# Subject Access Requests:
# A Data Controller's Guide

An Coimisiún um Chosaint Sonraí
Data Protection Commission

## Index

## Introduction

The General Data Protection Regulation (GDPR), under Article 15, gives Data Subjects the **right to request** access to  information which is directly or indirectly related to them ('personal data') which is being 'processed' (meaning 'used in any way') by 'Data Controllers' (meaning 'those who decide how and why data are processed') (see: Data Protection Basics), as well as other relevant information (as detailed below).

The **making of a request** by an identified or identifiable Data Subject, hereinafter referred to as an 'access request', **gives them the right to obtain** – subject to certain restrictions provided for under the GDPR and the DPA 2018 – access to and copies of such data and other relevant information which must be provided free of charge and in an accessible form. A Data Controller must ensure that the individuals whose data they are processing (or someone on the individual's behalf) are facilitated to lodge access requests (see: Principles of Data Protection). A Data Controller must provide a response to an access request in a certain manner and within certain time limits, as is detailed below.

A Data Controller's failure to adhere to obligations under Data Protection law (see Self-Assessment Checklist), including those related to the right of access, may result in the Data Subject lodging a **complaint to the DPC** (Data Protection Commission) which could lead to a fine and/or further corrective measures being imposed on the Data Controller. The DPC may also commence an own-volition inquiry into a Data Controller's organisation seeking to determine their compliance with data protection law (see: Guide to the Investigation Process). In the event **legal proceedings** are instituted by the Data Subject against the Data Controller, the latter may also be held liable for any material and non-material damage suffered by the Data Subject as a consequence of the Data Controller's breaches of data protection law obligations.

The majority of the complaints and queries the DPC receives each year concern individuals seeking to exercise their right of access (see the DPC's Annual Report for volumes received) The following guidelines outline the steps which need to be taken by a Data Controller in order to **answer an access request** in compliance with data protection law. It is a Data Controller's responsibility to ensure and be able to demonstrate compliance with the law. Although the DPC does not provide legal advice (see: What We Do) you may raise a concern with the DPC by accessing this link (see: Raise a concern) At the bottom of this page you will also find links to decisions of the DPC relevant to the handling of access requests.

This guidance has been developed for the purpose of identifying the core practical issues of compliance of Data Controllers with data protection legislation in relation to access requests as follows:

- How should I ensure requests are lodged and received?
- Should I verify the identity of the Data Subject, and if so how?
- Can third parties lodge a request?
- Can I ask the Data Subject to clarify their request?
- What are the deadlines to respond?
- Is there a procedure I should follow?
- What should the content and form of my response be?
- Are there instances in which I could charge for the response?
- When can I refuse to take action on the request?
- What if personal data is being held by a processor/What if I am a joint controller?

## *How should I ensure requests are lodged and received correctly?*

Data Subjects must be able to lodge access requests with a Data Controller, in accordance with the obligation of Data Controllers to **facilitate the exercise** of the rights of the Data Subjects (Article 12 GDPR). In order to comply with this obligation a Data Controller should consider two things. Firstly, it must ensure that their organisation has a **dedicated way for a Data Subject to make such a request,**

**and for a Data Controller to record such a request.** Data Controllers may wish to use standard or online forms for the lodgement of access requests. This can help streamline a Data Subject's access request, and can ensure consistency and timely responses to a request within a Data Controller's organisation.

For example, Data Controllers could establish a dedicated email address to be used by Data Subjects in order to lodge access requests and display that email address in an easily accessible part of its website. If that is not possible a controller must clearly state on its privacy notice a relevant contact in charge of data protection matters in the organisation.

Secondly, Data Controllers must ensure they do **not overlook access requests** by Data Subjects, just because the request is lodged in a different way than the internal point of contact established within the organisation for dealing with data protection issues. Data Subjects can always validly lodge an access request by contacting the organisation through any method of communication be it by phone, post, informal chat or in person. The GDPR does not require any particular form to be used to make a valid access request. The Data Controller may re-direct the Data Subject to the relevant department of the organisation dealing with access requests, or may re-direct the correspondence themselves by internal email or post, however the clock for complying with the relevant time limit begins from the day the request is received by the Data Controller. (See further below '**What are the deadlines to respond?**').

For example, a Data Subject submits their **request to the wrong department** of your organisation on a Monday and it is not received by the right department until the following day. The starting date for the access request is still Monday as that is the date it was received by the organisation. In short, the timeline for responding to an access request begins the day a SAR request is received, regardless of which department initially received it or how the SAR was submitted.

It is the responsibility of Data Controllers to adequately **train their employees** to be aware and take note of any access requests lodged (especially if the request is lodged orally) and to re-direct the access request to the relevant department within the organisation. The relevant department or Data Protection Officer ('DPO') should then contact the Data Subject to confirm receipt of the request and to inform the Data Subject of the way in which the access request will be dealt with, and the timelines for complying with the request. The Data Controller must also ensure all communications and the sending of any data relating to the access request is done in compliance with the data protection principles of security and confidentiality (see: Guidance for Controllers on data security).

As stated above, it is important that Data Controllers recognise when an access request has been lodged by a Data Subject. A Data Subject is not obliged to make the access request by reference to the GDPR, or by explicitly stating that it is an access request. Therefore, any request which a Data Controller believes **may** be an access request should be treated as such. If a Data Controller is in doubt of the request made, it can contact the Data Subject to clarify the request. In general, a Data Controller should consider that a request is an access request when the Data Subject has contacted the organisation asking for information "related to" them, and the Data Controller is not able to deal with such a request in the **normal course of business**. By this it is meant that the ordinary practice and procedure of the organisation can deliver the same information requested by the Data Subject within the timeline prescribed by data protection law without the need to formally treat it as an access request.

For example, if a bank customer asks for all their **bank statements** from the last 11 months, this could be considered as a data access request (given that bank statements constitute personal data related to individuals). However the bank, as controller, may be able to easily respond to the request through its available banking services and therefore there may be no need for formal treatment of the request in this case.

However, if a bank customer has a query in relation to a **loan application** he has submitted and emails the relevant staff member requesting an update on his loan application, including all the relevant correspondence between the bank managers in relation to his application – even without referring to data protection legislation – the staff member of the team in question should be able to categorize this as an access request and refer it to the dedicated team in charge of dealing with data protection in the bank.

**Minors and people with disabilities** may experience difficulties in lodging access requests. A Data Controller responsible for the processing of personal data related to these particular categories of Data Subjects is obliged to undertake all reasonable measures in order to facilitate their lodgement of access requests, which will depend on the circumstances of each case.

For example, if you are an optician dealing with the personal data of a person with low vision, you should ensure that the access request can be lodged and answered verbally.

In relation to minors, see the DPC's Children's Fundamentals. In respect of facilitating people with a disability, Data Controllers must comply with relevant legislation, such as the Disability Act 2005 and may also refer to the National Disability Authority recommendations.

## *Should I verify the identity of the requester?*

A Data Controller must adequately identify the requester's identity (meaning securely associate the Data Subject to a name and surname/to an organisation through a legitimate representative) having used all **reasonable measures** (Recital 64 GDPR) and should not require any further information from the requester unless the controller still has a **reasonable doubt** in relation to the requester's identity (Article 12(6) GDPR). Until the Data Subject's identity has been adequately established the access request is not effective and the clock for the purposes of the time limit to respond does not begin (see further below 'What are the deadlines to respond?').

For example, in the context of online services, a way a Data Controller could identify the requesting Data Subject would be by setting up **two-factor authentication**. In the event of the lodgement of an access request, the Data Subject could be requested to provide a unique code sent to a contact detail different from the one which the request is coming from, i.e. a phone number where the request was made via email.

Implementing a method of confirming the identity of the requesting Data Subject may be considered a technical and organisational measure put in place by an organisation in order to safeguard the security of personal data and prevent a data breach, which may occur if a Data

Controller disclosed information to unauthorised recipients. However, such a measure is justified where there is an actual **security requirement**, in this case coinciding with the existence of a reasonable doubt as to the identity of the requester. If there is no reasonable doubt, the measure could be seen as an obstacle to the exercise of a Data Subject's right, in breach of the obligation of controllers to facilitate the exercise of rights by Data Subjects and of the data minimisation principle.

For example, this might be the case where the controller, a retail company, is corresponding with customers asking for their past order details. If the request came from the same email address which was used by the customer to create their account for online shopping, there would be no apparent reasonable doubt about the Data Subject's identity and therefore, if further identification is required, the controller must be able to demonstrate that there was in fact a reason to seek to establish the identity (for example, the fact that the account had been recently locked due to a hacking event).

This principle is valid for **every type of data** processed. When the personal data processed is special category data, meaning data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data and biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation (see: Data Protection Basics), the risk in relation to the effect of unauthorised disclosure is higher, and Data Controllers should have systems in place in order to secure the handling of those data. However, when it comes to the exercise of data protection rights by Data Subjects, these measures must always conform to the principle of reasonable doubt outlined above.

For example, if the requester is lodging a request from **within their credit union account**, a request of further proof of identity attached to the request may not be justified (for example if you have duly verified the identity of the account holder at the moment of the creation of the account). However, if the request comes from **outside their credit union account**, even if the email address is the email that the account holder used to register their account, you may doubt that the person writing the email is the actual Data Subject, and may therefore be entitled to request further ID verification. In other words, your reasonable doubt lies in the question: why is the requester not using the system from within their account? The suggested method of response flow would be to redirect the requester to the lodgement of the request from within their account, or, in the alternative, provide proof of identification.

Furthermore, if a Data Controller does have reasonable doubt as to the identity of the requester, **verification should not exceed what is necessary** in order to be satisfied that the requester coincides with the Data Subject. In other words, it could be a failure of the obligation to facilitate the exercise of Data Subject rights and the data minimisation principle, if a Data Controller requires proof of identity which they did not need in order to confirm the requester's identity. A **proportionality assessment** taking into account the type of personal data being processed (e.g. special category data), 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 should be undertaken. A layered approach in terms of identification is also recommended in accordance with proportionality. It is also open to a Data Controller to ask a Data Subject security questions in order to confirm the Data Subject's identity. The security questions and answers would come from information that a

Data Controller already holds in relation to the Data Subject, and the Data Subject would be the only person who would know the correct answers to the security questions.

For example, it may be reasonable to require certification of an identification document by a member of An Garda Síochána only if you have proven doubts on the **genuineness of the document itself**, but it may not be necessary to require said certification as a default measure.

For example, it may be necessary to require a selfie with an identification document only if you still have a reasonable doubt that the corresponding individual **is the actual requester as identified in the document**

## *Can third parties lodge a request?*

The decision as to how to lodge a request is entirely up to the Data Subject, with no particular or formal method prescribed by data protection law. Therefore, a Data Subject may decide to authorise someone else (including a solicitor, an individual, not-for-profit body, organisation or association referred to by Article 80 GDPR) to lodge a request on their behalf. There is no need for the authorisation to bear particular formalities. The third party lodging the request must nonetheless be able to provide evidence that such **authorisation came from the Data Subject**. The issue of identification in these cases applies both to the identity of the requester and the person on whose behalf the request is made.

For example, a member of a credit union visits his local credit union branch to access his account regularly. He is married to another member of the credit union who is also known to the credit union employees. The spouse wants to look at the current balance in the account and lodges an electronic data access request on behalf of her spouse. The credit union, as controller, although they know both the account holder and the spouse, should nonetheless request from the spouse proof of authorisation from the account holder.

There may be cases in which specific authorisation is not available, but the right to request access to personal data could derive from more general types of representation, for example power of attorney or parental responsibility. In these cases, a Data Controller must consider whether to **contact the Data Subject** first (See, in relation to children, Children Fundamentals, pp 35-36) and whether to send the response to the access request directly to the Data Subject.

## *Can I ask the requester to further clarify their request?*

A Data Subject is entitled to request access to any or all of their personal data. A Data Controller who processes a **large quantity of information** concerning the Data Subject can request, as soon as possible after having received the request and before delivering the response to the access request, that the  Data Subject specify the information they want to be provided or the specific processing activities which they want access to (Recital 63 GDPR) and, in addition to this, may be entitled to extend the time to answer the access request (see below 'What are the deadlines to respond?'). Although it is in the interest of the Data Subject to cooperate in order to speed up the process, the Data Subject is **not obliged to answer**, and a Data Controller **must** comply with the access request even if the request for clarification remains unanswered. It is recommended that Data Controllers always document the reasons for the request for clarification, in accordance with the principle of accountability (see: Principles of Data Protection).

For example, an individual who has continuously resided in Dún Laoghaire for the past 30 years submits an access request for all their personal data held by Dún Laoghaire-Rathdown County Council. The amount of data processed by the Council is likely to be of a large quantity, spreading from planning applications to CCTV recordings. The Council may qualify as the controller which processes large quantities of information in relation to the requester, and may therefore be entitled to ask the requester to clarify whether, for example, they specifically require personal data related to one particular service offered by the Council and which is the relevant period of time to which said information may relate.

Even if Data Controllers are not processing large quantities of information related to the Data Subject as indicated by Recital 63 GDPR, nothing prohibits them, whenever it is **reasonable** to do so (for example, when a Data Controller is not sure what type of information the requester is looking for) to ask the requester to clarify their access request in the terms outlined above. However, if a Data Controller does not process large quantities of information concerning the Data Subject and cannot rely on the complexity of the request for extending the time for answering the request (see below: 'What are the deadlines to respond?'), the clock for the purposes of the timely answer to the access request would not stop.

## *What are the deadlines to respond?*

Data Controllers must provide information on the action taken on the access request without **undue delay** (Article 12(3) GDPR). This means that they must confirm as soon as possible whether they are processing personal data of the Data Subject and, if that is the case, Data Controllers must either:

a) provide all the information on processing and a copy of the personal data at issue as required by data protection law (see further below) or
b) notify the Data Subject that they need more time to answer the request (see below) or
c) notify the Data Subject that they will not take action on the request and the reasons for not doing so (see below: "Are there instances in which I could refuse to respond?").

The response to an access request may be considered untimely even before the maximum term provided for by law has expired, depending on the circumstances of the case.

For example, if at the time of the request the controller is processing certain personal data whose permanent deletion is imminent – i.e. will happen before the calendar month – because of the retention periods established by the data protection policies of the controller, an answer to the access request after the expiration of the retention period in question may be considered untimely even if it is delivered within the one calendar month from the request.

There is nothing in GDPR regulating the instance of a shorter **deadline** to respond imposed on a Data Controller by the Data Subject. The Data Subject may have valid reasons for such a special need, and since the mandatory term to respond is a maximum one, the Data Controller should at least justify why they cannot fulfil the request of the Data Subject under their obligation to facilitate the exercise of Data Subjects' rights, in accordance with the principle of accountability.

For example, the Data Subject has lost his home due to a fire, and the insurance company requires him to lodge certain data within strict time limits. The data are held by a bank and the Data Subject has no copies, as they have been destroyed. You are the Data Controller in the bank. If you have the data ready there, and the resources to speed up that specific Data Subject request, you should try to comply with the Data Subject's deadline.

The maximum time limit to provide information on the action taken on an access request, is **one calendar month from receipt** of the access request by identified or identifiable Data Subjects, regardless of the fact that such receipt is not on a working day. Exceeding the maximum time limit would automatically constitute a breach of the Data Controller's obligations. Data Controllers can be said to have received an access request at the moment in which their organisation has become aware or has had constructive notice of the access request lodged through their **established channels of communication,** without the need to take any further steps in order to identify the requester.

For example, an access request sent to an email address of an organisation which automatically replies indicating that the **email address is not monitored** and that no one will read the email sent might not be considered as a valid access request, in the sense of actually having reached an "established" channel of communication. A different conclusion may be reached in the absence of such warning, when the Data Subjects would be entitled to think that they are corresponding with an established channel of communication.

Once the Data Controller has determined the day in which the access request was received, in order to calculate the calendar month period, the actual days available to the Data Controller to prepare their answer may vary on a case-by-case basis as the Data Controller should consider that:

- the period shall end with the **expiry of the last hour** of whichever day of the following month falls on the same date as the day which initiates the period;
- the period includes public holidays, Sundays and Saturdays;
- the day which initiates the period is the day during which a valid access request was received;

For example, if you receive an access request on 22nd December, on 22nd January the following year the minute starting at 23:59 will be your last minute in order to respond to the requester, regardless of the intervening Christmas holidays.

- where the period ends on a public holiday, Sunday or Saturday, the period shall end with the expiry of the last hour of the **following working day**;
- where the day on which the period should expire does not occur in the month, the period shall end with the expiry of the last hour of the last day of that month.

For example, if you receive an access request on 31st August, September ends on its 30th day and your maximum one-month period to comply with the access request would expire accordingly.

The DPC strongly recommends the implementation of policies in organisations aimed at responding to access requests within **15 working days** in order for Data Controllers to answer as soon as possible. In order to validly respond to an access request, a Data Controller must provide the information requested in an intelligible manner (as seen further below). If clarifications requested by the Data Subject are provided after the expiration of the calendar month, the Data Controller may have therefore breached the obligation to validly respond to the request within the calendar month.

A Data Controller can **unilaterally extend the time** to respond by a **further two months only if it is necessary** to do so and in the event of **complex or multiple requests** (including requests related to the exercise of other data protection rights). In that case, within one month of receiving the access request, the Data Controller must let the requester know that they are extending the time limit and explain to them why the extension is necessary (Article 12(3) GDPR). Whether or not a Data Controller may be entitled to extend the deadline to reply depends on the circumstances of each case, but the following assessment questions should help Data Controllers identify a situation in which an extension may be legitimate:

- Is the amount of data **not readily available** to my system?

> For example, a bank has received a number of requests from an account holder, and the requests are related to various matters: an erasure of certain data from their account; a list of their online banking activity and the personal data related to all the financial investments they have conducted through the decades of their long term dealings with the bank. The bank would be expected to have the relevant information readily available on its systems and therefore an extension of time on the grounds of multiple access requests should not be necessary. However, if some data related to the earlier investments are still in hard copy format and are held in secured archives managed by third parties, it may be the case that a delay may occur and you may need to extend the time period.

- Do I have to employ **extra resources** in order to comply?

> For example, if the Data Subject expressly requests access to personal data that you have permanently deleted in adherence with your retention policy, and your organisation has not, in the normal course of business, access to the technology which can recover permanently deleted files from a laptop, and will need to employ an IT services company within your limited budget, that request may be considered a complex one. However, on the other hand, if you normally have access to those technologies or have the resources to easily employ third parties that could recover the data, the request may not be considered a complex one.

- Does my response need **considerable redaction** of third parties' data?

> For example, if the request concerns the reports of a road traffic accident in which multiple parties were involved, the amount of redaction of the reports may require meticulous work in order to extrapolate only the relevant data related to a certain individual. This may be considered a complex request as the redaction not only must be performed essentially by human beings, but a careful evaluation of whether personal data of others may also require disclosure may be necessary.

- Do I need to apply an **exemption**?

> For example, if you are facing an access request which necessarily requires you to disclose the personal data of third parties, you may need to obtain their consent or, in the absence of their consent, a Data Controller will need to have undertaken an assessment as to the

balance between the rights of the Data Subject and the third parties' rights. It may be the case that a practical solution can be reached, for example in the case of the release of CCTV footage a Data Controller could blur the images of any third parties in the footage, before releasing it as part of a subject access request.

If the access request does reasonably fall within one or more of the above mentioned scenarios, a Data Controller must still demonstrate why they cannot comply within one calendar month, and that the unilateral extension of time is therefore necessary. In particular, it is recommended that the Data Controller extends the time period to respond **as little as possible** (for example 1.5 months instead of two full months), in order to comply with the obligation to facilitate the exercise of data protection rights. In the alternative, the Data Controller may **partially satisfy the access request** and ask for more time in respect of the more complex issues in relation to it.

Using the above example on the hard copy documents not readily accessible to the bank, you might fulfil the request in relation to the other personal data readily available to you, and extend the period for responding to the complex issue of accessing the personal data contained in the hard copy files.

## *Is there a procedure for handling access requests that I should follow?*

There is no specific requirement obliging Data Controllers to adopt a specific procedure for handling access requests, provided that they are able to comply with the time limits (see above 'What are the deadlines to respond?') and to produce a response compliant with the other requirements necessitated by data protection law (see below 'What should the content and form of my response be?'). To that end, it is recommended that Data Controllers consider at least two main aspects in handling access requests: First, ensure to keep the requester informed and up to date and secondly, have a system in place to collect all the relevant information to be provided to the Data Subject. Data Controllers implementing such systems should also comply with their obligations under data protection by design and by default and, more generally, the **accountability** principle (see: Know Your Obligations).

An acknowledgment of receipt is a recommended practice. It allows both the Data Controller and the requester to **identify the date** from which the clock starts for responding to the request in time.

For example, if a Data Subject lodges their request to the customer service unit, the controller, a retail shop, a policy may be in place according to which every data protection related issue is to be forwarded to a dedicated data protection unit within the administration department, responsible for acknowledging receipt of such requests. The customer service agent will therefore forward the request to the data protection unit – preferably notifying the requester of that – and the data protection personnel may then  contact the Data Subject to acknowledge receipt of the request (including indicating whether the actual date of receipt was before the actual acknowledgment: it may be the case that if the customer service unit took a while before forwarding the request to the right unit, the actual date of receipt could be earlier) notifying him or her that it is preferable to correspond directly with them in order to maximise the timeframe for processing the request.

Keeping a proper **record system** of access requests is also recommended. In particular, where an access request is made orally, Data Controllers should record the time and details of the access request. Data Controllers may want to follow up with the requester in writing to confirm that they have correctly understood the request. Furthermore, it is good practice for Data Controllers to keep requesters **regularly updated** on the progress of their request, and give them sufficient notice in advance of any potential delays or requests for clarification.

Data Controllers are obliged to implement appropriate technical and organisational measures to ensure  that, by default, only personal data which are necessary for each specific purpose of the processing are processed (**data protection by default**) (see: Data protection by Design and by Default). That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.  Therefore, Data Controllers should have in place technical and organisational measures which allow for a good **data management** system, including by deploying automated means or Artificial Intelligence (AI), to control the extent of processing and the amount of data related to the specific Data Subject.

It is therefore recommended that Data Controllers put in place appropriate technical and organisational measures that – further to complying with data protection by default – will help in advance of an access request. These measures should aim to **facilitate the detection** of all personal data held about the Data Subject whose personal data are being sought in the access request. The definition of personal data is broad (see: Data Protection Basics) and likely to encompass a wide variety of information, and human-based search (at least in the final phases of collection) is recommended.

For example, you may use a **keyword** such as “name surname” of the Data Subject in order to find personal data. However, personal data could also be information which does not necessarily contain the name of the Data Subject, but through which the Data Subject can be nonetheless identified. This may be the case of particular comments made by an examiner in the context of the examination of the Data Subject.

## *What should the content and form of my response be?*

Data Controllers must ensure to provide the requester with all information they have requested and all the information they are entitled to under data protection legislation.

1) **Confirmation of processing**
   The Data Controller must confirm expressly that they – at the time of the receipt of the request – were processing personal data related to the Data Subject and, if a specific or targeted request for data has been made, they do process personal data in that specific respect.

2) **Access to personal data**
   The Data Controller must provide access to the requested personal data which were being processed as they were at the time the request was made, even if it appears that the personal data in question were inaccurate or lack a lawful basis for processing. Personal data includes, but is not limited to:

- Special categories of personal data as per Article 9 GDPR;
- Personal data relating to criminal convictions and offences as per Article 10 GDPR;
- Data provided by the data subject by way of forms, or in answers to a questionnaire;
- Observed data or raw data provided by the data subject by use of a service or device;
- Data which has been derived from other data, rather than directly provided by the data subject;
- Data which has been inferred from other data, rather than directly provided by the data subject;
- Pseudonymised data as opposed to anonymized data.

The Data Controller must allow the requester to have a meaningful interaction with the requested personal data by precisely singling them out for the Data Subjects (even if the data had originally been provided by the Data Subject themselves). Furthermore, the Data Controller must ensure to provide access to the personal data in a way that enables the requester to grasp the actual relationship between the information and the Data Subject, in other words why information is "related" to the Data Subject.

For example, if the personal data at issue is handwritten notes of the Data Subject, the Data Controller cannot simply provide the Data Subject with access to the notes as typed up by a secretary on a digital format as the handwriting itself constitutes personal data.

Most of the time, access to the requested personal data is fulfilled by the provision of the copy of the personal data (see further below). However, there may be instances in which access should be provided by other means such as when the right to a copy of the personal data is restricted to safeguard the rights and freedoms of others (see below 'When Can I refuse to comply with the request?').

3) **Information on processing**, including the purposes of the processing; the categories of personal data processed; who the personal data are shared with; how long the personal data will be stored; the existence of various Data Subject rights; the right to lodge a complaint with the DPC; information about where the data were collected from; the existence of automated decision-making (such as 'profiling'); and the safeguards in place if the personal data are transferred to a third country or international organisation.

Although Data Controllers might be tempted to simply "copy and paste" the information provided in the relevant privacy notice of the organisation, they should instead "adapt" that information to the specific case at issue. In other words, whereas the privacy notice is more generally directed to all actual and potential Data Subjects, the information on processing to be provided to the requester must relate to the specific processing activity in respect of the specific Data Subject whose data are the subject matter of the request.

For example, if your organisation deploys technologies which track the use of your organisation's website by the Data Subject, thus collecting behavioural data, the data privacy notice would already display, in general, who the recipients of the data collected from the general website users are. In an access request from a specific Data Subject you should, amongst the other information, indicate the specific recipients of the behavioural data collected from that specific Data Subject and you should also indicate the exact retention period applied to those data. Furthermore, as you must also indicate "meaningful information" on the logic involved in the automated processing activity, in order for the Data Subject to understand the reasons for any decisions you may take on the basis of the technologies undertaking automated processing.

**4) Copy of the personal data**

Data Controllers must provide a copy of the personal data requested (not necessarily a copy of the actual document or other support containing them) which were being processed at the time the request was made. This requires Data Controllers to furnish to the requester the data to which the Data Subject has the right to access in a durable format, meaning in a way that the personal data in question are capable of being retained by the requester in accordance with their own needs.

For example, the requirement to provide a copy of personal data which are held in a digital format by the controller will be fulfilled by enabling the requester to download their data in a commonly used electronic form, and not only by providing the requester access to the cloud service used by the controller to store the data.

Even if the requester has not explicitly asked, for example, for the copy of the personal data at issue, it is nonetheless recommended that whenever an access request is made, Data Controllers provide the requester with all the information referred to in Article 15 GDPR. As mentioned above, the notion of "personal data" is quite broad (see: Data Protection Basics), and it is the responsibility of the Data Controllers to provide access to all information constituting the personal data of the Data Subject.

For example, a Data Subject is a dissatisfied customer of the Data Controller, an insurance company, and has requested a copy of all the personal data related to them. The insurance policy data, records of their previous claims under the insurance policy and all correspondence with the Data Subject is already available to the Data Subject. The insurance company should make sure that they also provide the Data Subject with a copy of any internal material (appropriately redacted, if necessary) in which identification of the Data Subject may be possible, for example certain internal emails referring to the Data Subject's health situation discussed by the complaint management team.

When the requester has not made a general "all the Data Subject's data" request, but has clearly and explicitly limited the extent of their access request, the Data Controller should limit the response to the data requested. On the contrary, when there is no explicit delimitation of the access request, the Data Controller should furnish the requester with access to all the personal data which were the subject of processing operations at the time the request was made.

For example, if the Data Subject is your employee and has requested specifically their personal data relating to a disciplinary enquiry which was conducted in respect of them, you should not overwhelm the requester by furnishing alongside the relevant data pertaining to the enquiry all HR records generated by the Data Subject in the course of his two decades of employment with your organisation.

Individuating the relevant information constituting personal data of the Data Subject may be costly in terms of time and resources. Since Data Controllers are entitled to refuse a request which is excessive (see below: "Are there instances in which I can refuse to respond?"), they are not obliged to conduct searches which go beyond what is **reasonable** in terms of time and money, taking into account the circumstances of the case.

For example, you could easily retrieve information contained in an email that has been moved into the 'Deleted items' box whereas, if information is permanently deleted in accordance with your retention policy, although there might exist technology available in order to recreate that information, you may not be required to do so if that technology is not readily or already available to you.

As regards the form of the response, Data Controllers should follow the principle that an access request should be responded to in **the manner indicated by the requester**. Where no specific indication is made by the requester, Data Controllers should use the same format in which the access request was made. Either way, Data Controllers must ensure to provide the information in a secure manner. This includes when sending information through the post; this should be done by sending the access request data in a secure envelope or package, clearly marked as 'Private & Confidential' and 'For Addressee only' (see: Guidance on Data Security).

For example, where a request is made electronically, you should provide the required information in a commonly used electronic format, meaning that the Data Subject should not need to incur any costs in order to get access to the data, for example by having to buy a specific software. If transmitting personal data electronically, it is the responsibility of the Data Controller to ensure the personal data is transmitted in a secure manner at all times.

Data Controllers must provide the information indicated above **free of charge** (see below the limited exceptions to that principle) and in an **easily visible, intelligible and clearly legible** manner (Article 12.7 GDPR). This means, for example, that in certain circumstances – provided that the actual personal data is not altered – Data Controllers may also need to elaborate on the information sent on to the requester in order to contextualise them, and not simply send the information without a proper structure or explanation in place, especially if there is a lot of information processed.

For example, if you have received an access request from an employee in respect of an internal competition for a promotion which required the applicant to undertake various tests, you may be required to furnish their scores and answers, as they may constitute personal data, and you may need to further elaborate on how those scores were attributed to them if their attribution and/or rationale are not immediately intelligible.

Fulfilment of the above mentioned information quality requirements ultimately depends on the circumstances of each case, which must always be taken into account. In particular, if the request is answered using automated means through the employment of a software package or Artificial Intelligence (A.I.), although they may be suitable to all the above mentioned conditions, it is recommended Data Controllers ensure that not only pre-prepared explanations but also real **human interaction** is readily available to the requester after the response has been received in order to answer any questions the Data Subject may have.

For example, if you have implemented a data access response system based on automated means, which allows the Data Subject to "download" their personal data and which automatically presents all the information required by law, based on the information you possess on the Data Subject, you should also ensure that they have the contact details of your DPO and that any relevant question they may pose is answered.

Just as importantly, Data Controllers must ensure **not to disclose third party data** and must therefore adopt all technical and organisational measures and comply with confidentiality obligations under data protection law in order to prevent such risk (see: Redacting Documents and Records). Redaction of names may not be enough to render third party unidentifiable and Data Controllers may be at risk of inadvertently disclosing third parties data when responding to the access request because, for example, those third parties may be identified by reference to certain positions they hold or other information such as an employee number or their PPS number.

For example, if you are an employer and have received an access request in relation to personal data held by you on an employee's working performance, your records in relation to this may contain personal data in the form of minutes of discussions containing references to other employees. Not only must the names of the other employees be redacted before responding to the access request, but you must also make sure that other information that may otherwise identify them – such as references to their role/shift/payroll – is redacted too.

There may be instances in which the personal data that constitute the subject matter of the access request inevitably refers to two or more persons (so-called **mixed personal data**). In this case, see below: 'When can I refuse to comply with the request?'

## *Are there instances in which I can charge for providing the response?*

Access requests must be responded to free of charge (Article 12(5) GDPR), including where there is no data to be disclosed to the requester or the requester is not entitled to the response, for example because he or she is not the Data Subject and does not have an authorisation for the request. However, in exceptional circumstances, Data Controllers may charge a reasonable fee based on their administrative costs:

- If two or more access requests are **manifestly unfounded or excessive**, (it should be noted that there is a high threshold for a Data Controller to prove that the request is unfounded or excessive. This is also dependent on the amount of data processed by the Data Controller in relation to the Data Subject) in particular because of their repetitive character (alternatively, Data Controllers may refuse to respond to the request - see below 'When can I refuse to comply with the request?') (Article 12(5)(a) GDPR).

- If **additional copies** of the personal data at issue have been requested (Article 15(3) GDPR).

In both instances it is recommended, in case the requester contests the charging of the fee and, more generally, in accordance with the principle of accountability, that Data Controllers make sure they can demonstrate that they have in fact incurred, or may reasonably incur, administrative costs outside the general expenses of their organisation. Even if that is the case, the charging of the fee must also pass a **reasonableness test** which depends on the specificities of the actual fee (for example, whether it would give time for the requester to decide to withdraw the request) and the extent to which this could negatively affect the right of access of the Data Subject in the circumstances of the case.

For example, if the request for an additional copy of the data comes from a Data Subject alleging that he has lost the response email, even if you do incur additional costs in terms of time spent by your personnel re-sending the email and also in relation to the actual weight in terms of MB of the email itself, the charging could not pass the reasonableness test as the actual calculation of the fee would be close to nil and the fact that the Data Subject is not anymore in possession of his data means that if you make him pay, his right of access is affected by a fee.

## *When can I refuse to take action on the request?*

Data protection law sets out limited instances in which Data Controllers **should or may not take action** on an access request and Data Controllers should bear in mind two fundamental aspects: First, they may solely withhold the information that they are entitled to withhold as indicated in those instances, and secondly, even if they can demonstrate that their case falls within one of those instances, Data Controllers may still be liable for breaching data protection law if they fail to **inform the requester** in respect of any of the following information without undue delay and, in any event, within one calendar month from receipt of the access request (see above 'What are the deadlines to respond?') (Article 12(4) GDPR):

- The **reasons** for not taking action on the access request
  A reference as to which specific provision allows the Data Controller to disregard the access request and how it applies to the specific access request at issue.
- The possibility of lodging a **complaint** with a competent supervisory authority
  A standard notice making reference to the contact details of the DPC.
- The possibility of seeking **judicial remedy**
  A standard notice making reference to the fact that the requester may – in addition to the possibility of lodging a compliant – also seek a judicial remedy.

Some of the instances limiting the right to access in which a Data Controller should not take action on an access request are provided for directly by the GDPR:

a) Under Article 11, if Data Controllers **process information where they are unable to identify Data Subjects** (see: Anonymisation and Pseudonymisation), in accordance with data minimisation and purpose limitation principles (see: Principles of Data Protection), they may refuse to act on access requests related to that information unless the requesters themselves provide further information which would identify Data Subjects. It is therefore recommended that if Data Controllers invoke the applicability of Article 11, they **indicate**

**which additional information may be necessary** in order to exercise the right of access. Furthermore, even if the Article 11 exception applies, Data Controllers would still be obliged to comply with other data protection requirements when handling the information referred to in Article 11 (see: Know Your Obligations).

For example, if you are running a website and use technology to process anonymised browsing data of your users, having obtained their consent, in order to improve your website, one of your users may lodge an access request seeking all the personal data held by you/your processor in respect of their activities on the website and your tracking activity. If the requester is unable to provide you with further information, for example with cookies which can uniquely identify them in a browsing session, you may decline to answer the access request.

b) Under Article 12(5), where an access request is 'manifestly unfounded or excessive' Data Controllers may refuse to act on it. A high threshold must be met in order for Data Controllers to avail of this exception, as they must prove that the **request is** '**manifestly**' (i.e. in the eyes of a data protection professional) either:

- **Unfounded**, which means that the request does not concern personal data at all (bearing in mind the broad meaning of the term "personal data" – see Data Protection Basics) or, although it does concern personal data, it is obvious that the data are not handled by you.

For example, if an access request for personal data related to the issuing and handling of a birth certificate is lodged to the County Council, the request may be considered as "manifestly unfounded" as the object of the request, which is the data related to the birth certificate, are not handled by the County Council, but by the General Register Office and the Civil Registration Services Office.

- or **Excessive**, in particular taking into account whether the request is repetitive. Data Controllers should look at each single access request first and only thereafter operate a contextualisation in order to assess "excessiveness". The fact, on its own, that the access request re-occurs or the fact, of its own, that it would take a lot of time and effort of the Data Controller to provide the information, does not automatically imply excessiveness.

For example, an access request may be repetitious in its re-occurring, but that may be so because the personal data processed by the controller are constantly growing (e.g. if the request is made by the user of a social network platform).

c) Under Article 15(4), where **obtaining a copy** of the personal data **would adversely affect the rights and freedoms of others**, such as privacy, trade secrets, or intellectual property rights, including those of Data Controllers and Data Processors (see below 'What if personal data is being held by a processor/What if I am a joint controller?), Data Controllers may not provide the requester with the copy of the requested data.

This limitation is specifically concerned with the entitlement of Data Subjects to obtain a copy of their data (see above – 'What should the content and form of my response be?' under no. 4), and **should not affect the other entitlements** under their right of access, such as obtaining confirmation of processing and the information required by data protection law and otherwise access to the personal data (see above 'What should the content and form of my response be?' under no. 1, 2 and 3).

Data Controllers should endeavour to **comply with the request insofar as possible** whilst ensuring adequate protection for the rights and freedoms of others. Reliance on 15(4) should not result in a complete refusal to provide data to the Data Subject. The extent of compliance depends on the extent to which the provision of the copy of the data could be considered as "adversely affecting" those rights and freedoms which, in turn, depends on the circumstances of each case. The rights and freedoms considered by Data Controller should be protected under European or Irish Law. Firstly, Data Controllers should assess whether the provision of the copy of the data does have any effect at all on the rights and freedoms of others, and secondly, whether that effect is a negative one, in the sense that it limits said rights and freedoms.

For example, if the access request could negatively impact your **trade secrets** on an algorithm you are using in order to track the activities of the users of your website and implement targeted advertising, you may not be required to reveal the algorithm itself (potentially completely undermining your trade secret and therefore adversely affecting that right), when providing a copy of the behavioural data processed by you but, you should provide the Data Subject with all relevant information required by data protection law related to the targeted advertising of the requester, including indicating specifically all the recipients of the behavioural data and sufficient information in order for the Data Subject to understand the reasons for automatic decisions (see above: What should the content and form of my response be? Under nos. 1 and 2).

If access requests concern **mixed personal data**, the privacy and data protection rights of third parties may be affected by the provision of a copy of the mixed personal data. If Data Controllers are not in the position to obtain a valid consent from the third party (see: Legal Bases for Processing Personal Data), as above, the Data Controller will need to have undertaken an assessment as to the balance between the rights of the Data Subject and the third parties' rights. Again, it may be the case that a practical solution can be reached, as in the example given above, that in the case of the release of CCTV footage a Data Controller could blur the images of any third parties in any footage

The right of access, together with other data protection rights, is also subject to a number of limitations under Irish Law, most importantly under certain provisions of the Data Protection Act 2018 (see: Limiting Data Subject Rights), including:

- Section 43: processing for the purpose of exercising the right to freedom of expression and information, including processing for journalistic purposes or for the purposes of academic, artistic or literary expression,
- Section 59: processing for election purposes*,*
- Section 60: processing for important objectives of general public interest (e.g. to exercise or defend a legal claim or in relation to opinions given in confidence)*,*
- Section 61: processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,
- Section 68: processing of health data under the relevant legislation,
- Section 94: where it is necessary and proportionate for law enforcement purposes,
- Section 158: where it is necessary and proportionate to safeguard judicial independence and court proceedings, and
- Section 162: processing related to legal advice, privileged communications, or court orders.

If Data Controllers consider they are justified in withholding certain information pursuant to the provisions of the Data Protection Act 2018, or pursuant to other relevant Irish legislation (e.g. the Data Protection Act 2018 (Access Modification) (Health) Regulations 2022 (S.I. No. 121 of 2022) they will have to identify the relevant exemption, provide an explanation as to why it applies, often by conducting a **necessity and proportionality test** (See Limiting Data Subject Rights), and notify the requester of the possibility of lodging a complaint to the competent supervisory authority/seeking judicial remedy.

## *What if the personal data is being held by a processor or I am a joint controller?*

Data Controllers must ensure to validly answer the access request even if, in order to do so, they must engage with the entity which conducts processing operations on their behalf ("Data Processor") (for instance when Data Controllers need to retrieve the data from it in order to answer the access request), as **liability for compliance ultimately rests upon the Data Controller** (unless the Data Processor acts outside the instructions of the Data Controller or infringes obligations imposed directly on it by data protection law). The Data Processor should be obliged to assist the Data Controller in fulfilling their obligations, including those related to the exercise by the Data Subjects of their right of access, pursuant to the contract or legal act existing to regulate your relationship (see: A Practical Guide to Controller-Processor Contracts).

For example, if you use a cloud service provider in order to securely store the personal data of your employees in relation to HR issues you may want to make sure that the contract regulating the relationship between you and the service provider clearly states that whenever you notify them of an access request, they are obliged to provide you with the relevant data within three working days and in accordance with certain standards enabling you to ensure all relevant personal data of the relevant employee are securely handed over to you in order to comply with the access request.

If a Data Controller decides to **outsource the answering of access requests** to a Data Processor, they must ensure that the Data Processor will be able to comply with all the data protection obligations related to access requests, for whose infringement the Data Controller will ultimately bear liability if the Data Processor acts within their instructions. For these reasons, the legal document which regulates the relationship between Data Controller and Data Processor is of pivotal importance (see A Practical Guide to Controller-Processor Contracts).

If the Data Controller jointly determines the purposes and means of processing and is therefore a Joint Controller, the **Data Subjects may exercise their access rights in respect of and against each of the Joint Controllers** (Article 26(3) GDPR) notwithstanding any different provision existing in the legal document governing the relationship between them (Article 26(1) GDPR). This ultimately means that an access request may be validly lodged to one Joint Controller in respect of data that may be solely processed by the other Joint Controller and vice versa. It is therefore important that technical and organisational measures between Joint Controllers are in place to ensure that every request related to personal data processed by a Joint Controller, different to the Controller which received the access request, is dealt with within the deadlines. This can be facilitated by an in-depth consideration of the processing activities in the legal document governing the relationship between Joint Controllers.

---

## *Further guidance may be found in the decisions of the DPC*

Groupon International Limited - December 2020

Ryanair DAC - November 2020