The Federated Schools of the Upper Afan Valley

Data Protection Policy and GDPR Guidance

Policy Adopted:	***21st May 2018***	
Review Cycle:	***3 Years***	
Signed: M. Goodridge. *(Chair of Governors)*		
Review Dates:		Signed:
		Signed:
		Signed:
		Signed:
		Signed:

DATA PROTECTION POLICY

Contents

Version 1

April 2018

1. Neath Port Talbot County Borough Council [hereinafter referred to as "the Authority"] is committed to ensuring its compliance with the requirements of the Data Protection Act 1998, General Data Protection Regulations and the forthcoming Data Protection Act 2018 ('the Legislation'). We recognise the importance of personal data to our organisation and the importance of respecting the privacy rights of individuals. This Data Protection Policy ('the Policy') sets out the principles which we will apply to our processing of personal data so that we not only safeguard one of our most valuable assets, but also process personal data in accordance with the law.

2. It is the responsibility of all our employees to assist the Authority to comply with this Policy. In order to help employees comply, we have produced a Data Protection Policy Guidance Note ('the Guidance') which explains in more detail the requirements of the Legislation. Employees must familiarise themselves with both this Policy and the Guidance and apply their provisions in relation to any processing of personal data. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to dismissal. Furthermore, serious breaches of the legislation could also result in personal criminal liability for the staff concerned.

3. In addition, a failure to comply with this Policy could expose the business to enforcement action by the Information Commissioner (which could result in restrictions being imposed on our use of personal data) or to complaints or claims for compensation from affected individuals. There may also be negative publicity as a result of any breach that is made public.

4. For the purpose of this policy:

Data	means information which – (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or

	(c) but forms part of an accessible record as defined by section 68, or (e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).
Data Controller	means … a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Processor	in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Data Subject	means an individual who is the subject of personal data.
Inaccurate Data	means information or data that is incorrect or misleading as to any matter of fact.
Personal Data	means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Processing	in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including – (a) organisation, adaptation or alteration of the

	information or data, (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or (d) alignment, combination, blocking, erasure or destruction of the information or data.
Recipient	in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.
Sensitive Personal Data	means personal data consisting of information as to - (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by

	him of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
Third Party	means any person other than – (a) the data subject, (b) the data controller, or (c) any data processor or other person authorised to process data for the data controller or processor

Data protection principles

5. The Authority will comply with the following principles in respect of any personal data which it processes as a data controller. It must be:

5.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

5.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

5.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

5.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be

processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

5.6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Basis of Processing

6 The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever the Authority process personal data:

6.1 **Consent:** the individual has given clear consent for the Authority to process their personal data for a specific purpose.

6.2 **Contract:** the processing is necessary for a contract the Authority have with the individual, or because they have asked the Authority to take specific steps before entering into a contract.

6.3 **Legal obligation:** the processing is necessary for the Authority to comply with the law (not including contractual obligations).

6.4 **Vital interests:** the processing is necessary to protect someone's life.

6.5 **Public task:** the processing is necessary for the Authority to perform a task in the public interest or for the Authority's official functions, and the task or function has a clear basis in law.

6.6 **Legitimate interests:** the processing is necessary for the Authority's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if the Authority is a public authority processing data to perform the Authority's official tasks.)

Accountability

7. The Authority must

7.1 implement appropriate technical and organisational measures that ensure and demonstrate that we comply. This may include internal data protection policies

such as staff training, internal audits of processing activities, and reviews of internal HR policies.

7.2 maintain relevant documentation on processing activities;

7.3 appoint a data protection officer;

7.4 implement measures that meet the principles of data protection by design and data protection by default. Measures could include data minimisation, pseudonymisation or transparency;

7.5 allowing individuals to monitor processing; and

7.6 creating and improve security features on an ongoing basis.

7.7 use data protection impact assessments where appropriate.

External Arrangements

8. Where the Authority passes personal data to any external organisation, officers must ensure a Data Processing Agreement is in place. Suitable Data Processing Agreement can be obtained from the Legal Services Section.

9. In addition, any external contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the Authority. Specific terms must also be included and advice should be sought from the Legal Services Section in this regard.

Information Asset Registry

10. One of the requirements of the Legislation is to maintain a record of all the processing activities that take place within the Authority. For this, we need to identify:

10.1 what personal data we process;

10.2 what is the lawful basis for processing;

10.3 how we store and keep the data secure;

10.4 who has access to it;

10.5 who we share the data with and what sharing agreements are in place;

10.6 how long we keep it for.

11. The Authority has a dedicated Information Asset Registry which must be completed for all information that is held within each of the Authority's Directorates.

Data Protection Officer

12. The Council has appointed the Head of Legal Services as the Data Protection Officer.

13. The Data Protection Officer and his officers will work in conjunction with the ICT Section and all Directorates of the Council to compliance with the Legislation

14. The role of the Data Protection Officer includes

14.1 Information and advising officers of the Authority of their data protection obligations

14.2 monitoring compliance of policies and procedures. This includes monitoring responsibility and training of staff involved in data processing.

14.3 ensuring the Information Asset Registry is an active registry that identifies all systems that hold personal data

14.4 advising on the necessity of Data Protection Impact Assessment, the manner of their implementation and data breach reporting

14.5 serve as contact point for individuals on privacy matters, including subject access requests

Additional Requirements

15. Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

16. To view the Authorities Policies in relation to Incident Reporting and Information Security please view the documents on the following link:

http://intranet.neath-porttalbot.gov.uk/default.aspx?page=9414

16 Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

17. This Policy may be amended from time to time to reflect any changes in legislation.

DATA PROTECTION POLICY

GUIDANCE NOTE

1. INTRODUCTION

1.1 This Guidance Note ('the Guidance') forms part of the Data Protection Policy and provides supplementary information to enable employees to better understand and comply with the Data Protection Policy.

1.2.1 Neath Port Talbot County Borough Council [hereinafter referred to as "the Authority"] is required to comply with the Data Protection Act 1998, General Data Protection Regulations and Data Protection Act 2018 ('the Legislation') in respect of its processing of personal data (such as information about our customers, clients/service users, employees and contractors/suppliers). It is important for all employees to familiarise themselves with both the Data Protection Policy and this Guidance so that any processing of personal data can be carried out in accordance with the Legislation.

1.2.2 The Authority should be aware that there is other legislation regulating public access to information such as the Freedom of Information Act 2000 which sometimes must be read in conjunction with the Legislation. Further advice on this may be sought from the Legal Section

1.3 The Authority must comply with its obligations under the Legislation. In order to do this the Authority must comply with the Data Protection Policy and this Guidance whenever the Authority process personal data, as well as any other data protection related policy that may be applicable to the Authority's area of work. ANY FAILURE TO COMPLY WITH THIS POLICY MAY BE A DISCIPLINARY OFFENCE WHICH COULD RESULT IN DISMISSAL. NEGLIGENT OR DELIBERATE BREACHES OF THE LEGISLATION COULD ALSO RESULT IN CRIMINAL LIABILITY FOR THE AUTHORITY PERSONALLY.

Neath Port Talbot
County Borough Council

25th May 2018

This is when the General Data Protection Regulation (GDPR) will come into force. If you handle personal data in your role, it is essential that you are aware of the requirements.

The Data Protection Act

Although GDPR does broaden the requirements, particularly in relation to demonstrating accountability and transparency, many of the key principles are the same as those in the Data Protection Act 1998.

Throughout this guide, you will see this icon (inset). It will highlight handy tips that must be taken seriously and actions put in place.

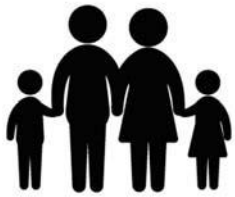
INDEX

Key Aspect 1 – Useful Definitions

Here are some key words (with definitions) that will be used throughout this practical guide:

Data Subjects

The data we collect and hold sometimes consists of details relating to a living individual (data subject). These are our citizens and they rely on us to keep their data safe.



Personal Data

This relates to a set of information that can identify a data subject or data subjects. As well as obvious personal identifiers in the data such as name and address, under GDPR this includes such things as genetic and biometric data.

Sensitive Personal Data

This relates to data which reveals an individual's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health or sex life.

The presumption is that, because information about these matters could be used in a discriminatory way and is likely to be of a private nature, sensitive personal data needs to be treated with greater care than other personal data.

Data Controller

This is the body which determines the purposes for which personal/sensitive data is processed. The Council as a whole is classed as a data controller so for our vast majority of our processing, Neath Port Talbot County Borough Council is the named data controller.

Key Aspect 2 – The Six GDPR Principles

As data controller, we must be accountable and keep records evidencing our compliance with the following GDPR principles. Such record keeping would include the logging of any new system onto our Information Asset Register.

1. Lawfulness, fairness and transparency

Personal data can only be processed if there is a lawful reason for doing so. It must be fair to the data subject and you must be fully transparent with the data subject as to why you are collecting their data and how it is going to be used and shared.

2. Purpose Limitation

Data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, although further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is permitted in certain circumstances.

3. Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

4. Accuracy

Personal data must be accurate and, where necessary, kept up to date. Where personal data is inaccurate every reasonable step should be taken to enable its deletion (where appropriate) or correction without delay.

5. Storage Limitation

Personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary. Such personal data can be stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in certain circumstances and subject to the implementation of the appropriate technical and organisational measures.

6. Integrity and Confidentiality

Personal data must be processed in an appropriately secure manner including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical or organisational measures.

Key Aspect 3 – Rights of the Data Subject

One of the key factors of GDPR is that data subjects are granted certain rights and protections relating to their personal data. This includes:

Collecting their Data

When we collect data from our citizens, we must *inform* them about the reasons why we are collecting it and their rights. We also have a duty to ensure the data collection is *limited* to what is necessary in relation to its purpose and we don't use it for a *different* purpose without consent or seeking legal advice beforehand.

Here are the four reasons why we are able to lawfully process personal data:

1. **Legal obligation**: the processing is necessary to comply with a legal obligation. If your service is statutory, this is the basis for you;
2. **Public task**: the processing is necessary to perform a task in the public interest or in the exercise of official authority. This is where you are empowered by law but not obliged to provide a service (e.g. council housing);
3. **Contract**: the processing is necessary as part of a stated or implied contract. This will apply where you offer paid-for or free membership schemes, such as Library membership;
4. **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose. This is the least favoured of your options because it gives increased responsibility for your data management.

So, if you collect personal data through an application form or survey for example, you must stipulate on the form "Why we are collecting this data" and "What we are going to do with the data" (privacy statement). You must also provide a link to the Council's privacy notice.

If you do not need to find out their date of birth for example when gathering the data on the form, you *must not ask for it!*

If you use this data for a different purpose without getting consent from the data subject, then you are breaking the second GDPR principle of purpose limitation.

Key Aspect 3 – Rights of the Data Subject

Objecting to use their Data

The GDPR includes the "right to object" meaning that the data subject can object to the processing of their personal data. If the objection is to direct marketing, the data subject does not need to give any reasons and staff must comply with the request.

When the data subject objects to other types of processing (i.e. not direct marketing) there are exemptions that apply. You will need to discuss this with your manager and take advice from the IGU before proceeding.

To demonstrate that you are complying with the GDPR first principle of processing personal data, that it is processed lawfully, fairly and in a transparent manner, you must maintain a record of any request made under the right to object to processing and notify the IGU of your actions.

Review existing processes to ensure that where you undertake marketing communications with citizens by email, you include an 'unsubscribe' option to allow them to object to the use of their information.

Accessing their Data

Our citizens are able to access their data via a subject access request. These requests must be handled without delay and within one month of receipt.

We must provide this information free of charge from 25th May 2018 and it is imperative that requests are taken seriously and handled efficiently.

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

We are able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Key Aspect 3 – Rights of the Data Subject

At all times, we must ensure that the data we have collected from our citizens now or in the past is accurate and up-to-date. Staff must take reasonable steps to ensure that where data is inaccurate, it is *rectified* without delay.

Just imagine your personal data being sent to the wrong address by your bank because the wrong house number was on their ICT system. How would you feel if your neighbour had opened the letter and read certain personal details about you?

Everyone is busy but staff are sometimes more concerned with completing their tasks than ensuring the data of our citizens is secure. This must change under GDPR or you are putting the Council at risk of fines and reputational damage.

Citizens have the right to contact the Information Commissioner to report where we have failed to keep their data accurate or their data has been breached. This could result in compensation to the citizen on top of the fine.

Storing Data

Citizens have the right to ensure that their data is not kept by us for longer than is necessary.

Staff must ensure *we do not hold data* any longer than required. Remember all data that we hold is open to subject access and Freedom of Information requests.

If your role consists of processing data, you are accountable for protecting this data from unauthorised or unlawful processing and against accidental loss, destruction or damage.

Staff are responsible for ensuring that all ICT devices are encrypted in case the device storing the data is lost or stolen.

Sharing Data

When Sharing Data you must ensure a Data Processing Agreement is in place and contact should be with made with the Legal Section when embarking on this

Key Aspect 3 – Rights of the Data Subject

Deleting Data

Under certain conditions, citizens can now request the erasure of their personal data. These are the conditions, one of which must be met:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed,
- where the legal basis for processing is consent, the data subject withdraws his or her consent for us to use it, or
- the personal data has passed the retention period defined in the corporate records retention schedule.

If any of our citizens' personal data has been made public via a third party then we must take reasonable steps to inform the data processors who are processing the personal data on our behalf that the data subject has requested that they want their data deleted.

The right to be forgotten only applies where the above conditions are met and there are further exemptions where we can refuse to comply with a request:

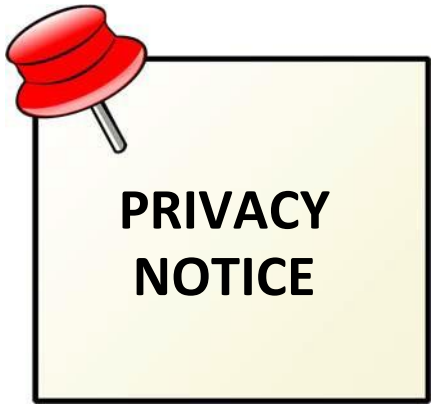
- If it conflicts with the "right of freedom and expression"
- An overriding need to adhere to legal compliance
- Reasons of public interest in the area of public health
- Scientific, historical research or public interest archiving purposes
- If the data is required for supporting legal claims.

Key Aspect 4 – Privacy Notices

Being transparent and providing accessible information to our citizens about how you will use their data is a key element of the GDPR. We must inform the data subjects at the first point of contact what to expect when we collect their personal data.

As part of our journey to GDPR compliance, we have written a new bilingual corporate privacy notice, which sits on our website.

This privacy notice must be embedded as a link in your correspondence when you are asking citizens to provide their personal data e.g. on an application or service request form.



Advice on privacy notes can be obtained from the Legal Services Section or ICT Section.

Inserting a Privacy Statement

When collecting personal data from the public (typically this is achieved through an online or a paper form), you have to provide more specific information than is contained in the overarching corporate privacy notice.

You must ensure there is a short privacy statement on the data collection document which explains your use of the data, who you share it with and what is the legal basis for your processing the data.

As mentioned in page 6 of this guide, there are four main legal reasons for the Council to be able to capture and process personal data and all data collection forms must make clear what the legal basis for processing is, if we want to be compliant with GDPR.

Key Aspect 5 – Providing Consent

We have already mentioned that consent is one of the legal reasons for processing and if we can avoid relying on consent then we should do so. Here is why:

An indication of consent must be unambiguous and involve a clear affirmative action.

If you are collecting sensitive data, the bar is set even higher. In that case you will need explicit consent, such as a written signed statement from the data subject.

I did not give my consent for you to use my personal details for this!

Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

Consent involves presenting the data subject with a clear statement regarding the personal data to be collected; and an explicit action agreeing with this statement (such as ticking a box saying 'I agree').

The form should say, "I consent" (or similar) for consent to be considered valid. *Silence or pre-ticked boxes* on webpages are banned under GDPR as they do not establish explicit consent.

Withdrawing Consent

The GDPR gives a specific right to withdraw consent. Where we are collecting data which is legally based on consent, we need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

We need to review our existing consents mechanisms to check they meet the GDPR standard. If they do, there is no need to obtain fresh consent.

It is important for staff to maintain appropriate records in order to evidence consent has been given.

Key Aspect 6 – Information Asset Registry (ISA)

Maintain a Register

One of the requirements of GDPR is to maintain a record of all the processing activities that take place within the Council. For this, we need to identify:

- what personal data we process;
- what is the lawful basis for processing;
- how we store and keep the data secure;
- who has access to it;
- who we share the data with and what sharing agreements are in place;
- how long we keep it for.

Please liaise with the Information Officers within your Directorates for access to the ISA and how to complete.

Providing an overview

The record will provide an overview of all data processing activities within our Council, and therefore enable us to demonstrate to the Information Commissioner what personal data is being processed, by whom and why.

Your responsibility

If you collect and hold personal data electronically within your service then you must identify the system on the record. You must keep this information up-to-date.

NOTE: If you have not identified your system on the record and a data breach happens within your area, the ICO will hand out far more significant fines.

Key Aspect 7 – Data Protection Impact Assessments

Assessing the Risk

Data Protection Impact Assessments (DPIA) are a method that we must introduce under GDPR for *assessing the risk* associated with the processing activity we undertake of personal data.

Whenever a new system is being designed or introduced, or an existing system is being changed via a project, staff must undertake a DPIA to determine the risk to individuals' privacy associated with the processing.

A DPIA will:

- Help the project have a clear data protection focus
- Allow appropriate organisational and technological measures to safeguard information to be built into any new operation.
- Challenge the designer to develop a way of working that will promote data protection principles
- Give practical solutions to enable a data subject to exercise their rights.

Just like the equalities impact assessments already undertaken within the Council, if you are not sure a full assessment is needed, you carry out a simple screening exercise which will guide your decision.

Data protection should not be a secondary function or consideration when designing a new processing activity. It is vital therefore, that staff, project leads and managers do not leave data protection principles and citizens' rights under GDPR to be considered at a late stage of the planning and design process.

Under GDPR, failure to carry out an impact assessment where one is necessary can lead to enforcement activity and a fine from the Information Commissioner.

Key Aspect 8 – Data Breaches

The Council has an existing process in place to detect, report and investigate a personal data breach. The Information Governance Unit are responsible for investigating and reporting all data breaches within the Council.

However, GDPR brings in a new breach notification timeframe under which we will have to notify the Information Commissioner of serious breaches within 72 hours of discovery of the breach. A failure to report a breach within the timeframe could itself result in a fine, as well as a fine for the breach itself. The fine could be up to **£17,000,000.**

These fines can be significant sums which, with the reputational loss that comes with the associated press coverage, may impact severely on the work of the Council.

Impact of a Data Breach

The first 24 hours are critical! A data breach can potentially have a range of significant adverse effects on the rights and freedoms of data subjects. The breach may cause them physical, material or non-material damage. They may as a result of the breach be at risk of domestic violence or of credit card fraud.

When a breach is identified you must report it as soon as you become aware of it in line with the Council's Policy:
http://intranet.neath-porttalbot.gov.uk/default.aspx?page=9414

Staff must respond quickly and efficiently to lower the impact of the breach.

Key Actions

When a data breach occurs, here are the *key actions* to undertake:

- if there is a high risk to the data subject from the breach(e.g. identify theft, fraud or domestic violence), they need to be told straight away so they can take actions to protect themselves;
- Containment is key. If we can retrieve the data for the unauthorised recipient, go get it straightaway;
- When retrieving the data from them, confirm that no copies of the data has been made or shared;
- Ask if they have read the whole document or just parts and if they know the person who should have initially received this information.
- Report the breach

Key Aspect 9 – Data Protection Officer (DPO)

GDPR introduces a requirement to appoint or designate a Data Protection Officer (DPO) with formal responsibility for data protection compliance across the Council. The Council's DPO is the Head of Legal Services who works with the ICT Section and all Directorates of the Council to ensure compliance with the legislation

The tasks of the DPO include:

- Informing and advising its employees of their data protection obligations,
- Monitoring compliance of policies and procedures. This includes monitoring responsibilities and training of staff involved in data processing,
- Ensuring the ISA is an active register that identifies all systems that hold personal data;
- Advising on the necessity of data protection impact assessments (DPIAs), the manner of their implementation and outcomes,
- Serve as the contact point for all data protection issues, including managing risks and data breach reporting,

Each Directorate of the Council has a designated Information Officer who has been coordinating GDPR issues in those respective Directorates:

Finance and Corporate Services And Chief Executives	Alison Forbes and Linda White
Social Services Health and Housing	Leighton Jones
Environment	Ross Williams
Education, Leisure and Lifelong Learning	Neil Place

For IT Related Advice please contact Ian John
For Legal Advice please contact Paul Watkins or Craig Griffiths

DEALING WITH REQUESTS FROM MEMBERS OF THE PUBLIC FOR ACCESS TO THEIR OWN PERSONAL INFORMATION

Introduction

1. The Data Protection Act 1998, General Data Protection Regulations and Data Protection Act 2018 ("the Legislation") provides the following rights for individuals:

    (a) The right to be informed
    (b) The right of access
    (c) The right to rectification
    (d) The right to erasure
    (e) The right to restrict processing
    (f) The right to data portability
    (g) The right to object
    (h) Rights in relation to automated decision making and profiling.

2. Requests for information can also be made on behalf of another person (where the person making the request has legal authority to do so, or where they have the consent of the subject), for example a parent on behalf of their child or a solicitor instructed by their client

3. This document sets out the guidance on the various rights the individuals have (as set out by the Information Commissioner – further detail of which can be found on the Information Commissioner Website www.ico.gov.uk) and sets out a four step process for handling requests for personal information that cannot be dealt with informally. Whilst timescales for completing each step are specified, if it is possible to handle and respond to a request in a shorter time, then we must do so.

AUTHORITY GUIDANCE ON RESPONSE

STEP 1

The request for information is received

The timescale for response begins when the request is received by the Authority, not the date it is received by the Officer responsible for dealing with it.

Notify the designated Officer and acknowledge request

A designated Officer within each Section of a Directorate should be designated to handle requests relating to that Section. This would normally be an Accountable Manager or other officer of middle management level and they must inform the Directorate's DPA/FOI Co-ordinator immediately when the request is received. A copy should be forwarded by the designated Officer to the Directorate's DPA/FOI Co-ordinator without delay and an acknowledgement letter should be sent to the requester by the Co-ordinator who will log details of the request on the database maintained by their Directorate.

If a blanket request is received e.g. for "all the information that the Authority holds on me" officers should engage with the requester and explain that in order to find the information it would be helpful for the requester to explain which Sections of the Authority they have had dealings with. The Authority does not retain a central database of all personal information.

Step 1 should be completed within 1–3 working days of receiving the request.

STEP 2

Begin compiling the information

The requested information must be retrieved and compiled as soon as practicably possible by the designated Officer.

Meet with the Head of Service or the Data Protection Officer (Head of Legal Services) or Corporate Solicitor

Where a request a made, the designated Officer will discuss the request with the Head of Service if necessary in order to decide how to respond to the request in line with the exemptions contained in the Legislation. It might be necessary to involve other officers, for example, the Corporate Solicitor or the Authority's Data

Protection Officer (Head of Legal Services) to obtain legal advice on issues arising from the request. However, it is important that any such meeting is arranged swiftly to ensure the final deadline can be met.

Step 2 must be completed within 10 calendar days of receiving the request

STEP 3

Arrange to provide the information

Following the decision as to how to deal with the request, the designated Officer will write to the requester to inform them that the information to which they are entitled to has been retrieved and confirm the method by which the information is to be provided to him/her or what steps are being taken by the Authority to deal with the request.

If the requester is agreeable, access may be made available by inspection only, however should the requester require a copy this should be supplied.

In most cases, we will ask the requester to collect the information from an Authority office. This is in the interests of security: as it is likely in many cases that the information will contain sensitive personal data that could cause significant distress or even harm if lost or misdirected.

If possible and with their agreement, a meeting can be arranged with the requester to provide an opportunity to explain the information, in order to avoid any misinterpretations, discuss queries etc., relating to the information being disclosed and/or withheld.

Step 3 must be completed within 25 calendar days of receiving the request

STEP 4

Conclude the Request

All the steps agreed to be implemented by the Authority should now be implemented and all necessary actions confirmed to the requester.

Where possible, any information should be collected by the requester or a person acting on their behalf from an Authority office or delivered in person by an Authority employee, if feasible. Before being provided with the information, the requester or their representative must show proof of identity – the need to do so will have been

made clear to them in the letter confirming arrangements for the provision of the information. In compiling information beware of accidentally including personal information about other people.

Information should not be sent via post unless approval is first given by an Accountable Manager and that method of delivery has been specifically requested by the requester. Any information that is posted must be sent via recorded delivery. A written record of delivery must be compiled in respect of any information which is hand delivered (e.g. by whom and when).

As soon as the requested has been completed the designated Officer should inform their Directorate's DPA/FOI Co-ordinator. The Co-Ordinator should be provided with a copy of the response sent to the requester (i.e. the response letter but not any copy documentation including the requested information) and the relevant details will be recorded in the Directorate's Subject Access Request database.

Step 4 must be completed within 30 calendar days of receiving the request

Administrative Practices
Separate files should be set up for each request and retained in the Directorate either by the DPA/FOI Co-ordinator or the officer dealing with requests for the Section. A processing record (see the annex attached) should be compiled and retained by the DPA/FOI Co-ordinator as a basis to provide statistical information.
The file used to process each request should be retained for two years. The file should be retained after compliance with the request by the DPA/FOI Co-ordinator.
Request figures should be notified by the DPA/FOI Co-ordinator to the central contact points in Legal Services every three months Alison Forbes a.forbes@npt.gov.uk Linda White l.white@npt.gov.uk.

The Corporate Solicitor will quality check a sample of requests and disclosures each year and the Directorate concerned will co-operate with the Corporate Solicitor and allow access to files for that purpose.

Should Officers require legal advice on any aspects of the above guidance they should contact the Authority's Corporate Solicitor by telephone on 01639-763761 or alternatively by email to p.watkins1@npt.gov.uk

RIGHTS UNDER LEGISLATION

The Right to be informed

What information is an individual entitled to under the Legislation?

Under the Legislation, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

What is the purpose of the right of access under Legislation?

The Legislation clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63).

Can I charge a fee for dealing with a subject access request?

The Authority must provide a copy of the information **free of charge**. However, the Authority can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The Authority may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that the Authority can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

How long do I have to comply?

Information must be provided without delay and at the latest within **one month of receipt**.

The Authority will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, the Authority must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

What if the request is manifestly unfounded or excessive?

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the Authority can:

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

Where the Authority refuses to respond to a request, the Authority must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

How should the information be provided?

The Authority must verify the identity of the person making the request, using 'reasonable means'.

If the request is made electronically, the Authority should provide the information in a commonly used electronic format.

The Legislation includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information. It is recognised however this is not always possible

The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

What about requests for large amounts of personal data?

Where the Authority process a large quantity of information about an individual, the Legislation permits the Authority to ask the individual to specify the information the request relates to (Recital 63).

The Legislation does not include an exemption for requests that relate to large amounts of data, but the Authority may be able to consider whether the request is manifestly unfounded or excessive.

The Right to Rectification

What is the right to rectification?

Under Article 16 of the Legislation individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

This right has close links to the accuracy principle of the Legislation (Article 5(1)(d)). However, although the Authority may have already taken steps to ensure that the personal data was accurate when the Authority obtained it; this right imposes a specific obligation to reconsider the accuracy upon request.

What do we need to do?

If the Authority receives a request for rectification the Authority should take reasonable steps to satisfy the Authority that the data is accurate and to rectify the data if necessary. The Authority should take into account the arguments and evidence provided by the data subject.

What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort the Authority should put into checking its accuracy and, if necessary, taking steps to rectify it. For example, the Authority should make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones.

The Authority may also take into account any steps the Authority have already taken to verify the accuracy of the data prior to the challenge by the data subject.

When is data inaccurate?

The Legislation does not give a definition of the term accuracy. However, the Legislation states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

What should we do about data that records a mistake?

Determining whether personal data is inaccurate can be more complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate and should be kept. In such

circumstances the fact that a mistake was made and the correct information should also be included in the individuals data.

What should we do about data that records a disputed opinion?

It is also complex if the data in question records an opinion. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified.

What should we do while we are considering the accuracy?

Under Article 18 an individual has the right to request restriction of the processing of their personal data where they contest its accuracy and the Authority are checking it. As a matter of good practice, the Authority should restrict the processing of the personal data in question whilst the Authority is verifying its accuracy, whether or not the individual has exercised their right to restriction. For more information, see our guidance on the right to restriction.

What should we do if we are satisfied that the data is accurate?

The Authority should let the individual know if the Authority is satisfied that the personal data is accurate, and tell them that the Authority will not be amending the data. The Authority should explain the Authority's decision, and inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

It is also good practice to place a note on the Authority's system indicating that the individual challenges the accuracy of the data and their reasons for doing so.

Can we refuse to comply with the request for rectification for other reasons?

The Authority can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If the Authority considers that a request is manifestly unfounded or excessive the Authority can:

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

In either case the Authority will need to justify the Authority's decision.

The Authority should base the reasonable fee on the administrative costs of complying with the request. If the Authority decides to charge a fee the Authority should contact the individual without undue delay and within one month. The Authority does not need to comply with the request until the Authority has received the fee.

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

The Authority must inform the individual without undue delay and within one month of receipt of the request about:

- the reasons the Authority 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.

The Authority should also provide this information if the Authority requests a reasonable fee or need additional information to identify the individual.

How can we recognise a request?

The Legislation does not specify how to make a valid request. Therefore, an individual can make a request for rectification verbally or in writing. It can also be made to any part of the Authority's organisation and does not have to be to a specific person or contact point.

A request to rectify personal data does not need to mention the phrase 'request for rectification' or Article 16 of the Legislation to be a valid request. As long as the individual has challenged the accuracy of their data and has asked the Authority to correct it, or has asked that the Authority take steps to complete data held about them that is incomplete, this will be a valid request under Article 16.

This presents a challenge as any of the Authority's employees could receive a valid verbal request. However, the Authority has a legal responsibility to identify that an individual has made a request to the Authority and handle it accordingly. Therefore the Authority may need to consider which of the Authority's staff who regularly interact with individuals may need specific training to identify a request.

Additionally, it is good practice to have a policy for recording details of the requests the Authority receive, particularly those made by telephone or in person. The Authority may wish to check with the requester that the Authority have understood their request, as this can help avoid later disputes about how the Authority have interpreted the request. We also recommend that the Authority keep a log of verbal requests.

Can we charge a fee?

No, in most cases the Authority cannot charge a fee to comply with a request for rectification.

However, as noted above, if the request is manifestly unfounded or excessive the Authority may charge a “reasonable fee” for the administrative costs of complying with the request.

How long do we have to comply?

The Authority must act upon the request without undue delay and at the latest within one month of receipt.

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

Can we extend the time to respond to a request?

The Authority can extend the time to respond by a further two months if the request is complex or the Authority has received a number of requests from the individual. The Authority must let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary.

The circumstances in which the Authority can extend the time to respond can include further consideration of the accuracy of disputed data - although the Authority can only do this in complex cases - and the result may be that at the end of the extended time period the Authority inform the individual that the Authority consider the data in question to be accurate.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

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

Can we ask an individual for ID?

If the Authority has doubts about the identity of the person making the request the Authority can ask for more information. However, it is important that the Authority only request information that is necessary to confirm who they are. The key to this

is proportionality. The Authority should take into account what data the Authority hold, the nature of the data, and what the Authority are using it for.

The Authority must let the individual know without undue delay and within one month that the Authority needs more information from them to confirm their identity. The Authority does not need to comply with the request until the Authority has received the additional information.

Do we have to tell other organisations if we rectify personal data?

If the Authority has disclosed the personal data to others, the Authority must contact each recipient and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, the Authority must also inform the individual about these recipients.

The Legislation defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

The Right to Erasure

What is the right to erasure?

Under Article 17 of the Legislation individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

When does the right to erasure apply?

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which the Authority originally collected or processed it for;
- the Authority are relying on consent as the Authority's lawful basis for holding the data, and the individual withdraws their consent;
- the Authority are relying on legitimate interests as the Authority's basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the Authority are processing the personal data for direct marketing purposes and the individual objects to that processing;
- the Authority have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- the Authority have to do it to comply with a legal obligation; or
- the Authority has processed the personal data to offer information society services to a child.

How does the right to erasure apply to data collected from children?

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 Legislation.

Therefore, if the Authority process data collected from children, the Authority 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. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

Do we have to tell other organisations about the erasure of personal data?

The Legislation specifies two circumstances where the Authority should tell other organisations about the erasure of personal data:

- the personal data has been disclosed to others; or
- the personal data has been made public in an online environment (for example on social networks, forums or websites).

If the Authority has disclosed the personal data to others, the Authority must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, the Authority must also inform the individuals about these recipients.

The Legislation defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Where personal data has been made public in an online environment, reasonable steps should be taken to inform other controllers who are processing the personal data to erase links to, copies or replication of that data. When deciding what steps are reasonable the Authority should take into account available technology and the cost of implementation.

When does the right to erasure not apply?

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- 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; or
- for the establishment, exercise or defence of legal claims.

The Legislation also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or

- if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).

Can we refuse to comply with a request for other reasons?

The Authority can refuse to comply with a request for erasure if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If the Authority considers that a request is manifestly unfounded or excessive the Authority can:

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

In either case the Authority will need to justify the Authority's decision.

The Authority should base the reasonable fee on the administrative costs of complying with the request. If the Authority decides to charge a fee the Authority should contact the individual promptly and inform them. The Authority does not need to comply with the request until the Authority has received the fee.

There are other proposed exemptions from the right to erasure that are contained in the Data Protection Act 2018.

Please see advice of the Corporate Solicitor or Head of Legal Services where advice is required on whether to refuse to comply with a request.

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

The Authority must inform the individual without undue delay and within one month of receipt of the request.

The Authority should inform the individual about:

- the reasons the Authority 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.

The Authority should also provide this information if the Authority requests a reasonable fee or need additional information to identify the individual.

How do we recognise a request?

The Legislation does not specify how to make a valid request. Therefore, an individual can make a request for erasure verbally or in writing. It can also be made to any part of the Authority's organisation and does not have to be to a specific person or contact point.

A request does not have to include the phrase 'request for erasure', as long as one of the conditions listed above apply.

This presents a challenge as any of the Authority's employees could receive a valid verbal request. However, the Authority has a legal responsibility to identify that an individual has made a request to the Authority and handle it accordingly. Therefore the Authority may need to consider which of the Authority's staff who regularly interact with individuals may need specific training to identify a request.

Additionally, it is good practice to have a policy for recording details of the requests the Authority receive, particularly those made by telephone or in person. The Authority may wish to check with the requester that the Authority have understood their request, as this can help avoid later disputes about how the Authority have interpreted the request. We also recommend that the Authority keep a log of verbal requests.

Can we charge a fee?

No, in most cases the Authority cannot charge a fee to comply with a request for erasure.

However, as noted above, where the request is manifestly unfounded or excessive the Authority may charge a "reasonable fee" for the administrative costs of complying with the request.

How long do we have to comply?

The Authority must act upon the request without undue delay and at the latest within one month of receipt.

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

Can we extend the time for a response?

The Authority can extend the time to respond by a further two months if the request is complex or the Authority has received a number of requests from the individual. The

Authority must let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

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

Can we ask an individual for ID?

If the Authority has doubts about the identity of the person making the request the Authority can ask for more information. However, it is important that the Authority only request information that is necessary to confirm who they are. The key to this is proportionality. The Authority should take into account what data the Authority hold, the nature of the data, and what the Authority are using it for.

The Authority must let the individual know without undue delay and within one month that the Authority needs more information from them to confirm their identity. The Authority does not need to comply with the request until the Authority has received the additional information.

Right to restrict processing

What is the right to restrict processing?

The Legislation gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information the Authority hold or how the Authority has processed their data. In most cases the Authority will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.

When does the right to restrict processing apply?

Individuals have the right to request the Authority restrict the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and the Authority are verifying the accuracy of the data;
- the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the Legislation) and the individual opposes erasure and requests restriction instead;
- the Authority no longer need the personal data but the individual needs the Authority to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to the Authority processing their data and the Authority are considering whether the Authority's legitimate grounds override those of the individual.

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:

if an individual has challenged the accuracy of their data and asked for the Authority to rectify it they also have a right to request the Authority restrict processing while the Authority consider their rectification request; or

- if an individual exercises their right to object under Article 21(1), they also have a right to request the Authority restrict processing while the Authority consider their objection request.

Therefore, as a matter of good practice the Authority should automatically restrict the processing whilst the Authority are considering its accuracy or the legitimate grounds for processing the personal data in question.

How do we restrict processing?

The Authority needs to have processes in place that enable the Authority to restrict personal data if required. It is important to note that the definition of processing includes a broad range of operations including collection, structuring, dissemination and erasure of data. Therefore, the Authority should use methods of restriction that are appropriate for the type of processing the Authority is carrying out.

The Legislation suggests a number of different methods that could be used to restrict data, such as:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website.

It is particularly important that the Authority consider how the Authority store personal data that the Authority no longer need to process but the individual has requested the Authority restrict (effectively requesting that the Authority do not erase the data).

If the Authority are using an automated filing system, the Authority need to use technical measures to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. The Authority should also note on the Authority's system that the processing of this data has been restricted.

Can we do anything with restricted data?

The Authority must not process the restricted data in any way **except to store it** unless:

- the Authority have the individual's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest.

Do we have to tell other organisations about the restriction of personal data?

Yes. If the Authority has disclosed the personal data in question to others, the Authority must contact each recipient and inform them of the restriction of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, the Authority must also inform the individual about these recipients.

The Legislation defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

When can we lift the restriction?

In many cases the restriction of processing is only temporary, specifically when the restriction is on the grounds that:

- the individual has disputed the accuracy of the personal data and the Authority are investigating this; or
- the individual has objected to the Authority processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of the Authority's legitimate interests and the Authority are considering whether the Authority's legitimate grounds override those of the individual.

Once the Authority have made a decision on the accuracy of the data, or whether the Authority's legitimate grounds override those of the individual, the Authority may decide to lift the restriction.

If the Authority does this, the Authority must inform the individual **before** the Authority lifts the restriction.

As noted above, these two conditions are linked to the right to rectification (Article 16) and the right to object (Article 21). This means that if the Authority are informing the individual that the Authority are lifting the restriction (on the grounds that the Authority are satisfied that the data is accurate, or that the Authority's legitimate grounds override theirs) the Authority should also inform them of the reasons for the Authority's refusal to act upon their rights under Articles 16 or 21. The Authority will also need to inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek a judicial remedy.

Can we refuse to comply with a request for restriction?

The Authority can refuse to comply with a request for restriction if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If the Authority considers that a request is manifestly unfounded or excessive the Authority can:

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

- refuse to deal with the request.

In either case the Authority will need to justify the Authority's decision.

The Authority should base the reasonable fee on the administrative costs of complying with the request. If the Authority decides to charge a fee the Authority should contact the individual promptly and inform them. The Authority does not need to comply with the request until the Authority has received the fee.

There are other proposed exemptions from the right to erasure that are contained in the Data Protection Act 2018.

Please see advice of the Corporate Solicitor or Head of Legal Services where advice is required on whether to refuse to comply with a request.

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

The Authority must inform the individual without undue delay and within one month of receipt of the request.

The Authority should inform the individual about:

- the reasons the Authority 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.

The Authority should also provide this information if the Authority requests a reasonable fee or need additional information to identify the individual.

How do we recognise a request?

The Legislation does not specify how to make a valid request. Therefore, an individual can make a request for restriction verbally or in writing. It can also be made to any part of the Authority's organisation and does not have to be to a specific person or contact point.

A request does not have to include the phrase 'request for restriction', as long as one of the conditions listed above apply.

This presents a challenge as any of the Authority's employees could receive a valid verbal request. However, the Authority has a legal responsibility to identify that an individual has made a request to the Authority and handle it accordingly. Therefore the Authority may need to consider which of the Authority's staff who regularly interact with individuals may need specific training to identify a request.

Additionally, it is good practice to have a policy for recording details of the requests the Authority receive, particularly those made by telephone or in person. The Authority may wish to check with the requester that the Authority have understood their request, as this can help avoid later disputes about how the Authority have interpreted the request. We also recommend that the Authority keep a log of verbal requests.

Can we charge a fee?

No, in most cases the Authority cannot charge a fee to comply with a request for restriction.

However, as noted above, where the request is manifestly unfounded or excessive the Authority may charge a "reasonable fee" for the administrative costs of complying with the request.

How long do we have to comply?

The Authority must act upon the request without undue delay and at the latest within one month of receipt.

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

Can we extend the time for a response?

The Authority can extend the time to respond by a further two months if the request is complex or the Authority has received a number of requests from the individual. The Authority must let the individual know within one month of receiving their request and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

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

Can we ask an individual for ID?

If the Authority has doubts about the identity of the person making the request the Authority can ask for more information. However, it is important that the Authority only request information that is necessary to confirm who they are. The key to this is

proportionality. The Authority should take into account what data the Authority hold, the nature of the data, and what the Authority are using it for.

The Authority must let the individual know without undue delay and within one month that the Authority needs more information from them to confirm their identity. The Authority does not need to comply with the request until the Authority has received the additional information.

Right to data portability

When does the right to data portability apply?

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

How do we comply?

The Authority 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. This enables other organisations to use the data.

The information must be provided free of charge.

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

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

How long do we have to comply?

The Authority must respond without undue delay, and within one month.

This can be extended by two months where the request is complex or the Authority receives a number of requests. The Authority must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where the Authority are not taking action in response to a request, the Authority must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Right to object

How do we comply with the right to object if we process personal data for the performance of a legal task or legitimate interests?

Individuals must have an objection on "grounds relating to his or her particular situation".

The Authority must stop processing the personal data unless:

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

The Authority must inform individuals of their right to object "at the point of first communication" and in the Authority's privacy notice.

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

How do we comply with the right to object if we process personal data for direct marketing purposes?

The Authority must stop processing personal data for direct marketing purposes as soon as the Authority receives an objection. There are no exemptions or grounds to refuse.

The Authority must deal with an objection to processing for direct marketing at any time and free of charge.

The Authority must inform individuals of their right to object "at the point of first communication" and in the Authority's privacy notice.

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

How do we comply with the right to object if we process 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 the Authority are conducting research where the processing of personal data is necessary for the performance of a public interest task, the Authority are not required to comply with an objection to the processing.

How do we comply with the right to object if my processing activities fall into any of the above categories and are carried out online?

The Authority must offer a way for individuals to object online.

Rights related to automated decision making including profiling

What is automated individual decision-making and profiling?

Automated individual decision-making is a decision made by automated means without any human involvement.

Automated individual decision-making does not have to involve profiling, although it often will do.

The Authority may obtain personal information about individuals from a variety of different sources. Internet searches, buying habits, lifestyle and behaviour data gathered from mobile phones, social networks, video surveillance systems and the Internet of Things are examples of the types of data organisations might collect.

Information is analysed to classify people into different groups or sectors, using algorithms and machine-learning. This analysis identifies links between different behaviours and characteristics to create profiles for individuals. There is more information about algorithms and machine-learning in our paper on big data, artificial intelligence, machine learning and data protection.

Based on the traits of others who appear similar, organisations use profiling to:

- find something out about individuals' preferences;
- predict their behaviour; and/or
- make decisions about them.

Automated individual decision-making and profiling can lead to quicker and more consistent decisions. But if they are used irresponsibly there are significant risks for individuals. The Legislation provisions are designed to address these risks.

What does the Legislation say about automated individual decision-making and profiling?

The Legislation restricts the Authority from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

For something to be solely automated there must be no human involvement in the decision-making process.

The restriction only covers solely automated individual decision-making that produces legal or similarly significant effects. These types of effect are not defined in the

Legislation, but the decision must have a serious negative impact on an individual to be caught by this provision.

A legal effect is something that adversely affects someone's legal rights. Similarly significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

When can we carry out this type of processing?

Solely automated individual decision-making - including profiling - with legal or similarly significant effects is restricted, although this restriction can be lifted in certain circumstances.

The Authority can **only** carry out solely automated decision-making with legal or similarly significant effects if the decision is:

- necessary for entering into or performance of a contract between an organisation and the individual;
- authorised by law (for example, for the purposes of fraud or tax evasion); or
- based on the individual's explicit consent.

If the Authority is using special category personal data the Authority can **only** carry out processing described in Article 22(1) if:

- the Authority have the individual's explicit consent; **or**
- the processing is necessary for reasons of substantial public interest.

What else do we need to consider?

Because this type of processing is considered to be high-risk the Legislation requires the Authority to carry out a Data Protection Impact Assessment (DPIA) to show that the Authority have identified and assessed what those risks are and how the Authority will address them.

As well as restricting the circumstances in which the Authority can carry out solely automated individual decision-making (as described in Article 22(1)) the Legislation also:

- requires the Authority to give individuals specific information about the processing;
- obliges the Authority to take steps to prevent errors, bias and discrimination; and
- gives individuals rights to challenge and request a review of the decision.

These provisions are designed to increase individuals' understanding of how the Authority might be using their personal data.

The Authority must:

- provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual;
- use appropriate mathematical or statistical procedures;
- ensure that individuals can:
- (a) obtain human intervention;
- (b)express their point of view; and
- (c)obtain an explanation of the decision and challenge it;
- put appropriate technical and organisational measures in place, so that the Authority can correct inaccuracies 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 that prevents discriminatory effects.

What if Article 22 doesn't apply to our processing?

Article 22 applies to solely automated individual decision-making, including profiling, with legal or similarly significant effects.

If the Authority's processing does not match this definition then the Authority can continue to carry out profiling and automated decision-making.

But the Authority must still comply with the Legislation.

The Authority must identify and record the Authority's lawful basis for the processing.

The Authority needs to have processes in place so people can exercise their rights.

Individuals have a right to object to profiling in certain circumstances. The Authority must bring details of this right specifically to their attention.