



# HILLINGDON

LONDON

## Data Protection Individuals' Rights Policy

May 2018

### Introduction

The GDPR introduces the following rights for individuals:

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object;
8. The right not to be subject to automated decision making including profiling.

### 1. The right to be informed

- 1.1 Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.
- 1.2 The type of information to be provided to individuals is the Council's purpose for processing their personal data, the retention periods for the data and who it will be shared with. This is known as 'privacy information'. This information must be provided to individuals at the time when personal data is collected from them. It must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
- 1.3 The Council is required to regularly review, and where necessary, update its privacy information. Any new uses of an individual's personal data must be brought to an individual's attention before processing starts.
- 1.4 If the Council obtains personal data from other sources, it must provide individuals with privacy information within a reasonable period of collecting the data and no later than one month.
- 1.5 It is often most effective to provide privacy information to people using a combination of different techniques which may include:
  - 1.5.1 dashboards;
  - 1.5.2 just-in-time notices;
  - 1.5.3 icons.

1.6 There are a few circumstances where the Council does not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.

1.7 The Council's Data Protection Privacy Notice has been published on its website.

## **2. The right of access**

2.1 Individuals have the right to receive confirmation from the Council that their data is being processed and they also have the right to access their personal data and supplementary information. This right allows individuals to be aware of, and verify, the lawfulness of the processing of their data.

2.2 The Council has published a Right of Subject Access Policy on its website.

## **3. The right to rectification**

3.1 The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. **If made verbally, the Council must introduce a system or policy whereby a record is made of the request.**

3.2 The Council has one calendar month to respond to a request for rectification. When the Council receives the request, it should take reasonable steps to satisfy itself that the data is accurate and to rectify the data if necessary. It should fully take into account the arguments made, and the evidence provided, by the individual. Greater efforts should be made by the Council to rectify data in circumstances where it is used to make significant decisions about individuals. The processing of the personal data in question should be restricted whilst the Council is verifying its accuracy.

3.3 The Data Protection Act 2018 states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

3.4 The Council should let the individual know if it is satisfied that the personal data is accurate within one month of receipt of the request, and tell them that it will not be amending the data. The Council's decision should be explained and it should inform the individual of their right to make a request to, and lodge a complaint to, the Information Commissioner's Office and also their ability to seek to enforce their rights through an application to a court.

3.5 The Council can refuse to comply with a request for rectification if it is manifestly unfounded or excessive. Although the Council is generally precluded from charging a fee to process a request, it can charge a "reasonable fee" to deal with the request or it can simply refuse to deal with it.

3.6 If the Council receives a justifiable request for rectification but it needs to maintain the personal data for evidence, it must, instead of rectifying the data, restrict its processing.

- 3.7 The GDPR does not specify how to make a valid request. However, a request to rectify personal data does not need to mention the phrase 'request for rectification' in order for it to be a valid request. A request will be held as being valid as long as an individual has challenged the accuracy of their data and have asked the Council to correct it, or has asked the Council to take steps to complete data held about them that is incomplete. If there is any uncertainty as to whether a proper request has been made, legal advice should be sought from the Council's Statutory Data Protection Officer.
- 3.8 The Council is able to extend the time to respond to a request by a further two months if the request is complex or it has received a number of requests from the individual. The Council must let the individual know without undue delay, and within one month of receiving their request, and explain why the extension is necessary.
- 3.9 If the Council has any doubts about the identity of the person making the request, it can ask for more information for the purpose of confirming who they are. The Council must let the individual know without undue delay and within one month that it needs this further information and it can refuse to comply with the request until such time as it has received this additional information.
- 3.10 If the Council has disclosed the personal data to others [such as data controllers, processors and persons who are under their direct authority], it must contact them and inform them of the rectification or completion of the personal data unless this proves to be impossible or involves disproportionate effort.

#### **4. The right to erasure**

- 4.1 Individuals have the right to submit a request to the Council that their personal data be erased. This is also known as 'the right to be forgotten'.
- 4.2 Individuals can make a request for erasure verbally or in writing. **If verbally, the Council should have in place a system or policy for recording the request.** The Council has a period of one calendar month in which to respond to the request.
- 4.3 The right is not absolute and it only applies in the following circumstances:
- 4.3.1 the personal data is no longer necessary for the purpose which the Council originally collected or processed it for;
  - 4.3.2 the Council is relying on consent as the lawful basis for holding the data and the individual withdraws their consent;
  - 4.3.3 the Council is relying on legitimate interests as the basis for processing, the individual objects and there is no overriding legitimate interest to continue the processing;
  - 4.3.4 the Council is processing the data for direct marketing purposes and the individual objects to this;
  - 4.3.5 the Council has processed the data unlawfully;
  - 4.3.6 the Council has to erase the data to comply with a legal obligation.

- 4.4 The right to erasure does not apply if processing of personal data is necessary for one of the following reasons:
- 4.4.1 to exercise the right of freedom of expression and information;
  - 4.4.2 to comply with a legal obligation;
  - 4.4.3 for the performance of a task carried out in the public interest or in the exercise of official authority;
  - 4.4.4 for the establishment, exercise or defence of legal claims;
  - 4.4.5 for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing.
- 4.5 The right to erasure will also not apply to sensitive personal data where processing is necessary for public health purposes in the public interest or if it is necessary for the purposes of preventative or occupational medicine.
- 4.6 The Council can also refuse to comply with a request for erasure if it is manifestly unfounded or excessive, taking into account whether it is repetitive in nature. Although the Council is generally precluded from charging a fee for the request, it can charge a "reasonable fee" to deal with the request or it can refuse to deal with it.
- 4.7 If the Council refuses to comply with a request for erasure, it should inform the individual without undue delay and within one month of the receipt of the request. The Council should give its reasons for refusal and explain to the individual that they have a right to make a request to, and lodge a complaint to, the Information Commissioner's Office and that they also have the ability to enforce this right through an application to a court.
- 4.8 If the Council receives a request for erasure but it needs to maintain the personal data for evidence, it must, instead of erasing the data, restrict its processing.
- 4.9 There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR.
- 4.10 If the Council processes data collected from children, it should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child - especially any processing of their personal data on the internet.
- 4.11 The GDPR does not specify how to make a valid request. A request to erase data does not need to mention the phrase 'request for erasure' in order for it to be a valid request. If there is any uncertainty as to whether a proper request has been made, legal advice should be sought from the Council's Statutory Data Protection Officer.

- 4.12 The Council is able to extend the time to respond to a request by a further two months if the request is complex or it has received a number of requests from the individual. The Council must let the individual know without undue delay and within one month of receiving the request and explain why the extension is necessary.
- 4.13 If the Council has any doubts about the identity of the person making the request, it can ask for further information. The Council must let the individual know without undue delay and within one month that it needs this further information to confirm their identity. The Council does not need to comply with the request until such time as it has received this additional information.
- 4.14 There are two circumstances where the Council should tell other organisations about the erasure of personal data:
- 4.14.1 it has been disclosed to others;
  - 4.14.2 the personal data has been made public in an online environment [for example, on social networks, forums or websites].
- 4.15 If the personal data has been disclosed to others such as data controllers, processors and persons who are under their direct authority, then the Council must contact each recipient to inform them of the erasure, unless this proves impossible or involves disproportionate effort.

## **5. The right to restrict processing**

- 5.1 Individuals have the right to request the restriction or suppression of their personal data. This is an alternative to requesting the erasure of their data. This right has close links to the right of rectification and the right to object. It is not an absolute right and it only applies in certain circumstances.
- 5.2 Individuals have the right to request that the Council restricts the processing of their data in the following circumstances;
- 5.2.1 the individual contests the accuracy of their personal data and the Council is verifying it;
  - 5.2.2 the data has been unlawfully processed by the Council and the individual requests restriction instead of erasure;
  - 5.2.3 the Council no longer needs the personal data but the individual needs the Council to keep it in order to establish, exercise or defend a legal claim; or
  - 5.2.4 the individual has objected to the Council processing its data and the Council is considering whether its' legitimate grounds override those of the individual.
- 5.3 Although this is distinct from the right to rectification and the right to object, there are close links between those rights and the right to restrict processing so that if an individual asks the Council to rectify or exercises their right to object, they can at the same time request that the Council restricts the processing of their personal data.

- 5.4 The GDPR suggests that there are a number of methods which the Council can use to restrict data such as:
- 5.4.1 temporarily moving the data to another processing system;
  - 5.4.2 making the data unavailable to users;
  - 5.4.3 temporarily moving published data from a website.
- 5.5 It is important that the Council considers how it should store data that it no longer needs to process but the individual has requested it to be restricted. If the Council is using an automated filing system, it will need to use technical measures to ensure that any further processing cannot take place and that data cannot be changed whilst the restriction is in place. A note should also be placed on the Council's systems to the effect that the processing of the data has been restricted.
- 5.6 The Council must not process the restricted data in any way **except to store it** unless:
- 5.6.1 it has the individual's consent;
  - 5.6.2 it is for the establishment, exercise or defence of legal claims;
  - 5.6.3 it is for the protection of the rights of another person; or
  - 5.6.4 it is for reasons of public interest.
- 5.7 If the Council has disclosed the personal data in question to others, then it must contact them (for example, data controllers, processors and persons who are under their direct authority) of the restriction of the personal data unless this proves impossible or involves disproportionate effort.
- 5.8 In many cases, the restriction of processing is only temporary. Once the Council has made a decision on the accuracy of the data, it may decide to lift the restriction but it must inform the individual before it does so. It will also need to inform the individual of their right to make a complaint to the Information Commissioner's Office and their ability to make an application to a court.
- 5.9 The Council can refuse to comply with a request for restriction if it is manifestly unfounded or excessive, taking into account whether it is repetitive in nature. Although the Council is generally precluded from charging a fee for the request, it can charge a "reasonable fee" to deal with the request or it can refuse to deal with it.
- 5.10 If the Council refuses to comply with a request for restriction, it must inform the individual:
- 5.10.1 of the reasons for the refusal;
  - 5.10.2 of their right to make a request to the Information Commissioner's Office or to lodge a complaint to this body;
  - 5.10.3 of their right to apply to a court.

- 5.11 The GDPR does not specify how to make a valid request. It can therefore be made verbally or in writing. **If made verbally, the Council should have a system or policy in place for recording the request.** A request for restriction does not need to mention the phrase 'request for restriction' in order for it to be a valid request. If there is any uncertainty as to whether a proper request has been made, legal advice should be sought from the Council's Statutory Data Protection Officer.
- 5.12 The Council is able to extend the time to respond to a request by a further two months if the request is complex or it has received a number of requests from the individual. The Council must let the individual know within one month of receiving their request and explain why the extension is necessary.
- 5.13 If the Council has any doubts about the identity of the person making the request, it can ask for more information. The Council must let the individual know without undue delay and within one month that it needs more information from them to confirm their identity. The Council does not need to comply with the request until such time as it has received this additional information.

## **6. The right to data portability**

- 6.1 This right allows individuals to obtain and reuse their personal data for their own purposes across different services. They can move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- 6.2 The right to data portability only applies:
- 6.2.1 to personal data an individual has provided to the Council;
  - 6.2.2 where the processing is based on the individual's consent or for the performance of a contract; and
  - 6.2.3 when processing is carried out by automated means.
- 6.3 In order to comply with the request, the Council must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data and enables other organisations to use the data. **The information must be provided by the Council free of charge.**
- 6.4 If an individual requests it, the Council may be required to transmit the data directly to another organisation if this is technically feasible. However, the Council is not required to adopt or maintain processing systems that are technically compatible with other organisations.
- 6.5 If the personal data concerns more than one individual, the Council must consider whether providing that information would prejudice the rights of any other individual.

- 6.6 The Council must respond to the request without undue delay, and within one month. This can be extended by two months where the request is complex or where the Council receives a number of requests. The Council must inform the individual within one month of the receipt of the request and explain why the extension is necessary.
- 6.7 When the Council is not taking any action in response to a request, it must explain why to the individual, informing them of their right to complain to the Information Commissioner's Office and to apply to a court without undue delay and at the latest within one month.

## **7. The right to object**

- 7.1 Individuals have the right to object to:
- 7.1.1 processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority [including profiling];
  - 7.1.2 direct marketing [including profiling]; and
  - 7.1.3 processing for purposes of scientific/historical research and statistics.
- 7.2 With regard to the first of the above criteria, an individual must have an objection on "grounds relating to his or her particular situation" and the Council must stop processing the personal data unless:
- 7.2.1 it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedom of the individual; or
  - 7.2.2 the processing is for the establishment, exercise or defence of legal claims.
- 7.3 As far as direct marketing is concerned, the Council must stop processing personal data for these purposes as soon as it receives an objection. There are no exemptions or grounds to refuse. The Council must deal with an objection to processing for direct marketing at any time and free of charge.
- 7.4 Finally, individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.
- 7.5 If the Council is conducting research where the processing of personal data is necessary for the performance of a public interest task, the Council is not required to comply with an objection to the processing.
- 7.6 If any three of the above processing activities are carried out by the Council online, then the Council must offer a way for individuals to object online.

## **8. The right not to be subject to automated decision making including profiling**

8.1 The GDPR contains provisions on:

- 8.1.1 automated individual decision-making [making a decision solely by automated means without any human involvement at all]; and
- 8.1.2 profiling [automated processing of personal data to evaluate certain things about an individual].

8.2 Examples of automated decision-making include:

- 8.2.1 an online decision to award a loan; and
- 8.2.2 a recruitment aptitude test which uses pre-programmed algorithms and criteria.

8.3 The Council is required to identify whether any of its decision making is automated and if so to:

- 8.3.1 give individuals information about the processing;
- 8.3.1 introduce simple ways for them to request human intervention or challenge a decision;
- 8.3.2 carry out regular checks to make sure that the Council's ICT systems are working as intended.

8.4 Automated individual decision-making does not have to involve profiling, although it often will do. The GDPR says that profiling is:

*"Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation health, personal preferences, interests, reliability, behaviour, location or movements."*

8.5 The GDPR restricts the Council from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals. Therefore, the Council is only able to carry out automated decision-making if the decision is:

- 8.5.1 necessary for entering into or performance of a contract between the Council and the individual;
- 8.5.2 authorised by law [for example, for the purposes of fraud or tax evasion]; or
- 8.5.3 based on the individual's explicit consent.

8.6 Because this type of processing is considered to be high-risk, the GDPR requires the Council to carry out a Data Protection Impact Assessment for the purpose of demonstrating that it has identified and assessed what those risks are and how the Council will address them.

8.7 The GDPR also requires the Council to:

8.7.1 give individuals specific information about the processing;

8.7.2 take steps to prevent errors, bias and discrimination; and

8.7.3 give individuals rights to challenge and request a review of the decision.