A guide on the rights of individuals

Data Protection Team

Version Control Sheet

Title:	A guide to the rights of individuals
Purpose:	To advise individuals of the procedures and principles to follow to comply with the current Data Protection legislation
Author:	Rachael Steel – Data Protection
Approved by:	Lee Henley – Data Protection Officer
Date:	September 2018
Version Number:	1.0
Status:	Final
Review Frequency:	As and when changes to Data Protection legislation take place
Next review date:	As and when changes to Data Protection legislation take place

Amendment History / Change Record

Date	Version	Key Changes / Sections Amended	Amended By

Contents Page

Data Protection - A guide on the rights of individuals

Introduction

This guide outlines your individual rights under the current Data Protection legislation.

Data protection legislation applies to personal information relating to living, identifiable individuals. This can be automatically processed information held on our computer systems, as well as information in our structured manual records, such as paper files. The legislation also applies to CCTV recordings and audio tapes.

Personal information – known as personal data in the legislation – is when an individual can be identified from the information held. Examples of personal information are:

- name and address
- National Insurance number
- bank account number
- a photograph or electronic image

The legislation **does not** apply to personal information relating to the deceased, companies or organisations. It also does not apply to statistical, de-personalised or anonymised information.

Why you have these rights

Data protection rights help you to make sure the personal information we are processing about you is:

- factually correct
- only available to those who should have it
- only used for specific purposes

Your rights

You have a range of rights when we collect your personal information. These are summarised below and each one is explained in this guide:

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. rights in relation to automated decision making and profiling

Where to send requests

Any requests relating to the individual rights set out in this guide can be sent to: Dpa@brentwood.gov.uk

1. The right to be informed

The right to be informed is an obligation we must comply with to demonstrate 'fair processing' of an individual's information.

What we mean by 'processing'
Processing can be any action taken with the information that is held, from the moment it is recorded to the date it is destroyed, including logging, tracking, emailing, making phone calls and printing.

To be fair to the individual, we must demonstrate that we are acting fairly and only using your data in the way we have said we will and that we are keeping it secure.

Information we should supply to you to demonstrate 'fair processing'
Data protection legislation sets out the information we should supply and when individuals should be informed. The information we provide to individuals is determined by whether or not we obtained the personal data directly from individuals from the outset.

The details below summarise the information we should supply to individuals – known in the legislation as the 'Data Subject' – the person who is the subject of the data.

Regardless of whether the data was obtained directly from the individual or from another source the individual must be informed of:

- the identity and contact details of the controller – the council – and, where applicable, the controller's representative – a supplier or partner – and the data protection officer (DPO) – for the purpose of the legislation.
- the purpose of the processing – what we need to do with the data – and the legal basis for the processing – that is, what we are legally permitted to do with the data
- who we will share the data with – this could be internal department, partners or agencies we are working with
- if we transfer the data to another country and the safeguards in place in that country
- the retention period or criteria used to determine the retention period – that is, how long we will keep the data for and how we determined the timeframe
- the rights the individual has under the legislation
- the right to withdraw, at any time, consent for processing
- the right to lodge a complaint with a supervisory authority – the Information Commissioner's Office
- the existence of automated decision making – where there is no human intervention at any stage – including profiling and information about how decisions are made, the significance and the consequences of those decisions

If the data has not been collected from the data subject directly – for example, it was provided by a third person or made in a referral – then in addition to the above we must also advise the individual of the categories of personal data that have been collected and where the personal data came from, including whether it came from publicly accessible sources.

If the personal data collected is required for the performance of a contract, a statutory requirement or a statutory obligation, we must advise the individual of any possible

consequences of failing to provide the personal data – an example of a contract might be applying for a council property or to receive a blue badge.

If the data has been collected directly from the individual, the individual must be informed of all of the above at the time the data is collected.

If the data has not been collected directly from the individual we must inform the individual of the above in a reasonable period of time – 1 month.

If the data is used to communicate with the individual then the above points must be notified to the individual at the first communication.

If the data is going to be shared in any way the individual must be notified of the above points before the sharing takes place.

2. The right of access

Information you're entitled to ask for under data protection legislation
You can ask us for a copy of all the personal information we hold that relates to you. This could be from our computer systems or in paper files. Individuals have the right to obtain:

- confirmation that their data is being processed
- access to their personal data

The right of access is also known as a 'subject access request'

How to ask for access to your personal information held by us
When you make this request we will ask that you:

- use our application form or ask for the information in writing, including via email
- provide one form of photo identification (ID)

These measures will help us to verify that we are providing the information to the correct person and not someone trying to impersonate you.

It will also help us if you:

- can provide sufficient details that will help us identify you and find your information – for example, a customer account number, any previous address or your date of birth

- are clear about which information you are looking for, as this will help us respond to you quickly

How long will it take to process your request
We will respond to you within 1 month of receiving your application, ID and any additional details we need to find your information.

We can extend this period by a further 2 months where requests are complex or numerous. If we need to do this, we will inform you within 1 month of receiving your request and explain why the extension is necessary.

When fees can be charged for dealing with a subject access request

We must provide you with one copy of the information free of charge.

Requests that are manifestly unfounded or excessive
Where we process a large quantity of information about an individual, we may ask the individual to be more specific about the information to which the request relates.

Where requests are manifestly unfounded or excessive, in particular because they are repeated, we can either:

- charge a reasonable fee, taking into account the administrative costs of providing the information
- refuse to respond

Where we refuse to respond to a request, we will explain our reasons to you, informing you of your right to complain to the relevant bodies within 1 month.

How the information will be provided
If your request is made electronically, we will provide the information in a commonly used electronic format. If you require the information to be printed, we will arrange this for you. A single copy will be provided free of charge, but any additional copies requested will incur a reasonable fee to cover the cost of producing them.

When your request for access to your personal information will be refused
Your request for copies of information held by us will be refused if:

- your request is not received in writing
- you are unable to provide an acceptable form of ID
- your request is identical to a recent request to which we have already responded
- your request is considered to be manifestly unfounded or excessive

When copies of your information will not be provided – non-disclosure
There are certain circumstances when we will not be able to provide you with copies of your personal information that we hold. Our decision not to disclose your personal information will always be in line with the appropriate Data Protection legislation. Below are some examples of where information would not be disclosed by us.

Example 1 – Any confidential references provided by us to a third party will not be released to an individual if we receive a request for information. This is due to the fact that the reference was provided in confidence.

Example 2 – If we are processing information relating to a council restructure that may result in redundancies or other changes to employment terms, this information would not be released during the restructure as the situation may change. At the point the re-structure is completed, the information would be disclosed if an enquiry were to be received.

Example 3 – We would not disclose any social service or health-related records to an individual if we felt that provision of this information would cause serious harm to the physical or mental health or condition of the individual or requestor. This decision would be made by a qualified social worker for social care records, and by a health professional for any health-related records.

3. The right to rectification

When personal data should be rectified
Individuals are entitled to have personal data rectified – changed – if it is inaccurate or incomplete.

If you have any concerns that we are holding information about you that is not factually correct, you can ask us to change or amend our records. In such a case, you should write to us and tell us what you believe is wrong with the personal information and what should be done to correct it.

If we have shared the personal information in question with third parties, we will inform them of the change where possible. We will also advise you which third parties the data has been shared with, where appropriate.

At the point we are notified of a request for rectification:

- we will mark our systems and records as being "in dispute" until we have completed our enquiries to establish if the requested change is valid or not
- we will consider the concerns you have raised and may contact you for clarification or further discussions
- if we are processing inaccurate information, this will be amended as soon as possible, in no more than 1 month – this may be extended by a further 2 months where the request for rectification is complex
- if we do not accept that the information held is incorrect, you will be notified of this decision within 1 month and we will inform you why we are not taking action in response to your request – at this point we will also explain to you the steps that are open to you should you wish to exercise your right to complain about our decision

4. The right to erasure

The right to erasure is also commonly referred to as 'the right to be forgotten'. The principle underpinning this right is to enable you to request the deletion or removal of personal data when there is no compelling reason for us to have it or use it

When the right to erasure applies
The right to erasure does not provide an absolute 'right to be forgotten'. Individuals do have a right to have personal data erased and to prevent processing:

- where the personal data is no longer necessary in relation to the purpose for which we originally collected and processed it
- if the processing was based on consent and the individual withdraws their consent
- when the individual objects to the processing and there is no overriding legitimate interest for us to continue using the personal data
- the personal data was unlawfully processed – that is, in breach of the legislation
- the personal data has to be erased in order to comply with a legal obligation

- the personal data is processed in relation to the offer of information society services to a child – that is, online businesses, apps or social networking sites aimed at children

There are some specific circumstances, however, where the right to erasure does not apply and we can refuse to deal with requests.

When we can refuse to comply with a request for erasure
We can refuse to comply with a request for erasure where the personal data is processed either:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest
- for archiving purposes in the public interest, scientific research historical research or statistical purposes
- for the exercise or defence of legal claims

How the right to erasure applies to children's personal data
There are extra requirements when the request for erasure relates to children's personal data.

When we process the personal data of children, we will pay special attention to situations where a child has given consent to processing and they later request for it to be deleted – regardless of age at the time of the request – especially on social networking sites and internet forums.

This is because a child may not have been fully aware of the risks involved in the processing when they first gave consent.

Time within which we must comply with data erasure requests
Upon receipt of a request for erasure, we will respond as soon as possible and within 1 month.

This can be extended by 2 months where the request is complex or if we receive a number of requests. If this is the case, we will inform the individual within 1 month of the receipt of the request and explain why the extension is necessary.

Telling other organisations about the erasure of personal data
If we have disclosed an individual's personal data to any third parties, we will inform those third parties when erasure of the personal data is requested, unless it is impossible or involves disproportionate effort to do so.

5. The right to restrict processing

When the right to restrict processing applies

Individuals have a right to block or stop us processing their personal data. When processing is restricted, we are permitted to store personal data but not to process it further.

We will be required to restrict the processing of personal data:

- where an individual challenges the accuracy of the personal data – in this case we will restrict the processing until we have verified the accuracy of the personal data
- where an individual has objected to the processing – where it was necessary for the performance of a public interest task or purpose of legitimate interests – and we are considering whether legitimate grounds for processing override the rights of the individual
- if we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim

If we have disclosed the personal data to third parties, we will inform them about the request to restrict processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

We must inform individuals when we decide to lift a restriction on processing.

Time within which we must comply with restriction of processing requests
Upon receipt of a request to restrict processing, we will respond as soon as possible and within 1 month.

6. The right to data portability

The right to data portability allows individuals:

- to obtain the personal data held by us and reuse it for their own purposes across different services or organisations
- to move, copy or transfer personal data easily from one it environment to another, in a safe and secure way without hindrance to usability
- to take advantage of applications and services that can use data to find them a better deal, or help them understand their spending habits

Example of data portability
Data portability is regularly used across the banking industry by providing personal current account customers access to their transactional data for their accounts, which they can upload to a third-party price comparison website to compare and identify best value. A price comparison website displays alternative current account providers based on their own calculations.

When the right to data portability applies
The right to data portability only applies:

- to personal data an individual has provided to a controller – in this case, the council

- where the processing is based on the individual's consent or for the performance of a contract – for example, a rental agreement or license application
- when processing is carried out by automated means

How we will comply with data portability requests
When responding to a data portability request, we must provide the personal data in a structured, commonly used and machine-readable form – for example, open formats such as CSV files. Machine-readable means the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information must be provided by us free of charge.

If the individual requests it, we may be required to transmit the data directly to another organisation, if this is technically possible. We are not required to adopt or maintain processing systems that are technically compatible with other organisations, however.

If the personal data concerns more than one individual, we must consider whether providing the information would prejudice the rights of any other individual.

Time within which we must comply with data portability requests
We will respond without undue delay to data portability requests, and within 1 month.

This can be extended by 2 months where the request is complex or if we receive a number of requests. If this is the case, we will inform the individual within 1 month of the receipt of the request and explain why the extension is necessary.

Where we are unable to process the request, we will explain why to the individual, informing them of their right to complain to the Information Commissioners Office and to a judicial remedy without undue delay. We will do this within 1 month.

7. The right to object

When the right to object applies
Individuals have the right to object to:

- processing based on our legitimate interests or the performance of a task in the public interest, or the exercise of official authority, including profiling
- direct marketing, including profiling
- processing for purposes of scientific or historical research and statistics

Processing personal data for the performance of a legal task or legitimate interests
Individuals must have an objection based on "grounds relating to their particular situation".

In these situations we must stop processing the personal data unless either:

- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- the processing is for the establishment, exercise or defence of legal claims

We must inform individuals of their right to object "at the point of first communication" and in our privacy notice.

This must be "explicitly brought to the attention of the data subject / individual and shall be presented clearly and separately from any other information".

Processing personal data for direct marketing purposes
We must:

- stop processing personal data for direct marketing purposes as soon as we receive an objection – there are no exemptions or grounds to refuse
- deal with an objection to processing for direct marketing at any time and free of charge
- inform individuals of their right to object "at the point of first communication" and in our privacy notice

About direct marketing
Direct marketing is the communication – by whatever means – of any advertising or marketing material that is directed to particular individuals.

Direct marketing includes:

- post addressed to you as an individual, promoting particular views or campaigns
- post addressed to you as an individual, promoting the selling of goods and products
- phone calls, emails and text messages to you as an individual, with the aim of selling goods and products

Direct marketing is known by many as 'junk mail'. Junk mail must be addressed to an individual, however, for it to be considered as direct marketing material. This means that leaflets, takeaway menus and 'To the Occupier' letters are not considered to be direct marketing.

How to stop direct marketing
Individuals have a right to tell us to stop using their personal information for direct marketing purposes. If you ask us to stop using your personal details for 'direct marketing purposes', then this is a legally binding demand to stop – or not to begin in the first place.

At the point you tell us to stop using your personal information in this way, we must stop within a reasonable time period – this is 1 month for email and text communications, and about 2 months for letters sent to you by post.

If you are considering telling any organisation to stop sending direct marketing communications to you:

- make sure you inform the organisation in writing – this can be an email, and you should retain a copy so you have proof of sending it
- make sure you explain that you're asking the organisation to stop – or not to begin – using your personal data for direct marketing purposes

- if your notice is ignored, you can enforce your rights by making a complaint to the Information Commissioner's Office

- if you receive direct marketing mail addressed to a previous occupier, you can still force the sender to stop sending this to you – this is because organisations have a legal responsibility to make sure that any personal data it processes relating to individuals is accurate and, where necessary, kept up to date

Marketing by telephone

Telephone marketing is also regarded as a form of electronic marketing.

Marketing which is undertaken in this way, or is sent by other electronic means – fax, email or text message – is subject to additional rules set out in the Privacy and Electronic Communications (EC Directive) Regulations 103 (PECR).

Organisations can make marketing calls to numbers not registered with Telephone Preference Service (TPS) if it is fair to do so. They must not call any number, however, that is registered with the Telephone Preference Service (TPS) unless the individual has specifically consented that they do not object to receiving their calls.

The TPS is a central register where you can register not to receive marketing calls. Once your number has been registered, it will become effective in 28 days. It's free to register and you can arrange this by phoning 0345 070 0707.

Organisations must not make a marketing call to a number they obtained for a different purpose. If they want to do so they must obtain the consent of the individual.

Organisations must not make marketing calls to you if you have advised them that you don't want to receive these calls. This is known as the right to opt-out.

Organisations must not make it difficult for you to opt-out by asking for forms to be completed. The calls must stop as soon as you have said that you don't want to receive the calls.

Organisations can only make automated or pre-recorded marketing calls – calls that play a recorded message – to you, if you have given prior consent to receiving these automated calls from them.

Marketing by email and text

Organisations can only send marketing texts or emails to you if you have agreed to this.

Organisations must not send marketing texts or emails to you if you have confirmed that you don't want to receive them. If an organisation continues to do so, this will result in the organisation not complying with the rules set out in the Privacy and Electronic Communications (EC Directive) Regulations 103.

Processing personal data for research purposes

Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.

If we are conducting research where the processing of personal data is necessary for the performance of a public interest task – for example, for public health or safety purposes – we are not required to comply with an objection to the processing.

Online processing of the activities above
If our processing activities fall into any of the above categories and are carried out online, we must offer a way for individuals to object online

8. Rights related to automated decision making and profiling

You have a right to make sure important decisions taken by us based on your personal information have had some form of human input and must not be automatically generated by a computer, unless you agree to this. This right is in place to make sure potentially damaging decisions are not taken without some form of human intervention.

When the right applies
Individuals have the right **not to be subject to a decision** when:

- it is based on purely automated processing – no human input
- it produces a legal effect or a similarly significant effect on the individual – for example, in assessing entitlement to social benefit payments by using an automated online form or when calculating an entitlement to social housing and their position on the waiting list

We must make sure that individuals are able to:

- obtain human intervention
- express their point of view
- obtain an explanation of the decision and challenge it

Automated decisions
The right does not apply to all automated decisions. It does not apply if the decision is:

- necessary for entering into or performance of a contract between us and the individual
- authorised by law – for example, for the purposes of fraud or tax evasion prevention
- based on consent

Furthermore, the right does not apply when a decision does not have a legal or similarly significant effect on someone.

Example of when the right does not apply
We were concerned that an individual who had undertaken electrical checks in our offices was charging us for works not completed. They invoiced us £3,000 for works carried out over 3 days.

Before starting the work, the individual was provided with a security pass that allowed them to access our offices. Each time they accessed an office, the individual would have to insert their security pass into the card reader. This automatically generated a record on our secure door entry log system, showing the date and time of access.

Prior to paying the invoice of £3,000 – or £1,000 per day – a report was taken from the door entry system and checked by the team manager responsible for paying the invoice. This report showed an entry for only 1 of the 3 days. It was therefore our view that the individual had only been in the offices for 1 of the 3 days and £2,000 was deducted from their invoice.

It is accepted that the decision had a significant effect on the individual as £2,000 was deducted from their invoice, but the right to object to the decision being taken by automated means would not apply because although the data collected to arrive at this decision was from an automated system, it was reviewed by a team manager resulting in some form of human input.

Profiling
Data protection legislation defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual – in particular to analyse or predict:

- their performance at work
- their economic situation
- their health
- their personal preferences
- their reliability
- their behaviour
- their location
- their movements

When processing personal data for profiling purposes, we must make sure appropriate safeguards are in place. We must:

- make sure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the potential consequences

- use appropriate mathematical or statistical procedures for the profiling

- implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors

- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects

Automated decisions taken for the purposes of processing 'special categories' of data **must not** concern a child, **nor be processed** unless either:

- we have the explicit consent of the individual

- the processing is necessary for reasons of substantial public interest on the basis of EU or member state law – this must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual

Special categories of data
The 'special categories' of data are:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- data concerning health, or sex life and sexual orientation
- genetic data
- biometric data where processed in order to identify a person