Data Subject Access Requests – FAQs

An Coimisiún um Chosaint Sonraí
Data Protection Commission

The majority of the complaints and queries the Data Protection Commission (DPC) receives concern individuals, or 'data subjects', seeking to exercise their **'right of access'**. The General Data Protection Regulation (GDPR), under Article 15, gives individuals the right to **request a copy** of any of their personal data which are being 'processed' (i.e. used in any way) by 'controllers' (i.e. those who decide how and why data are processed), as well as **other relevant information** (as detailed below). These requests are often referred to as 'data subject access requests', or 'access requests'. A similar right exists under section 91 of the Data Protection Act 2018, where personal data are processed for law enforcement purposes.

These requests must be responded to **free of charge** and in an **accessible** form, and controllers should seek to facilitate access requests being both made and responded to **easily**, including **electronically** where appropriate and where the individual wishes.

The following guidance should answer some of the most frequently asked questions by both individuals who are seeking copies of their personal data, as well as controllers who are struggling to deal with the access requests they are receiving.

When is an individual entitled to make an access request?

There are **no special conditions** that need to be satisfied in order for an individual to be entitled to make an access request. An individual can make an access request to any controller who they think might be processing their personal data.

What information is an individual entitled to when they make an access request?

There are actually **a few different aspects** to the right of access under Article 15 GDPR. First of all, individuals are entitled to **confirmation** of whether the controller is processing any of their personal data, which means any information which concerns or relates to them. Where that is the case, they are also entitled to **a copy** of their personal data. Further, individuals are entitled to other **additional information** about the processing of their personal data.

The additional information individuals are entitled to includes: 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. In many cases, controllers will already be providing this information to data subjects, such as through their privacy notice.

How broad can the scope of an access request be?

Whilst an individual is entitled to access to any or all of their personal data, where a controller processes a **large quantity of information** concerning the individual, the controller should be able to **request that the individual clarify** the request, by specifying the information or processing activities which they want access to or information on.

This should only be done where **reasonably necessary to clarify** a request, and **not to delay** in responding to it. Where a controller asks an individual to clarify their request, they should let them know as soon as possible. If the individual refuses to clarify the request, the controller will **still need to comply** with the original request.

Does an access request have to be made in writing?

The **GDPR does not set out any particular method** for making a valid access request, therefore a request may be made by an individual **in writing or verbally**. Where an access request is made verbally, the DPC recommends that controllers **record the time and details** of the request, so that they can ensure they comply with and do not misunderstand the request. Controllers may want to **follow up with individuals** in writing to confirm that they have **correctly understood** the request. The DPC would also encourage individuals to **submit written access requests where practical**, to avoid disputes over the details, extent, or timing of an access request.

Some controllers may wish to use **standard or online forms** for individuals to submit access requests through – Recital 59 GDPR even encourages this for electronic requests. Whilst such forms can help **streamline** the exercise of the right of access and support consistency and timely responses, controllers should keep in mind that access requests can still be **validly made by other means**, such as letter, email, telephone call, or even through social media.

Where an access request is made, a controller may invite or encourage the individual to submit it through their designated form instead, but they should make it clear that this is **not compulsory**, and the **deadline** for responding to the access request **begins to run** from the **time the valid request** is made by any means, not only through the designated form. Nevertheless, an online form will often be the most efficient method for an individual to make their request and have it responded to in a timely manner.

Does an access request have to be made to a specific contact point designated by the controller?

As with the question regarding the format an access request may take, where controllers have a particular **contact point or member of staff designated** for handling access requests, contacting them will normally be the **most efficient** way for an individual to have their request responded to promptly, but it should **not be considered mandatory**.

It is possible that a **valid access request** may be made to **any member of staff** of a controller. This may present a challenge, particularly in absence of sufficient awareness or training regarding data protection obligations. Controllers should **ensure** that **systems are in place** so that all valid access requests are actioned appropriately – particularly regarding staff who regularly interact with customers or the public.

As with standard forms, a controller may **encourage data subjects to contact the designated contact point**, but they **cannot oblige them** to do so. Therefore, where a request is made to another member of staff, the clearest approach may be to **forward the request** to the correct contact point, whilst **copying in the individual** and explaining the process for handling the request.

Are there other formalities required for a valid access request?

There are no other formal requirements for an access request to be valid, other than that the request is **sufficiently clear to act upon**, and that the **identity** of the requester is sufficiently clear. Individuals should be sufficiently clear about what information they are seeking, and **proof of their identity should only be requested where reasonable and proportionate** to do so. Where the controller does require more information or proof of identity, they should **inform the requester as soon as possible**, and the time limit for responding to the request begins when they receive the additional information.

Seeking proof of identity would be **less likely to be appropriate** where there was **no real doubt** about identity; but, where there are doubts, or the information sought is of a particularly sensitive nature, then it may be appropriate to request proof. Controllers should only request the **minimum amount of further information necessary** and **proportionate** in order to prove the requester's identity.

Further, there is **no need** for an individual to use a **particular form of words**, or even to specifically mention data protection legislation, to make a valid access request; however, it may be helpful for the **sake of clarity** to **mention** that the request is an **access request**, pursuant to the relevant data protection legislation.

How long does a controller have to respond to an access request?

Controllers who receive a valid subject access request must respond to the request **without undue delay** and at the **latest within one month** of receiving the request. Controllers can **extend the time** to respond by a further **two months** if the request is **complex** or they have received a **number of requests** from the **same individual**, but they must still let the individual know within one month of receiving their access request and **explain to them** why the extension is necessary.

Further, it is **good practice** for 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 or proof of identity.

How should controllers provide the information to individuals?

The general rule is that a controller should respond to an individual's access request in the **same way the request was made**, or in the way in which the **requester specifically asked** for a response. Where a request is made electronically, controllers should provide the required information in a **commonly used electronic format**, unless the individual requests otherwise.

Where an individual makes a verbal access request, they may want or be satisfied with a **verbal response** to their access request, depending on the nature of the request. Controllers should consider **keeping a record** of the verbal response issued, as well as what they understood the request to be. If a request asks that the response be made in writing, controllers should provide the response in writing to the address provided.

Can controllers charge a fee for responding to an access request?

In most cases individuals cannot be required to pay a fee to make a subject access request. Only in certain very **limited circumstances**, per Article 12(5) GDPR, where the initial request is 'manifestly unfounded or excessive' (which the controller must prove), can a controller charge a **'reasonable fee'** for the **administrative costs** of complying with the request. Controllers are also allowed to charge a reasonable fee, based on administrative costs, where an individual requests additional copies of their personal data undergoing processing.

Are there any other limitations on the right of access?

Under Article 12(5) GDPR, in **limited circumstances**, where an access request is **'manifestly unfounded or excessive'**, a controller may also, where appropriate, **refuse to act** on the request. This is, however, a **high threshold** to meet, and the controller must be able to **prove** that the request was manifestly unfounded or excessive, in particular taking into account whether the request is repetitive. There should be **very few cases** where a controller can justify a refusal of a request on this basis.

There is a **general limitation** on the exercise of the right of access under Article 15(4) GDPR, which states that the right to obtain a copy of the personal data undergoing processing should not negatively impact ('adversely affect') the **rights and freedoms of others**, such as privacy, trade secrets, or intellectual property rights. However, where a controller does have concerns about the impact of complying with a request, their response should **not simply be a refusal** to provide all information to the individual, but to **endeavour to comply** with the request insofar as possible whilst ensuring adequate protection for the rights and freedoms of others.

Whilst the right of access to personal data is a **fundamental data protection right** it is **not an absolute one**, and is subject to a number of **limited exceptions**. Article 23 GDPR allows for data subject rights to be restricted in certain circumstances. Any such restrictions must be set out in a 'legislative measure', **respect the essence** of the fundamental rights and freedoms, be **necessary and proportionate** in a democratic society, and **safeguard an interest of public importance**. The Data Protection Act 2018 contains certain provisions dealing with the restrictions of rights of data subjects, including sections 59, 60, and 61 in particular, which give further effect to the provisions of Article 23 GDPR.

Accordingly, if a controller considers that it is justified in withholding certain information in response to an access request it **must identify an exemption** under the GDPR or the 2018 Act, **provide an explanation** as to why it applies, and **demonstrate** that reliance on the exemption is **necessary and proportionate**.