

PERSONAL DATA REQUEST RESPONSE TEMPLATE GUIDANCE



PERSONAL DATA REQUEST RESPONSE TEMPLATE GUIDANCE

1. INTRODUCTION

This guidance document is designed to accompany the personal data request response template (the "Response Template") and to provide additional guidance and assistance to help you and/or your organisation in the event that you receive a personal data request. It is designed to be used in conjunction with the Response Template and the general Personal Data Request Guidance note and focuses on providing a useful overview of the Response Template as well as assistance in completing some of its more complicated provisions.

2. OVERVIEW OF THE RESPONSE TEMPLATE

The Response Template is designed to be tailored to the type of personal data request you have received. It is divided into:

- a summary section, which sets out all of the various potential requests you can receive;
- sections dealing with each individual type of request in turn; and
- an appendix containing the information which must be provided to an individual who
 requests that information as part of a subject access request (one of the six potential
 personal data requests an individual can make).

It is important to note that, although the template is clearly organised and divided into neat sections, it is unlikely that any personal data request you receive will be. The first task when you receive a personal data request, in addition to working out whether you hold any personal information about that individual, will therefore be to work out exactly what type of request(s) you have received and what personal information the individual is entitled to be provided with.

Sections in square brackets in the template are designed for you to delete or amend as applicable, depending on the requests you have received and your response to them. This guidance document will assist you in determining which sections you need to delete, include and amend.

3. SUMMARY SECTION

The summary section sets out a summary of the requests you have received. This is to help ensure that you meet your transparency obligations under the General Data Protection Regulation ("GDPR") and to help you categorise the requests when you respond to the individual.

It sets out the six potential requests you may receive: a subject access request, a rectification request, an erasure request, a restriction of processing request, a data portability request and an objection to processing request.

You should delete any requests which you have not received and amend the wording of this section to correspond to the requests you have received, if necessary. For example, if any individual has just asked you to confirm whether or not you are processing their personal data but not asked you to provide them with and a copy of it (i.e. a subject access request), you



can amend the wording of the first bullet point (in relation to a subject access request) accordingly to reflect this.

The second half of the summary section deals with your initial responses to the request.

The first option deals with a situation where you do not have to respond to a request because it is 'manifestly unfounded' or 'excessive'. This is very unlikely to apply in most instances and the paragraph can therefore be deleted in its entirety. If you determine that it does apply, however, you should complete the clause with the reasons why you consider it to be manifestly unfounded and/or excessive and include the subsequent paragraph informing the individual that they have the right to lodge a complaint with the Information Commissioner's Office (ICO) and the right to seek a judicial remedy.

Where the individual has requested a large amount of personal information, you are entitled to request clarification as to which processing activities their request relates to (for example, direct marketing). This should only be the case where it is unclear what the individual is asking for (for example, where they have simply made the whole range of personal data requests without specifying what uses of their personal information they are interested in).

The next paragraph deals with the ability to extend the time period for responding to a personal data request. Generally, this will only be the case where the individual has requested a large amount of personal information and it will be difficult to respond the to the individual within the one month time limit. This should not be the case in the majority of instances, unless, for example you have used the personal information for a range of different purposes and it has been widely dispersed throughout your organisation. It would not be the case, for example, where the only personal information the individual has submitted to you is via a contact form on your website.

The following paragraph should simply be tailored to reflect whether the individual is exercising one or more rights in their personal data request.

The final paragraph in the summary section addresses whether you can charge a fee for dealing with a personal data request. Generally, you are unable to charge a fee to act on and respond to a personal data request, including for providing the individual with a copy of their personal information. However, where the individual requests multiple copies of the <u>same</u> personal information, you are entitled to charge a reasonable fee to cover your administrative costs for doing so. It is important to note that you can only charge for administrative (i.e. no other) costs for complying with a request for additional copies of personal information.

4. SUBJECT ACCESS REQUEST

The subject access request is one of the more difficult requests to comply with. There are two aspects to a subject access request:

- (i) confirming whether or not you process an individual's personal information; and
- (ii) <u>if so, and if requested by the individual</u>, providing access to that individual's personal information and providing the individual with certain information about your processing (i.e. use) of their personal information.



Confirmation

The first part of the request, confirming whether or not your process the individual's personal information, should be relatively straightforward. You simply need to check whether or not you or your organisation possesses the individual's personal information and confirm to the individual whether or not that is the case.

Identity

The second part of the request is more difficult. If the individual requests access to the personal information, you must take "all reasonable measures" to verify the individual's identity. Carrying out identity checks which a bank or lawyer would do when identifying a new client should satisfy this requirement. It is very important to note that you must do this <u>before</u> providing access to any personal information. The risk here is that you could accidentally provide information to someone claiming to be someone they are not, and thereby commit a potential data breach.

It is possible that the individual may already be aware that they need to provide evidence to verify their identity and hence this section is split into two parts. The first part requires the individual to verify their identity if they have not done so. The second part deals with a situation where they have provided the documentation necessary to verify their identity.

The final aspect of a subject access request (providing information about your processing of the individual's personal information) is dealt with in Appendix 1. Further information on what to include in Appendix 1 is contained in the final section of this guidance note.

5. RECTIFICATION REQUEST

A rectification request is a request that you correct and/or complete any inaccurate or incomplete information you hold about an individual, for example, if their address, phone number or email address has changed.

This is one of the easier requests to comply with and you will either be able to update the information you hold about the individual based on the information they have provided to you. If they have not provided the information to you, you will need to request it from them. It is also possible, although less likely, that an individual whose personal information you do not process may request that their personal information is rectified. In such a case you should simply explain that you do not hold any personal information about them and are therefore unable to comply with their request.

6. ERASURE REQUEST

An erasure request is a request that you delete an individual's personal information. This can be an easy or difficult request to comply with depending on how much personal information you hold about the individual and how and where you store it.

You must also determine whether or not you are required to delete some or all of the personal information and, if you are, whether any exemptions apply.



This section is structured to allow you to tailor your response to reflect whether or not you are required to delete some, all or none of the information which the individual has requested you delete.

The third paragraph and the bullet points that follow deal with a situation where you are deleting none or only some of the personal information the individual has requested you delete. The statement "[none of the applicable grounds on which we must delete your personal information apply]" refers to the grounds contained in Article 17(1) of the GDPR. These are the grounds which must apply in order for you to be required to delete the individual's personal information and are as follows:

- the personal information is no longer necessary in relation to the purposes for which you collected or otherwise process it;
- the individual withdraws their consent to the processing of their personal information and consent is the only legal basis you have for processing their personal information;
- the individual has made an objection to processing request (see the section on objection to processing requests below) and you have no overriding legitimate grounds to continue to process their personal information;
- you have processed the personal information unlawfully (usually this will be because you have lacked a legal basis to process the personal information);
- the personal information has to be erased in order to comply with an EU or EU member state national law obligation to erase it; or
- the personal information has been collected in relation to the offer of online services (e.g. a website or app) to a child.

If none of these grounds apply, you do not need to delete the information. However, if any of them do apply, you must comply with the erasure request unless an **exemption** applies. The exemptions are set out in the Response Template. You should consider each of the exemptions carefully to determine if any are applicable in your circumstances. If no exemption is applicable, you must comply with the erasure request.

7. RESTRICTION OF PROCESSING REQUEST

This is a request by the individual that you cease processing the individual's personal data.

In order for you to be required to comply with a restricting of processing request, one of the relevant grounds referred to in Article 18(1) of the GDPR must apply. Those grounds are as follows:

- the individual must dispute the accuracy of their personal information (in which case you must stop processing the personal information for as long as it takes you to verify the accuracy of the personal information);
- you are processing the individual's personal information unlawfully and the individual opposes the erasure of their personal information and requests that you restrict your processing of their personal information instead;
- you no longer need the personal information for the purpose(s) for which you process
 it but the individual requires it for the establishment, exercise or defence of legal claims;
 or



• the individual has objected to the processing of their personal information pending the verification of whether your legitimate grounds for processing their personal information override those of the individual.

This section is divided accordingly between

- (i) circumstances in which one or more of these grounds apply, in which case you must comply with the request, and
- (ii) circumstances where none of these grounds apply, in which case you do not need to comply with the request.

8. DATA PORTABILITY REQUEST

This is a request that you provide the individual or a third party specified by the individual with their personal information in a structured, commonly used and machine-readable format (e.g. a CSV file).

This section is divided accordingly into a circumstance where the individual requests that you provide them with the personal information directly, where they request that you provide their personal information to a third party and the circumstances in which you are not required to comply with the request.

There are three circumstances in which you are not required to comply with a data portability request. The first is where one or more of the grounds in Article 20(1)(a) or 20(1)(b) does not apply. These grounds are the following three requirements, <u>all</u> of which must be satisfied before you are required to comply with the data portability request:

- the individual has provided you with the personal information;
- you process the individual's personal information on the basis of their consent or for the performance of a contract to which the individual is subject or in order to take steps, at the individual's request, prior to entering into a contract; and
- the processing of the individual's personal information is carried out by automated means (i.e. digitally rather than paper records).

Unless all three of these grounds apply, you do not need to respond to the request.

If these grounds do apply, you may not need to comply with the request if either of the following apply:

- your processing of the personal information is necessary for a task carried out in the public interested and/or in the exercise of official authority; or
- it is not technically feasible to transfer the personal information to a third party (if the individual has requested that you transfer their personal information to a third party).

Both of these exemptions are very unlikely to apply, particularly if you are a private company. Therefore, in the vast majority of cases, if the individual is able to satisfy all three of the grounds in Article 20(1)(a) and (b), you will be required to comply with the data portability request.

9. OBJECTION TO PROCESSING REQUEST

This is a request by the individual that you stop processing their personal information.



If you are processing the individual's personal information for marketing purposes (including profiling¹), you must comply with the request and stop processing the personal information for marketing purposes (and/or profiling, as the case may be). There are no exemptions or carveouts or pre-requisites to the individual's right to object to the processing of their personal data for marketing purposes (or profiling) so you must comply with it.

In cases where you process the individual's personal information for other purposes, whether the individual has the right to object will depend on whether the requirements for the right to apply are met and whether you can rely on any exemptions.

The requirement for an individual to have the right to be able to object to the processing of their personal information is that one of the following grounds must apply:

- your processing of their personal information is necessary for the performance of a task carried out by you in the public interest or in the exercise of official authority vested in you (the data controller), including profiling² based on such grounds;
- your processing of their personal information is done on the basis that it is necessary for your legitimate interests or those of a third party, including profiling based on such grounds;
- your processing of their personal information is done for direct marketing purposes, including profiling to the extent that it is related to such direct marketing; or
- your processing of their personal information is for scientific or historical research purposes or statistical purposes and such processing is not necessary for the performance of a task carried out for reasons of public interest.

If one of these grounds does apply, then you must cease processing the individual's personal information which is the subject of their request, unless:

- you can demonstrate compelling legitimate grounds for processing the individual's personal information which override their interests, rights and freedoms; and/or
- the processing is necessary for your establishment, exercise or defence of legal claims.

This section of the Response Template is divided up accordingly to allow you to delete or amend the paragraphs as required for your particular circumstances.

Where you do not comply with an objection to processing request because you are relying on your compelling legitimate grounds for processing the personal information overriding the individual's interests, rights and freedoms, you must state what those compelling legitimate grounds are and explain why those grounds override the individual's interests, rights and freedoms.

10. INFORMING THIRD PARTIES

are.

If the individual requests that you inform them of the third parties to whom you have disclosed their personal information in their request, you must inform them of who those third parties

¹ 'Profiling' is the use of personal information to predict an individual's behaviour, such as their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.



If they have not requested that you provide them with such information, you can delete this section.

11. APPENDIX

The Appendix of the Response Template relates only to a particular personal data request, the subject access request. If the individual has not made a subject access request (for example, they have only made an erasure request), then you can delete the Appendix altogether. You can also delete the Appendix altogether if the individual has made a subject access request which only asks you to confirm whether or not you are processing their personal information and not that you provide them with information about your processing of their personal information. However, it is very unlikely that an individual would only request the former information and not the latter, so it would be unusual if this were the case.

The Appendix contains all of the headings for the information you need to provide the individual with. You should therefore fill in the information required in square brackets. This will require a careful analysis of the personal information you hold about the individual, how you use their personal information, who you have disclosed it to and any other information required in the Appendix.

Your privacy policy should help you provide some of this information, such as the purposes of your processing of the personal information and the criteria used to determine the period of time for which you will store the personal information. However, you will need to consider the request individually and list exactly the purposes for which you process the individual's information, as the purposes for which you process an individual's information can vary on an individual basis, as can the period of time for which you will store it.

The right to complain to a supervisory authority has already been completed as this is a simple and straightforward information requirement so you do not need to provide any additional information here, unless you are based outside of the UK and the supervisory authority differs from the Information Commissioner's Office (ICO).

The final two paragraphs on the existence of automated decision-making, including profiling and safeguards used to transfer personal information outside of the European Economic Area (EEA) only need to be included if you use automated decision-making³, including profiling⁴ or transfer the personal information outside of the EEA (respectively). If you do not do either of the two, we would recommend, for the avoidance of doubt, that you include a negative statement in the relevant section, so that the individual does not follow-up with further questions or complain to the ICO (or other relevant supervisory authority). Examples of appropriate statements would be:

"We do not use automated-decision making (including profiling)", and

"We do not transfer your personal information outside of the EEA".

³ 'Automated decision-making' is where a decision is made by a machine without human involvement, such as where a machine decides whether or not a person should be taken on as a client.

⁴ 'Profiling' is the use of personal information to predict an individual's behaviour, such as their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.