Manifestly unfounded and excessive requests

At a glance

- Under Part 3 of the DPA 2018, individuals have rights of access, rectification, erasure, restriction, and to not be subject to automated decision-making.
- You may refuse to respond to a request if it is manifestly unfounded or excessive.
- Alternatively, you may charge a reasonable fee for dealing with the request.
- You must be able to demonstrate why it is manifestly unfounded or excessive.

Checklists

Responding to manifestly unfounded and excessive requests

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

☐ We understand the considerations we need to account for when deciding if a request is manifestly unfounded or excessive.

In brief

- What types of requests can we consider as manifestly unfounded or excessive?
- What general considerations should we take into account when deciding if a request is manifestly unfounded or excessive?
- What does manifestly unfounded mean?
- What does manifestly excessive mean?
- What should we do if we refuse to comply with a request?
- When can you charge a fee?

What types of requests can we consider as manifestly unfounded or excessive?

An individual has the right to request:

- access to their personal data;
- rectification of their personal data;
- restriction of the processing of their personal data;
- erasure of their personal data; and
- not to be subject to automated processing.

For further information about these rights, please see our Guide to Law Enforcement Processing.

If you process personal data for law enforcement purposes and you consider a request made in the exercise of any of these rights to be manifestly unfounded or excessive, you may refuse to comply with the request.

Alternatively, you can instead charge a reasonable fee to deal with the request (see When can you charge a fee?).

What general considerations should we take into account when deciding if a request is manifestly unfounded or excessive?

You should not have a blanket policy for determining whether a request is manifestly unfounded or excessive. You must consider each request on a case-by-case basis.

Whilst there may be characteristics that are indicative of a manifestly unfounded or excessive request (please see the next sections), you should only use these as a guide. You should not presume that a request is manifestly unfounded or excessive just because the individual has previously submitted requests which have been manifestly unfounded or excessive.

The inclusion of the word "manifestly" means it must be obvious or clear that the request is unfounded or excessive. You need to have a strong justification for why you consider a request to be unfounded or excessive. You must be able to demonstrate this justification to the individual and, if asked, to the Information Commissioner's Office (ICO).

What does manifestly unfounded mean?

A request may be manifestly unfounded if the individual clearly has no intention to access the information or is malicious in intent and/or is using the request to harass an organisation with no real purpose other than to cause disruption.

Factors that may indicate a manifestly unfounded request include where:

- the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
- the request makes unsubstantiated or false accusations against you or specific employees which are clearly prompted by malice;
- the individual is targeting a particular employee against whom they have some personal grudge;
- the individual makes a request but then offers to withdraw it in return for some sort of benefit from the organisation; or
- the individual systematically or frequently sends different requests to you as part of a campaign with the intention of causing disruption, eg once a week.

These factors are not intended to form a simple tick list that automatically mean a request is manifestly unfounded. You must consider a request in the context in which it is made, and the onus is on you is to be able to demonstrate that it is manifestly unfounded.

You should consider the particular situation and whether the individual genuinely wants to exercise their rights. If this is the case, it is unlikely that the request is manifestly unfounded. In most cases, use of aggressive or abusive language does not, in itself, demonstrate a manifestly unfounded request.

Example

An individual is unhappy with the outcome of a complaint to a regulator. The individual posts online that they plan to make a request for their information to be deleted every day until the employee that dealt with their complaint is fired.

You have already responded to their first erasure request and it is clear that their intention is to threaten or disrupt your organisation. You refuse these further requests on the grounds that they are manifestly unfounded.

What does manifestly excessive mean?

To determine whether a request is excessive you need to consider whether it is clearly or obviously unreasonable. You should base this on whether the request is proportionate when balanced with the burden or costs involved in dealing with the requests.

This will mean taking into account all the circumstances of the request, including:

- the nature of the information the request relates to;
- the context of the request, and the relationship between you and the individual;
- whether a refusal to carry out the request or even acknowledge that you hold relevant information may cause substantive damage to the individual;
- your available resources;
- if the request largely repeats previous requests and a reasonable amount of time hasn't elapsed; or
- whether it largely overlaps with other requests (although if it relates to a separate set of information it is unlikely to be excessive).

In most cases, a request is not excessive just because the request relates to a large amount of information, even if you find it a burden. As noted above, you must consider all the circumstances of the request. If it is a request for access, you should also consider asking them for more information to help you locate the information they want to receive. You should ensure that you have appropriate records management procedures in place to handle large requests and locate information efficiently.

A repeat request may not be excessive if a reasonable amount of time has passed since their last request. You should consider the following when deciding whether a reasonable interval has elapsed:

- the nature of the data – this could include whether it is particularly sensitive; and
- how often you alter the data:
    - If it's unlikely that the information has changed between requests, you may decide you do not need to respond to the same request twice.
    - If you have deleted information since the last request, you should inform the individual of this.
    - If you have collected new information since their last request then the request may also not be excessive.

Requests about the same issue are not always excessive. An individual may have legitimate reasons for making requests that repeat the content of previous requests. For example, if the controller has not handled previous requests properly, or if a response to a previous request has provided an individual with new information they were not previously aware of, prompting a new request. However, in other circumstances a request which effectively repeats the substance of a previous request may be excessive. This will depend on the individual circumstances.

A request may be excessive if an individual makes a new request before you have had the opportunity to address an earlier request. However, this is only the case if the substance of the new request repeats some of the previous request. It is unlikely to be excessive if the overlapping request is about a separate set of information.

A request for information will not automatically be excessive just because the information was previously made available as part of the criminal justice system. You need to consider the wider circumstances of the request, the fact that you have already provided the individual with the same information under another procedure should be considered alongside other factors, such as substantive damage to the individual, when deciding whether a request is excessive. This will particularly be the case if you have provided the individual with exactly the same information through an alternative statutory disclosure mechanism. For further information, please see 'Do we have to respond to the SAR if the individual has an alternative means of accessing their information?' in our detailed guidance on the Part 3 right of access.

Example

One month ago, you responded to an individual's subject access request for their information which included their conviction history. Since then, the individual has made a new request for their information and asked for their conviction history to be included again. The only new information that the police have collected since their request one month ago relates to a call to the police complaint department.

You consider that the amount of time needed to provide all the information, including their conviction history, compared to only providing the new information that has been collected since you responded to their last request. You decide that to provide all the information would be excessive, especially because of the overlap in information and the time elapsed since the last request.

You refuse to respond to the whole request again because it would be excessive. Instead, you notify the individual that their request is excessive and provide the individual with the additional new information that was collected over the last month.

What should we do if we refuse to comply with a request?

If you refuse to comply with a request, you must inform the individual of:

- the reasons why you have not complied with their request;
- their right to make a complaint to the ICO ; and
- their ability to seek to enforce this right through a judicial remedy.

As mentioned above, if you believe a request is manifestly unfounded or excessive you must be able to demonstrate this to the individual and, if asked, to the ICO.

When can you charge a fee?

You may charge a reasonable fee if you decide that a request is manifestly unfounded or excessive, but you still choose to respond to it.

If you decide to charge a fee, you should notify the requester and explain why. You do not need to take further action in response to the request until you have received the fee. The time limit for responding to the request begins once the requester has paid the fee. You should request the fee as soon as possible and at the latest within one month of receiving the request. You must not unnecessarily delay requesting it until you are nearing the end of the one month time limit. If you decide on a reasonable fee, you must be able to justify the cost, in case the requester makes a complaint to the ICO.

Section 53(4) allows for the Secretary of State to specify limits on the fees that controllers may charge to deal with a manifestly unfounded or excessive request by way of regulations. However, at present there are no regulations in place. As such, it is your responsibility as a controller to ensure that you charge a reasonable rate.

For further guidance on the factors that you should consider when determining a reasonable fee and how you should respond to a request when you are charging a fee, you should follow our UK GDPR right of access guidance – 'Can we charge a fee?'.

Example

An accused individual repeatedly requests a file of their personal information relating to their arrest through the right of access. You have given them the same file before, and you have not collected any more information since their initial request. The request is excessive, but you decide to respond to the request because you think they may have lost the file.

You tell the individual you are charging them a fee for this information, based on the cost of administration. Once you have received the fee, you provide the information within one calendar month.

Relevant provisions in Part 3 of the DPA 2018 – See Chapter 3, section 53