May 2022

International: EDPB guidelines on data access requests under Article 15 of the GDPR - takeaways for EU and US companies

In January 2022, the European Data Protection Board ('EDPB') issued Guidelines 01/2022 on data subject rights – Right of access[1]. Odia Kagan provides an in-depth analysis of what companies need to know and do regarding the Guidelines.

Petrovich9 / Essentials collection / istockphoto.com

The Guidelines contain many actionable 'do's' and 'don'ts'. Companies in the EU should listen closely but so should companies subject to the new US privacy laws which grant this right.

Accountability

You should always be able to demonstrate that your data subject access request process aims to give the broadest effect to the right of access and that it is in line with your obligation to facilitate the exercise of data subject rights.

Nature and scope of the request

The right of access includes three different components:

- confirmation as to whether data about the person is processed or not (this confirmation may be communicated separately, or it may be encompassed as part of the information on the personal data being processed);
- access to this personal data; and
- access to information about the processing, such as purpose, categories of data and recipients, duration of the processing, data subjects' rights, and appropriate safeguards in case of third country transfers.

The right to get a copy is a modality of providing access to the data.

How to prepare for receiving requests

The way you prepare for the exercise of access requests should be adequate and proportionate and depend on the nature, scope, context, and purposes of processing, as well as the risks to the rights and freedoms of natural persons, in accordance with Article 24 of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR').

You should introduce, where possible, mechanisms to improve internal communication between employees on requests received by those who may not be competent to deal with such requests (e.g. internal policies, access controls, log reviews).

You also need to mind your backups. If you need to restore from backup, have a system to track what you deleted in the live system may not have been deleted in the backup (like a delete request or an opt out or correction). Reviewing your log of deletions in the live production system may enable the controller to see that there is data in the back-up which is no more in the live system as it has been deleted, and which has not yet been overwritten in the back-up.

What to assess when getting a request

- Does the request concern personal data of the individual making the request?
- Does the request fall within the scope of Article 15 of the GDPR (or does a sector-specific law apply)? This is also important for US sector-specific laws that allow this, for example the Health Insurance Portability and Accountability Act of 1996 ('HIPAA').

- The individual does not need to specify legal basis, but if they refer to a specific law and not the GDPR then you need to handle in accordance with that law.
- If you have already replied under specific law, assess whether you need to comply under the GDPR as well or not.
- When in doubt, ask the data subject and allocate time for receiving the response that still allows you to respond in time.
- If you receive no response, you should interpret it, bearing in mind the obligation to facilitate the exercise of the person's right of access, as the information contained in the first request and act on its basis.
- Does the request refer to all or only parts of the data processed about the data subject?
- Any limitation of the scope of a request to a specific provision of Article 15 of the GDPR, made by the data subjects, must be clear and unambiguous (for example, 'I want to know the sources of the information and period of storage').

What not to assess

- Why the data subject is requesting access.
- Whether the requested data could be used by the data subject to defend themselves in court in the event of a dismissal or a commercial dispute with the controller. However, once litigation has commenced, the right of access may be limited by state law pertaining to information exchange during the course of active litigation.
- Whether a different kind of right of access with a different aim applies, such as in the context of an examination procedure or access to public documents (for example, under freedom of information laws).

Requirements for the making of a request

- You must deal with the request unless it is clear that the request is made under rules other than data protection rules.
- There are no specific requirements on the format of a request (statements like: 'I want access to my personal data" or 'I want to know information about me that you have' are enough).
- You must provide appropriate and user-friendly communication channels that can easily be used by the data subject. However, the data subject is not required to use these specific channels and may instead send the request to an official contact point of the controller. However, the California Consumer Privacy Act of 2018 ('CCPA') regulations require specific methods for submitting the requests.
- You are not obliged to act on requests that are sent to completely random, or apparently incorrect, addresses or to any communication channel that is clearly not intended to receive requests regarding data subject's rights if you have provided an appropriate communication channel that can be used by the data subject.

- You are also not obliged to act on a request sent to the email address of a controller's employee who may not be involved in the processing of requests concerning data subjects' rights (e.g. drivers, cleaning staff, etc.). Such requests shall not be considered effective if you have clearly provided the data subject with appropriate communication channel.
- However, if the data subject sends a request to an employee who deals with the data subject's affairs on a daily basis (single contact of a customer, such as a personal account manager), such contact should not to be considered as a random one. You need to make all reasonable efforts to handle such a request so that it can be redirected to the contact point and answered within the time limits provided for by the GDPR.
- If you have a queries email and a general contact email and get a request for a general access request, you need to make all reasonable efforts to make your people aware of the request and forward it and answer it in time.

Time

The date of receipt of the request by the company triggers, as a rule, the one month period for the controller to provide information on action taken on a request, in accordance with Article 12(3) of the GDPR.

You should confirm receipt of requests in writing, for example by sending emails (or information by post, if applicable) to the requesting persons confirming that their requests have been received and that the one-month period runs from day X to day Y.

The CCPA regulations require confirmation of the receipt of the request within 10 business days, as well as the provision of information about how the business will process the request.

Authentication/verification

The burden of proof is on you to demonstrate that you cannot identify a data subject. You are not required to acquire additional information just in order to identify (for example, for CCTV the individual needs to provide a particular day and time when the cameras may have recorded the event in question).

The CCPA regulations require a written, reasonable verification method.

If you are not able to identify data that refers to the data subject, you must inform the data subject about this and may refuse to give access unless the data subject provides additional information that enables identification. (e.g. for cookies - you need the cookie identifier and email is not enough). You can ask additional questions to the requesting person or request that the data subject presents some additional identification elements, if it is proportionate for example sending a one-time unique code sent to the user's mobile phone number, provided when the account was set up, (non-intrusive) security questions that were configured when the data subject registered their account, or employing multifactor authentication for access requests.

Where information collected online is linked to pseudonyms or other unique identifiers, the controller can implement appropriate procedures enabling the requesting person to make a data access request and receive the data relating to them.

If you have doubts about whether the data subject is who they claim to be, you must request additional information in order to confirm the identity of the data subject. The request for additional information must be proportionate to the type of data processed and the damage that could occur, etc., in order to avoid excessive data collection. You do not have to retain data just to comply with access rights (this is the same under the CCPA and the California Privacy Rights Act ('CPRA')). If you are not able to identify them, you need to inform the data subject, if possible, without undue delay and give reasons for not complying.

Proportionality assessment for identification

You must carry out a proportionality assessment, which must take into account the type of personal data being processed (e.g. special categories of data or not), the nature of the request, the context within which the request is being made, as well as any damage that could result from improper disclosure.

You must implement an authentication (verification of the data subject's identity) procedure in order to be certain of the identity of the persons requesting access to their data, and ensure security of the processing throughout the process of handling an access requests in accordance with Article 32 of GDPR, including, for instance, a secure channel for the data subjects to provide additional information. The CCPA regulations provide guidance for verification and the verification standard must be reasonable.

The method used for authentication should be relevant, appropriate, proportionate, and respect the data minimisation principle. Identification can be through the provision of the same credentials (e.g. online log-in) or via email or text message containing confirmation links, security questions, or confirmation code.

Asking for ID for verification

- Ask for an identification document only when strictly necessary, suitable, and in line with national law (e.g. this may not be appropriate even if you have asked for this information before, for instance, for hotels, banks, or car rentals). This may be the case for entities processing special categories of personal data or undertaking data processing which may pose a risk for data subject (e.g. medical or health information).
- You need to have systems in place that ensure a level of security appropriate to mitigate the higher risks for the rights and freedoms of the data subject to receive such data.
- The date of issue or expiry date, the issuing authority, and the full name matching with the online account are sufficient for the controller to verify the identity, always provided that the authenticity of the copy and the relation to the applicant are ensured.

- You should encourage the data subject to redact (blacken) the information on the ID that is not necessary for confirming the identity of the data subject, such as the access and serial-number, nationality, size, eye colour, photo, and machine-readable zone before submitting it, except where national legislation requires a full unredacted copy of the identity card. If they do not redact the unnecessary information and you are able to, then you should blacken it upon receipt.
- You should implement safeguards to prevent unlawful processing of the ID. e.g. not making a copy or deletion of a copy of an ID immediately after the successful verification of the identity of the data subject. Note in your records 'ID card was checked' instead of copying the card.
- Additional information such as the birth date of the data subject may only be required in case the risk of mistaken identity persists, if the controller is able to compare it with the information it already processes.
- Be mindful of whether this is prohibited in national law.

Requests by third parties

It is possible for a third party to make a request on behalf of the data subject (e.g. proxy or legal guardian). In some circumstances, the identity of the person authorised to exercise the right of access as well as authorisation to act on behalf of the data subject may require verification, where it is suitable and proportionate.

National laws governing legal representation (e.g. powers of attorney), which may impose specific requirements for demonstrating authorisation to make a request on behalf of the data subject, should be taken into account. You must be able to demonstrate the existence of the relevant authorisation to make a request on behalf of the data subject, except if national law foresees differently. The CCPA requires this as well.

You should collect appropriate documentation and, when in doubt, ask for additional information to confirm the identity of the person. For children, the best interests of the child should be the leading consideration in all decisions taken with respect to the exercise of the right of access in the context of children.

For third party portals:

- Ensure that the third party is acting legitimately on behalf of the data subject, as it is necessary to make sure that no data is disclosed to unauthorised parties.
- You have no obligation to provide the data under Article 15 of the GDPR directly to the portal. If you, for example, establish that the security measures are insufficient, it would be deemed appropriate to use another way for the disclosure of data to the data subject. Under such circumstances, when you have other procedures in place to deal with access requests in an efficient way, you can provide the requested information through these procedures.

Scope of the right of access

This only applies to information within the scope of GDPR, and it only applies to information which constitutes personal data (see the Article 29 Working Party's ('WP29') Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679; the WP29's Guidelines on the right to data portability; the Court of Justice of the European Union's caselaw (such as Joined Cases C-141/12 and C-372/12 *YS v. Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v. M, S,*); and WP29's Opinion 4/2007 on the concept of personal data).

Access to personal data means access to the actual personal data itself, not only a general description of the data or a mere reference to the categories of personal data processed by the controller. The California Attorney General ('AG') clarified that this is the case under the CCPA as well.

The obligation to provide access to the data does not depend on the type or source of the data. It applies to its full extent, even in cases where the requesting person had initially provided the controller with the data.

Aside from basic personal data, like name, address, phone number etc., a broad variety of data may fall within this definition, such as medical findings, history of purchases, creditworthiness indicators, activity logs, search activities etc:

- answers in an exam (but not the questions) are included;
- recordings of telephone conversations (and their transcription) between the data subject that requests access and the controller, may be included;
- CV submitted is included, as is the employer's summary of the interview including the the subjective comments on the behaviour of the data subject the HR officer wrote during the job interview [caveat employer as these will be fair game for employee access requests when the CPRA goes into effect];
- elements that have been used to reach a decision about e.g. employee's promotion, pay rise, or new job assignment (e.g. annual performance reviews, training requests, disciplinary records, ranking, career potential);
- observed data or raw data provided by the data subject by virtue of the use of the service or the device (data processed by connected objects, transaction history, activity logs such as access logs, history of website usage, search activities, location data, clicking activity, unique aspects of a person's behaviour such as handwriting, keystrokes, particular way of walking, or speaking);
- data derived from other data, rather than directly provided by the data subject (e.g. credit ratio, classification based on common attributes of data subjects, or country of residence derived from postcode);
- data inferred from other data, rather than directly provided by the data subject (e.g. to assign a credit score or comply with anti-money laundering rules, algorithmic results, results of a health assessment, or a personalisation or recommendation process) including personal data created by a service

provider e.g subsequent analysis or assessment (inferences are a specific category of personal information under the CCPA); and
- pseudonymised data as opposed to anonymised data.

Personal data concerning the person making the request should not be interpreted overly restrictively and may include data that could concern other persons too, for example, communication history involving incoming and outgoing messages. Information retained in a backup which is no longer part of the live record still needs to be produced.

The following is **not** personal data:

- legal analysis;
- location of the server on which the personal data of the data subject processed; and
- which security measures the controller has put in place.

Personal and non-personal data may be inextricably linked in mixed datasets and fall altogether under the scope of the right of access of the data subject to which the personal data relates.

In addition to providing access to the personal data, the controller has to provide additional information about the processing and on data subjects' rights. Such information can be based on what is already compiled in the controller's record of processing activities (Article 30 of the GDPR) and the privacy notice (Articles 13 and 14 of the GDPR). However, this general information may have to be updated to the time of the request or tailored to reflect the processing operations that are carried out in relation to the specific person making the request.

Even data that may be incorrect or unlawfully processed will have to be provided. However, to avoid the need for further communication on this, as well as to be compliant with the transparency principle, you should add information about the subsequent rectifications or deletions.

Where data is stored only for a very short period, there must be measures to guarantee that a request for access can be fulfilled without the data being erased while the request is being dealt with. (i.e. shorten the response time). You should inform the data subject as of the specific point in time of the processing to which the response refers. If you are aware that things changed, you should let the person know. The controller shall not deliberately escape the obligation to provide the requested personal data by erasing or modifying personal data in response to a request for access. The information must be complete, correct, and up-to-date, corresponding as close as possible to the state of data processing at the time of receiving the request. If you get a second access request, provided that it is not excessive, you need to produce the information again, even if you already produced it the last time. You can only inform of the changes if the data subject expressly agrees to do this.

How to provide the data

Unless explicitly stated otherwise, the request should be understood as referring to all personal data concerning the data subject and the controller may ask the data subject to specify the request if they process a large amount of data.

You must search for personal data throughout all IT systems and non-IT filing systems based on search criteria that mirrors the way in which the information is structured, for example name and customer number or reference number, or customer number user name, etc.

You must provide data and other information about the processing in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

When deciding which measures are appropriate, the controllers have to take into account all the relevant circumstances, including, but not limited to, the amount of data being processed, the complexity of their data processing, and the knowledge they have about their data subjects. You may need to do more if the data subject is a child or a person with special needs. Efforts to provide the information cannot be balanced against, for example, any interest the data subject may have in obtaining the personal data. Instead, the assessment should aim at choosing the most appropriate method for providing all information covered by this right, depending on the specific circumstances in each case.

If you process a vast amount of data on a large scale, you must undertake great efforts to ensure the right of access to the data subjects in a concise, transparent, intelligible, and easily accessible form, by using plain and clear language.

Even controllers that process a vast amount of data can choose to rely on manual routines for handling access requests. If the controller processes data in several different departments, the controller needs to collect the personal data from each department to be able to respond to the data subject request. For example: the administrator sends an enquiry through email to the different departments of the organisation asking them to collect personal data regarding the data subject. Representatives of each department give the administrator the personal data processed by their department. The administrator then sends all the personal data to the data subject together with the necessary supplementary information, for example and when appropriate, by email.

Some controllers may benefit from using automated processes to handle data subject requests. This could, for example, be the case for controllers that receive a large number of requests e.g. a self-service tool, however:

- if it is not possible to give all the information through the self-service tool the rest of the information should be provided in a different way; and

- you can encourage use of the self-service tool but even if you have it you must comply with requests sent in another manner.

If the data consists of codes or other 'raw data', these may have to be explained in order to make sense to the data subject.

You also need to inform the data subject that they become data controller of the data that they are given. You should not direct the data subject to different sources in response to an access request - do not make them actively search for the information. You also cannot direct the data subject to check the data stored in their own device or to check clickstream history or IP addresses on their mobile phone. You should document the approach to be able to demonstrate that the means chosen are appropriate

Formats

You can provide a copy of the data but you can also use other modalities, such as verbal information and on site access, if the data subject requests it. (First copy must be free of charge even if the cost of reproduction is high - e.g the cost of providing a copy of the recording of a telephone conversation). Regarding additional copies, you can chart a reasonable fee based on administrative costs.

A copy is (only) a copy of the personal data undergoing processing, not necessarily a reproduction of the original documents. For a copy to be deemed a copy the individual must be able to download it, not just access.

Sometimes it is appropriate to provide non-permanent modalities of access: oral information, inspection of files, onsite, or remote access without possibility to download. These modalities may be appropriate ways of granting access, for example in cases where it is in the interest of the data subject or the data subject asks for it. Non-permanent ways of access can be sufficient and adequate in certain situations, for example, it can satisfy the need of the data subjects to verify that the data in the record is correct by giving them a chance to have a glance at the original record. A controller is not obliged to provide the information through other ways than providing a copy but should take a reasonable approach when considering such a request. Generally, even then the data subject would have a right to a copy unless they waived it.

The data can be given in a transcript or a compiled form as long as all the information is included and this does not alter or change the content of the information, and as long as the compilation makes it possible for the data subject to be made aware and verify the lawfulness of the processing:

- You need to encompass all data covered by the right of access, but this is merely a way to present all that data without giving systematically access to the actual documents.
- In the case of a lot of email back and forth on a topic, the controller does not necessarily have to provide the emails in their original form by forwarding them to the data subject. Instead, the controller

could choose to compile the email correspondence containing the data subject's personal data in a file that is provided to the data subject.

- Making some kind of compilation and extraction of the data that makes the information easy to comprehend is also a way of complying with the requirements to provide the information in a way that is both intelligible and easily accessible.
- In some cases, the personal data itself sets the requirements to what format the personal data should be provided. When the personal data, for example, constitutes handwritten information by the data subject, the data subject needs, in some cases, to be provided with a photocopy of that handwritten information since the handwriting itself is personal data. That could especially be the case when the handwriting is something that matters to the processing, e.g. scripture analysis. The same applies in general for audio recordings since the voice of the data subject itself is personal data. In some cases, however, access can be given by providing a transcription of the conversation, e.g. if agreed upon between the data subject and the controller

Additionally, the formats that are not appropriate for data portability, e.g pdf, may still work for data access. You need to apply technical and organisational measures ('TOMs') and to ensure security. For physical documents, you may use registered mail or, alternatively, to offer, but not oblige, the data subject to collect the file against signature directly from one of the controller's establishments.

You can send the data by email, provided that all necessary safeguards are applied taken into consideration, for example, the nature of the data, or in other ways, for example, a self-service tool. Consider encryption (with information to the data subject on hot to access it) and password protection.

In the event of a request by electronic form means, information shall be provided by electronic means where possible and unless otherwise requested by the data subject, and as such, it should be noted that:

- 'commonly used electronic form' is not defined and will vary over time;
- what is commonly used should be based on the reasonable expectations of the individual and not upon what the controller uses in its daily operations; and
- the individual should not be obliged to buy specific software for access.

In cases where data security requirements would necessitate end-to-end encryption of electronic mails but the controller would only be able to send a normal email, the controller will have to use other means, such as sending a USB-stick by (registered) letter post to the data subject.

Concise and transparent

Hundreds of pages of log files by a social media company without any measures to facilitate the understanding of the log files is not sufficient. The information must be intelligible - i.e understood by the intended audience while keeping in mind special needs. The fact that the data is complex and hard to understand is not a

reason not to produce it but rather raises the requirement to make it understandable.

Raw data such as codes and activity history (eg. items viewed or purchased) still need to be included in the response but they need to be made understandable, for example, you need to provide an explanatory to translate the raw format into a use friendly form and break down the acronyms and symbols.

It also needs to easily accessible, meaning that you need to present in a way that is easy to understand, for example in terms of layout, appropriate headings, paragraphs, plain and clear language, languages of the relevant country, use of standardised icons (when helpful), data form for visually impaired (eg. oral information), and formats for people with special needs and children.

Vast amount of information - layered approach

You may need to take a layered approach if the amount of data is very vast and it would be difficult for the data subject to comprehend the information if given all in one bulk – especially in the online context. However, you need to provide all the layers at the same time if the data subject requests it.

The layered approach can only be used if it would not create an extra burden for the data subject or require disproportionate effort and cannot be made conditional on making a new request. You also need to explain that you are using a layered approach and how to get access to the different layers. This is to help the data subject decide what layers they want to access .

The layered approach should only be used when it would be difficult for the data subject if you gave the information in its entirety, so you need to demonstrate that the use of the layered approach adds value. You also need to give people the choice of whether to access all layers at once or if they would be satisfied with only accessing one or two layers.

You should put the most relevant information in the first layer as well as the information that has the most impact or that could surprise them, and you need to be able to demonstrate accountability for the choice of your layers.

Data in a raw format that has not yet been analysed or further processed, such as user activity on a website, can be on the second layer.

Costs

You should not pass on overhead costs or other general expenses to the data subject. When organising this process, you should deploy your human and material resources efficiently in order to keep the costs of the copy low. In line with the accountability principle, the controller should be able to demonstrate the adequacy

of the fee. If you decide to charge a fee (for additional copies), you must indicate the amount of costs you are planning to charge to the data subject in order to give the data subject the possibility to determine whether to maintain or to withdraw the request.

Timing

The information should be given as soon as possible. This means that, if it is possible to provide the requested information in a shorter amount of time than one month, the controller should do so. The time limit starts when the controller has received an Article 15 request, meaning when the request reaches the controller through one of its official channels. It is not necessary that the controller in fact has taken notice of it. The time period needs to be calculated in accordance with Regulation No. 1182/71 of the Council of 3 June 1971 determining the rules appliable to periods, dates and time limits.

If the last day of this time period falls on a weekend or a public holiday, the controller has until the next working day to respond.

When the controller needs to communicate with the data subject due to the uncertainty regarding the identity of the person making the request there may be a suspension in time until the controller has obtained the information needed from the data subject, provided the controller has asked for additional information without undue delay. The same applies for when a controller has asked, in accordance with Recital 63 of the GDPR, a data subject to specify the processing operations to which the request relates. Following the receipt of the request, a controller reacts immediately and asks the information it needs to confirm the identity of the person making the request. The latter replies only several days later and the information that the data subject sends to verify the identity does not seem sufficient which requires the controller to ask for clarifications. In this situation there will be a suspension in time until the controller has obtained enough information to verify the identity of the data subject

Under certain circumstances the controller can extend the time to respond to a request of access by two further months if necessary, taking into account the complexity and number of the requests. It should be emphasised that this possibility is an exemption from the general rule and should not be overused.

If controllers often find themselves forced to extend the time limit, it could be an indication of a need to further develop their general procedures to handle requests. Controllers who handle a large amount of data should have routines and mechanisms in place in order to be able to handle requests within the time limit under normal circumstances.

The mere fact that complying with the request would require a great effort does not make a request complex. Neither does the fact that a big company receives a large number of requests automatically trigger an extension of the time limit. However, when a controller temporarily receives a large amount of requests, for

example due to an extraordinary publicity regarding their activities, this could be regarded as a legitimate reason for prolonging the time of the response.

What constitutes a complex request varies depending upon the specific circumstances of each case. Some of the factors that could be considered relevant are, for example:

- the amount of data processed by the controller;
- how the information is stored, especially when it is difficult to retrieve the information, for example when data is processed by different units of the organisation;
- the need to redact information when an exemption applies, for example information regarding other data subjects; and
- when the information requires further work in order to be intelligible.

Limits and restrictions

The only exemptions to the right of access are those as set forth in the GDPR. However, 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. It is not permitted to limit or restrict the right of access in a contract between the controller and the data subject.

You may provide a data subject with tools to specify the scope of the request from the beginning:

- You may provide self-service tools (e.g. in online contexts).
- In the absence of these tools - when you process large amounts of information for a data subject and you have doubts that their generally worded request intends to encompass all those types of data, you may request the data subject to specify the information or processing to which the request relates before the information is delivered. In such case you must give meaningful information about all the processing operations concerning the data subject, like different branches of its activities, different databases, etc.

Rights of others

When the Article 15(4) of the GDPR assessment proves that complying with the request has adverse (negative) effects on other participants' rights and freedoms (step 1), the interests of all participants needs to be weighed taking into account the specific circumstances of the case and, in particular, the likelihood and severity of the risks present in the communication of the data.

Protecting the rights of others (this includes entities) should generally not result in refusing the data subject's request altogether. First, you should see if the conflict is resolved by leaving out or rendering illegible those parts that may have negative effects for the rights and freedoms of others. If that does not work, then

you must decide in a next step which of the conflicting rights and freedoms prevails.

Conflicting rights and freedoms include trade secrets or intellectual property and in particular the copyright protecting the software. These explicitly mentioned rights and freedoms should be regarded as examples. Consider also Article 8 of the EU Charter for Human Rights for the protection of personal data and the right to confidentiality of correspondence (e.g. privacy email correspondence in the employment context). However, economical interests of a company not to disclose personal data are not to be taken into account when applying Article 15(4) of the GDPR as long as there are no trade secrets, intellectual property, or other protected rights. The general concern that rights and freedoms of others might be affected by complying with the request for access is not enough to rely on Article 15(4) of the GDPR. In fact, the controller must be able to demonstrate that in the concrete situation rights or freedoms of others would factually be impacted.

If controllers do not provide full access to a data subject under Article 15(4) of the GDPR, they have to inform the data subject of the reasons without delay and at the latest within one month (Article 12(4) of the GDPR). The explanatory statement has to refer to the concrete circumstances and allow the data subjects to assess whether they want to take action against the refusal. It must include information about the possibility of lodging a complaint with a supervisory authority (Article 77 of the GDPR) and seeking judicial remedy (Article 79 of the GDPR).

If you plan to rely on a restriction based on national law, you must carefully check the requirements of the provision of the respective national legislation. You should lift the restrictions as soon as the circumstances that justify them no longer apply.

Manifestly unfounded

The manifestly unfounded or excessive concepts have to be interpreted narrowly. Controllers must be able to demonstrate to the individual why they consider that the request is manifestly unfounded or excessive and, if asked, explain the reasons to the competent supervisory authority. Each request should be considered on a case by case basis

A request for the right of access is manifestly unfounded if the requirements of Article 15 of the GDPR are clearly and obviously not met when applying an objective approach. A controller should not presume that a request is manifestly unfounded because the data subject has previously submitted requests which have been manifestly unfounded or excessive or if it includes unobjective or improper language

Excessive

Excessive requests depend on the specifics of the sector in which the controller operates. The more often changes occur in the controller's database, the more often the data subject may be permitted to request access without it being excessive. Restrictions of the right of access may also exist in Member States' national

law as per Article 23 of the GDPR and the derogations therein. You must check these.

When deciding whether a reasonable interval has elapsed, controllers should consider, in the light of the reasonable expectations of the data subject:

- How often the data is altered – is information unlikely to have changed between requests? If a data pool is obviously not subject to a processing other than storage and the data subject is aware of this, e.g. because of a previous request for the right of access, this might be an indication for an excessive request.
- The nature of the data – this could include whether it is particularly sensitive.
- The purposes of the processing – these could include whether the processing is likely to cause detriment (harm) to the requester if disclosed.
- Whether the subsequent requests concern the same type of information or processing activities or different ones.

It is considered that access requests every three months to a social media company is not excessive, but them every two months to a carpenter is. If you have an electronic process, it less likely that subsequent requests would be excessive.

The fact that it would take the controller a vast amount of time and effort to provide the information or the copy to the data subject cannot on its own render a request excessive. Requests can be regarded as excessive due to other reasons than their repetitive character. In the view of the EDPB, this encompasses particularly cases of abusively relying on Article 15 of the GDPR, which means cases in which data subjects make an excessive use of the right of access with the only intent of causing damage or harm to the controller.

A request should not be regarded as excessive on the ground that:

- no reasons are given by the data subject for the request or the controller regards the request as meaningless;
- improper or impolite language is used by the data subject; and/or
- the data subject intends to use the data to file further claims against the controller.

A request may be found excessive, for example, if:

- an individual makes a request, but at the same time offers to withdraw it in return for some form of benefit from the controller; or
- the request is malicious in intent and is being used to harass a controller or its employees with no other purposes than to cause disruption, for example based on the fact that:
    - the individual has explicitly stated, in the request itself or in other communications, that it intends to cause disruption and nothing else; or

- the individual systematically sends different requests to a controller as part of a campaign, e.g. once a week, with the intention and the effect of causing disruption.

In case of a manifestly unfounded or excessive request for the right of access controllers may, according to Article 12(5) of the GDPR, either charge a reasonable fee (taking into account the administrative costs of providing information or communication or taking the action requested) or refuse to comply with the request. However, they are not completely free to choose between the two alternatives either. In fact, controllers have to make an adequate decision depending on the specific circumstances of the case.

Controllers must be able to demonstrate the manifestly unfounded or excessive character of a request (Article 12(5) of the GDPR). Hence, it is recommended to ensure a proper documentation of the underlying facts

Before charging a reasonable fee, based on Article 12(5) of the GDPR, controllers should provide an indication of their plan to do so to the data subjects. The latter have to be enabled to decide whether they will withdraw the request to avoid being charged.

Information on the processing and data subject rights.

For information on how to produce this, consult the WP29 Guidelines on Transparency under Regulation 2016/679 | WP260 rev.01 (11 April 2018)[2].

You may use text from your privacy notice as long as this is precise and accurate as for the data subject request. However, information on recipients, categories, and sources of data may vary and this you need to tailored. (e.g. if you collect email or phone number or address but it's only email re: this particular person, you should list only email in the information provided). You should also include legal basis.

Information on the purposes, needs to be specific to the data subject. You can not just list general purposes without saying which apply in this case. Public authorities acting in the framework of a particular inquiry under national law are not recipients for the purpose of a Article 15 request.

You should generally name the actual recipients unless it is only possible to indicate the category. If you have the information at the time of the request, even if you didn't have it at the time of the Article 13 notice, you need to provide it. For example, in its privacy notice an employer gives information about which categories of data are passed on to 'travel agencies' or 'hotels' in case of business trips, in accordance with Articles 13(1)(e) and 14(1)(e) of the GDPR. If an employee makes a request for access to the personal data after business trips have taken place, the employer should then, concerning the recipients of the personal data pursuant to Art.icle 15(1)(c), indicate in its reply the travel agency(ies) and hotel(s) that received the data.

When you provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector, and the location of the recipients.

Regarding retention, reference, for example to 'deletion after expiry of the statutory storage periods' is not sufficient. If the triggering event has already occurred, the specific storage period shall be indicated. Indications concerning data storage periods will have to focus on the specific data relating to the data subject

In terms of the source, you also need to be specific. For example, regarding credit checks, it's not enough to say that you received information from credit companies but rather, in addition to the information that a creditworthiness information has been obtained, it would then *ex post* be necessary to disclose, which of the companies mentioned has been involved exactly.

For automated decision making, if possible, information under Article 15(1)(h) of the GDPR has to be more specific in relation to the reasoning that lead to specific decisions concerning the data subject who asked for access.

Odia Kagan Partner and Chair of GDPR Compliance & International Privacy
okagan@foxrothschild.com
Fox Rothschild LLP, Philadelphia

---

1. Available at: https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf
2. Available at: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025