Individuals Rights Policy

1.0 Introduction

The United Kingdom General Data Protection Regulation (UK GDPR) forms part of the data protection laws in the UK, together with the Data Protection Act 2018 (DPA 2018).

This policy is based on the information published by the Information Commissioner's Office (ICO) www.ico.org.uk/ .

2.0 Data Subjects Right of Access

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why we are using their data, and provide assurance that we are doing so lawfully.

Individual's entitlement

Individuals have the right to obtain the following from us:

- confirmation that we are processing their personal data;
- a copy of their personal data; and
- other supplementary information – this largely corresponds to the information that we provide in our privacy notice.

Personal data of the individual

An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone).

Therefore, it is important that we establish whether the information requested falls within the definition of personal data.

Other information

On request in addition to a copy of their personal data held, we also are required to provide individuals with the following information:

- the purposes of our processing;
- the categories of personal data concerned;
- the recipients or categories of recipient we disclose the personal data to;

- our retention period for storing the personal data or, where this is not possible, our criteria for determining how long we will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and

3.0 Recognising a request?

As the UK GDPR does not specify how to make a valid request an individual can make a subject access request to us verbally or in writing.

It can also be made to any part of our organisation and does not have to be to a specific person or contact point.

A request does not have to include the phrase 'subject access request' or Article 15 of the UK GDPR, as long as it is clear that the individual is asking for their own personal data.

This means any of our employees could receive a valid request.

However, we have a legal responsibility to identify that an individual has made a request to us and handle it accordingly. Therefore we will identify which of our staff who regularly interact with individuals will need specific training to deal with such a request.

We will check with the individual making the request that we have understood their request, as this can help avoid later disputes about how we have interpreted the request. We will keep a log of verbal requests.

UK GDPR recommends that we ‘provide a means for requests to be made electronically, especially where personal data are processed by electronic means’.

A Subject Access Request Form (SARF) that individuals can complete is made available via our website.

Even though we have a form, it should be noted that a subject access request is valid if it is submitted by any means, so we will comply with any valid requests we receive by either a letter, email or verbally.

Although we may encourage individuals to use a form, we will make it clear that it is not compulsory and will not try to use this as a way of extending the one month time limit for responding.

It is the ICO view that a subject access request relates to the data held at the time the request was received.

In many cases, routine use of the data may result in it being amended or even deleted while we are dealing with the request. So it would be reasonable for us to supply information we hold when we send out a response, even if this is different to that held when we received the request.

However, it is not acceptable to amend or delete the data if we would not otherwise have done so. Under the DPA 2018, it is an offence to make any amendment with the intention of preventing its disclosure.

4.0 Explaining the contents of the information we send to the individual?

The information we provide to an individual will be in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

This means that any additional information we provide in response to a request will be capable of being understood by the average person. However, we are not required to ensure that that the information is provided in a form that can be understood by the particular individual making the request.

5.0 Charging a fee

In most cases we will not charge a fee to comply with a subject access request.

However, where the request is manifestly unfounded or excessive we may charge a “reasonable fee” for the administrative costs of complying with the request.

We may also charge a reasonable fee if an individual requests further copies of their data following a request.

We will base the fee on the administrative costs of providing further copies and will be notified to the person making the data request.

6.0 Responding to a request?

We will act on the subject access request without undue delay and at the latest within one month of receipt.

We will calculate the time limit from the day after we receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

If the corresponding date falls on a weekend or a public holiday, we will have until the next working day to respond.

This means that the exact number of days we have to comply with a request varies, depending on the month in which the request was made.

For practical purposes, if a consistent number of days is required (e.g. for operational or system purposes), we will adopt a 28-day period to ensure compliance is always within a calendar month.

7.0 Extending the time for responding

We may extend the time to respond by a further two months if the request is complex or we have received a number of requests from the individual. We will let the individual know within one month of receiving their request and explain why the extension is necessary.

We will not extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- we are requesting proof of identity before considering the request.

8.0 Asking an individual to confirm their identity?

Should we have doubts about the identity of the person making the request we may ask for more information. We will only request information that is necessary to confirm who the person is. The key to this is proportionality.

We will let the individual know as soon as possible that we need more information from them to confirm their identity before responding to their request.

The period for responding to the request begins when we receive the additional information.

9.0 Dealing with requests for large amounts of personal data

Should we need to process a large amount of information about an individual we may ask them for more information to clarify their request. We will only ask for information that we reasonably need to find the personal data covered by the request.

We will let the individual know as soon as possible that we need more information from them before responding to their request.

The period for responding to the request begins when we receive the additional information. However, if an individual refuses to provide any additional information, we will still endeavour to comply with their request i.e. by making reasonable searches for the information covered by the request. However without full disclosure we may not be able to provide all of the data requested.

10.0 Requests made on behalf of others?

An individual may make a subject access request via a third party.

The third party may for example be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In

those cases, we will need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement.

This might be a written authority to make the request or it might be a more general power of attorney.

In any case we must be satisfied with the authority given before we can comply with the request.

11.0 Dealing with requests for information about children

Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a subject access request for information held about a child, we will consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then we will usually respond directly to the child. We may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

Note: What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so.

When considering borderline cases, we will take into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information.

This is particularly important if there have been allegations of abuse or ill treatment;

- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

In Scotland, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. This

presumption does not apply in England and Wales or in Northern Ireland, where competence is assessed depending upon the level of understanding of the child, but it does indicate an approach that will be reasonable in many cases.

12.0 Data which includes information about other people?

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual.

We are not required to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, we will take into account all of the relevant circumstances, including:

- the type of information that we would disclose;
- any duty of confidentiality we owe to the other individual;
- any steps we have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

So, although we may sometimes be able to disclose information relating to a third party, we will decide whether it is appropriate to do so in each case.

That decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to us disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, we will decide whether to disclose the information anyway.

For the avoidance of doubt, we cannot refuse to provide access to personal data about an individual simply because we obtained that data from a third party. The rules about third party data apply only to personal data which includes both information about the individual who is the subject of the request and information about someone else.

13.0 Data controller responsibility for dealing with requests

As a data controller, we are solely responsible for complying with and responding to a subject access request.

14.0 Refusing to comply with a request?

We may refuse to comply with a subject access request where we deem it to be manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If we consider that a request is manifestly unfounded or excessive we can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case we will justify our decision to the individual making the request.

15.0 Our decision to charge a fee to deal with the request

We will base the reasonable fee on the administrative costs of complying with the request. If we decide to charge a fee we will contact the individual promptly and inform them. We will not comply with the request until we have received the fee.

16.0 Refusal to comply with a request?

Where we believe the request is manifestly unfounded or excessive and we refuse to comply with the request we will inform the individual without undue delay and within one month of receipt of the request.

We will inform the individual about:

- the reasons we are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

We will also provide this information if we request a reasonable fee or need additional information to identify the individual.

17.0 Requests for large amounts of personal data

If we have to process a large amount of information about an individual we may ask them for more information to clarify their request. We will only ask for information that we reasonably need to find the personal data covered by the request.

We will let the individual know as soon as possible that we need more information from them before responding to their request. The period for responding to the request will begin when we receive the additional information.

Where an individual refuses to provide any additional information, we will endeavour to comply with their request i.e. by making reasonable searches for the information covered by the request, however in this case we may not be able to provide the personal data requested.

18.0 Requests made on behalf of others

The GDPR does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them.

In those cases, we will need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it will be the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

If we think an individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, we may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

In that case it will be necessary for us to be assured of the identity of both the individual and the person acting on their behalf.