# **Coordinated Enforcement Framework Action 2024:** implementation of the right of access by 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).*

*While the questionnaire is completely anonymous, we would like to point out that it falls to the participants to anonymise/pseudonymise the information contained in their responses. We therefore urge everyone filling out the questionnaire to exclude any personal data or information that could identify concerned parties.*

1. **Information about the controller**
	1. Sector specific information:
2. Please describe the sector of your activity:

[ ] public sector

[ ] private sector

1. 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)

1. 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. 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. 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)?
1. **Documentation of compliance with requests for access**
	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. 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.
2. **Process-related questions**
	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. 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.).
	1. 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:
8. (when and how) do you involve your DPO when digitizing processes,
9. do you update your record of processing activities accordingly,
10. (how) do you connect new tools or services with existing proceedings to collect information to be provided in case of access requests,
11. (how) do you verify and ensure the assistance required by any processor engaged in responding to access requests?
	1. 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.
	2. 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 the different groups of data subjects.
12. **Questions about the implementation of general requirements from Art. 12 GDPR**

***Formal aspects concerning access request and respective responses***

* 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.

* 1. 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.
	2. 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.

* 1. 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.
	2. 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)

* 1. 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***

* 1. 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.

* 1. 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.
	2. 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)?
	3. 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 requesting access?
	4. 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***

* 1. 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?
	2. 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?
	3. 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. 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)?
1. **Questions regarding the content of access requests and respective responses according to Art. 15 GDPR**

***General***

* 1. How do you identify which data you need to select in the context of an access request in accordance with Art. 15 GDPR?
	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?
	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?
	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***

* 1. 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***

* 1. 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.

* 1. 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?
	2. 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?
	3. 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***

* 1. 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)

* 1. 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)?
	2. 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)?
	3. 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***

* 1. 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***

* 1. 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.
	2. 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?
	3. 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?
	4. 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?
1. **Limitations of access requests**
	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?
	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.
	3. In which circumstances do you provide information about the identity of individuals within your organisation processing the data subject’s personal data?
	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).
	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. 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?
	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?
	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.
2. **Miscellaneous**
	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?
	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) – **Optional if your organisation wants to remain anonymous.**

List of annexes (Optional)