if it can be deduced from the correspondence held with the interested party. The controllers, for the most

part, have declared that they check the material before transmitting it to the interested party and, in the event that third-party data is present, they are obscured. If this is not possible, a balancing of interests is carried out also making use of the DPO's assessments  
Few controllers have procedures in place to manage access requests. From the responses it can be seen that few owners have equipped themselves with specific procedures for managing requests from interested parties.- Difficulty in quantifying any costs. Most cardholders do not charge fees for access. In particularly onerous cases, the owners refer to administrative rules relating to other contexts in order to quantify the costs to be charged to the interested party.

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

Below are the regulatory sources cited by the controllers to reject or limit the right of access.

- In a generic way: EU Regulation 2016/679, Data protection Code - Legislative Decree 196/2003, Legislative Decree 101/2018.
- In a timely manner: art. 12 par. 5 and 6, art. 15 par. 4 of the GDPR; Articles 123 and 132 of the DP Code (referring to article 6 of Directive 2002/58/EC).

Also cited, often erroneously, are national regulations on access to administrative documents, civic access, whistleblowing and, generically, other regulations on the protection of commercial secrets and intellectual property, in particular:

- Decree n.24/2023 implementing the EU directive on whistleblowing;
- art. 22 of Law 7.8.1990, n. 241 (access to administrative documents);
- Presidential Decree, 12/04/2006 n° 184;
- Civil Code and Criminal Code;

or other references are proposed such as art. 60 of the DP Code, which however concerns the limitation of access to administrative documents and civic access.

**c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.**

No specific reference on the matter. In relation to the answers provided by the controllers relating to the reasons for limited access or denial, however, it should be noted that in only two cases the EDPB Guidelines 1/2022 on the rights of interested parties are cited. It should be noted, among the others, that one of the only two citations present is made correctly, because in the other the Guidelines are indicated with the wrong name.

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

The absence of internal procedures, already defined, for the management of access requests (including limitation or denial practices) is mainly due to the fact that almost half of the respondents declare that they have not received access requests at all.

In various cases, therefore, the definition of "manifestly unfounded" or "excessive" remains in a theoretical and not well-defined area. In the only certain case of denial of access or limitation of access, the theoretical answer on the reasons for rejection appears sufficiently defined. In two other cases, the reason explained to justify the exercise of the right of access to data includes elements partly unrelated to the EDPB guidelines such as "requests formulated for mere delaying or specious purposes, or to exercise generalized control over the activity carried out by the 'Body', requests presented with "the sole intention of causing damage or prejudice to the data controller", without better clarifying the relevant cases.

Regarding the calculation of any costs associated with the access request, it is noted that some controllers have never addressed the problem, others refer to generic administrative costs, others with greater precision state that they proceed in analogy with other regulations, applying the same cost provided for procedures for accessing documents presented pursuant to law 241/90 or for generalized civic access.

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

The only difference noted is between the owners who received multiple access requests and those who did not receive any. In this regard, it is noted that in only 3 cases out of 49 the controllers declare that they considered some requests received to be manifestly unfounded or excessive. In one case, the number indicated is not even consistent with the answers because it indicates 50/50.

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

From the answers provided, the owners do not seem to perceive any particular critical issues and consequently do not suggest or identify solutions.

It would certainly be useful to anticipate the problem rather than defining a procedure only after receiving multiple requests from interested parties.

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

No particular best practices emerge other than the fact that some controllers declare that they have implemented specific procedures within them for the management of access requests, including those deemed to be rejected or limited. A good part of the controllers appear not to have analysed the problem at all, because they have not received requests or because they have arrived in small numbers. In order to calculate any costs to be charged for access requests formulated pursuant to the GDPR, it should be noted that some data controllers declare that they have operated in analogy with the Italian legislation on "access to administrative documents" - better known and used on a national scale - so as to overcome the indeterminacy of the point in question.

### Part III – Impressions on the levels of awareness and compliance

- 29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

- 29.1. Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

Big data controllers, belonging to the private sector, have declared that they receive a greater number of requests and are, consequently, more structured in the procedures adopted to respond to interested parties

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1. Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, “size” of the controller, etc.):

From the answers provided it is not possible to deduce whether there is a significant difference depending on the type of controller. However, the controllers who received a greater number of requests appear more attentive to the adoption of procedures that are more in line with the indications of the EDPB guidelines.

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

- Excessive formal requirements are required for submitting the application, with no alternative forms to the written form
- A differentiation of interested parties and their characteristics is not made in order to optimize the response to applicants: the information provided is not adapted to the most vulnerable subjects (minors, elderly people)
- In the answers provided, reference is made to the categories of recipients of the data (information that should already be present in the information provided to the data subject) instead of providing the names of the individual recipients
- Lack of transparency towards the data subject, in particular with respect to the timescales within which the request will be processed
- Differences in the feedback provided by the controllers in relation to those who have actually implemented procedures and also declared knowledge of the EDPB Guidelines.

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees’ right of access; right of access exercised in the public sector, or regarding data concerning health, 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 subject’s rights which can be found at the link: <https://www.garanteprivacy.it/home/i-miei-diritti/diritti/diritto-di-accesso>

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

No general, specific activity on the right of access, but multiple investigations have been launched on individual cases and clarifications have been sent to data subjects who have contacted the Garante or reported possible violations.

34) **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 activity specifically aimed at the subjects responding to the questionnaire since the data controller was not required to identify himself

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Very often

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Often

37) 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 content of EDPB Guidelines 01/2022 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: [FAQ on access in specific sectors](#)

b. No:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. **Yes: collection and publication of jurisprudential maxims (e.g. Court of Justice, EDPB binding decision, national authorities) on the topic of the exercise of rights**

# LI SA

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.
- Fact finding:
  - Fact finding + determining follow-up action based on the results: **Yes**
  - New formal investigation<sup>30</sup>:
  - Ongoing investigation:

- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),

- Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? **Yes**
- Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. **No**
- 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, in the course of its advisory activities, draw the attention of the controllers concerned to the inadequate or missing processes and/or implementation of the relevant provisions of the GDPR. In addition, as in the past, the LI SA will address the main issues identified at the next annual meeting of the DPOs in Liechtenstein and will raise the awareness of the DPOs in Liechtenstein with regard to the shortcomings identified through the survey.

- 3) For all SAs: 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) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.

Not applicable

- 5) For all SAs: 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 etc.)?

No

## Part I – Some numbers on the controllers addressed

---

<sup>30</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.



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/to 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?

-

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: Please select one or more answers.

- a. Public sector: 2 responding controllers
- b. Private sector: 3 responding controllers

10) Please specify the category<sup>31</sup> of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers

- a. Micro enterprise:
- b. Small enterprise:
- c. Medium-sized enterprise: 1 responding controller
- 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): 1 responding controller
- i. School / university / educational institution: 1 responding controller
- j. Other (please specify):

11) Please specify the nature of the (business) activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. education sector: 1 responding controller
- b. health sector:
- 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:

---

<sup>31</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).



- 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. other (please specify): 1 responding controller - This public company is organised by law into public bodies.

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. customers: 5 responding controllers
- b. potential customers: 5 responding controllers
- c. employees: 5 responding controllers
- d. job applicants: 5 responding controllers
- e. children: 3 responding controllers
- f. vulnerable adults: 1 responding controller
- g. patients:
- h. citizens (for public sector): 2 responding controllers
- i. applicants (for public services): 1 responding controller
- j. recipients (for postal services):
- k. other (please specify): 2 responding controllers - One controller also processes employees' emergency contacts, while a second controller also processes data relating to event attendees, project partners, and external speakers.

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. Less than 100:
- b. 100 - 200:
- c. 201 - 500:
- d. 501 - 2,000:
- e. 2,001 - 10,000:
- f. 10,001 - 50,000: 3 responding controllers
- g. 50,001 - 100,000: 1 responding controller
- h. 100,001 - 1,000,000: 1 responding controller
- i. 1,000,001 - 10,000,000:
- j. More than 10,000,000:

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.

- a. Contact data: 5 responding controllers
- b. Payment data: 5 responding controllers
- c. Identification data: 5 responding controllers
- d. Sensitive data within the meaning of Article 9 GDPR: 3 responding controllers
- e. Data of a highly personal nature within the meaning of Article 10 GDPR: 3 responding controllers
- l. Other (please specify): 1 responding controller - This controller also processes personal data in the context of assessments (e.g. performance).

15) How many requests for access in accordance with Article 15 GDPR did the responding controllers receive in 2023 (approximately)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. 0 request: 1 responding controller
- b. 1-10 requests: 3 responding controllers
- c. 11-25 requests: 1 responding controller
- d. 26-50 requests:
- e. 51-100 requests:
- f. 101-150 requests:
- g. 151-200 requests:
- h. 201-500 requests:
- i. 501-10,000 requests:
- j. >10,000 requests:
- k. No information:

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, "size" of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

No

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 1 responding controller
- b. >0–25%: 1 responding controller
- c. 26–50% requests:
- d. 51–75% requests: 2 responding controllers
- e. 76–100% requests: 1 responding controller
- f. No information:

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, "size" of the controller, sector)?

Yes, there is a difference in the percentages. Out of the five controllers we sent the questionnaire to, three controllers stated that requests for access were made by data subjects in order to exercise their data subjects' rights. One controller indicated that it did not receive any requests for access in 2023.

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 2 responding controllers
- b. >0–25%:
- c. 26–50% requests:
- d. 51–75% requests: 2 responding controllers
- e. 76–100% requests: 1 responding controller
- f. No information:

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, "size" of the controller, sector)?

There is a difference in the percentages among the five controllers surveyed. One of them did not receive any requests for access in 2023. Three controllers stated that most of the requests for access included a request to receive an insight into and inspection of and/or a copy of the personal data. The three controllers surveyed are private sector companies from different sectors (insurance, finance and manufacturing/production). Two of these controllers are large companies and one is a medium-sized company. The fifth controller, a company in the public sector, stated that with respect to their access requests received there was no case where the data subject was also asking for a copy of the personal data processed. However, it seems that there is no logical reason for these differences.

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 3 responding controllers
- b. >0–25%:
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests: 2 responding controllers
- f. No information:

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, "size" of the controller, sector)?

Except for the controller who did not receive any requests for access in 2023, 50 percent of the controllers surveyed stated that the requests for access included a specific request to receive information on the underlying processing activities. The other half of the controllers stated that the requests for access did not contain a specific request thereto. The two

controllers surveyed who did receive such a specific request are large companies that process many different categories of data, including special categories of data such as health data within the meaning of Article 9 of the GDPR and data of a highly personal nature within the meaning of Article 10 of the GDPR. This may explain the difference pointed out in the survey.

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 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. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.
- d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?
- e. What are differences that you have encountered between controllers in your Member State?
- f. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?

#### Issue: Varying storage periods for request for access

a.: All of the controllers surveyed reported different storage periods for requests for access and the related correspondence and responses. The periods vary from 1 to 30 years. One controller even stated that the relevant information on the request for access is stored for as long as the data subject's contractual relationship with the company exists. Accordingly, there seems to be no clarity among controllers in Liechtenstein about how long an access request and the related correspondence can legitimately be stored and when the data in physical and/or electronic form has to be deleted in order to respect the data protection principles in Article 5 GDPR (namely purpose limitation, data minimization, and storage limitation).

b.: Art. 5 (1) a, b, c, and e GDPR

c.: Not applicable

d.: Some controllers seem to make no difference between their regular customer relations and an access request according to the GDPR. Accordingly, the correspondence is stored within the same time limits as the other customer data. Furthermore, it is possible that certain controllers are worried about further access requests/data protection requests by the same data subject or wish to be prepared for hypothetical legal proceedings and for these reasons

decide to keep all the correspondence with the client (the “data subject”) for the whole contractual relationship. Besides, it seems that a lack of knowledge of the relevant provisions of the GDPR is a major problem and leads to excessively long storage periods as the results of the survey show.

e.: Three of the controllers surveyed indicated a storage period between 1 and 3 years for access requests. Two controllers indicated a vastly too long storage period (in one case up to 30 years and in one case for as long as the customer relationship lasts). Interestingly, both of these controllers are large companies in the insurance and financial sector. It seems that in these sectors there is more reluctance to delete access requests and the related correspondence within reasonable time, maybe due to generally high duties for protocolling customer relationships in these sectors.

f.: Those controllers who have not done so yet should urgently define clear storage periods for access requests (and other data protection requests) and related correspondence and include the applicable storage periods in their data retention policy, taking into account the relevant provisions of the GDPR (especially Article 5 (1) GDPR). The LI SA is aware of the importance of this issue and intends to pay special attention to this matter in its advisory activities. It will also include this issue as an awareness-raising measure in the upcoming annual meeting of DPOs in Liechtenstein.

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

No

### **Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”**

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

21) 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 3.4 in the questionnaire addressed to controllers.

#### **Issue: No pre-defined processes for handling requests for access**

a.: While four out of the five controllers have set up structured processes to handle access requests according to Article 15 GDPR, one controller has no pre-defined process and instead takes a pragmatic approach in dealing with them.

b.: Art. 12, 15 GDPR

c.: The EDPB only provides general guidance and examples in its Guidelines 01/2022. The process falls within the organizational discretion of a controller.

d.: The reasons for the missing or inadequate establishment of pre-defined internal processes for handling requests for access might be a lack of clear processes in an organization in

general or a lack of knowledge of the duties related to Articles 12 and 15 GDPR and of the problems which potentially can arise for a controller when not fulfilling these.

e.: While one of the controllers has no pre-defined process for handling access requests, the other four have each implemented a structured process. Three of them have implemented a process, which defines the internal responsibilities and procedures step by step from the receipt of the request to the actual provision of access. The fourth controller with numerous sub-departments has set up pre-defined processes in the form of a "manual" with recommendations, flow charts, and sample texts.

f.: The LI SA strongly recommends to implement a pre-defined structured process to handle access requests which involves a thorough description of all procedural steps to be taken and a clear assignment of responsibilities for each step. The LI SA will take up this issue with the controller still lacking a structured process and will strongly advocate for it at the upcoming annual meeting of DPOs in Liechtenstein.

### **Issue: Insufficient consideration of data subjects' rights when digitizing processes or when onboarding or integrating new digital tools**

a.: Two of the controllers only partially answered this question. It can be assumed that they have no or only insufficient procedures in place to consider data subjects' rights when digitizing processes or when onboarding or integrating new digital tools.

b.: Art. 25 (1) GDPR

c.: While there are no specific requirements mentioned in EDPB Guidelines 01/2022, controllers should implement processes to ensure that data subjects' rights and their implementation/safeguarding will be taken care of and respected in such situations.

d.: One of the two companies that provided little or insufficient information on this point has no defined process for handling requests for access. It seems that also when digitizing or onboarding or integrating new digital tools, data subjects' rights are not sufficiently taken care of within this organization. This might be due to a lack of awareness of the need (or unwillingness?) to effectively implement data protection rights and the necessary safeguards regarding data processing in order to comply with GDPR. Again, however, it is within the organizational discretion of the controller to implement formal processes to properly safeguard data subjects' rights when digitizing processes or when onboarding or integrating new digital tools.

e.: The other three controllers try to ensure that data subjects' rights are considered when digitizing their processes or when onboarding or integrating new digital tools. They involve the DPO when digitizing processes, regularly update their records of processing activities, and ensure the assistance of processors as part of their data processing agreements. They also demonstrate a clear awareness of the challenges of integrating new tools/services in existing processes to provide access to data, but apply different approaches depending on internal responsibilities.

f.: The LI SA will bring this issue to the attention of the relevant two controllers and will present it at the upcoming annual meeting of DPOs in Liechtenstein.

### **Issue: No confirmation of receipt of access requests**

a.: One of the controllers does not send a confirmation of receipt of the request for access to the data subject.

b.: -

c.: The EDPB considers this good practice in its Guidelines 01/2022, para. 57.

d.: The only controller who does not send a confirmation of receipt has implemented very few formalized procedures regarding the implementation of data protection rights overall.

e.: All other controllers send a confirmation of receipt to the data subject within a few days after receipt of the request for access or, where appropriate, after the identity of the data subject (and legitimacy of the request) has been established.

f.: Although the GDPR does not require it, the LI SA considers such a confirmation to be useful and good practice. It creates, at an early stage, a verifiable documentation of the handling of a request for access from a data subject. And it may be beneficial in terms of accountability pursuant to Art. 5 (2) GDPR. The LI SA will present the benefits of this practice to DPOs at the upcoming annual meeting of DPOs in Liechtenstein.

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

No

### **Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”**

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

23) 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 4.15 in the questionnaire addressed to controllers.

### **Issue: Data minimization when identifying data subjects**

a.: One of the data controllers did not show any real efforts to implement a differentiated procedure and minimize data when identifying data subjects. This data controller states that it identifies the data subject solely on the basis of proof of identity, without limiting itself to relevant data already at hand which might be sufficient to establish the identity otherwise.

b.: Art. 5 (1) c, 12 (2) GDPR

c.: EDPB Guidelines 01/2022, para. 58 et seq.



d.: Four out of the five controllers make great efforts to provide differentiated identity verification procedures that are also adapted to the respective relationship between the controller and the data subject (e.g. with a verification process via a customer portal) and therefore minimize the processing of data. Thus, the reason why one controller does not do so, probably lies in its minimal efforts towards compliance with data protection requirements as the identification procedure described by it is very simple and does not necessarily ensure data minimization as required by Article 5 GDPR.

e.: Four out of the five controllers stated that if the data subject has a (customer) account, the primary way of verifying the identity of the data subject is through this account. In the event that no such account exists the data subject is asked to provide identification documents in order to perform the identity check. One controller also explicitly gives data subjects the option of identifying themselves by a personal visit at the controller's premises.

f.: The LI SA will draw the attention of the data controllers concerned to the principle of data minimization as an important data protection requirement when performing identity checks at the next annual meeting of DPOs in Liechtenstein.

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

No

### **Section on "CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR"**

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

25) 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 5.18 in the questionnaire addressed to controllers.

#### **Issue: Inconsistencies in processing pseudonymised data**

a.: Pseudonymised data are personal data within the meaning of Article 4 No. 1 GDPR. The request for information pursuant to Article 15 GDPR relates to personal data of the applicant that is processed by the controller. This means that the controller must also inform about the processing of pseudonymised data. The information provided by the controllers on the subject of processing pseudonymised data and on whether they also provide information on such data processing as part of the response to the request for access to the data subject is, however, not very informative and also partly unclear. It can therefore be doubted whether access to pseudonymised data is actually given to data subjects by the controllers surveyed.

b.: Art. 4 No. 1, 15 GDPR

c.: EDPB Guidelines 01/2022, para. 45



d.: Given that one controller stated that it does not include pseudonymised data in its response to a request for access, and another controller did not provide any information on processing pseudonymised data at all, the LI SA is not sure to what extent the term "pseudonymised data" is correctly understood by the controllers concerned, namely being personal data.

e.: Apparently, not all of the controllers surveyed process pseudonymised data (or are not aware of it) and one controller even admits not including such data in the response to an access request. The majority, however, makes efforts to also include pseudonymised data when giving access, as long as it can be established which pseudonymised data is related to the requesting data subject.

f.: The LI SA will include relevant information in one of its upcoming newsletters in order to clarify that pseudonymised data are personal data and thus must be included in the response to a request for access. Furthermore, the LI SA will present this issue at the next annual meeting of DPOs in Liechtenstein.

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

No

### **Section on “LIMITATIONS OF ACCESS REQUESTS”**

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

#### **Issue: Lack of awareness of possible restrictions when providing specific personal data in response to a request for access**

a.: It appears that not all controllers surveyed are aware of the legal basis which allows them to restrict the disclosure of personal data when responding to a request for access. In fact, none of the controllers surveyed mentioned any legal basis in this respect, for example in relation to the protection of personal data of others (Article 15 (4) GDPR) or regarding personal data stored on backup servers (Article 34 LI-Data Protection Act) even though some of the controllers seem to have difficulties to provide access to data kept in backup files and log files.

b.: Art. 2 (1), (2) and 15 (4) GDPR; Art. 27 (4), 29 (4), 30 (1) b, 33 (1) a, b and 34 LI-Data Protection Act

c.: EDPB Guidelines 01/2022, para. 9, para. 19 and para. 95 with reference to ECJ C-141/12 and C-372/12; ECJ decision dated 22 June 2023, C-579/21.

d.: One possible explanation could be a lack of knowledge of the relevant articles in the GDPR and the LI-Data Protection Act. Furthermore, it might be unclear to controllers at times for what

purpose the data is (still) stored and therefore the applicability of articles like Article 34 LI-Data Protection Act might not be recognized.

e.: While some of the controllers surveyed indicated that they apply restrictions provided for by law when responding to a request for access, two controllers surveyed indicate that they make personal data available to the person requesting access in a general or comprehensive way and without applying any restrictions. The LI SA would like to note that this result is not entirely clear since the same two controllers' response to another question indicated that, if applicable, they apply restrictions provided for by law in respect of the protection of personal data of others.

f.: On this point as well, the LI SA is considering publishing information in a newsletter to clarify the different legal grounds to restrict access to personal data. Furthermore, the topic will be included in the presentation at the next annual meeting of all DPOs in Liechtenstein.

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

No

### Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

Only one of the controllers surveyed from the private sector indicates a low level of compliance concerning the provisions of the GDPR on the right of access.

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, “size” of the controller, etc.):

Most of the controllers surveyed are aware of and understand the EDPB Guidelines 01/2022, but make only little use of them in practice.

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

The LI SA is of the opinion that, in general, the principles of Article 5 GDPR in relation to the right of access are insufficiently complied with by the controllers surveyed. In particular, the majority of controllers surveyed do not pay enough attention to the requirements of letters a, b, c and e of Article 5 (1) GDPR when implementing the right of access.

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees’ right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF?

If yes, please provide the date, link to the guidance, and a short description of the guidance.

We have published comprehensive information on the right of access pursuant to Article 15 GDPR on our website: <https://www.datenschutzstelle.li/datenschutz/themen-z/auskunftsrecht>

This information covers the following topics: who can request access to data from whom, what data can be requested, how data can be obtained, in what form data can be obtained and what it costs, when there is a right of access, when data is restricted or refused, and what can be done about it, as well as information on the right of access to personal data relating to deceased persons.

The templates for submitting a request for access and a response to the access request can be found under the following link on our website: <https://www.datenschutzstelle.li/datenschutz/themen-z/auskunftsrecht> (“Downloads & Links”).

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? 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.

34) **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 inform the controllers surveyed about our findings as part of our general presentation of the CEF 2024 and the implementation of the right of access at the next annual meeting of DPOs in Liechtenstein on 11 November 2024. We will also remind the DPOs at this meeting of the support services offered by the LI SA. Any further action beyond this, e.g. on a bilateral basis between the LI SA and the controllers surveyed, will be left to the decision of the LI SA.

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Regularly

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Hardly ever

37) 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 content of EDPB Guidelines 01/2022 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:
- vi. Online or remote training sessions:
- vii. Conferences organised:
- viii. Others: please specify: [The LI SA will present the findings of the CEF questionnaire at the next annual meeting of DPOs in Liechtenstein on 11 November 2024. The LI SA will focus on the most important issues found and requiring attention, but also on general aspects regarding the implementation of the right of access as outlined in the EDPB Guidelines 01/2022. Following the presentation, the DPOs will have the opportunity to ask questions and will be invited to participate in an open discussion round.](#)

b. No

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes

c. **No**

# LT SA

State Data Protection Inspectorate of the Republic of Lithuania

## Introduction

- 1) What was the initial procedural framework of your action?
  - a. Fact finding: [Response]
  - b. Fact finding + determining follow-up action based on the results: [Response]
  - c. New formal investigation<sup>32</sup> : [Response]
  - d. Ongoing investigation: [Response]

Investigation on the implementation of the right of access by data controllers was included in the annual investigation plan of the LT SA. As a result of investigation, the decision determining whether an infringement has occurred will be adopted in respect of every controller.

- 2) Did you use the same questionnaire for all controllers, or did you use different questionnaire versions for different types of controllers?

We used the same questionnaire for all controllers.

## Part I – Some numbers on the controllers addressed

- 3) How many controllers did you contact?

LT SA contacted 10 controllers.

- 4) Out of the contacted controllers, how many controllers responded?

LT SA received responses (filled in questionnaires) from all 10 controllers.

Please specify the sectors of activity of the responding controllers.

- a. public sector: 5 responding controllers;
- b. private sector: 5 responding controllers.

- 5) Please specify the category<sup>33</sup> of the responding controllers.

- a. micro enterprise: 1 responding controller.
- b. medium-sized enterprise: 1 responding controller.
- c. large enterprise (more than 250 employees): 5 responding controllers.
- d. ministry: 1 responding controller.
- e. administrative authority/agency/office (e.g. job center): 2 responding controllers.
- f. school / university / educational institution: 1 responding controller.
- g. other (please specify): 3 responding controllers (healthcare institutions or enterprises).

---

<sup>32</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

<sup>33</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- 6) Please specify the nature of the (business) activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.
- education sector: 1 responding controller.
  - health sector: 3 responding controllers.
  - social sector: 1 responding controller.
  - insurance sector: 1 responding controller.
  - finance sector: 2 responding controller.
- 7) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers.
- customers: 4 responding controllers.
  - potential customers: 3 responding controllers.
  - employees: 7 responding controllers.
  - job applicants: 2 responding controllers
  - children: 1 responding controller.
  - patients: 3 responding controllers.
  - applicants (for public services): 2 responding controller.
  - other (please specify): 1 responding controller (present/former students).
- 8) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers.
- Less than 100: 1 responding controller.
  - 10,001 - 50,000: 2 responding controllers.
  - 50,001 - 100,000: 1 responding controller.
  - 100,001 - 1,000,000: 4 responding controllers.
  - 1,000,001 - 10,000,000: 2 responding controller.
- 9) Which types of personal data are mainly concerned by the processing activities of responding controllers?
- Contact data: 9 responding controllers.
  - Payment data: 3 responding controllers.
  - Identification data: 7 responding controllers.
  - Sensitive data within the meaning of Art. 9 GDPR: 6 responding controllers.
  - Data of a highly personal nature within the meaning of Art. 10 GDPR: 2 responding controllers.
- 10) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)?
- 0 request: 4 responding controllers.
  - 1-10 requests: 4 responding controllers.
  - 51-100 requests: 1 responding controller.
  - 501-10,000 requests: 1 responding controller.

tDid you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, "size" of the controller, sector)? If considered relevant, are there any

controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

The highest number of requests for access in accordance with Art. 15 GDPR was observed by the data controllers operating in the health sector. Difference in numbers could be explained by the fact, that not all of the controllers qualify data subjects' requests as belonging to the implementation of the right of access under GDPR, but rather as a "simple" inquiry to provide information.

- 11) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received?
- None of the requests: 4 responding controllers.
  - >0–25%: 3 responding controllers.
  - 26–50% requests: 1 responding controller.
  - 76–100% requests: 2 responding controllers.

## Part II – Substantive issues regarding controllers' level of compliance

### Section on "DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS"

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

With regard to best practices, some data controllers grant status "confidential" to received requests for the right of access, this mark ensures limited access rights for the employees of controller to the content of received requests and leads to more secure internal processing of the requests within data controller. Retention period for the documents, related to the request (request itself/ answers/ additional communications, etc.), is aligned with the statute of limitations of the complaint, set in Republic of Lithuania Law on Legal Protection of Personal Data (i.e. period not exceeding 2 years).

### Section on "PROCESS FOR HANDLING REQUESTS FOR ACCESS"

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

With regard to the best practices, data controllers usually designate person, responsible for handling data subjects' requests, in order to keep the process of request handling under control. Some data controllers send confirmation, after receipt of data subject's request, that way both data subject and controller have more clear understanding of the set time limits for request handling.

### Section on "IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR"



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

With regard to the best practices, when request is submitted during recorded phone call, having confirmed identity of the requesting person, data controller's employee sends the summary of the request to the requesting person by e-mail or any other communication method (i.e. to client's account). This practice helps to clearly define the content of the request.

### Part III – Impressions on the levels of awareness and compliance

15) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

- a. High (on the level of awareness).
- b. Too diverse levels to qualify (on the level of compliance).

16) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

- a. High (all 10 data controllers were aware of EDPB Guidelines, 8 out of 10 applied guidelines in practice (some controllers indicated the absence of the requests, subsequently absence of possibility to apply guidelines) and 6 out of 10 made respective changes to their request handling procedures and practices).

### Part IV – Actions by participating SAs

17) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

Yes. The LT SA aims to raise awareness and competences of data controllers and therefore conducts trainings, specifically yearly trainings for DPO's, both in public and private sector. In 2021 training topic of the right of access was covered.

18) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Very often. The LT SA refers to the EDPB Guidelines every time (complaint handling, monitoring, investigation procedures; also, in the procedural documents when the decisions of inspectorate are challenged before courts) when the guidelines are relevant to make the statement of reasons on related topic.

19) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Very often. Inspectorate refers to the EDPB Guidelines every time (complaint handling, monitoring, investigation procedures; also, in the procedural documents when the decisions



of inspectorate are challenged before courts) when the guidelines are relevant to make statement of reasons on related topic.

20) 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 content of EDPB Guidelines 01/2022 and if yes, which actions do you consider to be preferable?

- a. Yes:
  - i. More online guidance.
  - ii. Online or remote training sessions.

# LU SA

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:
  - c. New formal investigation<sup>34</sup>:
  - d. Ongoing investigation:
  
- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),
  - Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? **No (anonymous questionnaire)**
  - Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. **No**
  - If not, will this fact finding activity impact your enforcement activities and if yes, how? **The CNPD will continue its enforcement activities by carrying out investigations but also by enhancing awareness raising through its communication (conferences, online publications), training (regular training sessions and through other available tools as described under point 33)) and workshops. The results of the CEF will impact these different activities by adapting these different levers with the results of the CEF.**
  
- 3) For all SAs: 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) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.

**NA**
  
- 5) For all SAs: 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 etc.)?

## Part I – Some numbers on the controllers addressed

---

<sup>34</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

6) How many controllers did you contact?

NA, the CNPD made a survey open to voluntary participants. The CNPD published a post on its internet website with a link to the questionnaire.

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/to your questions.

2 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?

NA

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: Please select one or more answers.

- a. Public sector: 1 responding controller
- b. Private sector: 1 responding controller

10) Please specify the category<sup>35</sup> of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers

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

11) Please specify the nature of the (business) activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. education sector:
- b. health sector:
- c. social sector:
- d. insurance sector:
- k. finance sector: 1 responding controller
- e. IT sector:
- f. retail sector:
- g. logistics sector:

---

<sup>35</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- h. public transportation:
- i. telecommunications:
- j. postal services:
- k. advertising sector:
- l. marketing services:
- m. entertainment sector:
- n. information / journalism sector:
- o. scientific / historical research:
- p. credit scoring agency:
- q. public utility/infrastructure provider (e.g. energy):
- r. housing industry:
- s. manufacturing:
- l. other (please specify): [Administration \(1 responding controller\)](#)

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. customers: [2 responding controllers](#)
- b. potential customers: [1 responding controller](#)
- c. employees: [2 responding controllers](#)
- d. job applicants: [1 responding controller](#)
- e. children: [1 responding controller](#)
- f. vulnerable adults: [1 responding controller](#)
- g. patients:
- h. citizens (for public sector): [1 responding controller](#)
- i. applicants (for public services):
- j. recipients (for postal services):
- k. other (please specify):

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. Less than 100:
- b. 100 - 200:
- c. 201 - 500:
- d. 501 - 2,000:
- e. 2,001 - 10,000:
- f. 10,001 - 50,000:
- g. 50,001 - 100,000: [1 responding controller](#)
- h. 100,001 - 1,000,000: [1 responding controller](#)
- i. 1,000,001 - 10,000,000:
- j. More than 10,000,000:

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.

- a. Contact data: 2 responding controllers
- b. Payment data: 1 responding controller
- c. Identification data: 2 responding controllers
- d. Sensitive data within the meaning of Art. 9 GDPR: 1 responding controller (medical data / medicine treatment of underage scholars and medial data and health conditions of elderly inhabitants)
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR:
- f. Other (please specify):

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. 0 request: 1 responding controller
- b. 1-10 requests: 1 responding controller
- c. 11-25 requests:
- d. 26-50 requests:
- e. 51-100 requests:
- f. 101-150 requests:
- g. 151-200 requests:
- h. 201-500 requests:
- i. 501-10,000 requests:
- j. >10,000 requests:
- k. No information:

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, "size" of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

No significant difference was identified. Due to the small number of answers received for this survey, no relevant analysis can be made for this point.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests:
- b. >0–25%:
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests:
- f. No information: 1 responding controller (The controller explains that access requests represent a "Very small percentage" with regards to the rest of the data protection requests received - No access request processed by the second data controller)

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, "size" of the controller, sector)?

Not applicable – only one answer was provided to the CNPD for this question (no access request processed by the second data controller).

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests:
- b. >0–25%: 1 responding controller (note that this controller never received a request for a copy of personal data - 100% of the requests were asking for insights into a data processing activity i.e. it's lawfulness)
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests:
- f. No information:

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

Not applicable – only one answer was provided to the CNPD for this question (no access request processed by the second data controller).

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests:
- b. >0–25%:
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests: 1 responding controller
- f. No information:

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

Not applicable – only one answer was provided to the CNPD for this question (no access request processed by the second data controller).

## **Part II – Substantive issues regarding controllers’ level of compliance**

### **Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”**

19) 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 2.2 in the questionnaire for controllers.

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

No leading or best practices identified.

### Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

21) 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 3.4 in the questionnaire addressed to controllers.

#### Question 3.1:

- a. Name the issue(s) identified and briefly describe it.  
Absence of a structured /complete process description for processing requests for access (definition of the internal responsibilities, of the input channels, software, output channels).
- b. Which provision(s) of the GDPR (or national laws) does this concern?  
The GDPR does not contain concrete requirements for the access request process; EDPB also only provides general guidance and examples (para. 123 et seq.); the process falls within the organizational discretion of the controller.
- c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.  
EDPB Guidelines 01/2022 (§6) “Besides, the specific wording of Art. 15, and the precise deadline for the provision of data under Art. 12(3) GDPR, obliges the controller to be prepared for data subject inquiries by developing procedures for handling requests.” and (§42) “Depending on the particular circumstances, the controllers may, for example, be required to implement an appropriate procedure, the implementation of which should guarantee the security of the data without hindering the exercise of the data subject’s rights.”
- d. 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 access requests received that does not justify, for the data controller, a structured procedure.
- e. What are differences that you have encountered between controllers in your Member State?  
NA

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

-

#### Question 3.4:

- a. Name the issue(s) identified and briefly describe it.  
No sending of confirmations of receipt (the data controller thinks that it will answer quickly and therefore does not need to send a confirmation of receipt)
- b. Which provision(s) of the GDPR (or national laws) does this concern?  
-
- c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.  
EDPB Guidelines 01/2022 (§57): “The EDPB considers as good practice for the controllers to confirm receipt of requests in writing, for example by sending e-mails (or information by post, if applicable) to the requesting persons confirming that their requests have been received [...].”
- d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?  
A potential explanation is that the data controller confuses the answer to the access request and the confirmation of receipt but these are different things, even if the answer to the access request is likely to be short / with limited data.
- e. What are differences that you have encountered between controllers in your Member State?  
NA
- f. 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?

No leading or best practices identified.

### Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

- 23) 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 4.15 in the questionnaire addressed to controllers.

#### Question 4.6:



- a. Name the issue(s) identified and briefly describe it.  
Data controllers (2 data controllers) do not seem to take the special characteristics of data subjects (e.g. age of data subjects, visual impairment of data subject etc.) for answering to access requests into account in their procedures.
- b. Which provision(s) of the GDPR (or national laws) does this concern?  
-
- c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.  
EDPB Guidelines 01/2022 (§128): The EDPB expects controllers to take into account the knowledge they have about their data subjects, for example if the majority of the data subjects are children, elderly people or people with disabilities.
- d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?  
A potential explanation is that the data controllers have not been confronted with such cases and did not anticipate their occurrence.
- e. What are differences that you have encountered between controllers in your Member State?  
NA
- f. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?  
Identify the specific characteristics of all the data subjects that may send an access request and implement procedures and formats of answers that are tailored to them.  
Communication around the issue (see points 34 and 37 here below).

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

No leading or best practices identified.

### **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

25) 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 5.18 in the questionnaire addressed to controllers.

#### **Question 5.7:**

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

A data controller does not provide a tailored list of recipients in the answer to the access request. The data controller explains that it provides a detailed privacy notice at collection point addressing the data sharing practice with various recipients within the organisation.

- b. Which provision(s) of the GDPR (or national laws) does this concern?  
-
- c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.
- EDPB Guidelines 01/2022 (§113): “In the context of an access request under Art. 15, any information on the processing available to the controller may therefore have to be updated and tailored for the processing operations actually carried out with regard to the data subject making the request. Thus, referring to the wording of its privacy policy would not be a sufficient way for the controller to give information required by Art. 15(1)(a) to (h) and (2) unless the « tailored and updated » information is the same as the information provided at the beginning of the processing.”
  - EDPB Guidelines 01/2022 (§130): As previously stated in the WP29 Guidelines on Transparency (with regard to the notion of “provide” in Art. 13 and 14 GDPR), the notion of “provide” entails that “the data subject must not have to actively search for information covered by these articles amongst other information, such as terms and conditions of use of a website or app”.
- d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?  
-
- e. What are differences that you have encountered between controllers in your Member State?  
NA
- f. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?  
Communication around the issue (see points 34 and 37 here below).

#### Question 5.8:

- a. Name the issue(s) identified and briefly describe it.  
A data controller does not provide tailored information about the storage period in the answer to the access request. The data controller explains that it provides a detailed privacy notice at collection point that includes information about the method of definition of the storage period.

- b. Which provision(s) of the GDPR (or national laws) does this concern?  
-
- c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.
- EDPB Guidelines 01/2022 (§113): “In the context of an access request under Art. 15, any information on the processing available to the controller may therefore have to be updated and tailored for the processing operations actually carried out with regard to the data subject making the request. Thus, referring to the wording of its privacy policy would not be a sufficient way for the controller to give information required by Art. 15(1)(a) to (h) and (2) unless the « tailored and updated » information is the same as the information provided at the beginning of the processing.”
  - EDPB Guidelines 01/2022 (§130): As previously stated in the WP29 Guidelines on Transparency (with regard to the notion of “provide” in Art. 13 and 14 GDPR), the notion of “provide” entails that “the data subject must not have to actively search for information covered by these articles amongst other information, such as terms and conditions of use of a website or app”.
- d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?  
-
- e. What are differences that you have encountered between controllers in your Member State?  
NA
- f. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?  
Communication around the issue (see points 34 and 37 here below).

#### Question 5.14 / 6.5:

- a. Name the issue(s) identified and briefly describe it.  
A data controller does not provide the entire video file where the requesting data subject appears but only one screenshot of the video. The controller explains that when only sending a screenshot, it does not have to blur the other individuals' faces for the entire video but only for one image (blurring of the other individuals' face is a requirement to protect the freedoms of others before releasing a copy of the personal data to the requester) which is time saving for its organisation.
- b. Which provision(s) of the GDPR (or national laws) does this concern?  
-
- c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.

The possible limitations of the data provided are limited and largely arise from Art. 15 (4) GDPR. Time saving / lack of means is not a reason for not providing the entire set of personal data.

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

-

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

NA

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

Communication around the issue (see points 34 and 37 here below).

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

A controller systematically informs the data subject about the applicable legal basis for each processing operation in its answers to the access requests.

### Section on “LIMITATIONS OF ACCESS REQUESTS”

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

- 27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

#### Question 5.3:

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

A data controller asks the data subject to scope the DSAR to specifically address the concern he/she raises without informing the data subject about the processing operations that could concern the data subject.

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

-

- c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.

EDPB Guidelines 01/2022 (§35 b)). The EDPB expects controllers to inform the data subject about the relevant processing operations so they can make a choice/scope their request based on their interests.

- d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?  
-
- e. What are differences that you have encountered between controllers in your Member State?  
NA
- f. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?  
Communication around the issue (see points 34 and 37 here below).

### Question 5.3:

- a. Name the issue(s) identified and briefly describe it.  
A data controller asks the data subject to provide the rationale relating to its access request.
- b. Which provision(s) of the GDPR (or national laws) does this concern?  
-
- c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.  
EDPB Guidelines 01/2022 (§167): “Data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Art. 15 GDPR are met the purposes behind the request should be regarded as irrelevant.”
- d. Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?  
-
- e. What are differences that you have encountered between controllers in your Member State?  
NA
- f. What are possible solutions to this issue, for the responding controllers and/or the participating SAs (e.g. follow-up actions)?  
Communication around the issue (see points 34 and 37 here below).

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

No leading or best practices of the controllers identified in the answers received.

## Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, “size” of the controller, etc.):

One of the data controllers says that, from its point of view, the guidelines are of less use for its organisation and may be applicable for large data processing activities or for contractual and legitimate interest legal basis.

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

The following topics appear to be less implemented by controllers:

- Tailoring the information depending on who makes the request and what the scope of the request is.  
Some of the controllers make reference to the privacy notice in their answers to access requests without being more precise regarding the specific case of the data subject sending an access request, for example regarding information about the recipients and the retention periods. This does not comply with the expectations of the EDPB Guidelines 01/2022 §113 (“Other types of information, such as the information on recipients, on categories and on the source of the data may vary depending on who makes the request and what the scope of the request is.”).
- Specification of the information as per the purposes according to Art. 15(1)(a).  
Some of the controllers do not precise to which purpose(s) the data category(ies) is (are) linked but present this two information separately. This does not comply with the expectations of the EDPB Guidelines 01/2022 §114 (“If the processing is carried out for several purposes, the controller has to clarify which data or which categories of data are processed for which purpose(s).”)

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees' right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF?

If yes, please provide the date, link to the guidance, and a short description of the guidance.

In April 2024 the CNPD published a general guidance on the right of access. This guidance, made of a written description and a video aimed at a large public, focuses on the essential points of the right of access (what type of information a data subject can request, how to exercise the right, how the information should be provided, the time limit to be respected, the price of the copy). 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).

The link to this guidance can be found here after: <https://cnpd.public.lu/fr/particuliers/vos-droits/droit-acces.html> (FR) and here after <https://cnpd.public.lu/en/particuliers/vos-droits/droit-acces.html> (EN).

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

Apart from the element described under point 32, the CNPD has been taking action to prompt data controllers to respect the provisions of the GDPR, national laws and the EDPB Guidelines 01/2022 through different levers:

- Investigations resulting in fines and the request to follow remedial actions
- 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 of access (<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 of access 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>)).

34) **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).



Not applicable – the CNPD proposed an open anonymous questionnaire: therefore it cannot identify / contact the data controllers.

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Very often

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Not applicable: until now, no decisions have been made relating to the right of access since the publication of the guidelines. Other decisions have been made relating to other data subject's rights, but these guidelines were not applicable in these cases.

37) 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 content of EDPB Guidelines 01/2022 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: No (not planned at this stage)
- ii. Online or remote training sessions: Yes. Integration of the feedback of the CEF in the coming training sessions provided by the CNPD.
- iii. Conferences organised: Communication of the results of the CEF when the European report will be published (on the CNPD website, through conferences...)
- iv. 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 (which can be the right of access) 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 their choices made. The CNPD acts as moderator and mediator of this meeting. The topic of the right of access will probably be used during one of the next workshops.

b. No: -

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes: Yes. Awareness raising could be more 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 33) here above) that uses easily understandable language and practical cases and is aimed at small/medium sized organisation but also at individuals.

b. No: -



# MT SA

Office of the Information and Data Protection Commissioner

## 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 <sup>36</sup>:
- d. Ongoing investigation:

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

- Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? **No**
- Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. **No**
- 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 access in practice. Based on these results this Office is internally considering to provide more information on its portal targeted to better help organisations respond to data access requests.

3) For all SAs: 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) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.

a) 1.1, 1.2 1, 4.6, 4.10, 4.11, 5.7, 6.3,

b) No questions have been amended.

5) For all SAs: 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 etc.)?

**No other comments/remarks**

## Part I – Some numbers on the controllers addressed

---

<sup>36</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

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/to your questions.

16

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: Please select one or more answers.*

- a. Public sector:
- b. Private sector: 16

10) Please specify the category<sup>37</sup> of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers*

- a. Micro enterprise: 1
- b. Small enterprise: 1
- c. Medium-sized enterprise: 5
- d. Large enterprise (more than 250 employees): 9
- 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) Please specify the nature of the (business) activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. education sector:
- b. health sector: 1
- c. social sector:
- d. insurance sector: 2
- e. finance sector: 3
- f. IT sector:
- g. retail sector: 1
- h. logistics sector:
- i. public transportation:

---

<sup>37</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- j. telecommunications: 1
- k. postal services:
- l. advertising sector:
- m. marketing services:
- n. entertainment sector: 3
- 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
- u. other (please specify): 4

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. customers: 15
- b. potential customers: 11
- c. employees: 13
- d. job applicants: 10
- e. children:
- f. vulnerable adults: 1
- g. patients: 1
- h. citizens (for public sector): 1
- i. applicants (for public services): 1
- j. recipients (for postal services): 1
- k. other (please specify): 2

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. Less than 100: 1
- b. 100 - 200: 1
- c. 201 - 500: 1
- d. 501 - 2,000: 2
- e. 2,001 - 10,000:
- f. 10,001 - 50,000: 2
- g. 50,001 - 100,000: 1
- h. 100,001 - 1,000,000: 5
- i. 1,000,001 - 10,000,000: 3
- j. More than 10,000,000:

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? *Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.*

- a. Contact data: 15

- b. Payment data: 14
- c. Identification data: 15
- d. Sensitive data within the meaning of Art. 9 GDPR: 7
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR: 2
- f. Other (please specify): 3

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. 0 request: 5
- b. 1-10 requests: 5
- c. 11-25 requests: 1
- d. 26-50 requests: 1
- e. 51-100 requests: 1
- f. 101-150 requests:
- g. 151-200 requests:
- h. 201-500 requests: 2
- i. 501-10,000 requests: 1
- j. >10,000 requests: 1
- k. No information:

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

No such difference was identified

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 5
- b. >0–25%:
- c. 26–50% requests: 2
- d. 51–75% requests: 1
- e. 76–100% requests: 8
- f. No information:

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No such difference was identified.

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 5
- b. 0-25% requests: 4
- c. 26–50% requests: 1
- d. 51–75% requests: 1
- e. 76–100% requests: 6
- f. No information:

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No such difference was identified.

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 5
- b. >0–25%: 4
- c. 26–50% requests: 1
- d. 51–75% requests: 1
- e. 76–100% requests: 6
- f. No information:

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No such difference was identified

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 in the questionnaire for controllers:

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

No such issues were identified

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

Not applicable

- c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.

Not applicable

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

Not applicable

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

Not all controllers have a 'Policy' which provides guidance on handling and responding to right of access requests received from data subjects in accordance with article 15. Out of the controllers who have such a 'Policy' in place, not all subject it to a periodic review.

Not all controllers document requests for access, including when the information was requested, what was requested and when the data was provided.

Not all controllers forward the right of access requests received, to their DPOs.

Not all controllers ensure that all requests are stored in a secure ticketing system which is only accessible to the staff strictly concerned.

With regards to storage of information on access requests, retention periods vary, some controllers retain it for 3 years, others for 5 years, others for 6 years and others for 10 years, all from when the request is deemed to be satisfied. Other controllers on the other hand delete the information sent after 30 days and then retain the record indefinitely

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

Not applicable

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

Yes, a best practice worth mentioning is the sending of personal data relating to an access request in an encrypted format with relevant passwords sent through a separate manner.

## **Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

- 21) 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 3.4 in the questionnaire addressed to controllers.

No particular issues or challenges were identified. However the following differences are noticed in the manner requests for access are handled:

Not all controllers acknowledge receipt of the right of access request clearly informing the data subject of the procedure they will be following.

Not all controllers accept access requests through a variety of input channels. Similarly there are controllers who only offer email as an output channel.

Some controllers, upon receipt of what is deemed to be an excessive request a fee.

Upon request of what is deemed to be a "non-standard" request for access, there are controllers who involve their internal/external legal consultants.

Not all controllers have a self-service tool in place which enables data subjects to possibly download their personal data themselves

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

Yes, leading practices worth mentioning are the following:

When a response is provided via email this is done through a secure link which in itself includes a link to the company's privacy notice.

Controllers provide their employees with regular training sessions in order to enable them to immediately recognize a request for access and thus forward it to the departments concerned for the necessary handling with undue delay.

### **Section on "IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR"**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

23) 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 4.15 in the questionnaire addressed to controllers.

No such issues or challenges were identified. However the following differences were identified:

Whilst the majority of controllers specify the fact that all contact information to request access is to be found in the respective privacy policy, only very few controllers provide the same information also directly on their website.

Not all controllers distinguish between requests for access from members of staff/employees and requests from other data subjects.

Not all controllers are equally flexible when it comes to the input channels, in that some ask the data subjects to redirect their request through the officially recognised channels, rather than referring it themselves to the unit concerned. The same applies to the requirements as to the form of the requests for access. Whilst some controllers do not request any specific requirements, others put the request on hold until all the requirements are satisfied.

The forms in which the data is provided by controllers vary. There are those who provide it in any means be it in writing or electronically and there are those who provide it solely electronically. When provided electronically the format ranges between PDF, Excel, MP3, CD/DVD, Zip, CSV.

Even the forms of identification vary. There are controllers who have one established form or identification whereas there are others who have a different method of identification depending on the input channel. There are some controllers who ensure the definite identification of the data subject by requesting the presentation of a valid photo ID. There are controllers who ensure the definitive identification of the data subject by merely comparing the information provided with what they have on their records.

There are controllers who do not respond to access requests submitted via third parties. Among those who do respond to such access requests, there are controllers who not only send the information to the third party but also to the data subject himself.

With reference to the measures taken to ensure that requests for access are answered within one month of receipt, the majority of controllers have a strict procedure in place. There are controllers, however who do not have such a procedure in place and instead just handle the SAR immediately.

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

Yes, two practices worth mentioning concern the measures taken to ensure that requests for access are answered as expeditiously as possible:

An internal deadline of 27/28 days, to ensure that the one calendar month deadline is always met.

Sending an internal alert notification after 14 days of receipt of the request., followed by a second alert notification after 3 weeks and finally followed by a 3rd alert notification alert 3 day before the deadline.

### **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

25) 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 5.18 in the questionnaire addressed to controllers.

An issue identified in this group of questions concerns the number of times data subjects were asked by controllers to clarify their request for information. It is interesting to note that most controllers do not have any data or specific record available on this point, in that they keep no track of such field.

The following differences were identified:



Insofar as the granting of access to non-textual personal data is concerned, whilst the majority of controllers use Share Point, MP3/4 some of which are sent via a unique link which is password, protected, email using end to end encryption, other software, encrypted USB stick as the preferred communication channel. Meeting with the data subject in person and providing access there and then (differences in Q 5.13 - to rewrite this point and continue looking for differences in same question)

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

A best practice worth sharing concerns the manner in which information is provided to the data subject. Rather than merely providing the data subject with copies, a zip file containing several documents is provided. These are uniquely tagged and sub divided into different categories of data. Furthermore a covering letter with a detailed list of what each document contains is provided.

### **Section on “LIMITATIONS OF ACCESS REQUESTS”**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

One particular issues identified is that a number of controllers do not keep record of the number of access requests in which the information provided to the data subject was limited due to third party rights. The same applies to the total number of access requests considered to be manifestly unfounded or excessive.

The following differences were identified:

Whereas as a general rule, most controllers specify that they provide full disclosure of all data relating to the data subject unless restrictions apply, one controller specifically mentions that the internal communication about its customers and employees is not provided. Another controller mentions backups and duplicates as data which is not provided and specifies that the data subject isn't informed about the decision to leave out that personal data.

Whilst the majority of controllers specify that they consider an access request as manifestly unfounded or excessive if repetitive one controller goes deeper and specifies the following scenarios as amounting to such a request:

- If it is sufficiently clear that the individual has no real intention to exercise this right but is ultimately after some form of benefit,
- The request is malicious in intent and is used to harass the company with no real purposes other than to cause disruption,
- The request makes unsubstantiated accusations against the Company or specific employees.

Other differences are noted in so far as the fee is concerned. Not all controllers charge a fee. Out of those who charge a fee some base it on the administrative costs incurred for complying with the request.

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

A best practice worth sharing concerns the reply provided in the event of a frequent request which is a repeat of a previously answered request. One particular controller doesn't merely refuse to comply but provides the link to what was priorly shared.

### Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

No further comments to the ones already expressed in the above answers.

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, "size" of the controller, etc.):

No further comments.

31) In your opinion, which **topics concerning the right of access** or which parts of **the EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

From the feedback received, there are no topics concerning the right of access with particular reference to the EDPB Guidelines which aren't known or not well implemented. The only issues of concern which emerged are the lack of statistics by some controllers when it comes to the following:

- number of access requests in which the information provided to the data subject was limited due to third party rights,
- number of access requests considered to be manifestly unfounded or excessive,
- number of times data subjects were asked by controllers to clarify their request for information.

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees' right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF?

If yes, please provide the date, link to the guidance, and a short description of the guidance.

Yes, IDPC has published such guidance on its website in the form of factsheets. One factsheet is generic in nature and targeted towards the data subject. It explains that 'right of access' is one of the rights found in Chapter 3 of the GDPR and provides a brief explanation on how it can be exercised. The other factsheet is targeted more towards the data controller, providing a brief explanation on the implications of this right and giving insight on what a controller should do upon receipt of a right of access request. They were both published prior to the launch of the CEF and can be found via these links:

<https://idpc.org.mt/for-individuals/your-rights/>

<https://idpc.org.mt/for-individuals/guidance-on-the-right-of-access/>

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

Yes, actions towards controllers concerning the right of access were taken prior to the launch of the current CEF. These actions have been taking place, even before the GDPR came into force. They take the form of an investigation following the lodging of a complaint by the data subject alleging a breach of article 15 by the controller. When these investigations establish a breach of article 15 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 how restricting the right of access was a necessary measure he is ordered to comply with the right of access request after having redacted any personal data pertaining to third parties. If it is established that the controller failed to provide the data subject with all the information in relation to the processing including a copy of all the personal data undergoing processing, the controller is ordered to provide such data, taking into account the rights and freedoms of others. Some examples of the actions taken and outcome of these actions can be found via the following links:

[https://idpc.org.mt/wp-content/uploads/2024/01/CDP\\_COMP\\_885\\_2023.pdf](https://idpc.org.mt/wp-content/uploads/2024/01/CDP_COMP_885_2023.pdf)

[https://idpc.org.mt/wp-content/uploads/2023/12/CDP\\_COMP\\_589\\_2023.pdf](https://idpc.org.mt/wp-content/uploads/2023/12/CDP_COMP_589_2023.pdf)

34) **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 particularly the fact that no significant problems could be identified, there isn't any specific action towards the controllers contacted currently being planned. However more information targeted towards controllers on our portal and possibly other communication methods is considered.

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Very often

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Sometimes

37) 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 content of EDPB Guidelines 01/2022 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:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes:

b. No: **No**

## PL SA

Urząd Ochrony Danych Osobowych (Personal Data Protection Office)

### **Part I - Statistics on the Controllers Addressed.**

The supervisory authority has made the survey on how to implement the right of access available on its own website, so that any controller visiting the authority's website could freely access the survey. At the same time, the supervisory authority also sent the survey directly to one hundred controllers from different sectors, i.e. from both the private and public sectors, with a request to complete the survey by August 31, 2024. The same model questionnaire was used for each controller. The answers provided by the controllers were anonymous.

Seven responses were given, with four respondents representing controllers from the private sector and three from the public sector. The number of employees they employ ranges from 1 to 550. The controllers represent entities from: the financial sector, public transportation, utility/infrastructure delivery services (e.g., energy), and consulting and industry training activities.

Classified controllers authority themselves as: branch of a foreign entrepreneur (2), administrative body/agency/government (2), state-owned company, local government, micro-enterprise.

The most common categories of data subjects covered by the respondents' main processing activities were: customers, potential customers, employees, job applicants. Only one controller indicated that, in addition to those indicated, it also processes data of children and vulnerable adults (a controller from the public transportation sector).

The number of persons covered by the processing is approximately 3,301,200. The number of persons processed by each controller ranges from 200 (the smallest number of persons processed) to 1,300,000 (the highest number of persons processed), with the highest values in this regard for controllers in the public transportation sector. The data processed by type usually includes contact data, identification data, and payment data. The last category of data is processed by both controllers from the financial sector and the public transportation sector. Controllers from the finance sector additionally process employment data and data on the credit agreements concluded by these individuals.

As for personal data from Article 9 GDPR, health data are processed by controllers from the public transportation sector (to the extent of granting fares reduced) and providers of public utilities (e.g., information that a person living with an electricity service recipient is using life-saving equipment).

Processing of Article 10 GDPR data does not occur among the respondents, and only the controller from the public transportation sector indicated that it processes criminal record data,

but did not elaborate on which data subjects it processes this information (however, it can be assumed that this refers to applicants for employment with the controller).

Requests for data access under Article 15 of the GDPR in 2023 were not common among survey respondents, with a total of 34 requests per seven controllers, which is approximately less than 5 requests per controller for the entire calendar year.

Controllers in the utility supply (energy) and public transportation sectors indicated that they had 20 and 11 data access requests in 2023, respectively, and these accounted for 15% and 46% of all data protection requests. Four controllers indicated that they did not receive a single data access request last year, and one indicated that the number of requests was “negligible” and accounted for less than 0.01% of total requests. In contrast, where the right of access was exercised, almost all requests for the right of access included requests to obtain inspection and control or copies of personal data, and requests to access to information on basic processing activities (90-100% of requests).

## **Part II – Substantive issues concerning the level of compliance of controllers' activities.**

### **Section 'DOCUMENTATION OF COMPLIANCE WITH ACCESS REQUESTS'**

As a rule, the controllers covered by the survey have established internal procedures for processing requests for access to data and documenting the actions taken in this regard (regarding 2.1. of the survey), e.g. the process is regulated by the Information Security Policy (ISP).

In case of three respondents, it is also a rule that the procedure for processing requests is attended by employees with authorization to access record systems, and requests are initially analyzed from the formal point of view (the identity of the applicant is checked). At various stages of request review, i.e., in preliminary assessments and in drafting a response to the request, the Data Protection Officer is involved. None of the respondents declared that they do not have a DPO in their organizational structure. Requests for access to data are recorded in a variety of ways

- either in systems accessed by employees with access rights, or in email inboxes dedicated to the collection of requests and their processing by designated employee(s).

The retention periods for requests for access from data subjects and related correspondence, including responses, most often depend on the duration of the contract associated with the data subject, as well as the possible assertion of claims under the contracts. In addition, the Ordinance of the Minister of Culture and National Heritage of October 20, 2015 on the classification and qualification of documentation, the transfer of archival materials to state archives and the destruction of non-archival documentation, as well as the Code of Administrative Procedure, have been indicated as legal bases for the storage of such data by individual controllers.

### **Section "PROCEDURE FOR PROCESSING REQUESTS FOR ACCESS"**

Regarding questions related to the process of access requests, the answers provided show that the most common channels for data subjects to submit requests are electronic correspondence (email), with controllers providing for the possibility of submitting requests by letter (snail mail), verbally (at the controller's premises), by phone and through on-line forms. The methods of submitting a request under Article 15 of the GDPR are usually indicated in the information clause provided by the data controller on its website. Employees of the data controller also have the opportunity to submit requests through internal electronic communication channels (e.g., by submitting a request on an electronic form to the DPO).

Participation in the processing of requests usually involves designated employees with a supporting role of the DPO, as well as lawyers and a compliance officer. The supervisory role of the DPO in the process of responding to the request is indicated, i.e., the DPO controls the correctness and timeliness of processing requests. Storage and processing of access requests is decentralized, kept in a separate record of access requests. Responses are usually provided through the same channel by which they were transmitted to the controller, unless the requester requests a response in another form.

In their responses, data controllers indicated that, in general, the exercise of the right of access to data is already covered by digitization. Often, digitization in this regard is already provided for at the design stage of individual digital tools. Registers of processing activities, on the other hand, are kept on an ongoing basis, and in the case of individual respondents not less than once per calendar year. On the other hand, small data controllers (which are micro-enterprises), who declare a lack of financial resources for the implementation of specialized IT systems, use systems available online, guided in their selection also by the fact that these solutions allow handling data access requests at the same time.

The overwhelming majority of respondents indicated that they systematically control the processing of requests for access under Article 15 of the GDPR, i.e. the number of access requests received, the date of receipt, the relevant status of processing requests. Only one of the controllers stated that it does not carry out inspections of requests at all. Those who carry out these activities indicate that the process of controlling the process of examining requests usually involves the DPO (or entire teams of DPOs), as well as employees of individual organizational units. In the case of natural persons conducting business activity, the control is carried out by entrepreneurs on their own.

Acknowledgements of receipt of access requests are not sent to the applicant. Confirmation of receipt of the request takes place only in special situations resulting, e.g. from the fact that the request was submitted by the data subject in person and the person wants to receive confirmation of this action. If the data subject submits a request using other than the generally provided communication channels provided by the controller, which, as indicated by the respondents, is a rare situation, because the number of contact channels is wide, do not result in leaving the request without consideration. In such a case, the request is forwarded within the organizational structure of the controllers in accordance with the jurisdiction in order to give it further action.



The respondents indicated that they generally do not provide for formal requirements as to the request itself *sensu stricto*, but the only condition for accepting the request for processing is usually confirmation (authorization) of the identity of the applicant.

Answers are usually given in pdf format, and less often in other extensions such as doc, xls. Answers are often given by e-mail.

The following data security measures are indicated as data security measures applicable to granting access in accordance with Article 15 of the GDPR (item 4.5 of the survey): sending responses by encrypted e-mail, keeping the software (including CMS and plug-ins) up to date, the website and requests used in the process are protected against the main known attacks. It has also been indicated as security measures that the request for digital access can be completed by e-mail protected by end-to-end encryption, the request for digital access can be completed by other means protected by encryption such as *end to end*, persons shall be identified by a known and up-to-date electronic identification system. In addition, individuals are identified through an existing account using their customary method of authentication or identification of the service, by means of a known and current electronic identification system, or the individual is otherwise authenticated to access the response to his or her request. Controllers also apply protection against SQL code injection, against DDoS attacks and protection against cross-site scripting.

## **Section "IMPLEMENTATION OF GENERAL REQUIREMENTS UNDER ARTICLE 12 GDPR"**

An analysis of the answers provided shows that when responding to a request for access to data in the light of the transparency requirements set out in Article 12(1), first sentence, of the GDPR, controllers do not implement a special procedure in relation to persons due to their specific personal characteristics, such as age, poor eyesight, etc. However, individual respondents give answers in simple and understandable language. Only one of the respondents indicated that when exercising the right of access to data, they apply the provisions of the Act of 19 July 2019 on ensuring accessibility to persons with special needs. Two respondents indicated that they do not follow a special procedure due to the fact that they usually do not have knowledge of the special needs of the applicants.

It is worth noting that none of the controllers received a request for access to oral information (e.g. provided over the phone) in 2023.

On the other hand, the identification of the data subject exercising the right of access to data is carried out by some controllers in such a way that if the person submits a telephone request, he or she is subject to authorization by the PESEL - personal identification number (the last 8 digits). If a person submits a request by e-mail, he or she are asked to provide data such as the contractor's number. If a person submits a request via eBOK, he or she are obliged to log in to his or her account. If the request is submitted in writing, the correspondence is also subject to verification in order to identify the person – however, it has not been precisely indicated how this identification is carried out. In the case of a personal visit to the controller's office, the basis for verification is the inspection of the identity document. In the case of



electronic documents, the signature (<https://www.gov.pl/web/gov/podpiszdokument-elektronicznie-wykorzystaj-podpis-zaufany>) is verified. Verification also takes place in such a way that the controller compares the data from the request of the data subject with the data already held.

It was also indicated that the confirmation of identity consists in providing the name and surname of the applicant and in verifying the identity by asking the person one, or if possible due to the scope of information processed about this person – two questions about who this person is (e.g. PESEL number, address of residence, e-mail address provided for contact, customer identification number) and, for example, what services resulting from the contract with the controller he or she uses.

Except for controllers who have never received requests for access to data submitted by third parties, they are responded to when the third party has the right to act on behalf of the data subject. This applies in particular to statutory representatives (legal guardians) and attorneys who demonstrate authorization to do so.

The respondents indicated that there are rare situations in which the identity of the person submitting the request for access to data is questionable, but if such a doubt arises, it is caused by the fact that the applicant is not able to provide basic data identifying him or her, e.g. an individual customer number, if he or she has one due to the contract being performed.

The respondents' answers regarding the implementation deadline show that in order to ensure an immediate response to requests for access in accordance with Article 15 of the GDPR, the flow of information between the individual departments of the entrepreneur involved and the participation of the DPO as a coordinator and controller of activities aimed at responding to the request are of great importance.

### **Section "CONTENT OF REQUESTS FOR ACCESS AND RESPONSES PURSUANT TO ART. 15 GDPR"**

The answers provided show that the controllers, unless the scope of the requested data has been strictly indicated in the request, provide answers with regard to the full (all) personal data held. Information on the recipients of personal data is provided in information clauses during the collection of data, however, when the data subject requests this information, it is made available to him or her.

It is rare for respondents to process pseudonymised data, but when the request concerns such data, their connection to the identity of the applicant occurs after the data have been restored to their original form. A demand for clarification of a request for access to data is most often the result of doubts as to the identity of the applicant – less often when the precise scope of data to which the request relates has not been indicated.

Of the respondents, only two controllers asked data subjects to explain their request for information.

Regarding the layered approach to providing feedback to the data subject so as to avoid being overwhelmed by shared messages, controllers do not use such an approach when sharing data within the scope of the request. The exception are controllers who make data available in the form of tables detailing the categories of processed data (one such case).

With regard to the retention period in accordance with Article 15(1)(d) of the GDPR, controllers will normally provide the data subject with information on the duration of the processing for each of the processing purposes separately. It is not a common practice to indicate the data retention period for each type of operation or category of data, such a solution was declared by only two respondents. Despite this, in 2023, data subjects objected to the content of the information provided pursuant to Article 15(1)(a) to (h), Article 15(2) of the GDPR or only commented on the incompleteness of the information provided in the case of one of the controllers.

The analysed lists show that copies of data are made available to the data subject in various forms, but the most commonly used should be an extract from the database, and to a lesser extent full or partial documents containing personal data, transcripts, communication to which the data relate. The preparation of a specific compilation for a specific proposal should be considered the least common.

Access to documents containing personal data is limited by controllers to the extent required by applicable law, e.g. due to the protection of classified information, data covered by trade secrets or due to the protection of privacy of third parties. Some controllers have adopted the principle that they do not provide documents containing personal data of natural persons other than the applicant. Only few of them anonymize such data before exercising the right of access.

Two controllers stated that they provide access to non-text personal data by providing access to CCTV recordings or playing back a telephone conversation, and they perform these activities only when the data subject appears at the controller's headquarters in person and it is possible to verify his or her identity.

## **Section "RESTRICTIONS ON ACCESS REQUESTS"**

With regard to situations in which access to data is denied to the requester, two basic reasons are indicated: the lack of possession of the applicant's data in the controller's resources and the inability to confirm the identity of the person requesting access to data. The respondents did not indicate any other circumstances. In cases of refusal to exercise the right, the data subjects are informed by the controllers about the refusal and its grounds.

With regard to data that are not provided to applicants in connection with an access request, respondents indicated that they do not usually provide data constituting classified information and "other legally protected information", such as information constituting trade secrets. Information the disclosure of which could adversely affect the functioning of the security system of information processed by the controller is also not made available. One of the respondents indicated that he or she does not share CCTV recordings involving third parties,

while another indicated that he or she provides the right to access all data held. The above indicates that the scope and type of data made available depends on the interpretation of the controller.

The approach to sharing the data of persons who process personal data within the controller is not uniform. Individual controllers categorically indicate that they do not make such data available under any circumstances, others make it available when the applicant requests such information in an explicit manner, and still other controllers share only the data of the DPO and persons coordinating the system by means of which the data is processed.

In 2023, a total of 10 requests were found for which access to data was restricted due to the rights of third parties, with only two controllers representing the public sector experiencing such a situation. Controllers representing the private sector indicated that they did not have such cases last year.

As indicated by the respondents, in their opinion, the request is clearly unjustified (or excessive) within the meaning of Article 12(5) of the GDPR, when the applicant is not able to confirm he or she identity, the appropriate power of attorney to act on behalf of the applicant has not been presented, the request has been submitted to an extent exceeding the rights of the GDPR, it is not for information purposes, the controller has imposed a fee for the handling of the request and has informed the data subject, but the person has not paid the fee, the person's requests are manifestly unjustified or excessive, in particular due to their constant nature, the personal data are not processed by the controller.

### **Part III – Impressions on the level of awareness and compliance**

The level of knowledge of data controllers and their compliance with the provisions of the GDPR in the provision of access to data should be assessed as high, however, it should be borne in mind that the number of controllers who took part in the survey is not large, which may affect the measurability of the results obtained. It should be noted that all controllers involved have declared that they are familiar with the content of the EDPB Guidelines 01/2022 on data subject rights – Right of access (version 2.0 adopted by the European Data Protection Board on 28 March 2023).

## PT SA

Comissão Nacional de Proteção de Dados - CNPD

### 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<sup>38</sup>: **Yes**
  - d. Ongoing investigation:
  
- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),
  - Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)? -
  - Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available. -
  - If not, will this fact finding activity impact your enforcement activities and if yes, how?  
-
  
- 3) For all SAs: 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) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.  
**a) We excluded question 1 because our action was addressed towards controllers from the private sector**  
**b) We didn't amended any question**
  
- 5) For all SAs: 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 etc.)?  
**We had many open questions that made processing the answers very complex**  
**Some controllers responded to some questions with documents with many pages and documents**

---

<sup>38</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

## Part I – Some numbers on the controllers addressed

6) How many controllers did you contact?

11

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/to your questions.

11

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?

There's no 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: Please select one or more answers.*

- a. Public sector: 0
- b. Private sector: 11

10) Please specify the category<sup>39</sup> of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers*

- a. Micro enterprise: 1
- b. Small enterprise:
- c. Medium-sized enterprise: 1
- d. Large enterprise (more than 250 employees): 9
- 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): [If considered relevant, please specify the replies received by controllers]

11) Please specify the nature of the (business) activity of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. education sector:
- b. health sector: 2
- c. social sector:
- d. insurance sector:
- e. finance sector: 2
- f. IT sector:
- g. retail sector: 2

---

<sup>39</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- h. logistics sector:
- i. public transportation:
- j. telecommunications: 3
- 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. other (please specify): 2 controllers from real state sector

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. customers:
- b. potential customers:
- c. employees:
- d. job applicants:
- e. children:
- f. vulnerable adults:
- g. patients:
- h. citizens (for public sector):
- i. applicants (for public services):
- j. recipients (for postal services):
- k. other (please specify): In the questionnaire, the number of data subjects per category was not asked, therefore it was not collected.

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. *Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.*

- a. Less than 100:
- b. 100 - 200:
- c. 201 - 500: 1
- d. 501 - 2,000:
- e. 2,001 - 10,000: 1
- f. 10,001 - 50,000:
- g. 50,001 - 100,000:
- h. 100,001 - 1,000,000:
- i. 1,000,001 - 10,000,000: 7
- j. More than 10,000,000: 1

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? *Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.*

- a. Contact data: 11
- b. Payment data: 11
- c. Identification data: 11
- d. Sensitive data within the meaning of Art. 9 GDPR: 3
- e. Data of a highly personal nature within the meaning of Art. 10 GDPR: 2
- f. Other (please specify):
  - a) Financial data
  - b) Professional data
  - c) Digital channels navigation data
  - d) Data profiling
  - e) Household data
  - f) Education background data
  - g) Health Insurance and pensions data
  - h) Telecom traffic data
  - i) Contract data for products and services
  - j) Video surveillance data

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. 0 request: 1
- b. 1-10 requests: 3
- c. 11-25 requests: 2
- d. 26-50 requests:
- e. 51-100 requests: 1
- f. 101-150 requests:
- g. 151-200 requests:
- h. 201-500 requests: 2
- i. 501-10,000 requests: 1
- j. >10,000 requests: 1
- k. No information:

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

We identified a significant difference in the numbers; hence, we will try to understand the reasons following the responses we received. We have completely unexpected answers which in some cases may be related to their interpretation of the question.

One of the controllers from retail sector, mentioned that he received a total of 512235 access requests, which is much higher than the rest. The second and third highest number of access requests was 939 and 315 requests, both from health sector.

The other controller from the retail sector received a total of 16 access requests which we also consider a very low number considering the size of the company and the number of data subjects potentially affected by the treatments.

This could be one of the most important issues to investigate with controllers in the inspection actions that we will carry out later.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 7
- b. >0–25%:
- c. 26–50% requests: 1
- d. 51–75% requests: 1
- e. 76–100% requests: 1
- f. No information: 1

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

In general, controllers do not collect this data and do not process it, so it was complex for them to answer.

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 1
- b. 26–50% requests: 3
- c. 51–75% requests:
- d. 76–100% requests: 5
- e. No information: 2

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No we didn't any significant difference in the percentages of the responding controllers.

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? *Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.*

- a. None of the requests: 7
- b. >0–25%: 1
- c. 26–50% requests:
- d. 51–75% requests:
- e. 76–100% requests: 1
- f. No information: 2



18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No we didn't any significant difference in the percentages of the responding controllers.

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

19) 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 2.2 in the questionnaire for controllers:

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

- The main challenge for questions with open answers in which controllers could freely answer and still attach documents, was the appreciation of a large volume of information to understand the processes for documenting compliance with requests. It was really very complex and challenging. Most controllers refer their responses to attached documents, to the privacy policies published on their websites, of which only a small part concerns the right of access. The analysis of the information transmitted will be done in more detail later.
- The companies we chose for this action, due to their size, have mostly predefined processes for handling requests for access, different input channels, different organizational units involved and external entities.
- There are very different answers on the retention period of data relating to access requests, some of which indicate a lack of information from controllers

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

Art. 15 GDPR

Art. 21 n. 3 of Portuguese national law (Law No. 58/2019 of August 8)

c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.

-

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

a) The questionnaire was designed to allow controllers to respond very freely. The lengthy and the level of detail of the questionnaire, with answers in free text, and the need to assess additional documents made it a greater challenge.

b) The answers on the period of retention of information on requests for access by data subjects may have been confused with the period of retention of data of the data subjects themselves. From the responses received, we understand that this misunderstanding may have occurred

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

- a) We have controllers that document very well the procedures related to requests for access to personal data and, on the other hand, we have others that do not give due importance.
- b) Some controllers are able to identify very clearly the information flows from the moment a request for access enters, until the moment of their satisfaction and conservation of the information.
- c) Few controllers have identified the procedure in cases of access requests by courts, police or other authorities.
- d) We have a company that did not receive any request for access in the year 2023, which was a surprise given the area of activity in which it is located.

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

- a) A detailed study shall be carried out for each undertaking on the importance of establishing effective and transparent procedures for the right of access.
- b) Carrying out targeted actions towards companies that appear to be poorly informed about the right of access of data subjects.
- c) Regarding the retention period, we consider that the controllers answered about the retention time of the personal data proper of the customers and not about the requests for access submitted. However, this issue will have to be investigated.

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

No there are not.

## Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

21) 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 3.4 in the questionnaire addressed to controllers.

It has been noted that some organisations do not have a designated DPO. Although this is not mandatory in this kind of situation. If cases of DPO designation it would make it easier to protect the data subjects rights. Some data controllers do not require delivery and read receipts for e-mails sent to data subjects, and therefore cannot guarantee that the reply sent is actually received and read by the data subject.

Provision of the national law: Art 13 of the national law implementing the GDPR (Law No. 58/2019 of August 8) in the national legal system.

If data controllers are not legally obliged to have a DPO, they prefer not to incur this cost, and this is reflected in the fact that there are companies that could provide more protection of citizens' rights if they had a DPO, but choose not to do so.

Possible solutions: The possible tightening of what constitutes large-scale processing of special categories of data, or even the obligation for the company to have a DPO for a certain number of clients, as is the case with the national law for the public sector, which defines that above a certain number of citizens who may be affected, the public entity is obliged to have a DPO.

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

No, there are not.

### **Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

23) 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 4.15 in the questionnaire addressed to controllers.

a) There are several references to previous issues to the procedures for processing access requests because some controllers had already described the procedures. Issues related to the functioning of the communication channels where data subjects can obtain information to exercise their right, included in the privacy policies, are not always easy to apprehend.

b) It appears that most controllers do not mention adequate measures to satisfy requests for access from holders with some type of disability or limitation, such as age, visual impairment, language comprehension, etc. (Art. 12 GDPB).

Potential explanation: Lack of awareness of the importance of these issues

Differences between controllers: Some do not have information on these topics because they do not process this data

Possible solutions: Investigate the concrete and precise reasons for us to create mechanisms of clarification and awareness of controllers.

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

a) Some controllers have implemented service processes adapted to meet the specific needs of holders, including contracting with a subcontractor to ensure that requests for sign language access are met.

b) In the particular case of a hospital, it is verified that in cases of cognitive limitations, or other type of disability, it privileges medical intermediation with the support of a third party to provide access to personal data.

### **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

25) 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 5.18 in the questionnaire addressed to controllers.

- a) Regarding the number of requests where it was necessary to request clarification of the solicit of the data subject, most controllers do not process this information.
- b) In situations where data subjects have objected to the content of the information received because it is incomplete, most controllers do not process this data.
- c) Some controllers do not clarify how they select the documents to provide access, nor do they guarantee that they take care to preserve the data of third parties that are in the documents delivered, other business secrets covered by confidentiality commitments.

Provision of the GDPR: Art. 15(1)(a) to (h) and Art. 15(2) GDPR

Potential explanation: They are not enlightened and aware to take measures to exclude excessive data from documents.

Differences between controllers: Some have very detailed information about access to non-text data such as images and video and others say nothing about it.

Possible solutions: Take action with controllers to clarify the importance of correcting procedures to document requests for access to personal data.

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

- a) With regard to voice data, in a call recording situation, there was the good practice of sending an audio file, by encrypted e-mail, with sms token message sent to the phone number of the data subject.
- b) Non-textual data, such as speech, can also be transcribed *ipsis verbis* for the data subject to read.

## **Section on “LIMITATIONS OF ACCESS REQUESTS”**

*The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.*

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

It should only be noted that it is unusual for there to be no requests for access to personal data that have been subject to an information restriction, and that there is no indication in the responses given by data controllers that there were any requests in 2023 that were considered manifestly unfounded or excessive.

A possible explanation for the low number of access requests reported by data controllers could be that citizens are not very aware of the rights that the GDPR aims to protect, which also explains why the reported access requests did not lead to refusals because they were manifestly unfounded or excessive. Possible solutions: it may be necessary to consider stepping up publicity activities, possibly by setting up enquiry hotlines open to citizens, which can make the public more aware of this European regulation, its content and the mechanisms that can be used to protect citizens' rights.

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

No, there are not.

### Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

PT SA directed this action at private sector controllers, so it only registers differences in relation to the size of the data processing carried out by each controller. We have a wide range of questions to look into after this action because, even in companies that are more organized in terms of procedures, with a DPO and a team dedicated to data protection matters, we find answers in certain areas that we have to investigate. The level of compliance as a rule is related to the volume of personal data processed and the categories of personal data processed. In the health sector, we have generally found a good level of awareness and compliance.

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, “size” of the controller, etc.):

Our overall impression of the level of awareness and understanding of the data controllers we consulted regarding the EDPB Guidelines 01/2022 on the right of access is favourable. The fact that we have chosen large companies with a high number of data processing operations and a high number of potential data subjects affected by their processing, allows us to conclude that the majority are aware of the guidelines.

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

Based on the results of this CEF the parts of the EDPB Guidelines 01/2022 on the right of access are the least-known or the least implemented by controllers are:

- a) Aim of the right of access, structure of article 15 GDPR and general principles
- b) Requests made via third parties / proxies
- c) Exercising the right of access through portals / channels provided by a third party

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees' right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF?

If yes, please provide the date, link to the guidance, and a short description of the guidance.

Since the entry into force of the GDPR, the following guidelines have been published and disseminated by the Portuguese SAS:

Guideline no. 1/2018 (02.10.2018)

Availability of personal data of students, teachers and other staff on the website of higher education institutions

Guideline no. 1/2019 (25.03.2019) on the processing of personal data in the context of electoral campaigns and political marketing

Directive/2019/2 (03.09.2019) on the processing of personal data in connection with intelligent electricity distribution networks

Directive/2022/1 (25.01.2022) on electronic direct marketing communications

Directive/2023/1 (10.01.2023) on organisational and security measures applicable to the processing of personal data

These are published on the website of the Portuguese SAS: <https://www.cnpd.pt/decisoes/diretrizes/>

Guidelines have also been developed and disseminated, among which the following stand out:

Guidelines (08.04.2020) on the use of technology to support distance learning

Guidelines (17.04.2020) on remote control in teleworking arrangements

Guidelines (19.05.2020) on the collection of student health data

Guidelines (21.05.2020) on distance learning in higher education

Guidance (23.05.2020) on remote control in teleworking arrangements

Guidance (13.11.2020) on the processing of personal health data regulated by Decree 8/2020 of 8 November

Directive (11.04.2023) on the incompatibility of the cumulation of EPD/RAI obligations

Directive (11.04.2023) on the supply of personal data processed in the context of administrative procedures

Directive (11.04.2023) on access to personal data held by public bodies as subcontractors

Directive (18.04.2023) on the publication on the Internet of the minutes of meetings of collegial bodies

Directive (18.04.2023) on the webcasting of meetings of local authority bodies

The guidelines of the European Data Protection Board and other national authorities relevant to the issue of the right of access, or others deemed relevant, are published on the website of the Portuguese SA.

All can be consulted at: <https://www.cnpd.pt/organizacoes/orientacoes-e-recomendacoes/>

**33) Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

No prior action was taken. We wanted the answers to be as realistic as possible, so no prior action was taken to ensure that the answers obtained reflect reality as much as possible.

**34) 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 measures that we are considering to undertake, to carry out initially is a more detailed investigation of each controller's procedures based on the replies received. The SA will decide on which controllers are to be subject to a very targeted inspection on the spot. A final decision will be taken for each controller and potentially corrective measures will be adopted, either orders and/or sanctions (reprimands and/or fines).

This CEF will continue throughout 2025.

**35) In general** (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Often.

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Often.

37) 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 content of EDPB Guidelines 01/2022 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:

b. Others: please specify: **Create FAQs**

c. No:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes: **Yes. Produce interactive material for an information campaign.**

b. No:



# NL SA

## Autoriteit Persoonsgegevens (AP)

### 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<sup>40</sup>:
  - d. Ongoing investigation:

- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question),

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

**No, it will not affect the AP's enforcement activities.**

- 3) For all SAs: 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.

**All questions were used. However, some additional yes/no questions were introduced to prevent meaningless answers**

- 4) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.

**Questions that focussed on merely access were broadened to include the immediate request for information. In practice, data subjects use the right for information and access in conjunction. Therefore, it did not make sense to limit the questions to the right to access.**

- 5) For all SAs: 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 etc.)?

**Many organizations indicate that the questionnaire was complex and long. Some questions were very technical in nature that smaller, less professional organizations had issues answering the questions. This led to some controllers quitting the questionnaire or giving answer that were not relevant to the questions posed.**

### Part I – Some numbers on the controllers addressed

---

<sup>40</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

6) How many controllers did you contact?

5570 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/to your questions.

252 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?

Filling out the questionnaire was on a voluntary basis and was sent to DPO's with the request to relay the questionnaire to their controllers. However, not all DPO information was kept up to date by DPO's leading to non-deliverables and no replies. Some organizations expressed that the questionnaire was complex or indicated that they were so small that the AP would not benefit from their responses. In addition, the AP asked DPOs to spread the questionnaire between their organizations. Some DPOs acted as external DPO and consolidated the answers of the organizations into one response.

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: Please select one or more answers.

a. Public sector:	136
b. Private sector:	116

10) Please specify the category<sup>41</sup> of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers

c. Micro enterprise:	14
d. Small enterprise:	44
e. Medium-sized enterprise:	35
f. Large enterprise (more than 250 employees):	49
g. Non-profit organisation:	36
h. Ministry:	9
i. Local authority:	35
j. Administrative authority/agency/office (e.g. job center):	4
k. School / university / educational institution:	20
l. Other (please specify):	6

11) Please specify the nature of the (business) activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

---

<sup>41</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

a. education sector:	22
b. health sector:	71
c. social sector:	21
d. insurance sector:	13
e. finance sector:	15
f. IT sector:	14
g. retail sector:	4
h. logistics sector:	1
i. public transportation:	1
j. telecommunications:	3
k. postal services:	0
l. advertising sector:	0
m. marketing services:	1
n. entertainment sector:	0
o. information / journalism sector:	2
p. scientific / historical research:	2
q. credit scoring agency:	0
r. public utility/infrastructure provider (e.g. energy):	4
s. housing industry:	2
t. manufacturing:	2
u. other (please specify):	74

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

a. customers:	130
b. potential customers:	52
c. employees:	185
d. job applicants:	82
e. children:	47
f. vulnerable adults:	48
g. patients:	655
h. citizens (for public sector):	57
i. applicants (for public services):	87
j. recipients (for postal services):	7
k. other (please specify):	30

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

a. Less than 100:	56
b. 100 - 200:	31

c. 201 - 500:	27
d. 501 - 2,000:	24
e. 2,001 - 10,000:	36
f. 10,001 - 50,000:	24
g. 50,001 - 100,000:	14
h. 100,001 - 1,000,000:	23
i. 1,000,001 - 10,000,000:	14
j. More than 10,000,000:	3

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.

a. Contact data:	224
b. Payment data:	120
c. Identification data:	162
d. Sensitive data within the meaning of Art. 9 GDPR:	133
e. Data of a highly personal nature within the meaning of Art. 10 GDPR:	44
f. Other (please specify):	32

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

a. 0 request:	134
b. 1-10 requests:	79
c. 11-25 requests:	18
d. 26-50 requests:	6
e. 51-100 requests:	3
f. 101-150 requests:	3
g. 151-200 requests:	2
h. 201-500 requests:	3
i. 501-10,000 requests:	4
j. >10,000 requests:	0
k. No information:	0

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

We have not identified any significance difference based on the amount of data subjects whose personal data are processed. The questionnaire was on a voluntary basis.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

a. None of the requests:	8
b. >0–25%:	24
c. 26–50% requests:	10
d. 51–75% requests:	10
e. 76–100% requests:	66
f. No information:	134

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

The questionnaire was sent out to be filled in on a voluntary basis to a limited and randomly selected group of controllers. Smaller organization struggled with the text of the questionnaire and found the questions to be less applicable to their organization. Some organizations asked if they were allowed to not fill in the questionnaire because their expectation was that their questions would not contribute enough to the CEF.

17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

a. None of the requests:	17
b. >0–25%:	20
c. 26–50% requests:	13
d. 51–75% requests:	6
e. 76–100% requests:	62
f. No information:	134

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

Over half of the responding controllers indicated that they did not receive any data subject request in 2023. Some stated that since the GDPR came into effect, they had never received any data subject requests.

18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

a. None of the requests:	52
b. >0–25%:	31
c. 26–50% requests:	8

d. 51–75% requests:	4
e. 76–100% requests:	23
f. No information:	134

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

No

## Part II – Substantive issues regarding controllers’ level of compliance

### Section on “DOCUMENTATION OF COMPLIANCE WITH REQUESTS FOR ACCESS”

- 19) 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 2.2 in the questionnaire for controllers:
- Name the issue(s) identified and briefly describe it.

#### Variation in retention periods for access requests

There’s no commonly used retention period for access requests. Some controllers have yet to determine a retention period, due to never have been confronted with a request. Some controllers try to connect to existing legislation to determine the retention period. For instance, tax law (mostly 7 years) or healthcare law (20 years). Government agencies base their retention period on the Archive act and retain documentation for 10 years. Retention periods range from 6 months to 20 years. Exceptions are that never delete documentation concerning data subject rights.

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

Article 15, 12, 5, 30 & 32 GDPR

- If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.
- Did you identify a potential explanation why this has been an issue for some or all of the responding controllers?

There are no guidelines nor any national legislation that prescribe how long information regarding data subject rights should be retained in what circumstances. Controllers have to decide and set retention periods themselves. Without these guidelines, some controllers may keep data for excessively long periods to avoid losing information they think might be needed for the future – whether for legal, business or regulatory reasons.

Furthermore, documentation might be stored in older systems or databases that may not have a built-in mechanism for automatically deleting or archiving data after a certain period. Alternatively, controllers might forget to set the retention period.

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

Controllers that are bound by sectoral legislation in the health care sector and public sector usually connect data retention periods of data subject right requests to the general period that is stated in that legislation. Controllers outside of those sectors either connect to retention periods in tax legislation or have set a period based on best guess.

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

#### **Retention periods in guidelines**

SA's and EDPB could set a standard retention period in guidelines in order to harmonise retention periods of data subject rights across controllers in the EU.

#### **Adopt data retention policy**

Controllers should adopt retention policy that outline how long various types of data will be stored. This also helps controllers get insight into which data is actually being processed in their organisation.

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

No

### **Section on “PROCESS FOR HANDLING REQUESTS FOR ACCESS”**

The questions here are the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

- 21) 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 3.4 in the questionnaire addressed to controllers.

- a. Issue(s)

30% of responding controllers do not have a pre-defined process for handling request for access. Being unprepared for an access request can lead to delays in handling said request and to incomplete responses.

Around 20% of responding controllers indicate that their DPO is responsible for handling data subject requests. This could interfere with the DPO's task of monitoring compliance with the GDPR. Only tasks that do not lead to conflict with the DPO's tasks should be assigned to a DPO.

One third of responding controllers indicate that they do not particularly consider the right of access when digitizing processes or integrating new digital tools. This could make retrieving and/or exporting personal data in order to comply to an access requests a difficult exercise. This also leads to challenges when complying to other data subject rights, for instance the right to be forgotten.

One third of responding controllers indicate that do not monitor or systematically control the handling of requests of access. This exposes controllers to the risk that some access requests are not handled or concluded too late. Of the remaining controllers that do monitor or control the handling of access requests, the AP observed that these controllers handled these

requests centrally either via a case handling system or other centralized process, for instance a designated department.

25% of controllers do not send confirmations of receipt of the request to data subjects. This can expose controllers to the risk that they do not respond within a month to the access request, since a clear starting point of the request is not registered. This also exposes controllers to the risk that a data subject will file a complaint with a SA or start litigation in court.

**b. Provision(s)?**

Article 5(b), 12, 15, 38(6), 39(1)(b) 25 GDPR

**c. Caselaw**

**d. Explanation?**

- Some controllers have never been confronted with an access request. This can be due to the specific sector the controllers are active in, not having to deal with consumers, patients, etc., only B2B interactions, or the size of the enterprise of a controller is limited/small.
- Smaller organizations do not have the means to have specialized privacy officers or are limited in personnel thereby combining multiple roles into one person/position.
- Even though awareness regarding personal data protection has increased greatly since the coming into effect of the GDPR, in some cases the focus of digitizing or integrating new software is set on improving primary business processes. not combined with improved compliance with GDPR standards.

Some controllers have never been confronted with an access request. This can be due to the specific sector the controllers are active in, not having to deal with consumers, patients, etc., only B2B interactions, or the size of the enterprise of a controller is limited/small.

Processing personal data and handling data subject request might not be a core process of a controller. In addition, the size of the controller and the sector in which the controller is active in might affect how structured the internal processes of a controller are, including the processing of personal data.

**e. Differences between controllers?**

Some controllers have not considered data subject requests in their processes and are unprepared, while others have an extensive procedure in place. This can be due to the sector a controller is active in or has taken steps to certify different processes in their organization.

**f. Solutions**

Even though it is advised to have the DPO involved in the process of handling data subject requests, this should be limited to consultation of the DPO. The actual handling and final responsibility of the process should be assigned to an executive or department as not to interfere with the DPO's independent position as the internal GDPR supervisor.

When digitizing processes of integrating new tools, controllers should assess whether personal data will be processed. If so, controllers should take measures during implementation to be able to comply with access requests. For example, updating the register of processes.

Controllers should always send confirmation of receipt when receiving a data subject right request. This confirmation helps set the deadlines before which the controller should present



the data subject with a response. This also helps set the expectations of data subjects and can prevent unnecessary litigation and filing of complaints with SAs.

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

No

### **Section on “IMPLEMENTATION OF GENERAL REQUIREMENTS FROM ARTICLE 12 GDPR”**

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

23) 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 4.15 in the questionnaire addressed to controllers.

No immediate issues or challenges.

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

No

### **Section on “CONTENT OF ACCESS REQUESTS AND RESPECTIVE RESPONSES ACCORDING TO ARTICLE 15 GDPR”**

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

25) 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 5.18 in the questionnaire addressed to controllers.

a. Issue(s)

#### **• Generic referral to privacy notices**

A number of controllers indicate that they only refer to or use text modules of their privacy notice. Referring to just the privacy notice is insufficient to inform the data subject regarding the reasons and grounds a controller processes the personal data of the data subject. It might be the case that not all processing grounds and goals are applicable to the data subject's situation therefore causing the data subject to be confused or angry with the controllers. This brings the risk that data subject will have to guess which parts are applicable to them and why, if the controller does not specify which parts are related to the data subject. Simply referring to the privacy notices also act contrary to article 12(1) GDPR to provide the data subject with information that is in a transparent, intelligible and easily accessible form, since privacy notices tend to be technical in nature.

b. Provision(s)?

Article 15, 12, 13, 14 GDPR

c. Caselaw

d. Explanation?

- It might be easier and quicker for organisations to refer to a privacy policy instead of reviewing and compiling specific information for each request. Moreover, when an organisation receives large amount of access requests, they resort to generalised responses to manage workload.
- Furthermore, it might be hard for controllers to indicate which process is applicable to a particular data subject when personal data are stored in a central database that is used for different purposes.

e. Differences between controllers ?

- Some controllers have not considered data subject requests in their processes and are unprepared, while others have an extensive procedure in place. This can be due to the sector a controller is active in or has taken steps to certify different processes in their organization.

f. Solutions

- Specify to access request responses to data subjects  
Controllers should handle access requests on a case-by-case basis and specify to the specific data subject what personal data is processed for which purposes and what the legal ground for that processing is. Controllers should refrain from using technical terms, that might be commonly used in the organisation or sector, but not known to the specific data subject, unless this is necessary to comply with the access request.

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

No

## Section on “LIMITATIONS OF ACCESS REQUESTS”

The questions here as the same as in the first section above. Please make sure to cover subquestions a) to f) as listed above.

27) Please explain the **main issue(s) or challenge(s)** that you have identified (if any) in your evaluations/actions with respect to Questions 6.1 to 6.8 in the questionnaire addressed to controllers.

a. Issue(s)

Refusals of requests due to cost concerns

Not all data controllers notify data subjects when they reject a request under Article 15(4). This failure to inform individuals about the status of their requests constitutes a breach of their rights under GDPR. It also reflects poorly on the organisation’s commitment to transparency and data protection.

In some cases, these explanations are simply overlooked, or the notification to the data subject is deemed unnecessary. Moreover, a few controllers even claim that there is no legal obligation to issue such notifications, which highlights a misunderstanding of GDPR requirements.

The reasons provided by data controllers for rejecting requests are often unclear or incomplete. For instance, some controllers argue that the data in question is irrelevant to the data subject or that the request does not apply to the data being processed. Controllers also assess why a data subject requests access.

In some responses, controllers indicate that they ‘never’ disclose employee identities. This appears to contradict GDPR expectations, particularly when case law suggests that such information should be provided if it is necessary for the data subject to fully exercise their rights. Although employees processing data on behalf of the controller are not generally considered recipients of data, and therefore excluded from the information that needs to be provided, their identities may need to be disclosed if it helps the data subject understand and exercise their rights effectively. This inconsistency in handling requests further complicates compliance.

Lack of standardised procedures for balancing conflicting rights

**b. Provision(s)?**

Articles 12(4)(5), 15, (4) GDPR.

**c. Caselaw**

**d. Explanation?**

Misinterpretation of GDPR rules. They could be using this article as a broad justification to deny access requests without properly assessing whether the request is genuinely ‘manifestly unfounded or excessive’.

Access requests can be both costly and time-consuming. As a result, some controllers – especially smaller ones – might refuse requests in an effort to save resources.

Controllers may be overly cautious fearing that granting certain access requests could expose them to abuse or misuse. This leads them to reject requests as a protective measure for their organisation.

Data controllers sometimes make their own decisions about whether to notify data subjects when rejecting requests. They tend to prioritise practical concerns, such as whether the information is relevant or whether notifying the individual might cause confusion, rather than strictly adhering to the transparency rules of the GDPR.

Some controllers may prioritise protecting their employees’ privacy, fearing that disclosing employee identities could lead to harassment. This concern could drive them to adopt non-disclosure policies. Additionally, internal company policies might restrict the sharing of employee information to maintain confidentiality and protect the workforce.

There might be a general lack of awareness about the specific requirements and recommendations from the EDPB, particularly regarding Article 15(4) GDPR. This lack of understanding can lead to varying interpretations of obligations and to inconsistencies in how controllers handle access requests.

**e. Differences between controllers?**

Some controllers have not considered data subject requests in their processes and are unprepared, while others have an extensive procedure in place. This can be due to the sector a controller is active in or has taken steps to certify different processes in their organization.

**f. Solutions**

SA’s and EDPB should develop and share clear guidelines that include examples of correct refusal practices under GDPR. This would help controllers better understand when and how to refuse access requests while staying compliant.

SA’s should promote transparency by encouraging controllers to publish reports on their refusal practices, possibly in an anonymised way. This would allow other organisations to learn from each other and foster more consistent handling of requests.

Even when the requested data seems irrelevant or confusing, controllers should properly explain why a particular request has been rejected. This ensures that data subjects are properly informed and can take appropriate follow-up steps, if necessary.

Controllers should adopt policies that balance the privacy of their employees with the rights of data subjects. These policies should specify the conditions under which employee identities can be shared while ensuring privacy is still protected. A case-by-case approach is recommended when dealing with these requests.

Controllers should create a clear procedure for Article 15 GDPR requests which includes EDPB's recommended three-step assessment framework.

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

No

### Part III – Impressions on the levels of awareness and compliance

29) What is your general impression of the **level of compliance** of the controllers you consulted concerning the **GDPR provisions** relating to the right of access?

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

29.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.):

Heavy regulated sectors, for example healthcare, finance and government, show a higher level of compliance when compared to less regulated sectors. However, within heavy regulated sectors the level of compliance again differs depending on the size of the controller, the amount of funds available to a controller and whether processing personal data is a core activity of a controller.

30) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

30.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, "size" of the controller, etc.):

Regard the response under 29.1.

31) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

Paragraph 13

Paragraph 19

Paragraph 74

Paragraph 75

Paragraph 99

Paragraph 113

Paragraph 114

Paragraph 117

Paragraph 118

Paragraph 141

Paragraph 152

Paragraph 189

## Part IV – Actions by participating SAs

32) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees' right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF? If yes, please provide the date, link to the guidance, and a short description of the guidance.

Yes, the Dutch SA has different items on its website to help controllers with the right to access.

- Title: For organisations: privacy rights in practice (Dutch: Voor organisaties: privacyrechten in de praktijk)

URL: <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacyrechten-avg/voor-organisaties-privacyrechten-in-de-praktijk>

Description:

On this page controllers can find general information that is applicable to all data subject rights requests, for instance controlling the ID of the requesting person

- Title: For organisations: right to access in practice (Dutch: Voor organisaties: recht op inzage in de praktijk)

URL: <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacyrechten-avg/voor-organisaties-recht-op-inzage-in-de-praktijk>

Description:

On this page controllers can find specific information regarding access requests. Controllers are indicated what they have and do not have to provide to data subjects.

- Title: Sample summary for access requests (Dutch: Voorbeeldoverzicht bij inzageverzoek)

URL: [https://www.autoriteitpersoonsgegevens.nl/uploads/imported/voorbeeldoverzicht\\_bij\\_inzageverzoek\\_def.pdf](https://www.autoriteitpersoonsgegevens.nl/uploads/imported/voorbeeldoverzicht_bij_inzageverzoek_def.pdf)

Description: An example that controllers can use to give access to data subjects. In the example, it is explained that there is no legal frame how access to personal data

should be granted and that the summary alone is insufficient to grant access to personal data. However, it does give controllers a concrete example to work with.

33) **Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

The Dutch SA receives on average 16 article 77 GDPR complaints per week regarding data subject rights. In handling these complaints, the AP primarily uses informal enforcement, in the form of prima facie letters and informal contact, to enforce the GDPR and provide guidance on matters of data subject rights.

Regarding reprimands, fines and orders subject to penalty, the AP has imposed the following:

AP fined one controller in 2020 for charging data subjects that requested digital access to personal data. Data subjects could request for access free of charge once per year.

AP fined one controller in 2022 for always requesting a copy of an ID whenever a data subject requested access to personal data.

AP fined one controller in 2024 for hindering data subjects requesting access request by hiding the digital access request form. The controller also did not present the personal data in an intelligible and easily form. Finally, the controller failed to provide information regarding retention of the personal data and which measures were in place when personal data was transferred outside of the EEA.

AP reprimanded 4 controllers in 2023, 5 controllers in 2022, 2 controllers in 2021, 1 controller in 2020 and 1 controller in 2019. In most cases, the controllers did not respond in time to access requests of data subjects. In other cases, the controllers failed to provide all necessary information to the data subjects.

34) **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).

This has yet to be decided by AP.

35) In general (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Very often

36) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?

Very often

37) 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 content of EDPB Guidelines 01/2022 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: [This has yet to be decided by AP.](#)

b. No:

38) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes: [At the level of the EDPB the Guidelines may be revisited to update the content with the latest case law developments and field experience of SA's.](#)

b. No:

# SI SA

Information Commissioner of the Republic of Slovenia

## 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<sup>42</sup>
  - d. Ongoing investigation
  
- 2) If your action is oriented toward “Fact Finding” (i.e. the first two responses in the previous question)
  - Did you clearly identify the responding controllers (as opposed to obtaining anonymous responses)?  
**Partially. Both options were provided (anonymous and identifiable responses).**
  - Following the results of the fact-finding exercise, do you plan to launch formal investigations relating to the right of access in the near future? If so, please provide more detail if available.  
**Yes, we plan to initiate three formal investigations targeting the areas identified as requiring further and more detailed examination: healthcare, banking, and policing. However, we cannot provide more detailed information on the content at this stage.**
  - If not, will this fact finding activity impact your enforcement activities and if yes, how?  
**N/A.**
  
- 3) For all SAs: 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 types of controllers received the same questionnaire.**
  
- 4) For all SAs: If applicable, please specify a) which questions of the consolidated questionnaire you did not include in your questionnaire version; b) in which questions you have amended the wording of the consolidated questionnaire – please specify the amended wording used per question.  
**To clarify the changes and amendments we have made to the wording of the questions, we have created an Excel file comparing the questions from the Slovenian national questionnaire with those in the provided EDPB version. Along with the comparison table, we are also providing our national version of the questionnaire in the annex.**
  
- 5) For all SAs: 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 etc.)?  
**We have no other general comments or remarks.**

## Part I – Some numbers on the controllers addressed

---

<sup>42</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.



6) How many controllers did you contact?

3563

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/to your questions.

408

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 primary reasons for the discrepancies between the responses to the two previous questions include inaccuracies in the DPO database emails due to DPOs not updating their contact information in a timely manner, a lack of interest from DPOs in responding to the questionnaire, and the excessive length of the questionnaire itself.

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: Please select one or more answers.

- a. Public sector: 250
- b. Private sector: 153

10) Please specify the category<sup>43</sup> of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers

- a. Micro enterprise: 30
- b. Small enterprise: 39
- c. Medium-sized enterprise: 44
- d. Large enterprise (more than 250 employees): 44
- e. Non-profit organisation: 4
- f. Ministry: 13
- g. Local authority: 15
- h. Administrative authority/agency/office (e.g. job center): 77
- i. School / university / educational institution: 70
- j. Other (please specify)  
Other public sector - 36  
Public authority - 27  
Other private sector - 8

11) Please specify the nature of the (business) activity of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. education sector: 108
- b. health sector: 59
- c. social sector: 43

---

<sup>43</sup> Information on the categories in lit. a.-c. can be found at [https://single-market-economy.ec.europa.eu/smes/sme-definition\\_en?prefLang=de](https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=de).

- d. insurance sector: 10
- e. finance sector: 28
- f. IT sector: 29
- g. retail sector: 20
- h. logistics sector: 6
- i. public transportation: 5
- j. telecommunications: 3
- k. postal services: 4
- l. advertising sector: 4
- m. marketing services: 3
- n. entertainment sector: 6
- o. information / journalism sector: 4
- p. scientific / historical research: 15
- q. credit scoring agency: 0
- r. public utility/infrastructure provider (e.g. energy): 13
- s. housing industry: 4
- t. manufacturing: 7
- u. other (please specify):
  - Other public sector activities - 113
  - Other private sector activities – 46

12) Please specify the categories of data subjects that are mainly concerned by the processing activities of the responding controllers. Please indicate the number of (responding) controllers to whom the respective option is applicable: Please select one or more answers.

- a. customers: 244
- b. potential customers: 94
- c. employees: 270
- d. job applicants: 147
- e. children: 94
- f. vulnerable adults: 38
- g. patients: 60
- h. citizens (for public sector): 73
- i. applicants (for public services): 52
- j. recipients (for postal services): 1
- k. other (please specify): 31
  - Students, other education participants, adult education participants
  - Parents
  - Event visitors, end-users of our clients' services, electricity consumers, users of social welfare services
  - Workers exposed to ionising radiation
  - Debtors
  - Offenders
  - Farmers

13) Please specify the approximate number of data subjects concerned by the processing activities of the responding controllers. Please indicate the number of (responding)

controllers to whom the respective option is applicable: Please select one or more answers.

- a. Less than 100: 29
- b. 100 - 200: 28
- c. 201 - 500: 52
- d. 501 - 2,000: 92
- e. 2,001 - 10,000: 63
- f. 10,001 - 50,000: 53
- g. 50,001 - 100,000: 21
- h. 100,001 - 1,000,000 \*
- i. 1,000,001 - 10,000,000 \*
- j. More than 10,000,000 \*

\* Those three options were consolidated into one ("More than 100.000")  
More than 100.000 – 98

14) Which types of personal data are mainly concerned by the processing activities of responding controllers? Please indicate the number of (responding) controllers to whom the respective option is applicable. Please select one or more answers.

- a. Contact data: 383
- b. Payment data: 314
- c. Identification data: 294
- d. Sensitive data within the meaning of Art. 9 GDPR: 110
- e. Health related data: 128
- f. Data of a highly personal nature within the meaning of Art. 10 GDPR: 51
- g. Other (please specify):
  - data on the characteristics and preferences of individuals - 62
  - purchase data - 64
  - data from official records - 214
  - data on social transfers and other forms of financial assistance from the state or municipality - 92
  - financial and other data on assets - 72
  - data on children or minors - 171
  - pseudonymised data on individuals - 47
  - data obtained about an individual in connection with the use of a service or device - 107
  - data we generate ourselves about an individual on the basis of previously obtained data - 87

15) How many requests for access in accordance with Art. 15 GDPR did the responding controllers receive in 2023 (approximately)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. 0 request
- b. 1-10 requests:  
Between 0 – 10 requests - 354
- c. 11-25 requests
- d. 26-50 requests  
Between 11 – 50 requests - 23
- e. 51-100 requests: 7

- f. 101-150 requests
- g. 151-200 requests
- h. 201-500 requests  
Between 100 – 500 requests – 8
- i. 501-10,000 requests  
More than 500 requests – 3  
More than 1000 requests – 4  
More than 5000 request - 0
- j. >10,000 requests: 3
- k. No information: 6

15.1 Did you identify any significant difference in the numbers of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)? If considered relevant, are there any controllers that have a very high/low number of access requests received in comparison with the overall number of data subjects whose personal data are processed by the controller?

Respondents processing personal data of more than 10.000 data subjects reported receiving an average of 0 to 10 access requests. Similarly, those processing personal data of fewer than 200 data subjects also reported an average of 0 to 10 requests. This suggests that the number of access requests does not necessarily correlate with the number of data subjects concerned. On the other hand, this could point out to controllers not properly identify access requests as such or not properly registering access requests in their document management system.

16) In 2023, for the responding controllers, what was the percentage of access requests in regards to the rest of the data protection requests received? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.

- a. None of the requests: 253
- b. >0–25%: 97  
1-10% - 94  
11-25% - 3
- c. 26–50% requests: 5
- d. 51–75% requests:
- e. 76–100% requests  
More than 50% - 21  
100% - 21
- f. No information: 11

16.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

We have observed significant variations in the percentages of responding controllers. **Controllers reporting 0% of data subject requests** were categorized as follows: 152 from the public sector and 97 from the private sector. Within specific categories of entities, the distribution showed education leading with 52 responses, followed by administrative units with 46, while non-profits had the fewest at 3 and ministries at 6. In terms of business activities,

the education sector reported 78 responses, with telecommunications receiving the fewest at 1. Public transport and entertainment each reported 2 responses, and real estate had 3. Regarding the number of data subjects, the response sizes were: 66 responses for the 500-2.000 range, 40 responses for the 2.000-10.000 range, and 8 responses for the 50.000-100.000 range.

**For controllers where 50% or more of the total requests received were data subject access requests**, the size distribution of data subjects was as follows: 21 responses involved entities with more than 100.000 data subjects, and the fewest, 2 responses, involved up to 200 data subjects. The public sector accounted for 24 responses, while the private sector had 18. Among the categories of entities, large companies reported the most with 12 responses, while non-profit organizations and medium-sized companies each had the fewest with 1 and 2 responses, respectively. In terms of business activity, health was the most reported with 8 responses, followed by financial services with 7, and the fewest were in real estate, logistics, research, and entertainment with 1 each.

- 17) Out of the access requests received in 2023 by responding controllers, what was the percentage that included a request to receive an insight into and inspection of and/or a copy of the personal data? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.
- a. None of the requests
  - b. >0–25%
  - c. 26–50% requests
  - d. 51–75% requests
  - e. 76–100% requests
  - f. No information

This question was not included in our questionnaire.

17.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

N/A.

- 18) Out of the access requests received in 2023 by responding controllers, what was the percentage of requests that included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed)? Please indicate the number of times the controllers responded within the ranges set out below. Please select one or more answers.
- a. None of the requests: 286
  - b. >0–25%
    - 1-10% - 65
    - 11-25% - 3
  - c. 26–50% requests: 6
  - d. 51–75% requests
  - e. 76–100% requests
    - More than 50% – 14
    - 100% - 15
  - f. No information: 19

18.1) Did you identify any significant difference in the percentages of the responding controllers? If so, what would be a potential explanation for this significant difference (e.g. number of data subjects concerned, “size” of the controller, sector)?

We observed significant differences in the percentages of responding controllers regarding requests for information on their underlying processing activities. Among those reporting that 100% of their requests were for information on processing activities, 8 private sector and 7 public sector controllers reported this response. Larger and smaller businesses each contributed 3 responses, while micro-businesses and government entities contributed just 1 each. The most active sectors were education and insurance, each with 3 responses, while financial services, logistics, and IT each had only 1 response.

For controllers reporting that 0% of the requests received were for information on processing activities, 174 responses came from the public sector and 108 from the private sector. Administrative units (58 responses) and education sectors (52 responses) reported not receiving such requests the most, whereas non-profits (4 responses) and ministries (9 responses) were among those receiving 0% of such requests. In terms of sectors, education again reported the highest number of entities not receiving such requests (82), with telecommunications, postal services, and advertising each reporting only 2. In this group, entities processing data of 500 to 2.000 subjects were most common, with 68 responses, while those processing data of 50.000 to 100.000 subjects were the least common, with just 6 responses.

One potential explanation for these differences could be the nature and visibility of the data processing activities in different sectors. For instance, sectors like education and insurance, which reported both high and low percentages of requests, may experience varying levels of public engagement depending on the specific type of data being processed or the visibility of their activities. In contrast, sectors such as administrative units and ministries, which reported higher numbers of 0% access requests, may attract less public interest or scrutiny due to the routine nature of their data processing activities. Additionally, in some sectors or entities, no clear patterns or differences were observed, suggesting that other factors, such as the size of the entity or the public's general awareness of data rights, may not play a significant role in influencing the volume of requests.

## **Part II – Substantive issues regarding controllers’ level of compliance**

Given that the challenges and issues we have identified are deeply interconnected and often overlap, we have chosen to emphasise and analyse the identified substantive issues collectively in this section of the report. By considering these issues as interrelated rather than isolated, we aim to provide a more comprehensive understanding of their broader implications and to develop more cohesive strategies for addressing them.

<b>Issue 1: Lack of awareness and knowledge among controllers and data subjects regarding the right of access</b>
---

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

A significant issue we have identified is the widespread lack of awareness and understanding among controllers regarding the right to access as stipulated by the GDPR. Controllers often confuse this right with other rights, such as a procedural right under Article 82 of our national General Administrative Procedure Act (the so-called “right of access to file”), or with rights related to public information access or even general contractual claims. This confusion could lead to misapplication of the law and improper handling of access requests.

Additionally, our practical experience highlights that the lack of awareness and knowledge among controllers frequently results in errors when distinguishing between various GDPR provisions and properly applying them to specific scenarios. For example, controllers might fail to recognize the differences between the right of access to personal data under Article 15 of the GDPR and other similar rights, such as the right to access administrative file under national procedural laws. This confusion often leads to incorrect handling of access requests—either by denying valid requests based on misinterpretation of the legal basis or by providing data in situations where it should not be disclosed.

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

This issue concerns Articles 12 and 15 of the GDPR, which outline the rights of data subjects to access their personal data and information about data processing. The issue does not lie predominately in the legislation, but in the need of further awareness-raising initiatives and actions.

**c. If relevant, please also refer to the relevant case law of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.**

-

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

The issue likely stems from insufficient training and awareness-raising efforts focused on the distinct rights granted under the GDPR, as well as a general lack of emphasis on these rights in the context of broader legal and administrative processes. Controllers may also lack the resources or expertise needed to adequately differentiate between various rights and their respective procedural requirements.

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

Some controllers, particularly those in smaller organizations or sectors less familiar with GDPR requirements, generally struggle more with understanding and implementing these rights. Larger organizations or those in highly regulated sectors generally tend to have more robust procedures in place but still face challenges in distinguishing between access to personal data and information about data processing.

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

Possible solutions include targeted training sessions for controllers to improve their understanding of the right of access, the development of clearer guidelines and templates for handling access requests, and increased efforts to raise awareness among data subjects about their rights under the GDPR.

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

-

<b>Issue 2: Confusion between access to personal data and information about data processing</b>
---

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

Controllers are frequently failing to differentiate between access to personal data and requests for information about data processing, leading to confusion and the improper handling of access requests, despite data subjects being entitled to both. However, our experience shows that requests for information about data processing are often overlooked as a mandatory obligation under the GDPR and are rejected more frequently than requests for copies of personal data.

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

This issue also pertains to Articles 12 and 15 of the GDPR, which distinguish between the right to access personal data and the right to receive information about how that data is processed.

**c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.**

EDPB Guidelines 01/2022 clarify the distinction between these rights, emphasizing that data subjects should be provided with both access to their data and comprehensive information about the processing activities related to their personal data (see section 2.2. of the guidelines).

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

The issue may arise from a lack of legal knowledge or misinterpretation of GDPR provisions. Controllers might not fully understand the obligations imposed on them, leading to an improper application of the law, particularly in more complex cases involving multiple types of personal data or processing activities.

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

No specific differences have been encountered among controllers.

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

Implementing detailed training programs focused specifically on the distinctions between different types of data access rights, as well as developing standardized procedures for handling such requests, could help mitigate this issue.

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

-



**Issue 3: Inadequate proper request handling procedures and lack of legal knowledge among controllers**

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

There is a notable deficiency in well-defined procedures for handling access requests among controllers. This includes uncertainty regarding who is responsible for processing such requests and in how & in what manner they should be handled. Additionally, controllers often lack the legal knowledge necessary to assess the rights of data subjects properly.

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

This issue primarily concerns Article 12 of the GDPR, which mandates that controllers provide transparent and easily accessible procedures for handling data subject requests, and Article 15, which outlines the right of access.

**c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.**

EDPB Guidelines 01/2022 emphasize the need for clear and efficient procedures to handle data access requests and the importance of providing thorough and legally sound responses (see section 5 of the guidelines).

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

This issue may be due to a lack of resources or expertise within organizations, particularly those with smaller teams or less experience with GDPR compliance. Additionally, there may be insufficient emphasis on the importance of adequate procedures in the broader context of organizational governance.

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

Organizations with larger legal or compliance departments generally have more structured procedures in place, whereas smaller organizations or those with limited resources often struggle to establish clear processes for handling access requests.

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

Developing and distributing clear guidelines and templates for handling data access requests, along with providing targeted legal training for those responsible for these procedures, could improve compliance (this has specifically been noted in our already conducted national training sessions). Encouraging the establishment of dedicated roles or teams for GDPR compliance might also be effective (beyond “just” the DPO’s comprehensive involvement).

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

-

**Issue 4: Insufficient reasoning in decisions and misuse of Article 15(4) GDPR’s exception**

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

This lack of detailed reasoning leaves data subjects without a clear understanding of the rationale behind issued decisions, particularly when access is denied or limited. Furthermore, there is a noticeable tendency among some controllers to misuse the exception provided under Article 15(4) GDPR, specifically by making broad and unsupported claims that the requested personal data is classified, copyrighted, or constitutes trade secrets. These generalized assertions often lack the necessary specific evidence or legal basis to substantiate the refusal of access.

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

This issue concerns Article 15(4) of the GDPR, which deals with the exceptions to the right of access, and Article 12, which requires that any restrictions or refusals be communicated clearly and with sufficient reasoning.

**c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.**

The EDPB Guidelines 01/2022 emphasize the importance of transparency and proper justification when refusing access, particularly in paragraph 174 of the guidelines.

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

This issue may be attributed to a lack of legal expertise or a misunderstanding of the requirements for justifying exceptions to the right of access. Controllers may be over-relying on general exceptions without adequately considering the specific circumstances of each individual request.

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

No specific differences have been encountered among controllers.

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

Enhancing legal training for controllers, particularly on the proper application of Article 15(4) exceptions, could help address this issue.

**Issue 5: Significant delays and unjustified extensions in responding to access requests**

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

A recurring issue is the significant delays in responding to access requests, with many controllers extending deadlines without sufficient justification. This could undermine the effectiveness of the data subject's right of access (and the formal legality of the procedure itself).

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

This issue concerns Article 12(3) of the GDPR, which mandates that controllers respond to access requests within one month, with the possibility of extending this period by an additional two months only when necessary and only with proper justification.

**c. If relevant, please also refer to the relevant caselaw of the Court of Justice of the EU or to EDPB Guidelines 01/2022 on the right of access.**

The EDPB Guidelines 01/2022 emphasize the importance of adhering to the prescribed timelines under the GDPR and the need for controllers to provide clear and valid reasons when extending those deadlines (see section 5.3. of the guidelines).

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

The delays and unjustified extensions may be due to insufficient resources, understaffing, or a lack of prioritization of GDPR compliance within some organizations. Controllers may also lack adequate knowledge or expertise in handling data subject requests, leading to procedural inefficiencies and extended processing times.

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

No specific differences have been encountered among controllers.

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

Implementing stricter internal tracking and monitoring systems for access requests can help ensure that deadlines are met. Furthermore, providing additional resources or personnel dedicated (specifically) to GDPR compliance could reduce the incidence of delays. Controllers should also be encouraged to streamline their internal processes to handle requests more efficiently.

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

-

### **Part III – Impressions on the levels of awareness and 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 of access?

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

19.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, size, etc.)

-

20) In particular, what is your general impression of the **level of awareness and understanding** of the controllers you consulted concerning **EDPB Guidelines 01/2022** on the right of access.

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

20.1) Comments (if any, e.g. differences regarding different types of controllers, such as between public and private sectors, “size” of the controller, etc.)

-

21) In your opinion, which **topics concerning the right of access** or which parts of the **EDPB Guidelines 01/2022** on the right of access are the least-known or the least implemented by controllers based on the results of this CEF?

This CEF action highlighted key challenges, particularly the frequent confusion between GDPR access rights under Article 15 and other similar rights, such as those in general administrative (such as access to file) or contractual legal framework. This confusion suggests a significant gap in understanding GDPR provisions among controllers, leading to frequent mishandling of access requests. Additionally, the analysis of the results emphasise the need for clear and reasoned rejections of access requests, an area where many controllers fail to comply adequately.

Procedural compliance, especially the standardized processes for handling requests and adhering to stipulated response timelines, is another area where implementation lags. Many organizations lack effective mechanisms (and resources) to process requests efficiently within the stipulated time frames, impacting compliance and the rights of data subjects. These critical areas remain under-implemented and are indicative of a broader need for enhanced clarity and focus in data protection practices.

## Part IV – Actions by participating SAs

22) Have you already published **guidance** (e.g. factsheets, guidelines, Q&A) on the implementation of the right of access? Please include any **general or targeted guidance you have adopted** (e.g. employees’ right of access; right of access exercised in the public sector, or regarding data concerning health, etc.), including before launching the CEF? If yes, please provide the date, link to the guidance, and a short description of the guidance.

We actively publish guidance and other non-binding opinions on the exercise of the right to access, focusing on specific guidelines tailored to particular subjects. For example, our non-binding opinions on this matter<sup>44</sup>, guidance for managers of multi-apartment buildings<sup>45</sup> and

---

<sup>44</sup> See: <https://www.ip-rs.si/mnenja-zvop-2/?id=13176&asId=as0&search=&tag%5B%5D=Pravica+do+seznanitve+z+lastnimi+osebnimi+podatki&oseba=&pubfromdate=&pubtodate=&sub=Iskanje>

<sup>45</sup> See: <https://www.ip-rs.si/publikacije/priročniki-in-smernice/smernice-po-splošni-uredbi-o-varstvu-podatkov-gdpr/smernice-za-upravnike-večstanovanjskih-stavb>

those involved in employment relations<sup>46</sup> (among others) illustrates this targeted approach. While we have not published any standalone guidance exclusively addressing the right of access in general terms, we incorporate these principles comprehensively within our broader guidelines. This integrated approach ensures that the right to access is contextualized and practically applicable across various sectors and scenarios. We also publish our binding decisions, also in relation to access requests.

**23) Have you taken any actions** (i.e., fact finding exercises, informal contact, prior consultation, investigation, enforcement actions) towards controllers concerning the right of access **prior to** launching the CEF 2024? Please provide a brief overview of the actions you have taken and the outcome of these actions.

We have conducted a few informal meetings with specific controllers, such as the Police and the Prison Administration of the Republic of Slovenia. Our approach generally involves holding sector-specific advisory meetings when we identify challenges, ensuring that any issues are promptly addressed in collaboration with the relevant entities. Additionally, we organized two seminars specifically for the public sector and two for other stakeholders, all of which were very well-received, generating significant interest and high levels of participation. We plan to continue these efforts with further initiatives in the future.

**24) 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 results of this CEF24 action, we plan to initiate<sup>47</sup> three formal investigations targeting specific entities: a healthcare center, a bank, and a law enforcement authority. These investigations are scheduled to initiate this year with the objective of concluding by year-end. Additionally, we will conduct a more comprehensive analysis of the data collected, including responses to additional questions we set in our national questionnaire, to further assess the necessary actions and recommendations for the controllers involved.

**25) In general** (whether during the CEF 2024 Action or more generally when taking other outgoing decisions or guidance relating to the right of access), how often do you **rely on or refer to the EDPB Guidelines** on the right of access in your outgoing decisions or guidance relating to the right of access?

Very often. In our practice, both during the CEF24 and in other decisions or guidance relating to the right of access, we consistently rely on and refer to the EDPB Guidelines on the right of access. These guidelines serve as a fundamental reference point in all our evaluations, opinions and decisions, ensuring that our actions align with established best practices and legal standards within the broader EU framework. This approach helps maintain consistency and accuracy in enforcing data protection rights and providing clear guidance to controllers.

**26) Do you rely on or refer to the EDPB Guidelines on the right of access in decisions related to the exercise of other data protection rights than the right of access?**

---

<sup>46</sup> See: <https://www.ip-rs.si/publikacije/prirocniki-in-smernice/smernice-po-splosni-uredbi-o-varstvu-podatkov-gdpr/varstvo-osebni-podatkov-v-delovnih-razmerjih>

<sup>47</sup> At the time of publication of this report, the investigations will be under way and the controllers will be informed thereof.

Sometimes.

27) 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 content of EDPB Guidelines 01/2022 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
- ii. Online or remote training sessions: Yes
- iii. Conferences organised
- iv. Others: please specify

b. No

28) In your opinion, should more actions be carried out **at the level of the EDPB** to communicate and raise awareness with respect to the content of EDPB Guidelines 01/2022 and if yes, which actions would be preferable?

a. Yes

b. No: Yes

In our opinion, further actions at the level of the EDPB to communicate and raise awareness regarding EDPB Guidelines 01/2022 are not necessary at this time. The current level of communication and the dissemination mechanisms in place seem to be adequate. The guidelines are accessible and have been sufficiently integrated into the operational practices of relevant stakeholders. Instead of additional EDPB efforts, us as SAs should take a proactive role in raising awareness and communicating the guidelines more effectively within our jurisdictions. Continued monitoring with periodic reviews of the guidelines and their implementation by SAs might therefore be more beneficial than expanded communication efforts at the EDPB level.