2024 Coordinated Enforcement Action

Implementation of the right of access by controllers

Adopted on 16 January 2025

EXECUTIVE SUMMARY

In October 2020, the European Data Protection Board ('**EDPB**') decided to set up a Coordinated Enforcement Framework ('**CEF**') with a view to streamlining enforcement and cooperation among supervisory authorities. Since then, two CEF actions have been completed: the first one in 2022 on the use of cloud services by public bodies and the second one in 2023 on the designation and position of data protection officers. For the third year, the EDPB chose the topic of 'the implementation of the right of access by controllers'. One particular focus of this CEF action are the EDPB Guidelines 01/2022 on data subjects rights – Right of access ('**Guidelines 01/2022**').

Throughout 2024, 30 supervisory authorities ('**SAs**') across the EEA launched coordinated investigations into the compliance of certain controllers with the right of access under the GDPR[1]. The CEF action was implemented at national level in one or several of the following ways: (1) fact-finding exercise, (2) assessment to identify if a formal investigation is warranted, and/or (3) commencement of a formal enforcement investigation, or follow-up of ongoing formal investigations.

Between November 2023 and February 2024, these SAs discussed the aims and the means of their actions in the context of the CEF action. In this context, the SAs agreed on a questionnaire to use when contacting controllers. 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. A total of 1,185 controllers responded to the questionnaire. These controllers are equally private entities ranging from SMEs to big companies active in many different industries and fields, as well as various types of public entities.

The present report aggregates the findings of all the SAs participating in the CEF action[2]. Overall, around two thirds of participating SAs evaluated the level of compliance of responding controllers with respect to the right of access to be from 'average' to 'high'. One important factor identified as having an impact on the level of compliance was the volume of access requests received by controllers, as well as the size of the controller's organisation. The survey results suggest that the level of compliance was generally higher for controllers who received a larger number of access requests, or for larger organisations. However, SAs were surprised about the large number of controllers responding having received a very low number of access requests in 2023 – which could suggest that not all access requests are actually recognised as such, potentially pointing to overall awareness issues.

Based on the survey results, controllers were less aware about the content of Guidelines 01/2022. These Guidelines provide extensive guidance to - among others - help controllers implement the different elements of the right of access, but also touch upon the facilitation of this right and its exceptions and limitations. As a result of this lower level of awareness, some aspects that are developed in Guidelines 01/2022 were not followed in practice by some controllers. Despite this, participating SAs observed positive findings across the EEA. These include the implementation of best practices mentioned in Guidelines 01/2022 or additional ones proactively implemented by controllers, such as user-friendly online forms enabling data subjects to submit an access request easily, self-service systems to allow data subjects to autonomously download their personal data in few clicks and at any time and procedures to regularly audit the process for handling access requests internally.

[1] And the corresponding right of access applicable to EU institutions under Regulation (EU)) 2018/1725, which are supervised by the European Data Protection Supervisor (EDPS) who participated in this CEF action.
[2] The SAs' national reports are attached to this report and provide further detail on the results obtained and the analyses and observations made at national level. These were submitted over the course of September 2024 and represent the situation at that point in time.

Particular attention is paid to challenges identified by SAs and/or respondents during the CEF action. For each challenge identified, a list of non-binding recommendations or points of attention is included that controllers or SAs may take into account to address the challenges identified, without prejudice to the provisions of the GDPR/EUDPR and to SAs' powers under data protection law.

Challenges and list of recommendations / points of attention
Lack of awareness about the scope of access to be provided
• Controllers should **pre-assess the scope** of Art. 15 GDPR from the outset to be aware about which type of information may contain personal data. • Controllers should **pre-assess where** (e.g. which instances and databases) **to verify** once they receive an access request. The EDPB recommends referring to the record of processing activities (Art. 30 GDPR) to precisely identify possible storage locations of personal data. The record of processing activities should be kept up to date, e.g. for new processing activities, new IT systems / processors, new organisational structures.
Indefinite, excessive or inconsistent retention periods relating to access requests
• Controllers should **fix a retention period** for access request communication based on **objective criteria** and **document** their reasoning in accordance with Art. 5 (2) GDPR. • **Statutory retention periods** for other types of documents or records should **not be applied by default**. Controllers should carefully assess whether these provisions actually cover access request communication, and document their assessment. • Controllers should ensure that access request communication is **stored separately** from other information about the data subject which may be subject to other retention periods and also other access and role management rights within the controller's organisation. • Further **guidance** from SAs on uniform and **meaningful criteria for determining retention periods**, including on national legislation and defence against legal claims, could help controllers in selecting appropriate retention periods.
Lack of documented internal procedures
• The EDPB could issue further **guidance** regarding **best practices** for documenting compliance with Art. 15 requests. • SAs could promote the adoption of **Codes of Conduct**, pursuant to Art. 40 GDPR, in order to identify standardised procedures for the effective application of the right of access, also in view of the different categories of controllers. • A proper **exchange between all relevant internal actors** within controllers' organisations should be established to properly qualify and filter requests from the outset. • Controllers should ensure that all employees are **trained to recognise** an access request no matter the submission channel and are **aware of the appropriate channel** to transfer it to. • Controllers should ensure that they are **actively reviewing** and (where necessary) **improving their data protection practices**. Such reviews may, among others, consider Guidelines 01/2022. • When in doubt whether an individual's request is an access request pursuant to Art. 15 GDPR, controllers should **verify** this **with the individual** making the request. • Controllers could provide **guidance to data subjects on different types of requests** and their scope. A good practice could be setting up a web form guiding the requester through a series of preliminary questions aiming, e.g. to help the person assess whether they chose the appropriate channel to obtain what they look for, allowing for a more streamlined process.
Barriers to the facilitation of the right of access
• Controllers should ensure that they are prepared to **handle access requests** even if the request is **not submitted through a dedicated data protection channel**. • Controllers should assess each access request received on a **case-by-case basis** in order to determine if **further identification or authentication** of the data subject is required.

• Controllers should be made aware of their obligation to **demonstrate their need for further identification documents** to confirm the identity of the data subject. • SAs could issue further **guidance** focused on best practices for adhering to a controller's **accessibility** requirement.
Inconsistent and excessive interpretations of the limits to the right of access
• SAs and the EDPB could develop **guidance** including examples of **correct refusal practices** / **use cases** resulting in a limitation of access, either based on the GDPR or national law. • **Communication** by the EDPB and SAs on **recent CJEU case-law** could increase controllers' awareness. **Guidelines 01/2022** could also be **slightly updated** in light of such case-law. • Controllers should be aware that in cases where they restrict a data subject's right to access, they should be able to **demonstrate** /explain **the reasoning** for doing so. • Controllers should adopt policies that **balance the rights and freedoms** of themselves and third parties with the rights of data subjects, in particular where the right of privacy of their employees is concerned, and assess Art. 15 (4) GDPR situations in a **case-by-case approach.**
Excessive interpretation of the possibility to ask for specification of access requests
• SAs could foster the knowledge of the **difference** between **specification** as per recital 63(7) GDPR and the "**layered approach**" promoted by the EDPB. • The EDPB could include brief **clarifications** on such difference **in Guidelines 01/2022**. • Controllers should assess each access request on a **case-by-case basis** to verify whether the conditions of recital 63 s. 7 GDPR are met, and **inform** the data subject **about any processing activities potentially concerning them** in their request for specification. • **Upfront**, controllers could provide data subjects with **self-service tools** or possibilities to pre-select one, several or all processing activities which they would like to receive information on.
Provision of insufficiently detailed or tailored information to data subjects
• Controllers should handle access requests on a **case-by-case basis** and inform the specific data subject which personal data is processed for which purposes, as well as include **information** as listed in Art. 15 (1), (2) GDPR which is **tailored to the specific data subject and access request**. • Controllers are responsible for accurately recording to which entities precisely they disclose personal data and where these recipients are located, to be able to **name the actual recipients in accordance with Art. 15 (1) lit. c GDPR**. A comprehensive updated record of processing activities is helpful to fulfil this responsibility.

For the challenges identified, recommendations also include for SAs to foster the knowledge about the respective specific sections or paragraphs in Guidelines 01/2022, which contain extensive guidance and several practical examples that may help controllers in addressing the challenges raised, as well as to foster the knowledge about respective applicable CJEU case-law. Where applicable, it is also recommended that SAs revise their publications on the right of access in light of Guidelines 01/2022 and/or the recent CJEU case-law, and raise awareness about this fact.

Against this background, the results of this CEF action suggest that raising awareness about Guidelines 01/2022 is necessary, both at national and EU level. Both controllers and data subjects need to be made aware of their obligations and their rights, respectively. Small updates or clarifications to Guidelines 01/2022, e.g. on recent CJEU case-law have also been suggested by SAs in light of the findings of this CEF action.

This report also includes information about the participating SAs' actions relating to the right of access, both independently of and in context with the CEF action, regarding enforcement, additional guidance or conferences and information campaigns. Some of the actions undertaken by SAs are still ongoing at national level, especially when formal investigations were launched. Accordingly, this report does not constitute a definitive statement of the actions carried out within the CEF action.

Table of contents

1 INTRODUCTION

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

In October 2023, the EDPB selected the topic of the '**Implementation of the right of access by controllers**' for its 2024 CEF action[5]. The EDPB decided to prioritise this topic given that this right stands at the heart of data protection[6]. It is one of the most frequently exercised data protection rights, and one which SAs receive many complaints about. In particular, this right enables individuals to be aware of the processing of their personal data, and check whether their personal data is processed in a compliant manner by controllers. In addition, it often enables the exercise of the other data protection rights, such as the right to rectification and erasure. Last but not least, this CEF action takes place shortly after the EDPB adopted Guidelines 01/2022 on data subject rights - Right of access in March 2023 ('**Guidelines 01/2022**')[7].

Building on common preparatory work, the EDPB announced the initiation of the action on 28 February 2024[8]. Throughout 2024, 30 SAs across the EEA launched coordinated investigations into compliance with the right of access. More specifically, eleven SAs have initiated new **formal investigations** as part of this CEF action. Nineteen SAs stated that the initial procedural framework of their action **was fact-finding**. Among them, eight SAs indicated that they would determine **follow-up actions** based on the results. In particular, at least two SAs plan to launch formal investigations relating to the right of access in the near future.

The present report aggregates the findings of SAs participating in the CEF action, and provides a state of play of their work. In particular, the first part of this report presents statistics regarding the controllers addressed by each SA, while the second part analyses the positive findings but also the challenges and issues identified. In addition, it presents an overview of the actions already implemented or ongoing, including guidance, enforcement actions or potential actions by SAs.

The SAs' national reports are attached to this report and provide further detail on the results obtained and the analyses and observations made at national level[9].

With this third CEF action, the EDPB intends to:

[3] EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679 (EDPB, 20 October 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_documents_20201020_coordinatedenforcementframework_en.pdf.
[4] EDPB Strategy 2024-2027, adopted in April 2024.
[5] 'EDPB picks topic for 2024 Coordinated Action', 17 October 2023, available at https://www.edpb.europa.eu/news/news/2023/edpb-picks-topic-2024-coordinated-action_en.
[6] The right of access of data subjects is enshrined in Art. 8 of the EU Charter of Fundamental Rights.
[7] EDPB Guidelines 01/2022 on data subject rights - Right of access, version 2.1, adopted on 28 March 2023.
[8] 'CEF 2024: Launch of coordinated enforcement on the right of access', 28 February 2024, available at https://www.edpb.europa.eu/news/news/2024/cef-2024-launch-coordinated-enforcement-right-access_en.
[9] These national reports were submitted by participating SAs over the course of September 2024. They therefore represent the situation at this point in time. Furthermore, it should be noted that all eight German SAs participating in this CEF action have drafted a common report with their consolidated findings. The findings presented in this consolidated report may not be valid for other German SAs which have not participated in this CEF action. Lastly, not all findings, impressions, possible explanations or solutions expressed in the participating German SAs' report are valid or apply in full to each participating German SA.

- **ensure that the right of access can be effectively exercised by data subjects and assess how controllers comply with the right of access in practice,**
- **raise awareness of the requirements applicable to the right of access and the content of Guidelines 01/2022,**
- **collect the experience and conclusions of the participating SAs under this CEF action for analysis.**

2 BACKGROUND AND METHODOLOGY

2.1 Legal background and background on EDPB and SA activities relating to the right of access

The right of access was already set out in Directive 95/46, albeit with a limited scope[10]. The right of access was subsequently enshrined in the Charter of Fundamental Rights of the EU[11] and then in the GDPR. Art. 12 GDPR[12] defines the modalities for the exercise of the rights of the data subject, including the right of access. Art. 15 GDPR[13] further develops the three different components of the right of access, namely[14]:

- confirmation as to whether personal data is processed or not with respect to the data subject exercising their right of access,
- access to such personal data and
- access to information about the processing, such as purpose, categories of personal data and recipients, duration of the processing, data subjects' rights and appropriate safeguards in case of third country transfers.

The Court of Justice of the EU ('**CJEU'**) has adopted landmark decisions relating to the right of access, both under the previous Directive 95/46/EC and the GDPR. In no less than ten preliminary rulings addressed to national courts, the CJEU clarified - among others - the scope of the right of access and its application[15]. The CJEU for example clarified the limitations of the right of access: Data subjects are

[10] Recital 41 and Art. 12 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In particular the access to information was limited to "at least" the purposes of the processing, the categories of data concerned, the recipients or categories of recipients to whom the data are disclosed and knowledge of the logic involved in any automatic processing of data concerning the data subject at least in the case of the automated decisions.

[11] Art. 8 (2) of the Charter.

[12] Art. 14 of Regulation (EU) 2018/1725 (EUDPR) applies to the EU institutions, bodies, offices and agencies (EUIs), which are supervised by the European Data Protection Supervisor (EDPS). This provision is, *mutatis mutandis*, identical to Art. 12 GDPR, except on the following: the possibility to charge a reasonable fee to the data subject in certain situations (Art. 12 (5) lit. b GDPR) is **not** mirrored in Art. 14 (5) EUDPR.

[13] Art. 17 EUDPR applies to EUIs. This provision is, *mutatis mutandis*, identical to Art. 15 GDPR, except on the following: the second sentence of Art. 15 (3) GDPR ('For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs') is **not** mirrored in Art. 17 (3) EUDPR.

[14] Guidelines 01/2022, paras. 17-20.

[15] Judgment of 7 May 2009, *Rijkeboer*, C 553/07, ECLI:EU:C:2009:293; Judgment of 12 December 2013, *X*, C 486/12, ECLI:EU:C:2013:836; Judgment of 17 July 2014, *YS and Others*, C 141/12, ECLI:EU:C:2014:208; Judgment of 20 December 2017, *Nowak*, C-434-16, ECLI:EU:C:2017:994; Judgment of 9 July 2020, *Land Hessen*, C-272/19, ECLI:EU:C:2020:535; Judgment of 12 January 2023, *Österreichische Post*, C-154/21, ECLI:EU:C:2023:3; Judgment of 4 May 2023, *Österreichische Datenschutzbehörde and CRIF*, C-487/21, ECLI:EU:C:2023:369; Judgment of 22 June 2023, *Pankki S*, C-579/21, ECLI:EU:C:2023:501; Judgment of 26 October 2023, *FT*, C-307/22, ECLI:EU:C:2023:811; Judgment of 24 May 2024, *Addiko Bank d.d.*, C-312/23, ECLI:EU:C:2024:458. There are also several pending referrals before the CJEU.

not required to give reasons for their access request and their requests cannot be refused on the basis that they serve a purpose other than that of acquiring knowledge of the data processing and verifying its lawfulness[16].

SAs receive a lot of complaints from data subjects regarding the exercise of this right across the EEA and many decisions relate to this matter. SAs cooperate very regularly among themselves as part of the one-stop-shop ('**OSS**') mechanism to handle the complaints they receive and reach consensus. At the date of publication of this report, more than 270 final decisions relating to the right of access are available in the EDPB register of OSS final decisions[17].

The EDPB has adopted extensive guidance on this topic in its Guidelines 01/2022. In particular, these Guidelines include a user-friendly flowchart which summarises the steps that controllers should follow when they receive a request from data subjects. Twenty-nine SAs 'often' or 'very often' rely on or refer to Guidelines 01/2022 in their outgoing decisions or guidance relating to the right of access. This holds true for decisions or guidance adopted during the CEF action and more generally when taking other outgoing decisions or guidance relating to the right of access. In addition, it is noteworthy that these Guidelines have a broader impact, as twelve SAs 'often' or 'very often' rely on or refer to them in decisions related to the exercise of *other* data protection rights than the right of access.

The EDPB also published an 'SME Guide', which is addressed to smaller controllers and is available in 18 different EU languages. This guide sets out a checklist explaining what to do concerning data subject rights and how to handle data subject rights requests. More specifically, it includes a section dedicated to the right of access[18].

2.2 Methodology of the CEF action

Participating SAs first agreed on a questionnaire drafted in English designed to contact the respective controllers, which was then translated into the relevant EU languages and sent to the controllers of each SA's choice at national level. The questionnaire was drafted in a neutral manner to allow participating SAs to decide which controllers should be addressed (e.g. public or private controllers, specific sectors or cross-sectoral approach), by which means to address them and in which procedural context (e.g. enforcement or fact-finding). Lastly, only certain questions were considered mandatory to be included in the national questionnaires, to allow SAs flexibility e.g. depending on the specific controllers contacted. Some SAs decided not to include all the questions of the commonly-built questionnaire when contacting controllers[19].

One has to bear in mind the following elements when reviewing the results of the survey:

- The questionnaire has been translated in eighteen languages and answered in those local languages. While translations have been proofread by SAs, the wording of the questions may have been understood or interpreted differently depending on language or cultural differences.

[16] See, inter alia, Judgement of 26 October 2023, *FT*, C-307/22, ECLI:EU:C:2023:811, para. 38, 52, and Judgment of 24 May 2024, *Addiko Bank d.d.*, C-312/23, ECLI:EU:C:2024:458, para. 40.

[17] Available at https://www.edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en. Decisions can be filtered depending on the GDPR provision(s) they relate to. In this case, the search was done based on Art. 15 GDPR.

[18] The EDPB data protection guide for small business, available at https://www.edpb.europa.eu/sme-data-protection-guide/home_en.

[19] This was for example the case when the SAs already had the relevant information at their disposal.

- Each participating supervisory authority developed its own strategy for the recipients of this commonly-built questionnaire.
    - Some SAs decided to contact thousands of controllers (e.g. SI, BG, and NL SAs) while others targeted a smaller pool (e.g. around a dozen for DK, EE, FI, and HU SAs).
    - A few SAs made it possible for controllers to complete the survey without providing their identity (e.g. IT, LU, MT, NL and PL SAs). In contrast, other SAs contacted previously identified controllers.
    - Certain SAs targeted a specific sector or category of controllers: in the public sector (e.g. European Union institutions[20] for the EDPS), in the private sector (e.g. finance industry for CZ and EL SAs, hotels and insurance companies for HR SA, insurance companies for EE SA and retail sector for DK SA). However, overall almost all SAs contacted both public and private sector controllers.
    - EDPS and SI SA contacted the controllers through their DPOs, while others contacted controllers through different contact persons.
    - The survey was either mandatory or optional for controllers to complete, depending on whether the questionnaire was completed as part of an enforcement action. Some controllers reported that they found the questionnaire complex and long. This may have led certain controllers not to fully complete the questionnaire (where it was optional) or giving answers that were not relevant to the questions posed.
    - Overall SAs sent the same questionnaire to the controllers they contacted at national level. However, some SAs slightly modified certain questions (e.g. to tailor them to specific controllers or sectors or adjust them to a pure enforcement context). A few SAs sent follow-up questions to responding controllers to clarify certain points.
    - Some SAs asked controllers to provide documentation on their internal processes and analysed such documentation in light of the controllers' input, while others did not.

3 SOME FIGURES

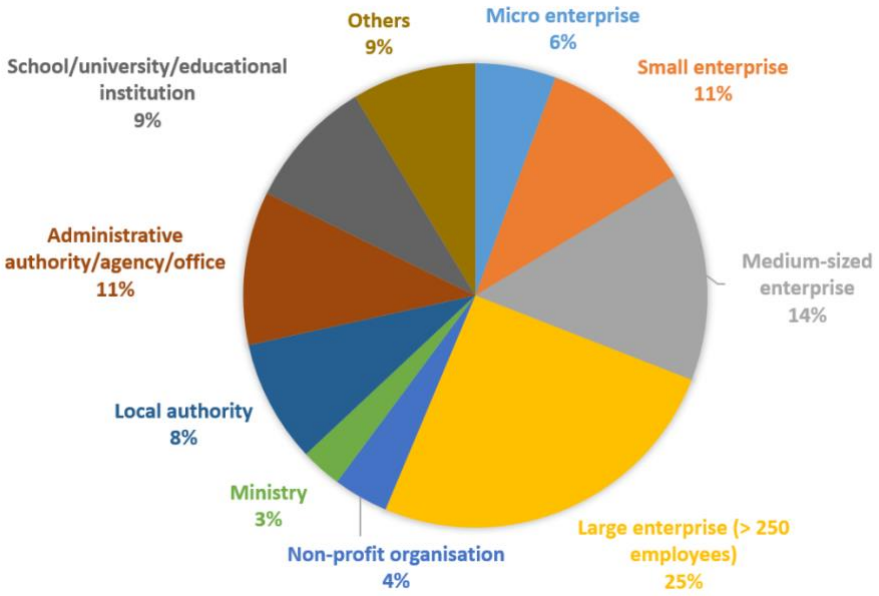
This section provides some figures on the controllers which responded to the survey and the data they provided[21].

3.1 Responding controllers and their processing activities

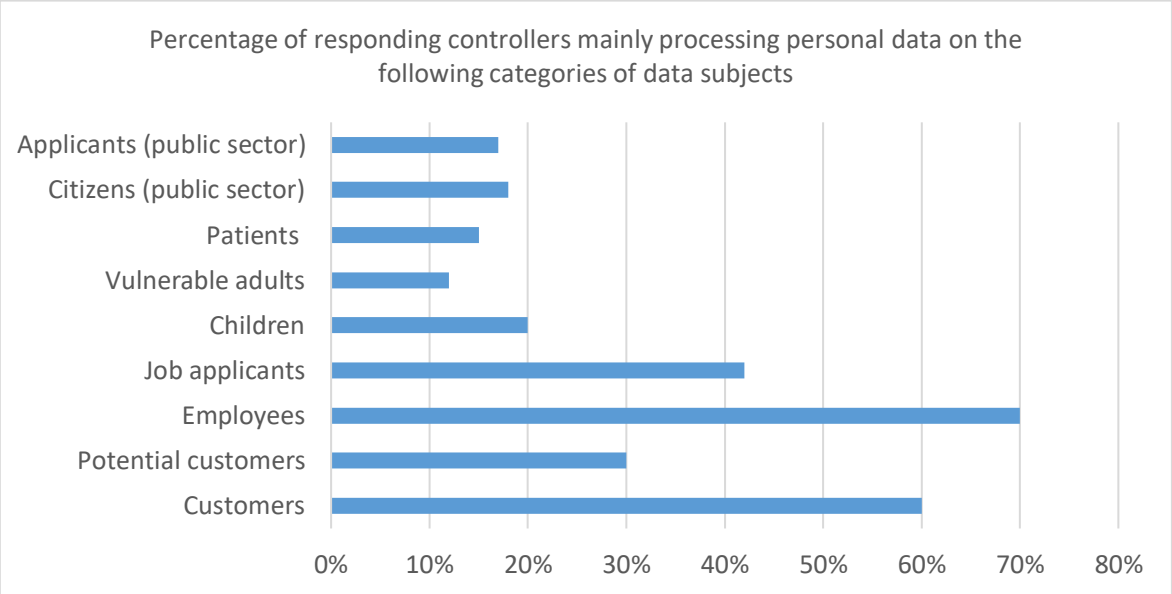
A total of **1,185 controllers responded across the EEA**[22]. The private and public sectors were equally represented[23].

[20] This refers to EU institutions, bodies, offices and agencies.
[21] This section does not include the figures of one of the participating SAs.
[22] In total 13,893 controllers were contacted by all the participating SAs. However, the figures of LT SA were not included in Section 3. SI, BG, and NL SAs contacted thousands of controllers and had a lower response rate than the other participating SAs, which has an impact on the overall response rate. The SAs which opened new formal investigations encountered no gap between the controllers contacted and those responding. It is worth noting that these SAs used the questionnaire in the context of their audits. Other factors that may play a role in explaining the gap in the response rate are the following: the voluntary nature of the questionnaire, the lack of centralised data available in controllers' organisations regarding the access requests received and the absence of a specific procedure in handling or documenting those requests, the possible lack of interest where the questionnaire was voluntary, the fear of controllers of the SAs opening an investigation, the fact that the questionnaire sent was rather long and extensive and the lack of controllers' resources.
[23] More precisely, 594 responding controllers were from the public sector while 600 from the private sector.

These controllers were active in multiple activities and industries, given that most SAs picked controllers across sectors[24], the ones being the most represented being the health, finance and education sectors[25]. The responding controllers belonged to the following categories of entities:



Based on the survey results, the processing activities of the responding controllers mainly concerned the following categories of data subjects[26]:



[24] For more detail please see the national reports in Annex 1. Controllers can be active in more than one industry.
[25] 16%, 13% and 12% of the responding controllers were active in these sectors, respectively.
[26] For example, this means that according to the chart displayed, 60% of the responding controllers reported to process personal data relating to their customers as one of their main data subject categories. For this question, responding controllers could indicate one or several data subject categories.

The processing activities of the responding controllers related to varying numbers of data subjects. The responses ranged from controllers processing personal data relating to less than 100 data subjects to controllers processing personal data relating to more than 10 million of data subjects[27].

This means that these data subjects could potentially exercise their right of access towards the responding controllers, while the survey showed, however, that the number of access requests actually received by the responding controllers seems surprisingly low (see Section 3.2 below).

The processing activities of the responding controllers involved - among others - the following categories of personal data[28]:

Categories of personal data[29]	Percentage of responding controllers who reported processing such data
Contact data	95%
Payment data	74%
Identification data	72%
Sensitive data within the meaning of Art. 9 GDPR	31%

[27] For example this means that according to the displayed chart 12% of responding controllers reported to process personal data relating to between 2,001 and 10,000 data subjects.
It must be noted that for this question, all EUIs were classified in the category "50,001-100,000" given that they process personal data of their staff members, amounting to approximately 60,000 staff members in total. Please see the EDPS' report in Annex 1 for more detail on this topic.

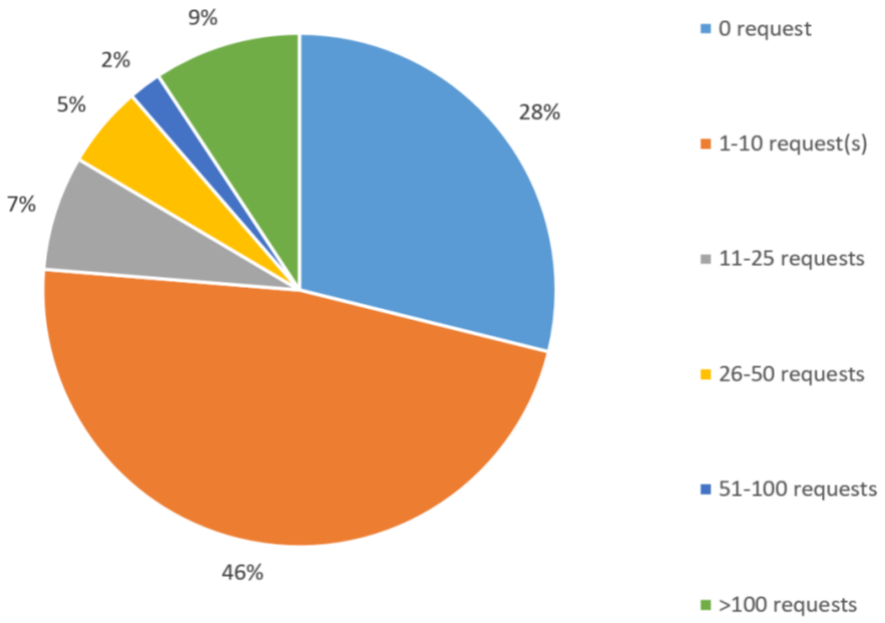
[28] For example this means that 74% of responding controllers reported to process payment data. For this question, responding controllers could indicate one or several categories of personal data.

[29] Many SAs reported that the responding controllers also processed other types of personal data such as device data, traffic data, finance data, geolocation data, HR-related data, etc. The table above is therefore not exhaustive.

Data of a highly personal nature within the meaning of Art. 10 GDPR	19%

3.2 Access requests reported by responding controllers

Responding controllers reported to have received the following approximate number of access requests in 2023:



Many SAs were surprised about the proportion of controllers reporting having received zero to 10 access request(s) in 2023, which amounted to around 74% of responding controllers. This was for example the case even for a few large controllers, controllers processing personal data relating to many data subjects or for controllers regarding which SAs received questions or complaints from data subjects. Possibly, the right of access is either not sufficiently known to data subjects or is only used in limited circumstances (e.g. when there is already a dispute between the data subject and the controller). Another explanation could be that some controllers are not aware of what an access request is or are not able to distinguish them from other types of request, and thus cannot recognise such requests when they receive them (please see Section 4.2.1 below). In addition, as many controllers do not have a centralised system to manage the requests received, they are therefore unable to track and report on these requests when asked. Against this background, it seems likely that the number of access requests actually received was underreported.

Some SAs observed very diverse results on the number of access requests received in 2023 at national level depending on the responding controllers, which could be explained by the elements mentioned in the previous paragraph. However other factors could also play a role, namely: (1) the controller's size, (2) the controller's sector and activity (e.g. regulated sector, B2C or B2B), (3) the importance of the controller on the market and its public exposure, (4) the nature and volume of personal data processed, (5) the number of data subjects whose personal data is being processed and/or (6) the existence of decisions issued by the relevant SA regarding compliance with the right of access in a specific sector, raising awareness on this right.

Only 25% of responding controllers reported that access requests corresponded to more than 25% of the total number of data subjects' requests received in 2023. This percentage was expected to be higher by some SAs, given the central role that the right of access can play to exercise other data protection rights, such as the right to erasure.

As recalled above, the right of access is composed of three elements (please see Section 2.1). Data subjects can exercise their right of access fully with respect to the three elements or chose only one or two elements in their access request[30]. Out of the access requests received in 2023, 44% of the responding controllers reported that none of these included a specific request to receive information on the underlying processing activities (e.g. for which purposes the personal data is processed). This means that these controllers received access requests not mentioning this transparency element of the right of access in particular. This is the case for example when data subjects submit a general access request (e.g. to receive the whole set of information required under Art. 15 GDPR or to receive a copy of personal data) without the data subjects asking to obtain a specific piece of information. Only 21% of controllers reported having received such specific requests limited to one or two of the elements of the right of access.

4 POSITIVE FINDINGS AND CHALLENGES IDENTIFIED DURING THE CEF ACTION

This section summarises the participating SAs' impressions about the levels of compliance and awareness of responding controllers when it comes to the right of access and Guidelines 01/2022. It highlights a few positive findings before turning to some of the challenges identified during the CEF action, either by the participating SAs or by respondents themselves.

For each challenge identified below, a list of non-binding recommendations or points of attention is included for controllers, SAs and the EDPB, without prejudice to the provisions of the GDPR/EUDPR and to SAs' powers under data protection law. It is also worth noting that neither these challenges nor these recommendations are exhaustive, but they include those that the EDPB considers the most relevant or which were indicated by multiple participating SAs. Additional findings or recommendations can be found in the respective SA's national reports provided in the Annex.

4.1 Level of compliance and positive findings

Overall, as many as **eleven SAs found the level of compliance of responding controllers concerning the GDPR provisions relating to the right of access to be 'high'** and one SA even found it 'very high'. In contrast, seven SAs considered such level 'average'.

According to ten SAs, the levels of compliance encountered were too diverse or the number of respondents was too low to be able to describe the average level of compliance[31]. Many SAs observed varying levels of compliance among responding controllers. One important factor identified as having an impact on the level of compliance was the **volume of access requests received** by responding controllers. The controllers that receive a higher number of requests were more likely to have formalised an internal process to handle them properly in comparison with controllers which have not

[30] E.g. Guidelines 01/2022, para. 51.

[31] LT SA indicated that they found the level of compliance of controllers "high" but at the same time that the levels of compliance of individual responding controllers were too diverse to qualify. This input has not been integrated above.

yet received a request or who rarely received requests. However, some of the controllers which declared having received no access request in 2023 still had an internal procedure in place.

Diverse levels of compliance can be observed for controllers operating within the same sector but also across different sectors. According to a few SAs, some sectors were showing a higher level of compliance than others. This was for example observed for regulated sectors (e.g. healthcare, banking/finance, government and telecommunications).

Other factors, such as the responding controllers' size, resources and line of business, also seemed to play a role in the level of compliance. A few SAs found that large-sized controllers had more sophisticated internal processes and extensive documentation in place, e.g. using trained staff and privacy management software to review, respond to, as well as track the requests. In that regard, one SA reported a lower level of compliance in the public sector than in the private sector due to less available resources.

In contrast, **SAs had the overall impression that responding controllers were less aware about Guidelines 01/2022**[32], with ten SAs reporting a level of awareness 'average' or 'low' and only nine SAs qualifying it as 'high' or 'very high'. Here again, receiving a higher number of access requests was associated with a higher level of awareness of Guidelines 01/2022, which were more integrated into the controllers' processes and documentation. According to some SAs, although some controllers were aware of and understood the content of the Guidelines, this did not mean that they actively applied them in practice when responding to access requests.

Participating SAs identified specific areas of the Guidelines which seemed to be less well-known and/or less implemented among responding controllers. The challenges described in the subsections below mention these areas and suggest specific recommendations to address these.

However, participating SAs also **encountered positive findings across the EEA**. These include the implementation of best practices mentioned in Guidelines 01/2022 or additional best practices proactively implemented by controllers[33]:

- In that regard, Guidelines 01/2022 were considered a very valuable resource by some controllers. A number of them highlighted that they reviewed and revised their internal procedures and practices following the EDPB's adoption of these Guidelines. This included improving their response templates, improving the level of information to be provided to data subjects, training staff members and raising awareness internally.
- Some controllers use data protection software/digital tools which allow them to efficiently manage and track the access requests from the date of their receipt until the provision of the response to the data subject (e.g. through a ticketing system or by prioritising the requests depending on their due date). In addition, this allows them to ensure that each step is completed by the relevant staff members and to document such steps. Certain controllers also use a system of automatic alerts to provide a timely response.
- Some controllers have a good access and role management in place to ensure that the information linked to the access requests is available on a need-to-know basis to the relevant staff members or teams.
- Some controllers have internal effective role allocation in place, such as appointing (and giving appropriate training to) data protection champions in each department to deal with data access requests. In some cases, the internal procedure entrusts a dedicated team with the

[32] However, the Guidelines were not available in Czech and Hungarian when the questionnaire was first sent out, which may have affected the level of understanding among the respondents. However, at the date of adoption of this report, Guidelines 01/2022 are available in 23 languages.

[33] This list is not exhaustive. Please see each national report in the Annex for further positive findings.

handling of access requests and sets out an escalation process (e.g. to the relevant people in the legal department or to the DPO), for example where the request is complex.

- One SA noted that 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 website. This practice can foster a greater level of transparency and ultimately facilitate the exercise of the data subjects' rights.
- Some controllers use optional online forms to facilitate data subjects' exercise of their right of access in practice.
- Some controllers use self-service systems/portals to allow data subjects to autonomously download their personal data in few clicks and at any time. Such systems facilitate an efficient and timely handling of access requests and conveniently include a verification mechanism tool.
- Some controllers have implemented a procedure to audit on a regular basis the internal process in place to respond to access requests. In one case, it was reported that the DPO carried out the audits themselves, which is a good example of the DPO monitoring the controller's compliance with the GDPR (Art. 39 (1) lit. b GDPR).
- Some controllers provide explanatory information to ensure intelligibility of the personal data provided or send a list detailing what each provided document contains.

4.2 Challenges identified during the CEF action

The following sections detail some of the challenges identified during the CEF action, either by the participating SAs or by respondents themselves, which the EDPB considers to be the most relevant or the most frequent. Additional findings or recommendations can be found in the respective SA's national reports provided in the Annex.

4.2.1 Lack of awareness about the scope of access to be provided

Several SAs have identified concerns regarding the awareness of controllers as to the scope of the personal data that access must be provided to.

- The scope of research within a controller's organisation to compile all relevant personal data often seems to be defined too narrowly. SAs noted that some controllers only search the most commonly used internal databases, or that they send out pre-defined sets of personal data without verifying whether additional personal data is processed concerning the requesting data subject.
- Controllers seem to exclude certain types of files, formats or data entirely from their replies to access requests. E.g. not all controllers seem to be aware that personal data may also be contained in non-textual files, meta data or back-up data. One SA found that some controllers, as a rule, do not include communications between the controller and the data subject. Another SA found that one controller does not include pseudonymised data, and another SA noted that one controller considers traffic data excluded from access. One controller specified that internal communication about the data subjects are not provided.
- Several SAs note that a number of controllers does not ensure that the data provided access to correspond as closely as possible to the state of the data processing at the time of receiving

the request[34]. Data with short retention periods will often be deleted after receipt of the access request before it can be included in the reply[35].

- Another concern is noted in case of repeated access requests. Several controllers seem not to provide full access, but, as a rule, only inform the data subject about changes since their last request, even if the data subject has not limited their request in this regard[36].
- Some SAs noted difficulties for certain controllers regarding the scope of the obligation to provide a copy of the personal data undergoing processing (Art. 15 (3) GDPR), in that they only provide the compiled personal data, but as a principle, never include extracts of documents or even entire documents containing the personal data in question in their replies to access requests.

In cases described above, some or even substantial parts of the personal data processed in relation to a specific data subject will not be included in the reply to an access request. The EDPB recalls that Art. 15 GDPR covers all personal data processed concerning a requesting data subject. Controllers are not in a position to limit their replies to data they consider "relevant" or "important" for the data subject, or that can be easily compiled for a reply. Access should also be provided to personal data the controller knows or assumes is already known to or in possession of the data subject[37]. This is in line with the overall aim of the right of access, which enables data subjects "to be aware of, and verify, the lawfulness of the processing" taking place at the specific controller[38]. In general, and outside the limitations on the right of access[39], it is thus not the controller, but only the data subject who can limit the scope of the access request[40]. In addition, the right to receive a copy of the personal data undergoing processing (Art. 15 (3) GDPR) can entail the right of the data subject to obtain copies of extracts from documents or even entire documents which contain, inter alia, those personal data, if this is essential in order to enable the data subject to effectively exercise their rights, in particular to verify how accurate and exhaustive the data are, as well as to ensure they are intelligible, while taking account of the rights and freedoms of others[41]. Controllers having difficulties compiling all personal data related to an access request may, in some instances, not have a complete overview themselves of which processing activities they conduct and which type and format of personal data is concerned by these activities. This overview is not only needed to be able to comply with access requests, but when it comes to compliance with other data protection obligations, in particular compliance with the data protection principles enshrined in Art. 5 (1) GDPR, like ensuring the integrity and confidentiality of personal data, as well as the principle of accountability (Art. 5 (2) GDPR)[42].

Suggested recommendations to address this challenge:

- Controllers should pre-assess the scope of Art. 15 GDPR from the outset to be aware about which type of information may contain personal data and would thus generally have to be included in the response to an access request.

[34] Cf. Guidelines 01/2022, paras. 34 and 37.
[35] Cf. Guidelines 01/2022, para. 38 on appropriate measures to facilitate the right of access in these cases.
[36] Cf. Guidelines 01/2022, para. 111.
[37] Guidelines 01/2022, paras. 19 and 111.
[38] Recital 63 GDPR.
[39] Guidelines 01/2022, Sections 4.2.5 and 6.
[40] Guidelines 01/2022 paras. 35 and 51.
[41] CJEU, Judgment of 24 May 2024, *Addiko Bank d.d.*, C-312/23, ECLI:EU:C:2024:458, para. 33; Judgement of 26 October 2023, *FT*, C-307/22, ECLI:EU:C:2023:811, para. 79; Judgement of 4 May 2023, *Österreichische Datenschutzbehörde*, C-487/21, ECLI:EU:C:2023:369, para. 45.
[42] See Art. 4 EUDPR applicable to EUIs.

- Controllers should pre-assess where (e.g. which instances and databases) to verify once they receive an access request. The EDPB recommends referring to the record of processing activities to precisely identify possible storage locations of personal data. The record of processing activities (Art. 30 GDPR) should be kept up to date at all times, including when onboarding new IT systems or processors, enlarging the organisational structure of the controller and beginning new processing activities.
- SAs could foster the knowledge of the Guidelines' relevant paragraphs as well as the CJEU case-law cited above, in particular when taking actions based on data subjects' complaints for access requests answered incompletely. Guidelines 01/2022 could also be slightly updated in light of the case-law cited above.
- Where applicable, SAs should revise publications on the right of access in light of recent CJEU case-law and raise awareness about this fact.
- Please also see suggested recommendations in Section 4.2.3.

4.2.2 Indefinite, excessive or inconsistent retention periods relating to access requests

SAs noted several issues concerning the retention periods applied by controllers to access requests and related communication and documentation.

- Some controllers seem to store access requests and related communication indefinitely. The replies suggest that this could be the case for controllers which are rarely confronted with these requests, but it could also be due to controllers' unawareness that the principles of data minimisation and storage limitation also apply to the personal data contained in this communication.
- Some controllers do not seem to store the related communication separately, but together with other information on the data subject (e.g. customer file, applicant for public service file). Thereby, it automatically is subject to the retention periods defined for this other type of information (e.g. business record, tax documentation, archive retention periods).
- Some controllers apply statutory retention periods applicable to other types of documentation, e.g. legal requirements to retain tax documentation, health treatment documentation, business records, archive acts etc. SAs suggest that, in some instances, this is due to different interpretations of national law or potentially unclear provisions.
- Controllers also give different reasonings for why they have chosen a specific retention period (e.g. as long as the relevant data is processed, as long as a contractual relationship with the data subject exists, archive reasons, defence against legal claims, determine effective answers to recurring access requests etc.). In some cases, controllers do not give any reasoning or legal basis at all.
- In particular where controllers state that they retain the communication for defence against legal claims, they base the retention period on different statutory limitation periods for such claims.

Overall, the survey suggests that there is an inconsistent approach to retaining access request documentation across the board, but also in each participating Member State and in some cases even in one sector. SAs note extreme differences in retention periods in the same Member State (e.g. NL: 6 months to 20 years; EE: 3 years to 10 years and longer in some cases; CZ: 3 years to 45 years; LI: 1-30 years; EL: 5 to 20 years, MT: 30 days to 10 years).

The EDPB acknowledges that the GDPR does not stipulate specific retention periods. Controllers face a tension between compliance with the obligation to delete personal data contained in access request communication and the need to prove fulfilment of access requests e.g. in an audit or a legal dispute. Also, different retention periods can apply in specific cases, e.g. where specific legislation applies or the data is needed in the context of preparing or defending a concrete legal claim.

However, in accordance with the principle of storage limitation (Art. 5 (1) lit. e GDPR), controllers must ensure and be able to demonstrate (Art. 5 (2) GDPR)[43] appropriate retention periods for such personal data. Any retention must be objectively justifiable[44]. Controllers should also take into account that in particular the aggregated data package containing all personal data processed in relation to the requesting data subject sometimes offers detailed insight into the data subject's private life.

Suggested recommendations to address this challenge:

- Controllers should fix a retention period for access request communication based on objective criteria and document their reasoning in accordance with Art. 5 (2) GDPR.
- Statutory retention periods for other types of documents or records should not be applied by default. Controllers should carefully assess whether these provisions actually cover access request communication, and document their assessment.
- Controllers should ensure that access request communication is stored separately from other information about the data subject which may be subject to other retention periods (please also see Section 4.2.1 above) and also other access and role management rights within the controller's organisation.
- Further guidance from SAs on uniform and meaningful criteria for determining retention periods, including on national legislation and defence against legal claims, could help controllers in selecting appropriate retention periods. In addition, SAs could support and encourage controllers to take up this issue with broader awareness-raising activities and individual information and guidance for respective responding controllers.
- Please also see suggested recommendations in Section 4.2.3.

4.2.3 Lack of documented internal procedures

Various SAs findings note a lack of detailed internal documented procedures for dealing with access requests. Although it is not a legal requirement for controllers to have a procedural document detailing how it responds to access requests, it is apparent that a lack of a formal documented procedure can heighten the possibility of an infringement of a data subjects rights. This was particularly observable in smaller organisations. Several SAs note that responding controllers have difficulties recognising and handling access requests.

- Controllers indicate such difficulties in particular where requests do not specifically refer to the GDPR.
- Controllers also appear to have difficulties distinguishing access requests from other types of requests, like general requests for information, customer complaints or requests pertaining to administrative document access.

[43] See Art. 4 EUDPR applicable to EUIs.
[44] Cf. Guidelines 01/2022, para. 37 regarding personal data deletion in the context of handling an access request; Art. 5 (1) lit. e, 5 (2) GDPR.

- SAs also identified cases in which access requests go unrecognised if they are submitted through communication channels through which controllers do not expect to receive them.

The EDPB specifies in Guidelines 01/2022 that controllers should be prepared to receive, handle, and provide an appropriate response to these requests without undue delay. Although the GDPR does not specify what preparations a controller should implement in respect of its responsibilities pursuant to Art. 15 GDPR, Guidelines 01/2022 do indicate that these preparations should be adequate and proportionate in order for the controller to fulfil its obligations[45]. Having documented internal procedures can aid a controller in demonstrating it compliance with Art. 12 and 15 GDPR in line with the principle of accountability. The results of the CEF action appear to draw a correlation between the lack of documented internal procedures and a heightened possibility of an infringement of Art. 15 GDPR. This challenge was largely apparent in smaller organisations, or in organisations where the number of access requests received was relatively low. Here, internal procedures regarding the handling of access request were often not documented or if documented were less detailed than those in larger organisations where a higher number of access requests were received. One SA noted that controllers who received a greater number of access requests appeared more attentive to the adoption of formalised procedures in line with Guidelines 01/2022.

A concern, highlighted by various SAs, was that controllers often find it difficult to identify access requests, in particular when the request is submitted through alternate channels that are not designated for dealing with data subject right requests. The EDPB acknowledges that some access requests may be difficult to recognise. However, it must be underlined that the GDPR does not introduce any formal requirements for access requests. In particular, data subjects are not required to indicate a specific legal basis or reference the GDPR access right specifically[46]. If the controller has doubts as to which right(s) the data subject wishes to exercise, it is recommended to ask the data subject making the request to explain its subject matter (notwithstanding controller's obligation to act without undue delay)[47]. Also, controllers should undertake all reasonable efforts to facilitate the exercise of the right of access (Art. 12 (2) GDPR), which includes ensuring that access requests sent via channels which are not specifically designated for data protection requests are handled appropriately[48].

Without a clear defined procedure for responding to access requests, various issues can arise during the lifespan of the access request. One notable challenge observed surrounding access requests being received through channels other than a dedicated channel for these requests was a lack of acknowledgement of the request being sent to the data subject, as well as a delay in forwarding the request to the appropriate data protection unit/individual responsible for dealing with these requests. This may lead to potential delays in responding to the data subject. The EDPB acknowledges that a controller is not legally obliged to send confirmation/acknowledgement of an access request however it is considered good practice[49]. A lack of acknowledgement of the data subject's request may contribute to the controller failing to fulfil the data subjects' access request within the statutory timeframe under Art. 12 (3) GDPR. Similarly, this may also result in the controllers' failure to notify the data subject should it require an extension of the statutory timeframe in order to fulfil the access request. One SA noted that a lack of acknowledgement of the access request often leads to complaints being lodged with the authority.

[45] Guidelines 01/2022, para. 42.
[46] Guidelines 01/2022, paras. 47, 48 and 50.
[47] Guidelines 01/2022, para. 48.
[48] Guidelines 01/2022, paras. 53 et seq. including practical examples.
[49] Guidelines 01/2022, para. 57.

The results of the CEF action indicate that the size and structure of the organisation often plays a key role in determining if the organisation has internal documented procedures for the handling of access requests. In smaller organisations, resources may not be allocated to have a dedicated data protection unit, which can for example result in one individual being responsible for responding to access requests. This can be problematic, both in terms of active compliance (e.g. one individual is expected to ensure that the access request has been fulfilled within the statutory timeframe and contains all personal data sought by the data subject) and in terms of preserving long-term compliance (e.g. ensuring access requests are handled when the individual is on leave, sick etc.). Internal documented procedures aid in ensuring that there is a procedure to follow should the person responsible for responding to these requests be unavailable.

Suggested recommendations to address this challenge:

- The EDPB could issue further guidance regarding best practices for documenting compliance with Art.15 requests, including detailed internal documented procedures.
- SAs could promote the adoption of Codes of Conduct, pursuant to Art. 40 GDPR, in order to identify standardised procedures for the effective application of the right of access, also in view of the different categories of controllers.
- A proper exchange between all relevant internal actors within controllers' organisations should be established to properly qualify and filter requests from the outset. This can include the involvement of the controllers' DPOs, e.g. to provide general guidance on recognising access requests or for more complex access requests.
- Controllers should ensure that all employees are trained to recognise an access request no matter the channel it is submitted through, and are aware of the appropriate channel to transfer it to[50].
- Controllers should ensure that they are actively reviewing and (where necessary) improving their data protection practices. Such reviews may, among others, consider Guidelines 01/2022.
- When in doubt whether an individual's request is an access request pursuant to Art. 15 GDPR, controllers should verify this with the individual making the request.
- Controllers could provide guidance to data subjects on different types of requests and their scope. A good practice could be setting up a web form guiding the requester through a series of preliminary questions aiming to help the person identify whether they chose the appropriate 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. However, controllers should still keep in mind that the GDPR does not introduce formal requirements for access requests.

4.2.4 Barriers to the facilitation of the right of access

SAs also identified concerns relating to the facilitation of the right of access, namely barriers in place which can prevent the data subject from exercising this right.

- Some controllers required data subjects to use a specific mechanism (i.e. web-form) to exercise their right of access.

[50] Cf. Guidelines 01/2022 para. 54: "*It should be noted that the controller is not obliged to act on a request sent to a random or incorrect e-mail (or postal) address, not directly provided by the controller, or to any communication channel that is clearly not intended to receive requests regarding data subject's rights if the controller has provided an appropriate communication channel, that can be used by the data subject*."

- Controllers noted difficulties in identifying and authenticating (i.e. confirming the identity of) data subjects when an access request is received[51].
- Some controllers request further information in order to identify and/or authenticate the data subject for most/all access requests they receive.
- Several SAs note that in some cases, controllers do not always consider the accessibility needs of a data subject when fulfilling access requests (i.e. fulfilling an access request verbally).

Controllers should be prepared to receive and handle a request for access no matter the means in which it is received. There is no correct or standard way to exercise the right of access, and there should not be a barrier in place to prevent/hinder a data subject from exercising their rights. Guidelines 01/2022 reiterate that the GDPR does not provide for any formal requirements for access requests[52], that a controller shall facilitate the exercise of the right of access[53] and should not refuse to act upon access requests unless it is in a position to demonstrate it is unable to identify the data subject (Art. 12 (2) GDPR). Responding SAs commented that controllers' use of a formal mechanism (i.e. web form) to submit an access request may be perceived as a barrier to exercising data subject rights. Some SAs commented that some controllers' use of specific formal requirements (i.e. requiring requests to be submitted in written form) formed a barrier to data subjects gaining access to their personal data, in some cases controllers stating that only receipt of a request in written form would trigger the start of the statutory timeframe pursuant to Art. 12 (3) GDPR.

Another SA noted that some controllers did not differentiate between types of data subjects, which can lead to the format of the information provided to the data subject not being adapted to the accessibility needs of that data subject, in particular for vulnerable individuals. Additionally, some of the responding SAs noted that some controllers do not accept oral access requests and/or requests for personal data to be provided orally at all, without further examination of the specific request[54]. One SA identified that a controller would only accept an access request submitted in a written format and would not accept an access request made over the phone. This is particularly concerning as these controllers did not demonstrate their ability to adhere to the accessibility needs of data subjects and to provide personal data in a way which is intelligible and easily accessible for the data subjects[55].

Another barrier identified through the findings of the CEF action was linked to the authentication of data subjects. One SA found that 70% of the participating controllers do not provide a response to an access request verbally due to a lack of authentication of the data subject. However, 30% of the responding controllers did offer a verbal response to an access request when the data subject provided multiple identifiers for authentication, such as a client or ID number, or when working in sectors that process the personal data of vulnerable individuals, such as the elderly, the visually impaired, or persons with cognitive or other disabilities. Furthermore, a few participating SAs observed the use by some controllers of a generic request for (additional) information to confirm the identity of the data subject on receipt of any access request (e.g. identification documents). Controllers have an obligation to ensure the security of personal data and to mitigate the risk of unauthorised disclosure of same. It is important to note that controllers can and should request a form of identification or additional information that enables authentication of the data subject should it have reasonable doubts of the identity of the individual[56]. This request for additional information should be proportionate to the type of data being processed by the controller, the nature of the request, the context in which the request is being made as well as any damage that could result from

[51] Cf. Guidelines 01/2022, paras. 58 et seq.
[52] Guidelines 01/2022, para. 50.
[53] Art. 12 (2) GDPR.
[54] Cf. Art. 12 (1) GDPR.
[55] Cf. Guidelines 01/2022, para. 128.
[56] Art. 12 (6) GDPR, Guidelines 01/2022, para. 63.

improper disclosure[57]. The controller should be able to demonstrate the reasonable doubt if requested. An indiscriminate request for an identification document for all access requests may constitute excessive processing of personal data[58] and may create an unnecessary barrier to the data subjects' right of access. A controller should determine if it requires additional information in order to confirm the identity of the data subject on a case-by-case basis.

Suggested recommendations to address this challenge:

- Controllers should ensure that they are prepared to handle access requests even if the request is not submitted through a dedicated data protection channel[59].
- Controllers should assess each access request received on a case-by-case basis in order to determine if further identification or authentication of the data subject is required in order to fulfil the request.
- Controllers should be made aware of their obligation to demonstrate their need for further identification documents to confirm the identity of the data subject upon receipt of an access request if requested.
- SAs could issue further guidance focused on best practices for adhering to a controller's accessibility requirement.

4.2.5 Inconsistent and excessive interpretations of the limits to the right of access

SAs also noted several issues concerning the interpretation of the limits and restrictions to the right of access by responding controllers.

Relating to Art. 12 (5) GDPR ("manifestly unfounded or excessive"), SAs note that:

- Some controllers interpret this restriction too broadly. For example, requests are refused due to their lack of precision, or due to cost concerns, or controllers ask the data subject to narrow the request or pay a fee[60]. One SA found that controllers charge a fee for data subjects requesting access more than once a year – possibly based on national legislation passed prior to GDPR and which has since been revoked.
- Some controllers refuse handling access requests due to (suspected) intentions of the data subject to pursue objectives not directly related to data protection. This is not only in contradiction to Guidelines 01/2022[61], which only detail very limited circumstances in which the intentions of the data subject can lead to an access request falling under the exception of Art. 12 (5) GDPR[62], but also to recent CJEU case-law[63].
- Some controllers state that they have not received a large number of access requests or none at all, and therefore have not established an internal definition of use cases for the limitations

[57] Guidelines 01/2022, paras. 70 et seq.
[58] Guidelines 01/2022, paras. 65, 70 et seq.
[59] Cf. Guidelines 01/2022, para. 54: "*It should be noted that the controller is not obliged to act on a request sent to a random or incorrect e-mail (or postal) address, not directly provided by the controller, or to any communication channel that is clearly not intended to receive requests regarding data subject's rights if the controller has provided an appropriate communication channel, that can be used by the data subject*."
[60] Cf. Guidelines 01/2022, paras. 22 and 166.
[61] Guidelines 01/2022, paras. 13 and 167.
[62] Guidelines 01/2022, paras. 189 et seq.
[63] CJEU, Judgment of 26 October 2023, *FT*, C-307/22, ECLI:EU:C:2023:811, para. 52.

in Art. 12 (5) GDPR. On the other hand, one controller stated that given the burden of proof relating to Art. 12 (5) GDPR is on the controller, it would simply never use this exception at all.

With regard to Art. 15 (4) GDPR ("rights and freedoms of others"):

- Controllers do not provide entire copies of the personal data processed (e.g. no video footage at all or only a few images instead of entire video material), but only parts for reasons of time or cost efficiency (e.g. avoid blurring other individuals' faces in the (entire) video material).
- Based on Art. 15 (4) GDPR, some controllers never disclose information about their employees handling the personal data of the requesting data subject. However, occasionally it may be required to share information about the identity of these individuals[64].
- Two SAs found that controllers who base their refusal to act on an access request in whole or in part on Art. 15 (4) GDPR do not comply with their obligation to inform the data subject accordingly[65].
- On the other hand, some SAs found that several controllers seemed not to be aware that they can (and should) protect the rights and freedoms of others based on Art. 15 (4) GDPR when handling access requests. These controllers' replies seemed to suggest they would provide access to all relevant personal data without limitation at all times, or they did not cite any legal bases limiting or restricting the right of access.

As overall concerns with regard to limiting the right of access, SAs noted that there seems to be a tendency of controllers to interpret the limits and restrictions of the right of access too broadly, both when it comes to the specific limitations of Art. 12 (5) and 15 (4) GDPR as well as when it comes to national legislation limiting the right of access in accordance with Art. 23 GDPR[66].

- In some cases, the reasons for refusing to act on access requests are vague or unclear (e.g. controllers stating that the personal data was "irrelevant to the data subject" or that "the requests do not apply to data being processed".
- One SA suggests that for some controllers, there seems to be a systematic use of the limits of the access right to refusing employees access to professional mails and phone recordings relating to them.
- Some controllers seem to rely on limits or exceptions contained in Art. 13, 14 or 17 GDPR, or limits or exceptions in national legislation relating to access to other types of information (e.g. administrative documents, civic access, whistleblowing, commercial secrecy and IP), which do not apply to the right of access.

The EDPB acknowledges that access requests can be both costly and time-consuming for controllers to handle properly, and that controllers may fear that granting access could expose their organisation to abuse or misuse. Some SAs suggest that controllers would consider refusing to act on access requests to be a protective measure for their organisation. In particular with regard to providing access to employee data, the EDPB also recognises the controllers' intention of protecting their own workforce.

[64] CJEU, Judgment of 22 June 2023, *Pankki S*, C-579/21, ECLI:EU:C:2023:501, para. 83, where *"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."*
[65] Cf. Art. 12 (4) GDPR, Guidelines 01/2022, para. 174.
[66] See Art. 25 EUDPR for restrictions to the right of access applied by EUIs.

However, the EDPB also recalls that the GDPR only provides for very few limits of the right of access. The right of access is without any general reservation to proportionality with regard to the efforts the controller has to take to comply with the data subject´s request[67]. In particular, the concepts of "manifestly unfounded or excessive" should be interpreted narrowly, as "the principles of transparency and cost free data subjects rights must not be undermined"[68]. There are several ways in which controllers can reduce the burden of handling access requests without recurring to limits or restrictions, such as implementing well-structured procedures, data maps or record of processing activities (please see Section 4.2.3 above), training staff appropriately, or using technical tools to assist dealing with requests.

Suggested recommendations to address this challenge:

- SAs and EDPB could develop guidance including examples of correct refusal practices / specific scenarios or use cases resulting in a limitation of access (with regard to GDPR limitations, but also on a national level regarding provisions implemented in accordance with Art. 23 GDPR) to help controllers understand the boundaries within which access requests can be fully or partially rejected.
- Communication by EDPB and SAs on the cited recent CJEU case-law could increase controllers' awareness about the above-mentioned topics. Guidelines 01/2022 could also be slightly updated in light of these decisions.
- Controllers should be aware that in cases where they restrict a data subject's right to access, they should be able to demonstrate /explain the reasoning behind such a restriction to the data subject.
- Controllers should adopt policies that balance the rights and freedoms of themselves and third parties with the rights of data subjects, in particular where the right of privacy of their employees is concerned, and assess Art. 15 (4) GDPR situations in a case-by-case approach.

4.2.6 Excessive interpretation of the possibility to ask for specification of access requests

As an additional aspect, several SAs have identified difficulties for controllers concerning the possibility to request data subjects to specify the information or processing activities to which the access request relates[69]. In particular, SAs have found that controllers tend to ask data subjects to specify their request:

- without verifying whether the controller actually processes a large quantity of information concerning the data subject requesting access in accordance with recital 63 s. 7 GDPR;
- by default for any access request received, without any pre- or plausibility check conducted in the databases of the controller;
- without verifying whether the access request leaves any doubt about the scope of the information that the data subject requests access to;
- without informing the data subject about the processing activities that concern them[70].

In some instances, controllers would expressly make the specification a pre-condition for the further handling of the request. In contrast, one SA noted that responding controllers did not address the

[67] Guidelines 01/2022, p. 5, para. 166.
[68] Guidelines 01/2022, para. 175.
[69] Cf. Recital 63 s. 7 GDPR, Guidelines 01/2022, para. 35b with several practical examples.
[70] Cf. Art. 12 (2) GDPR, Guidelines 01/2022, para. 35b, after example 4.

possibility to ask for specification of an access request under recital 63 s. 7 GDPR in their replies. For the controllers in question, the requirements are potentially fulfilled; it is unclear whether these controllers are aware of said possibility.

The EDPB recalls that the possibility to ask data subjects to specify their request, in accordance with recital 63 s. 7, is not open to all controllers and for all access requests, but subject to conditions which are further elaborated on in Guidelines 01/2022, para. 35b. Furthermore, requesting a specification should not aim at a limitation of the reply to the access request and "shall not be used to hide any information on the data or the processing"[71]. Therefore, when asking data subjects to specify their request, controllers "shall at the same time give meaningful information" about the processing operations that could concern the data subject (Art. 12 (2) GDPR)[72].

In particular, the EDPB reiterates that asking data subjects to specify their request should not be confused with the "layered approach" in providing access[73]. The specification request is about understanding the *scope* of the data subjects' request to clarify whether the data subject wishes to receive access to *all* or only *parts* of the personal data processed concerning them. It is therefore related to the *content* of the access to be provided. The "layered approach", on the other hand, concerns the *format*, or *presentation*, of the access to be provided. Therefore, requesting data subjects to specify on the scope of access "as a first step", while providing full access upon specification "as a second step" is not considered to be a "layered approach" as promoted by the EDPB in Section 5.2.4 of Guidelines 01/2022.

Suggested recommendations to address this challenge:

- SAs could foster the knowledge of the cited Guidelines' paragraphs, e.g. via awareness raising activities or in particular when taking actions based on data subjects' complaints, including clarifications on the difference between specification as per recital 63 s. 7 GDPR and the "layered approach" promoted by the EDPB.
- EDPB could include brief clarifications on the difference between specification as per recital 63 s. 7 GDPR and the "layered approach" in Guidelines 01/2022.
- Controllers should assess each access request on a case-by-case basis to verify whether the conditions of recital 63 s. 7 GDPR are met, and inform the data subject about any processing activities potentially concerning them in their request for specification.
- Upfront, controllers could provide data subjects with self-service tools or with possibilities to pre-select one, several or all processing activities which they would like to receive information on[74], always taking into account that the GDPR does not provide formal requirements for access requests and that, where a data subject "confirms to seek all personal data concerning him or her, the controller of course has to provide it in full"[75].
- Where applicable, SAs should revise publications on the right of access in contradiction with Guidelines 01/2022, para. 35b.

4.2.7 Provision of insufficiently detailed or tailored information to data subjects

[71] Guidelines 01/2022, para. 35b, after example 5.
[72] Guidelines 01/2022, para. 35b, after example 4.
[73] Guidelines 01/2022, Section 5.2.4, in particular para. 143.
[74] Guidelines 01/2022, para. 35b.
[75] Guidelines 01/2022, para. 35b, after example 5; cf. Art. 15 (1), 15 (3) GDPR, Recital 63 GDPR.

The survey also revealed concerns with regard to the level of detail and preciseness of information provided to data subjects in accordance with Art. 15 (1) and (2) GDPR.

- Several SAs have noted that responding controllers provide information that is not tailored to the specific request of the specific data subject, in particular when it comes to information listed in Art. 15 (1), (2) GDPR. For instance, certain controllers simply refer to their privacy policy or pre-defined sets of information.
- In particular when it comes to information about recipients of personal data (Art. 15 (1) lit. c GDPR), a large number of responding controllers only provide categories, and only name individual recipients in case of a specific request of the data subject.
- Retention periods (Art. 15 (1) lit. d GDPR) are often only specified in very general terms, without distinguishing between processing activities or data categories[76].
- One SA found that responding controllers generally tend to provide only the pre-determined requested type of data, but rarely provide additional information about the processing.

It may be easier for controllers to refer to pre-existing documents like privacy policies instead of compiling specific information for each request, in particular for controllers receiving large numbers of access requests. Also, SAs suggest that the difficulties for controllers to provide tailored information per access request could result from the data management within the controller's organisation.

However, the EDPB recalls that the information provided to data subjects in accordance with Art. 15 (1) and (2) GDPR should be tailored to the specific data subject and the specific access request[77]. In particular, pre-existing documents should only be referred to after careful assessment of the specific access request. This is because, on the one hand, these documents often do not contain all information required under Art. 15 (1) and (2) GDPR. On the other hand, not all information provided in these documents may apply to the specific data subject, leaving them to guess which information applies to them specifically (e.g. how long exactly their data will be retained). This is problematic both in light of the aim of the right of access "to be aware of, and verify, the lawfulness of the processing"[78] as well as in light of the controller's obligation to facilitate the exercise of data subjects rights (Art. 12 (2) GDPR).

With regard to recipients (Art. 15 (1) lit. c GDPR) specifically, it should be recalled that the CJEU has already provided further clarification[79]. In difference to Art. 13 and 14 GDPR, which lay down an obligation on the part of the controller, Art. 15 GDPR lays down a genuine right of access for the data subject. As a result, unless the data subject has not chosen otherwise, the controller is required to name the actual recipients, unless it is impossible to identify those recipients or the controller demonstrates that the data subject's requests for access are manifestly unfounded or excessive as per Art. 12 (5) GDPR.

Suggested recommendations to address this challenge:

- Controllers should handle access requests on a case-by-case basis and inform the specific data subject which personal data is processed for which purposes, as well as include information as listed in Art. 15 (1), (2) GDPR which is tailored to the specific data subject and access request.

[76] Cf. Guidelines 01/2022, para. 118.
[77] Guidelines 01/2022, paras. 112 et seq.
[78] Recital 63 GDPR.
[79] CJEU, Judgment of 12 January 2023, *Österreichische Post*, C-154/21, ECLI:EU:C:2023:3, in particular para. 36; cf. also Guidelines 01/2022, para. 117.

- Controllers are responsible for accurately recording to which entities precisely they disclose personal data and where these recipients are located, to be able to name the actual recipients in accordance with Art. 15 (1) lit. c GDPR[80]. A comprehensive updated record of processing activities is helpful to fulfil this responsibility.
- SAs could foster the knowledge of the cited Guidelines' paragraphs as well as the CJEU case-law, e.g. via awareness raising activities like publications, newsletters etc.
- Where applicable, SAs should revise publications on the right of access in light of recent CJEU case-law and raise awareness about this fact.

4.2.8 Conclusion on raising awareness on Guidelines 01/2022

The recommendations suggested for each challenge above include targeted awareness-raising actions relating to specific parts of Guidelines 01/2022 that are they less known and/or less implemented in practice. More generally, 27 SAs in total consider carrying out actions **at national level** to communicate and raise awareness with respect to the content of Guidelines 01/2022. Regarding the means of such actions, they plan to:

- offer more online or remote training sessions (e.g. in videos or podcasts addressed to data subjects);
- offer more online guidance through Frequently Asked Questions addressed to specific sectors; best practices and use cases for SMEs; and updating guidance already issued in light of findings of the CEF action;
- discuss about the findings of the CEF action in networking conferences or workshops addressed to controllers, but also to data subjects;
- integrate the findings of the CEF action in their general consulting/advisory practice, e.g. during regular exchanges with stakeholders (e.g. controllers of different sectors or DPOs, industry or sectoral associations).

Section 5 below provides more detail on which actions have already been taken at national level and which actions participating SAs are considering to take following this CEF action.

In addition, 18 SAs consider that more actions should be carried out **at EDPB level** to communicate and raise awareness with respect to the content of Guidelines 01/2022. While it was noted that the publication of this report in 2025 will increase awareness, additional awareness-raising actions suggested by SAs mainly revolve around publishing more content on the right of access on the EDPB's website, in particular:

- Content with respect to the decisions of the CJEU and decisions of SAs. In that regard, the EDPB recalls the existence of the EDPB register which makes it possible to filter the One-Stop-Shop decisions relating to the right of access[81]. In addition, a project was commissioned and completed in parallel to this CEF action as part of the Support Pool of Experts to analyse these OSS decisions and draft a "case digest" on this topic[82];
- Interactive material or the publication of a user-friendly poster or flyer;
- Promoting the flowcharts annexed to Guidelines 01/2022;
- Publishing Frequently Asked Questions to complement Guidelines 01/2022;
- Developing further information on individual Sections of Guidelines 01/2022, possibly collected outside of the immediate text of the Guidelines as separate resources of information

[80] Also see EDPB Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s), adopted on 7 October 2024, paras. 30, 31 and 89.
[81] https://www.edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en.
[82] Available at https://www.edpb.europa.eu/system/files/2025-01/oss-case-digest-right-of-access_en.pdf.

(e.g. on Section 6.4 at national level of the Member States, a list of existing regulations on limitations of the right of access).

In addition to the specific measures listed above, EDPB could also foster the knowledge about Guidelines 01/2022 in discussions with stakeholders or policymakers in the context of other legislative or administrative projects.

5 ACTIONS TAKEN BY SAS RELATING TO THE RIGHT OF ACCESS

This section maps out the actions carried out by SAs at national level in relation to the right of access – both independently from and in the course of this CEF action – and summarises them depending on their nature (e.g. whether they relate to enforcement or guidance). However, this section does not aim to present a comprehensive overview of all actions conducted by SAs, nor does it list ongoing actions that are not finalised and on which SAs have not yet publicly communicated. Each individual report of the participating SAs detailing their respective actions is available in **Annex 1** attached to this report.

5.1 Enforcement

SAs have a number of powers at their disposal in accordance with Art. 58 GDPR, including corrective powers such as issuing reprimands or orders to comply or fines, for cases of non-compliance with the requirements of Art. 15 GDPR. In accordance with Art. 83 (5) GDPR, if a controller does not fulfil its obligations in respect of data subjects' rights pursuant to Art. 12 to 22 GDPR, it can be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. However, in some Member States, some public sector controllers cannot be fined under the GDPR due to restrictions imposed by the national legislator.

Several SAs indicate that undertaking enforcement actions often derives from individual data subjects' complaints submitted to the authorities. Issues arising from complaints often relate to the scope of the access request, restrictions on the right of access, providing information pertaining to categories of recipients of personal data, and lack of action by controllers on access request within the statutory timeframe under Art. 12 (3) GDPR. The findings of this CEF action highlight that complaints lodged to SAs regarding the right of access often result in formal investigations and administrative proceedings, which can in turn result in the issuing of corrective measures.

Prior to this CEF action, SAs have already taken action at national level to enforce the data subject's right of access. For instance, HR SA issued a fine of 146,667 EUR to a banking institution as a result of the bank's refusal to comply with Art. 15 (3) GDPR wherein it refused to provide a data subject with a copy of their personal data. Furthermore, IE SA has taken corrective actions as a result of infringements of Art. 15 GDPR, notably, issuing a reprimand to an airline who failed to provide a data subject with a copy of all the personal data it processed concerning them at the time of the request, and further failed to notify the data subject of its need for an extension of the statutory timeframe under Art. 12 (3) GDPR[83]. In 2023, IE SA also issued three enforcement notices pertaining to non-compliance and incomplete responses to an Art. 15 request[84].

[83] Decision of 10 November 2022, available at https://www.dataprotection.ie/sites/default/files/uploads/2021-02/10.11.2020_Decision_Complaint_RyanairDAC.pdf.
[84] Details of enforcement notices available in the IE SA's Annual Report 2023, p. 22 and p. 110 https://www.dataprotection.ie/sites/default/files/uploads/2024-05/DPC%20EN_AR%202023_Final%20.pdf.

As part of this CEF action, various SAs plan to initiate formal investigation into matters of concern as a result of their fact-finding exercise. SI SA plans to initiate three formal investigations which will target specific entities, namely, a healthcare centre, a bank and a law enforcement authority. SI SA plans to further assess the information received from the CEF questionnaire to determine any necessary actions or recommendations, which may be suitable to undertake. One DE SA plans to conduct an on-site audit of one of the controllers who partook in the CEF questionnaire, furthermore, several participating DE SAs will consider the possible launch of formal investigations and consider issuing corrective measures.

Several of the participating SAs (PT, CZ, FI, HU) plan to undertake a further analysis of the information compiled to determine if further action is required, such as corrective measures.

5.2 Guidance

As mentioned throughout this report, the EDPB has adopted extensive guidance on the right of access in its Guidelines 01/2022. In light of the findings of the CEF action, small additions or amendments to these Guidelines have been suggested as possible recommendations by some SAs (please see Section 4.2 above). A few participating SAs highlighted that these Guidelines could be slightly updated, in particular in line with the most recent decisions of the CJEU on the right of access, notably C-487/21; C-579/21; C-307/22, C-312/23. With regard of the SAs' plans to further raise awareness of these Guidelines, please see Section 4.2.8 above.

Certain SAs have developed their own general and specialised guidelines on the matter. For instance, ES SA has published comprehensive guidance dedicated to the rights of data subjects and the obligations of controllers in respect to those rights. This is compiled into specific sections for various sectors and topics where the most relevant issues for controllers are addressed. It contains a Q&A section which includes an online assistant to answer frequently asked questions by data subjects[85]. LI SA has also published comprehensive guidance on the right of access on their website. This guidance covers who can request access to data, what data can be requested, how data can be obtained, in what form data can be obtained, what cost can be occurred with the right of access, when data is restricted or refused as well as information on the right to access to personal data relating to deceased persons[86]. Along similar lines, IE SA has published various specialised guidelines on this topic, including guidelines aimed at controllers and ensuring their compliance, as well as guidance aimed towards data subjects which details the right of access and a FAQ section which provides further guidance in relation to the right of access[87]. EDPS has also published a factsheet on data subject rights, detailing the right

[85] ES SA, Exercise your rights, 16 July 2024, available at https://www.aepd.es/derechos-y-deberes/ejerce-tus-derechos , FAQs your rights available at https://www.aepd.es/preguntas-frecuentes/1-tus-derechos.

[86] LI SA, Right to information pursuant to Art. 15 GDPR, available at https://www.datenschutzstelle.li/datenschutz/themen-z/auskunftsrecht.

[87] IE SA, Data Subject Access Request FAQ's, October 2019, available at https://www.dataprotection.ie/sites/default/files/uploads/2019-10/FAQ%20Guide%20to%20Data%20Subject%20Access%20Requests_Oct19.pdf.
Subject Access Request: A Data Controllers Guide, October 2022 available at https://www.dataprotection.ie/sites/default/files/uploads/2022-10/20221005%20Subject%20Access%20Requests%20A%20Data%20Controller%27s%20Guide.pdf.
The Right of Access available at https://www.dataprotection.ie/en/individuals/know-your-rights/right-access-information#Access.
Access and Portability available at https://www.dataprotection.ie/en/organisations/know-your-obligations/access-and-portability#Access.

of access[88]. Focusing on individuals as well as small to medium sized organisations, LU SA launched an interactive tool named DAAZ that utilises easily understandable language and practical cases to raise awareness of data protection for those with limited data protection knowledge. Further general or specialised guidance by participating SAs can be found in the respective national reports in the Annex.

5.3 Conferences and information campaigns

Several of the participating SAs plan to publish their findings of the CEF action with the aim to raise awareness with controllers and the public, and many SAs will accompany these findings with recommendations to controllers based on their analysis of the CEF action. BG SA plans to launch an information initiative, part of the constant awareness-raising national campaign since 2018, on its website presenting the results of this CEF action in a way that engages the attention of both data subjects and controllers, fostering a positive national trend in awareness of the right to access. The goal of this campaign will be to educate individuals on how they can exercise this right and empower the public with the knowledge to effectively manage their personal data and know their rights pursuant to the GDPR. LI SA organises an annual meeting/training for all DPOs, during which they are provided with information about the SA's work, recent legal developments and other updates. LI SA utilised this meeting, held in November 2024, to inform controllers of their findings of this CEF action, this formed part of their general presentation of this CEF action and the implementation of the right of access. Similarly, HU SA organised an annual conference in 2024 for all DPOs, and included presentations regarding the right of access. Lastly, FI SA aims to send relevant guidance to some controllers who partook in the questionnaire. Similarly, some participating DE SAs also noted that they aim to create information sessions and training events for controllers to provide guidance and ensure compliance with Art. 15 GDPR.

6 CONCLUSION

This CEF action has enabled participating SAs to share, discuss and analyse their experience and conclusions on the implementation of the right of access by controllers. Based on the survey results, many of the participating SAs evaluated the level of compliance of responding controllers with respect to the right of access to be from 'average' to 'high'. One important factor identified as having an impact on the level of compliance was the volume of access requests received by controllers, as well as the size of the controller's organisation. However, the results suggest that controllers are less aware about the content of Guidelines 01/2022. As a result, some aspects that are developed in Guidelines 01/2022 are not followed in practice by some controllers. Despite this, participating SAs observed positive findings across the EEA. These include the implementation of best practices mentioned in Guidelines 01/2022 or additional ones proactively implemented by controllers.

This CEF action allowed the identification of a number of challenges to the handling of access requests by controllers and thus to the exercise of the right of access by data subjects in practice. Participating SAs have formulated several recommendations for controllers, SAs and the EDPB to take into account. While the CEF action has raised the awareness of the responding controllers about the applicable requirements and some of the elements of Guidelines 01/2022, the results of this CEF action suggest that raising awareness about Guidelines 01/2022 as well as fostering the knowledge about respective

FAQs Difficulties with my Subject Access Request? available at https://www.dataprotection.ie/en/faqs/access-and-rectification/difficulties-my-subject-access-request#Access%20Request.

[88] EDPS, Your Data, Your Rights, available at https://www.edps.europa.eu/system/files/2022-01/22-01-21_infographic_dataproday22_en.pdf.

applicable CJEU case-law is necessary more broadly, both at national and EU level, to ensure that the right of access can be effectively exercised by data subjects in practice. To that end, both controllers and data subjects need to be made aware of their obligations and their rights, respectively. Guidelines 01/2022 contain extensive guidance and several practical examples that may help controllers in addressing the challenges raised.

The present report is the state of play, at the end of 2024, of the CEF action regarding the implementation of the right of access by controllers. It may need to be subsequently updated to take into account the progress of procedures which have not yet been completed to date and /or given the issues identified.

ANNEX 1: NATIONAL REPORTS BY SUPERSIVORY AUTHORITIES

The national reports were submitted by participating SAs over the course of September 2024. This means that they represent the situation at this point in time.