Commissioner for Ethical Standards in Public Life in Scotland

DATA PROTECTION POLICY and PROCEDURES

Date policy adopted: 01/04/2011
Review frequency: 3 years or on the advice of the Information Commissioner's Office
Date of last review: 25/05/2018
Date policy must be reviewed by: 24/05/2021

The contents of this policy have been developed with reference to the *General Data Protection Regulations*, the *Data Protection Bill* as drafted at 23 March 2018 and guidance available on the Information Commissioner's website, in particular the *Guide to the General Data Protection Regulation* available during May 2018.

CONTENTS

PART 1: Policy

1. Background

1.1 The General Data Protection Regulation and the Data Protection Act 2018 ('the GDPR') stipulate how personal data should be managed and give individuals certain rights regarding the information held about them.

1.2 The GDPR applies to processing carried out by organisations operating within the EU. It is currently anticipated that the requirements of the GDPR will be adopted by the UK after it leaves the EU.

1.3 The Information Commissioner's Office ('ICO') is responsible for upholding information rights in relation to personal data across the UK.

1.4 The Commissioner for Ethical Standards in Public Life in Scotland ('Commissioner') is a 'public authority' in terms of s7(1)(b) of the Data Protection Act 2018.

1.5 In order to carry out his functions, the Commissioner processes personal data.

1.6 This document outlines the Commissioner's policy and procedures in relation to the GDPR.

1.7 The Commissioner has separate policies relating to the requirements of the Freedom of Information (Scotland) Act 2002 and the Public Records (Scotland) Act 2011.

2. Commissioner's Statement

2.1 The Commissioner is committed to ensuring that personal data is managed safely, effectively and in line with the requirements of the GDPR.

3. Personal data

GDPR Article 4(1)

3.1 Personal data means any information relating to an identified or identifiable living individual (the 'data subject').

3.2 'Identifiable living individual' means a living individual who can be identified, directly or indirectly from the information held, in particular by reference to:

a. an identifier such as a name, an identification number, location data or an online identifier (e.g. an IP address), or
b. one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

3.3 Personal data can include addresses, telephone numbers, photographs, video and audio recordings and other personal details. It also includes any expression of opinion about a living individual or any indication of intentions about that individual.

3.4 The GDPR applies to personal data held both electronically and in paper filing systems.

3.5 Personal data that has been anonymised does not fall within the scope of the GDPR.

3.6 Personal data that has been pseudonymised can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

4. Processing personal data

GDPR Article 4

4.1 Processing means any operation performed on personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4.2 The GDPR applies to 'controllers' **and** 'processors'.

a. A controller determines the purposes and means of processing personal data. The Commissioner is a data controller.
b. A processor is responsible for processing personal data on behalf of a controller.

4.3 The Commissioner is registered with the ICO as a data controller. Details of the Commissioner's registration can be found on the ICO's website – https://ico.org.uk/esdwebpages/search.

5. Special categories of personal data

GDPR Article 9(1)

5.1 The GDPR recognises the following as special categories of personal data.

a. Data revealing:
   i. Racial or ethnic origins
   ii. Political opinions
   iii. Religious or philosophical beliefs
   iv. Membership of a trade union
b. Genetic data
c. Biometric data for the purpose of uniquely identifying a person
d. Data concerning health
e. Data concerning an individual's sex life or sexual orientation

5.2 Processing special category data is prohibited unless in one or more of the following specific circumstances.

a. The data subject has given explicit consent
b. It is necessary to meet statutory obligations in relation to employment legislation
c. To protect the vital interests of an individual where they are physically or legally incapable of giving consent
d. Processing carried out in relation to its legitimate activities by a foundation, association or not-for-profit body with a political, philosophical, religious or trade union aim and solely relates to the personal data of members, former members and those who have regular contact with the body. Data should not be disclosed outside the body without the consent of the data subjects.
e. The personal data are manifestly made public by the data subject
f. For the establishment, exercise or defence of legal claims
g. For the purpose of substantial public interest
h. For the purposes of preventative or occupational medicine
i. For reasons of public interest in the area of public health
j. For archiving purposes in the public interest

6. Criminal convictions and offences

GDPR Article 10

6.1 A lawful basis and either legal authority or official authority is required to process personal data about criminal convictions or offences.

6.2 Further guidance should be sought from the ICO when processing this form of information.

7. Data protection principles

Article 5(1)

7.1 The GDPR requires that personal data be:

a. processed fairly, **lawfully** and transparently
b. collected only for specified, explicit and legitimate purposes and **not further processed** in a manner incompatible with those purposes
c. adequate, relevant and **limited** to what is necessary
d. **accurate** and, where necessary, kept up to date, Inaccurate data should be erased or rectified without delay.
e. **not be kept** for longer than necessary
f. held **securely** and appropriate measures shall be taken against unauthorised or unlawful processing and against its accidental loss, damage or destruction.

7.2 The Commissioner is responsible for and must be able to demonstrate compliance with the principles.

8. Lawful basis

GDPR Article 6(1)

8.1 The first principle requires that the Commissioner processes all personal data lawfully, fairly and in a transparent manner. There are six lawful ways to process personal data.

8.2 **Public task:** the processing is **necessary** for a) carrying out a specific task in the public interest or b) in exercising official tasks, functions, duties or powers, and the task has a clear basis in law. This is the most common basis for the Commissioner to process personal data.

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

8.4 **Contract:** the processing is **necessary** for fulfilling a contract with an individual, or because the individual has asked for specific steps to be taken before entering into a contract.

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

8.6 **Legitimate interests:** the processing is **necessary** for the Commissioner'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 does not apply when processing data to perform official tasks. However, authorities can rely on this condition when processing requests made under the Freedom of Information (Scotland) Act 2002.

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

9. Rights of the individual

9.1 The GDPR gives individual's certain rights.

9.2 Requests made under these rights are known as information requests.

9.3 **The right to be informed**

GDPR Article 13 and 14

Individuals have the right to be informed about the collection and use of their personal data. Individuals must be informed of this right at the time their personal data is collected. The Commissioner achieves this through reference to and publication of Privacy Notices.

9.4 **The right of access**

GDPR Article 15

Under the GDPR, individuals have the right to obtain confirmation that their data is being processed, **access to their personal data** and other supplementary information (normally available through the Privacy Notice). When the individual asks for this, it is called a subject access request.

9.5 **The right to rectification**

GDPR Article 16

The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.

9.6 **The right to erasure**

GDPR Article 17

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. The right is not absolute and only applies in certain circumstances.

9.7 **The right to restrict processing**

GDPR Article 18

Individuals have the right to request the restriction or suppression of their personal data. This is an alternative to requesting the erasure of their data.

9.8 **The right to data portability**

GDPR Article 20

The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

9.9 **The right to object**

GDPR Article 21

The GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask for the processing of their personal data to stop.

9.10 **Rights in relation to automated decision making and profiling**

GDPR Article 22

The GDPR restricts the making of solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals. The Commissioner does not currently process personal data in this way.

9.11 Detailed procedures for responding to information requests are available in PART 2 of this document.

10. Accountability

GDPR Article 5(2)

10.1 The GDPR introduces a new data protection principle that says organisations are responsible for, and must be able to demonstrate, compliance with the other principles.

10.2 There are a number of measures that can, and in some cases must, be taken including:

a. adopting and implementing data protection policies
b. maintaining documentation of the Commissioner's processing activities
c. appointing a data protection officer
d. recording and, where necessary, reporting personal data breaches
e. putting written contracts in place with organisations that process personal data on the Commissioner's behalf
f. taking a 'data protection by design and default' approach
g. carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests
h. adhering to relevant codes of conduct and signing up to certification schemes
i. implementing appropriate security measures.

11. The role of the ICO

11.1 The ICO is responsible for enforcing and promoting the UK's data protection laws. The ICO:

a. investigates complaints brought to them and issues legally enforceable decisions
b. promotes good practice and offers advice to individuals and organisations
c. maintains a register of data controllers
d. investigates data breaches.

11.2 The ICO has a number of powers to enforce the GDPR and can issue penalties of up to £17,000,000 (€20M) or 4% of turnover.

12. Our roles and responsibilities

12.1 Ultimate responsibility for compliance with the GDPR lies with the Commissioner.

12.2 In order that the Commissioner can meet this responsibility, all staff members and contractors with access to personal data must be able to:

a. consider the implications of data protection to their role
b. recognise personal data
c. keep all personal data securely
d. Only disclose personal data for authorised purposes
e. Keep all personal data accurate and up to date
f. Dispose of personal data safely and in accordance with the Retention Schedule.

g. identify an information request
h. forward information requests to those staff members trained to respond
i. familiarise themselves with and follow the Commissioner's data protection policy and procedures

12.3 The Business Manager acts as the Commissioner's information officer and is responsible for:
a. recording all information requests received
b. monitoring whether responses are issued within the terms of the GDPR
c. providing advice to the Commissioner and other staff members about the GDPR and on how to respond to information requests
d. providing the Management Team with statistics on information requests and reviews, highlighting any key issues and trends and flagging any lessons to be learned
e. maintaining their knowledge of GDPR and data protection best practice
f. maintaining this policy and other guidance
g. assisting the Data Protection Officer in their duties, including the reporting of personal data breaches.

12.4 The Business Officer assists the Business Manager with these duties and provides cover for annual leave, etc.

12.5 Data protection matters will be reviewed at meetings of the Management Team.

12.6 Line managers will identify whether the staff members for whom they are responsible have sufficient knowledge of data protection and the Commissioner's procedures. Knowledge in this area will be examined during the staff member's annual appraisal and any specific training requirements identified. Issues arising during the year will be referred to the Business Manager who will arrange ad hoc training as necessary

12.7 Staff members concerned about handling personal data should contact their line manager without delay.

12.8 Any misuse of personal data by employees will be treated extremely seriously and may constitute a disciplinary offence under the disciplinary policy.

13. Training arrangements

13.1 The Commissioner will:
a. provide training to ensure that all staff members have sufficient knowledge of the data protection
b. ensure that staff members with responsibility for responding to information requests have undertaken appropriate training to ensure that responses meet statutory requirements
c. provide appropriate training for staff members responsible for providing advice and guidance
d. ensure that training is refreshed on a regular basis

13.2 Arrangements will be flexible, allowing for ad-hoc training when necessary.

14. Identifying information requests

14.1 The Commissioner must respond to information requests within one month. Therefore, it is important that all information requests are identified promptly.

14.2 Postal requests or those sent to general inboxes will be captured by the Casework Co-ordinators. In addition, the Commissioner operates a dedicated Information Requests email inbox (InfoRequest@ethicalstandards.org.uk). Emails to this address are forwarded to the main 'investigations' mailbox and to the Business Manager and Business Officer.

14.3 Staff members should be aware that they may receive information requests directly to their own mailbox. These still constitute valid requests and must be answered within one month of the email arriving in the inbox.

14.4 Staff members should arrange for a colleague to check their email inbox if they are absent for any length of time in case any requests have been sent directly to them. This should be done even where an out of office alert has been activated –a request is still considered as received by the authority even if an out of office alert has been sent back to the requester.

The following section outlines procedures to be used when implementing key elements of the above policy. These procedures will normally be undertaken by the information officers or the Data Protection Officer (DPO).

PART 2: Procedures

At the time of drafting these procedures the GDPR had not come into effect and the Data Protection Act 2018 had not been passed. As such, guidance in some areas was preliminary or not available. Once in operation case law and other precedents and good practice will further clarify the data protection regime.

Therefore, the following procedures should always be supplemented by reviewing the guidance available on the ICO's website, in particular the Guide to the General Data Protection Regulations.

15. Documenting our processing activities

15.1 The Commissioner must be able to show that he has identified what personal data is held, how it is processed and properly considered which lawful basis applies to each processing activity.

15.2 The Commissioner achieves this through audits of the personal data held ('data audits').

15.3 The Commissioner maintains a File Plan and Retention Schedule. This sets out the folder structure and retention periods for all data held by the Commissioner. This spreadsheet acts as a template for the data audit.

15.4 A copy of the spreadsheet is prepared for each of the three functions, those being office, appointments and standards. For each electronic folder, record managers identify and record:

a. A brief description of the content of the folder
b. Confirmation whether it contains personal data
c. A brief description of that data
d. Confirmation whether it contains special category personal data
e. A brief description of that data
f. Who it comes from
g. What it is used for
h. Who it is sent to
i. How long it is kept
j. What risks are associated with processing the personal data
k. How those risks are mitigated
l. What further actions are required
m. The lawful basis for processing
n. The secondary lawful basis if processing special category personal data

15.5 Current data audits are available here: O:\Records Management\Critical Documents\Data Protection\Data Audits

15.6 These records will be updated if the Commissioner begins to process new types of personal data or the purpose for processing data changes.

16. Informing people - Privacy Notices

16.1 Individuals have the right to be informed about the collection and use of their personal data and their rights in relation to the data held.

16.2 Individuals must be provided with 'privacy information' as outlined in the table below. This is done through a Privacy Notice.

What information do we need to provide?	Personal data collected from individuals	Personal data obtained from other sources
The name and contact details of your organisation	✓	✓
The name and contact details of your representative	✓	✓
The contact details of your data protection officer	✓	✓
The purposes of the processing	✓	✓
The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained	✘	✓
The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third countries or international organisations	✓	✓
The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data	✘	✓
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓	✘
The details of the existence of automated decision-making, including profiling	✓	✓

16.3 Privacy information must be provided to individuals at the time their personal data is collected. The Commissioner achieves this by publishing Privacy Notices on his website and making reference to Privacy Notices in forms, acknowledgements and email signatures.

16.4 Privacy information must be concise, transparent, intelligible, easily accessible and use clear and plain language.

16.5 Privacy information should be reviewed regularly and updated where necessary.

16.6 The Commissioner has developed two Privacy Notices.

a. Current, former and prospective employees - http://www.ethicalstandards.org.uk/publications/publication/848/privacy-statement-for-employees-etc
b. People using the Commissioner's services - http://www.ethicalstandards.org.uk/privacy-policy/

17. Responding to information requests

17.1 The GDPR gives individuals certain rights. Requests made under these rights are known as information requests.

17.2 This section outlines the procedures to be used when responding to requests made under each right.

17.3 General procedures to be used when responding to any request are set out at the end of this section.

17.4 The following procedures should always be supplemented by reviewing the guidance available on the ICO's website, in particular the Guide to the General Data Protection Regulations.

17.5 The right of access

17.5.1 Under the GDPR, individuals 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).

17.5.2 Individuals request their personal information by making a 'subject access request'.

17.5.3 The GDPR does not prevent an individual making a subject access request via a third party. In these cases, the Commissioner must be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

17.5.4 There are additional reasons why information may be withheld. For example, Schedule 2 section 7 of the DPA 2018 allows personal data gathered in the pursuance of certain of our regulatory functions to be withheld.

17.6 The right to rectification

17.6.1 The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete. Personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

17.6.2 As a matter of good practice, the processing of the personal data in question should be restricted whilst its accuracy is verified.

17.6.3 When a request for rectification is received, reasonable steps should be taken to ensure that the data is accurate and to rectify the data if necessary.

17.6.4 Determining whether personal data is inaccurate can be 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.

17.6.5 If, following investigation, the data is to be corrected or completed, then the requester should be informed of the fact and given details of how and when the amendment will be carried out.

17.6.6 If the investigation concludes that the personal data is accurate and/or complete, the individual must be informed that the data will not be amended. An explanation for the decision along with details of their right to further remedy should be given.

17.7 The right to erasure

17.7.1 The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. The right is not absolute and only applies in certain circumstances.

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

a. the personal data is no longer necessary for the purpose for which it was originally collected or processed
b. the individual withdraws their consent, where consent is the lawful basis for holding the data
c. the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing, where 'legitimate interests' is the lawful basis for processing
d. the personal data is processed for direct marketing purposes and the individual objects to that processing
e. the personal data has been processed unlawfully
f. a legal obligation requires the erasure or
g. the personal data has been processed to offer information society services to a child.

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

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

17.8 The right to restrict processing

17.8.1 Individuals have the right to request the restriction or suppression of their personal data. This is an alternative to requesting the erasure of their data.

17.8.2 This is not an absolute right and only applies in certain circumstances.

17.8.3 Individuals have the right to request restriction of the processing of their personal data in the following circumstances:

a. the individual contests the accuracy of their personal data and the accuracy of the data is currently being verified (right to rectification)
b. the data has been unlawfully processed and the individual opposes erasure and requests restriction instead
c. the personal data is no longer needed but the individual needs it kept in order to establish, exercise or defend a legal claim or
d. the individual has objected to the data processing (right to object), and the Commissioner is considering whether your legitimate grounds override those of the individual.

17.9 The right to data portability

17.9.1 The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

17.9.2 The right to data portability only applies when:

a. the lawful basis for processing this information is consent **or** for the performance of a contract; and
b. the processing is carried out by automated means (ie excluding paper files).

17.9.3 Currently, the Commissioner holds only a limited volume of data under these two conditions, for example the PAA allocation database. The information is held in MS Excel spreadsheets, MS Access databases and Sage.

17.10 The right to object

17.10.1 The GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask for the processing of their personal data to stop.

17.10.2 It is good practice to suspend processing when such a request is received.

17.10.3 Individuals have the right to object to the processing of their personal data if it is for direct marketing purposes. This is an absolute right and there are no exemptions or grounds for refusal.

17.10.4 Individuals can also object if the processing is for:
a. a task carried out in the public interest
b. the exercise of official authority vested in the controller or
c. the controller's legitimate interests (or those of a third party).

17.10.5 In these circumstances the right to object is not absolute. An individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation.

17.11 Rights in relation to automated decision making and profiling

17.11.1 The GDPR restricts the making of solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

17.11.2 The Commissioner does not currently undertake this form of processing.

17.12 Responding to requests made under these rights

17.12.1 *Identifying a rights request*
The GDPR does not specify how individuals should make requests. Therefore, requests could be made verbally or in writing and will not necessarily refer to the GDPR, data protection or these rights. A response must be issued without delay and with one month.

17.12.2 *Acknowledging a rights request*
An acknowledgement should be issued to the requester within three working days of receipt of the request. This should confirm that their request is being processed under the terms of the GDPR, inform them of the statutory response time and, where necessary, confirm how the requester wishes to receive any information that may be supplied to them, e.g. by post or email; on paper or, if electronically, in what format.

17.12.3 *Recording the rights request*
Any 'rights' requests should be recorded in the Information Request database. This database allows the request, timeframe and result to be recorded. This allows us to monitor activity in this area, allocate resources and ensure that responses are issued in a timely manner.

17.12.4 Clarifying the rights request

a. It may be necessary to clarify the request, particularly if the request has been made verbally. This should be done in writing, normally by email. Checking that a request is understood can help avoid later disputes about how the request was interpreted. The request for clarification should be issued as soon as possible, normally within three working days. The formal time limit for responding begins when the additional information is received. The rights request will be suspended until clarification is received.

b. However, if an individual refuses to provide any additional information, a reasonable attempt at a response should be undertaken.

17.12.5 Verifying the requester's identity

a. The requester's identity should be verified before the request is actioned, in particular when releasing personal data to the individual.

b. It is important that only enough information to confirm the individual's identity is requested. The Commissioner does not wish to obtain, process and store more personal data than is necessary. The key to this is proportionality. Take into account what data is held, the nature of the data, and its purpose. An appropriate combination of evidence should be obtained and should match the information we hold. Be cautious not to reveal personal data when asking for verification.

c. The request for verification should be issued as soon as possible, normally within three working days. The formal time limit for responding begins when the additional information is received. The requester should also be informed of their right to further remedy (see section below). The rights request will be suspended until clarification is received.

17.12.6 Charging fees

a. The GDPR does not allow fees to be charged for providing, amending, erasing, restricting or transferring personal data under these rights.

b. However, if the request is manifestly unfounded, excessive or repetitive in nature, a "reasonable fee" may be charged for the administrative costs of complying with the request.

c. The individual should be contacted without undue delay and within one month with details of the fee, the reasons for charging it and methods of payment. They should also be informed of their right to further remedy (see section below). The rights request will be suspended until the fee is received.

17.12.7 Responding in good time

a. Information must be provided without delay and at the latest within one month of receipt of the request or the receipt of any clarification or ID verification required.

b. The time limit begins from the day after the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month (e.g. request received on 3rd September, must comply by 4th October).

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

d. If the corresponding date falls on a weekend or a public holiday, responses should be issued on the next working day.

17.12.8 Extending the time period

The time period may be extended by a further two months where requests are complex or numerous. If this is the case, the individual must be informed without undue delay and within one month of receiving their request, explaining why the extension is necessary.

17.12.9 Which dataset does the request apply to?

a. A subject access request relates to the data held at the time the request was received. However, in many cases, routine use of the data may result in it being amended or even deleted whilst dealing with the request. In that case, it is reasonable to supply the information held when issuing a response, even if this is different to that held when the request was received.

b. However, it is not acceptable to amend or delete the data if this would not otherwise have occurred. It is an offence to make any amendment with the intention of preventing its disclosure.

17.12.10 Formats for providing the information

The Commissioner will normally provide any information requested in a commonly used electronic format. However, the format and method should be agreed with the requester at an early stage of the process, i.e. the acknowledgement, clarification or verification stage.

17.12.11 Refusing to respond

a. When a request is manifestly unfounded, excessive or repetitive in nature, the Commissioner can charge a reasonable fee (see above) or refuse to respond.

b. If refusing to respond, the individual should be contacted without undue delay and within one month with the reasons for refusal. They should also be informed of their right to further remedy (see section below).

c. There are other proposed exemptions from the rights contained in the draft DP Bill. Once the DP Bill is finalised, ICO will update their guidance accordingly, and provide further detail on the application of these exemptions.

17.12.12 Informing other organisations

a. If the personal data has been disclosed to others, each recipient must be contacted and informed of the rectification, completion, erasure, restriction or transfer of the personal data (as appropriate) - unless this proves impossible or involves disproportionate effort. If asked to, the individual must also be informed about these recipients.

b. 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 available technology and the cost of implementation should be taken into account.

17.12.13 Further remedies

a. There are a number of occasions when a requester should be informed about their right to further redress. Primarily, this occurs when responding to a request in particular when it has been refused, but there are other instances as noted above.

b. The individual must be informed without undue delay and within one month of receipt of the request, about: the reasons for the refusal or other action; their right to make a complaint to the ICO; and their ability to seek to enforce this right through a judicial remedy.

17.12.14 Further information is available in the ICO's Guide to the General Data Protection Regulations available at www.ico.org.uk.

18. Data Protection Officer

18.1 The GDPR introduces a duty for public authorities to appoint a data protection officer (DPO).

18.2 The DPO's tasks are:

a. to inform and advise the organisation about its obligations under the GDPR and other data protection laws
b. to monitor compliance with the GDPR and other data protection laws, and with our data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits
c. to advise on, and to monitor, data protection impact assessments
d. to cooperate with the ICO and
e. to be the first point of contact for the ICO and for individuals whose data is processed.

18.3 The Commissioner has entered an agreement with the Scottish Parliamentary Corporate Body for the provision of DPO services. Details of the service are available here:

..\..\..\Critical Documents\Records Management\SPCB - CESPLS MoU DPO Services May 2018 SIGNED.pdf

18.4 The GDPR requires that the DPO's contact details are published and provided to the ICO.

19. Personal data breaches

19.1 The GDPR introduces a duty on all organisations to report certain types of personal data breach to the ICO. This must be done within 72 hours of becoming aware of the breach, where feasible.

19.2 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

19.3 This includes breaches that are the result of both accidental and deliberate causes.

19.4 When a personal data breach has occurred, both the likelihood and the severity of the resulting risk to people's rights and freedoms must be established.

19.5 On becoming aware of a breach

a. Make all reasonable attempts to contain it. For example, contact IT Support to contain a virus or retrieve documents from backup.
b. Notify your line manager, the Business Manager or the Commissioner as appropriate. They will review the situation and advise. The next step may be to contact the Data Protection Officer who will advise how to proceed.
c. Identify what the risks to the individual's rights and freedoms might be. It's important to focus on the potential negative consequences for individuals.
d. Assess the likelihood of the risks occurring. If it's likely that a risk will occur, then the ICO must be notified of the breach; if it's unlikely to occur then the breach does not have to be reported. In any event, the breach and the reasons for reporting or not reporting to the ICO should be documented.
e. Finally, assess the likelihood and impact of the risk occurring. If this is assessed as 'high' then those concerned directly should be informed without undue delay.

19.6 A notifiable breach should be reported to the ICO without undue delay and not later than 72 hours after becoming aware of it. If it takes longer than this, reasons for the delay must be given.

19.7 A controller is considered to have become "aware" when they have a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

19.8 It is for the DPO to report a breach (see 18.3 above). Breaches are reported by calling the ICO's helpline, 0303 123 1113. Normal opening hours are Monday to Friday between 9am and 5pm. However, lines are closed after 1pm on Wednesdays for staff training. The ICO will record the breach and offer advice about what to do next.

19.9 Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of global turnover. The fine can be combined with the ICO's other corrective powers.

20. Contracts with suppliers

20.1 Whenever a processor is used (a third party who processes personal data on behalf of the Commissioner) there needs to be a written contract in place.

20.2 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 controller.

20.3 Contracts must also include as a minimum the following terms, requiring the processor to:

a. only act on the written instructions of the controller
b. ensure that people processing the data are subject to a duty of confidence
c. take appropriate measures to ensure the security of processing
d. only engage sub-processors with the prior consent of the controller and under a written contract
e. assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR
f. assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
g. delete or return all personal data to the controller as requested at the end of the contract and
h. submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

21. Data protection by design and default

21.1 Under the GDPR, there is a general obligation to implement technical and organisational measures to show that data protection has been considered and integrated into any processing activities.

21.2 The ICO has published guidance on privacy by design. They are working to update this guidance to reflect the provisions of the GDPR. In the meantime, the existing guidance is a good starting point for organisations.

22. Data protection impact assessments

22.1 The GDPR introduces a new obligation to carry out a Data Protection Impact Assessment (DPIA) before processing that is likely to result in a high risk to individuals' interests.

22.2 If a DPIA identifies a high risk that cannot be mitigated, the ICO must be consulted.

22.3 A DPIA must be completed before beginning any type of processing which is "likely to result in a high risk". In particular, the GDPR requires a DPIA if planning to:

a. use systematic and extensive profiling with significant effects
b. process special category or criminal offence data on a large scale or
c. systematically monitor publicly accessible places on a large scale.

22.4 The ICO also requires a DPIA if planning to:

a. use new technologies
b. use profiling or special category data to decide on access to services
c. profile individuals on a large scale
d. process biometric data
e. process genetic data
f. match data or combine datasets from different sources
g. collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')
h. track individuals' location or behaviour
i. profile children or target marketing or online services at them or
j. process data that might endanger the individual's physical health or safety in the event of a security breach.

22.5 Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data.

23. Codes of Conduct and Certification

23.1 The GDPR endorses the use of approved codes of conduct and certification mechanisms to demonstrate that controllers and processors comply.

23.2 No such schemes are currently in operation.

24. Security

24.1 Personal data must be processed securely.

24.2 Every aspect of the processing of personal data should be considered, not just cybersecurity.

24.3 The ICO will take into account the technical and organisational measures in place when considering an administrative fine.

24.4 Any security measures should seek to ensure:

a. Confidentiality - the data can be accessed, altered, disclosed or deleted only by those authorised to do so and only within the scope of the authority given to them
b. Integrity - the data should be accurate and complete
c. Availability - the data remains accessible and usable, that is, if personal data is accidentally lost, altered or destroyed, it should be recoverable in a timely manner.
d. Resilience - systems can continue operating under adverse conditions, such as those that may result from a physical or technical incident and they can be restored to an effective state in a timely manner.

24.5 The following procedures should be followed:

24.5.1 *Paper records (work in progress)*

a. All personal information in the form of paper records should be kept securely in a lockable location.
b. Paper records should not be left unattended when personal data is being processed.
c. The Commissioner operates a clear desk policy to reduce the risk of unauthorised access to and loss of or damage to personal data outside normal working hours.
d. When paper records containing personal data are no longer required, they should be disposed of securely either by shredding or via confidential waste.

24.5.2 *Electronic records*

a. To avoid unauthorised disclosure, care must be taken to site monitors so that they are not visible to unauthorised people.
b. Screens should not be left unattended when personal data is being processed.
c. All staff must employ a password-protected automatic screen-saver.

d. Where personal data is held or sent electronically, the risk of unauthorised access should be assessed and the information password protected as necessary.

24.5.3 *Home and offsite working*

a. Particular care must be taken with any data handled offsite, for example paper records used at home or electronic data on portable devices or home PCs.
b. Where personal data is processed offsite this Data Protection Policy will apply.
c. Staff should ensure that all work is kept confidential and, in the case of electronic data, that files are not exposed to infection from viruses, etc.
d. Staff should ensure that all equipment which may contain personal data, e.g. laptops or smart phones, is kept secure at all times and is not exposed to the risk of theft.
e. Staff should ensure that no information is stored on the hard drive of their laptops, either those provided by the Commissioner or if using their own.

24.5.4 *Telephone*

Personal information should not be given over the telephone unless the identity of the requester has been confirmed.

24.5.5 *Post and courier*

The following guidance should be followed when sending personal information by post:

a. Confirm the name, department/organisation (if appropriate) and address of the recipient
b. Seal the information in a robust envelope
c. Mark the envelope "Private and Confidential"
d. When necessary, ask the recipient to confirm receipt

24.5.6 *Storage, Retention and Disposal*

All paper and electronic records should be stored in accordance with the Commissioner's Records Management Plan.

24.5.7 *Security breaches and data loss*

Employees should report any concerns about security breaches or data loss to their Line Manager and the Business Manager as soon as they become aware of the issue.

25. International Transfers

25.1 The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

25.2 The Commissioner does not currently transfer personal data outside the EU.

26. Exemptions

26.1 Member States can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard.

26.2 Please refer to the ICO's website for the latest guidance.

27. Children

27.1 Children need particular protection when collecting and processing their personal data because they may be less aware of the risks involved.

27.2 Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

27.3 The Commissioner does not normally process the personal data of children. However, there may be instances where a child makes a complaint, requests information or where we receive information about children as part of our other activities.

27.4 Please refer to ICO's guidance when dealing with information about children.

28. The data protection fee

28.1 There is a new charging structure for data controllers to ensure the continued funding of the ICO.

28.2 There are three different tiers of fee and controllers are expected to pay between £40 and £2,900.

a. Tier 1 – micro organisations. Maximum turnover of £632,000 in the financial year or no more than 10 members of staff. The fee for tier 1 is £40.
b. Tier 2 – small and medium organisations. Maximum turnover of £36 million in the financial year or no more than 250 members of staff. The fee for tier 2 is £60.
c. Tier 3 – large organisations. If not meeting the criteria for tier 1 or tier 2, the fee is £2,900.

28.3 Public authorities should categorise themselves according to staff numbers only. They do not need to take turnover into account.

28.4 The ICO regards all controllers as eligible to pay a fee in tier 3 unless and until informed otherwise.

28.5 If a registration (or notification) under the 1998 Act is currently held, the new data protection fee is not payable until the registration expires. The ICO will write before this happens with a reminder that the registration is about to expire and to explain what to do next.