Equality and Human Rights Commission

Data protection policy

Equality and Human Rights Commission

Contents

Part 1: Introduction

The UK Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR) regulates the processing of information relating to individuals – personal data, special categories of data and data relating to criminal convictions or offenses.

Personal data is any information related to a natural person (normally called data subjects) that can be used to directly or indirectly identify the person. This can include reference to any identifiers such as an ID number, location data or an online identifier such as an IP address.

Special categories of data include information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sex life or sexual orientation, or genetic or biometric data used to uniquely identify an individual.

Data relating to alleged or actual criminal convictions or offenses is another category of data which must be handled with care.

During the course of its activities the Equality and Human Rights Commission (the Commission) will obtain, hold, use and disclose personal data about its stakeholders, clients, suppliers, staff, Commissioners, committee members and other third parties. The Commission recognises that the correct and lawful processing of this data is important. This policy sets out how the Commission will process all types of personal information to enable it to perform its functions in line with legal requirements.

This data protection policy is based on the requirements of the GDPR and the Data Protection Act 2018.

1.1 Responsibilities

The Audit and Risk Assurance Committee (ARAC) will provide oversight of data protection risk assessment and assurance on behalf of the Board.

The Executive Group is the senior management team that will approve data protection documentation/processes and is accountable to the Board for data protection compliance and assurance.

The Senior Information Risk Owner (SIRO) is the executive director accountable to the Executive Group and the Board for information risk.

The Information Governance Steering Group (IGSG) supports the SIRO to develop and improve the management of information governance and data protection matters at the Commission.

The data protection officer (DPO) is responsible for advising the Commission on data protection. More details about the DPO role can be found in the Accountability section of this policy. The DPO will report to the Executive Group, the Audit and Risk Assurance Committee (ARAC) and the Board.

The Data Owners are responsible for protecting information in their service areas and will ensure that personal data is collected, used, stored, shared and disposed of in line with the Commission's policies and procedures, GDPR and the Data Protection Act 2018. The Corporate Correspondence Unit will deal with all requests under the Data Protection Act 2018/GDPR received from data subjects in relation to their personal data.

All Commission staff are responsible for ensuring that:

- they comply with this policy and all related policies and procedures for handling personal data
- any personal data held in either electronic or paper format, is processed securely and in line with the requirements of the GDPR and Data Protection Act 2018
- personal information is not disclosed deliberately or accidentally, either orally or in writing, to any unauthorised third party
- any incidents or breaches are reported immediately in line with internal reporting requirements
- they promptly forward any form of personal data related requests from data subjects to the Corporate Correspondence Unit and, when asked to do so, they provide responses promptly to requests and reviews

- personal data is managed and retained in line with the corporate Records Management and Retention Policy and Procedure, and associated retention schedule
- they only process personal data for the intended purposes
- the information provided to the Commission in connection with their employment or engagement is accurate and as up-to-date as possible, and
- personal data they collect and use to perform their functions is as up-to-date as possible.

Part 2: Data protection principles

1.2 Summary of data protection principles

The GDPR covers both computerised and manual records which contain personal data, and sets out a number of rights and principles which those who use personal information, such as the Commission, must follow. The Commission and its employees must comply with the data protection principles of good practice which underpin the GDPR. These state that personal data will be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals
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
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
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. 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

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.

1.3 Fair, lawful and transparent processing

The GDPR does not intend to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the GDPR and the Data Protection Act 2018. These include, among other things:

- data subject consents to the processing
- processing is necessary for the performance of a contract with the data subject
- processing is necessary for the compliance with a legal obligation to which the data controller is subject
- legitimate interest of the data controller or the party to whom the data is disclosed
- processing is necessary for the protection of the vital interest of the data subject or of another natural person, or
- processing is for the performance of public interest task or the task of an official authority.

When special categories or criminal convictions data are being processed, additional conditions must be met. When processing this class of personal data as data controllers in the course of its business, the Commission will ensure that those requirements are met.

In the course of the Commission's work, it may collect and process personal data to enable it to:

- carry out its regulatory duties including, but not limited to, the consideration and investigation of complaints and policy issues, formal enforcement actions, providing advice and information
- maintain accounts and records

- support and manage staff, Commissioners and committee members
- send promotional communications about the services provided
- undertake research
- maintain a public register
- carry out internal and external support functions
- carry out corporate administration, and
- use CCTV systems for staff and visitor safety and crime prevention.

The Commission may process data received directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data received from other sources (including, for example, in court proceedings, or from business partners, sub-contractors and others).

Special category information, or information relating to criminal convictions or offenses, may be processed by the Commission for a number of reasons, including but not limited to:

- equal opportunity monitoring
- meeting the needs of individuals with protected characteristics
- disciplinary or grievance proceedings
- fulfilling a legal obligation, and/or
- fulfilling the Commission's role and function including for purposes of litigation.

Any personal, special categories, or criminal conviction data that the Commission holds will only be held for the purposes for which it was gathered. All Commission staff must be aware and respect their obligations in relation to the confidential nature of the information that they handle and, in particular, any duty of confidentiality that may exist.

The Commission will process personal data in line with the individual's reasonable expectations, ensuring fairness.

The Commission will ensure that individuals are informed about how their personal data will be processed and will make this information available to them. The Commission will be clear from the outset (at the point of collection)

why personal data is collected and what it intends to do with it, and will provide such notices to the relevant individuals.

1.4 Collected for specified and legitimate purpose(s)

The Commission will identify a specific purpose or purposes for data which it collects, uses, stores, discloses and shares, and will also ensure that it is not used for any other purpose(s) that is incompatible with the original purpose(s).

1.5 Adequate, relevant and limited data processing

The Commission will only collect the minimum personal data required for the specific purpose notified to the data subject. The Commission will anonymise and pseudonymise personal data whenever possible to ensure that data is further protected.

1.6 Accuracy

The Commission will ensure that personal data it holds is accurate and kept up-to-date and will check the accuracy of any personal data at regular intervals. Inaccurate or outdated personal data will be deleted or amended and all reasonable steps will be taken to maintain accurate records.

1.7 Retention

The Commission holds different types of information for different lengths of time, depending on the legal and operational requirements, and will keep some personal information longer than others in line with financial, legal or archival requirements.

The Commission will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. When personal data is no longer needed, it will be disposed of securely unless there are legal or other grounds for retaining the data.

1.8 Security of personal data

The Commission will ensure that appropriate security measures are in place to ensure personal data processed in the organisation is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Personal data will only be transferred to third parties with appropriate assurance of security and with appropriate security controls in place.

The Commission will implement and maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality:** only people who are authorised and need to access the data can access it.
- **Integrity:** personal data will be accurate and trustworthy for the purpose for which it is needed.
- **Availability:** authorised users will be able to access the data when they need it for authorised purposes.

The steps the Commission will take to ensure the security of personal data include:

- managing access to personal data on a ‘need-to-know’ basis
- putting in place policies, procedures and protocols to ensure the security of personal data
- ensuring ongoing training and awareness for staff
- obtaining security assurance of third parties and putting in place agreements to protect personal data
- where appropriate, using pseudonymisation and encryption of personal data
- maintaining ongoing review and testing of processing systems and services
- undertaking data quality checks to ensure data is accurate
- restoring access to personal data in a timely manner in the event of a physical or technical incident, and
- regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Part 3: Accountability

The Commission will maintain a comprehensive data protection management programme across the organisation and will include an internal governance structure to foster a culture of data protection across the organisation. This will include:

- an information asset register (IAR) and a record of processing activities (ROPA)
- data protection by design and by default
- undertaking data protection impact assessments (DPIA) where required
- policies and procedures including a security incident management process
- contracts with third parties, and
- appointment of a data protection officer.

The Commission will also ensure that it pays the required data protection fees to the ICO under the Data Protection Act 2018.

1.9 Information asset register and record of processing activities

An information asset register (IAR) will be maintained containing details of what information the Commission holds and how the Commission complies with the data protection principles in relation to that data. A record of processing activities (ROPA) will be maintained. The records will comprise of information relating to all data processing activities at the Commission. The ROPA will be made available to the ICO upon request.

1.10 Data protection by design and by default

The Commission will take steps to ensure that new or changed data processing activities consider data protection principles as part of the activity design process. One of these measures is through data protection impact assessments.

The Commission will ensure that the default position of activities relating to data processing is to protect the privacy and data protection rights of individuals, for example, by restricting access.

1.11 Data protection impact assessments

The Commission will carry out data protection impact assessments (DPIAs) as and when required.

DPIAs will set out the details of the data processing activity and include an assessment of the risks posed to individuals. Where risks arise, the Commission will put in place measures and safeguards to minimise these risks

1.12 Policies and procedures including security incident management

The Commission will put in place policies and procedures to ensure compliance with GDPR and the Data Protection Act 2018. This will include a security incident management process.

In the event of a personal data breach, the Commission will respond accordingly, and will notify the ICO within 72 hours of becoming aware of the breach unless it is unlikely to result in a risk to individuals. Where notification of breach is not made within 72 hours, the Commission will provide a reasonable justification for the delay. The Commission will also have due consideration as to whether it is appropriate or required to notify data subjects of the breach.

Where the Commission processes special category data or data relating to criminal convictions or offenses, it will have an appropriate policy document in place as set out in the Data Protection Act 2018.

1.13 Contracts with third parties

There will be instances where the Commission will work with third parties in relation to the processing of personal data.

When the Commission uses data processors to process personal data, the Commission will ensure an appropriate contract or data processing agreement is in place to ensure that such third parties will only process the data on documented instructions of the organisation, unless required otherwise by law. The Commission will only work with data processors that can demonstrate security appropriate to the risk associated with the type of data they will be processing. The Commission will ensure that its data processors provide information necessary to demonstrate compliance with their obligations under the GDPR.

Where the Commission works collaboratively or jointly with other organisations, the Commission will ensure that an appropriate agreement is in place to ensure data protection and security, for example, through a data sharing agreement.

1.14 Appointment of a data protection officer (DPO)

As a non-departmental public body, the Commission is required to appoint a data protection officer (DPO) to advise the organisation on its obligation under the GDPR and other data protection laws. The DPO is responsible for advising the organisation; raising awareness and training staff; monitoring compliance with data protection laws and internal data protection related policies, and related audits; the assignment of responsibilities; advising on the need for, completion of, and approach to data protection impact assessments (DPIAs); and acting as the point of contact with the Information Commissioner's Office (ICO).

When advising the Commission, the DPO will have due consideration to the risk associated with data processing activities, taking into account their nature, scope, context and purpose.

The DPO will be also be available to data subjects with regards to the Commission's processing of their data.

The Commission will provide the ICO with the name and contact details of the DPO.

Part 4: The rights of data subjects

The Commission will process all personal data in line with data subjects' rights. Data subjects include, but are not limited to, members of the public, staff (past and present), Board and committee members and others who have dealings with the Commission.

The GDPR gives certain rights to individuals in respect of personal data that the Commission holds about them. These rights are:

a) the right to be informed

b) the right of subject access

c) the right to rectification

d) the right to data erasure

e) the right to restrict processing

f) the right to data portability

g) the right to objection, and

h) rights with respect to automated decision-making and profiling.

1.15 Right to be informed

Data subjects have a right to be informed on how their data is being processed and this is normally referred to as a privacy notice.

The Commission will publish, or make available, privacy notices to data subjects in line with the right to be informed

1.16 Right of subject access

A data subject may make a subject access request (SAR) at any time to find out what personal data the Commission holds about them and obtain a copy of that data. The organisation will respond to SARs within one month of receipt but this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject will be informed of the need for the extension.

The Commission will not charge a fee for the handling of normal SARs but reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

There may be instances where the Commission applies exemptions to the release of certain data, for example, data relating to a third party, and the Commission will notify the data subject of what exemptions it has applied and any justification for it.

1.17 Right to rectification

If a data subject informs the Commission that their personal data held by the organisation is inaccurate or incomplete, requesting that it be rectified, the personal data in question will be rectified, and the data subject informed of that rectification, within one month of receipt of the data subject's notice. This can be extended by up to two months in the case of complex requests, and in such cases the data subject will be informed of the need for the extension.

In the event that any affected personal data has been disclosed to third parties, those parties will be informed of any rectification of that personal data.

This right will be complied with in so far as it applies in law to the particular circumstances of the case.

1.18 Right to data erasure

In some circumstances data subjects may request that the Commission erases the personal data it holds about them.

When such valid requests are made requests for erasure will be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. This can be extended by up to two months in the

case of complex requests, and in such cases the data subject will be informed of the need for the extension.

In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties will be informed of the erasure unless it is impossible or would require disproportionate effort to do so.

The right to erasure may not apply in situations where the Commission is legally obliged to retain the data, where it obtained the data under a legal basis other than consent or legitimate interests, or where there is another overriding reason to retain it.

1.19 Right to restrict data processing

In certain circumstances subjects may request that the Commission ceases to process personal data it holds about them.

If a data subject makes a valid request, the organisation will retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

In the event that any affected personal data has been disclosed to third parties, those parties will be informed of the applicable restrictions on processing it unless it is impossible or would require disproportionate effort to do so.

This right primarily applies in the event that a data subject has contested the accuracy or legitimacy of the processing activity, and while the accuracy or consideration is in question.

1.20 Right to data portability

If a data subject has directly provided information to the Commission, they may have a right to data portability. This allows individuals to obtain and reuse their personal data for their own purposes across different services. This right will only apply:

- 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.

All requests will be complied with within one month of the data subject's request, but this can be extended by up to two months in the case of complex or numerous requests, and in such cases the data subject will be informed of the need for the extension.

1.21 Right to objection

Data subjects have the right to object to the processing of their personal data. This right applies where data is processed for:

- direct marketing purposes
- a task carried out in the public interest
- the exercise of any official (statutory) authority, or
- the legitimate interests of the Commission.

The right to object also applies to processing for scientific or historical research, or statistical purposes, however, it is more limited.

Where a data subject objects to the processing of their personal data and it meets the conditions of the GDPR the Commission will cease such processing.

1.22 Rights in respect of automated decision-making and profiling

In the event that the Commission uses personal data for the purposes of automated decision-making or profiling and those decisions have a legal (or similarly significant) effect on data subjects, data subjects have the right to challenge such decisions under the GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the organisation. The Commission will respect these rights in so far as they apply in the circumstances.

1.23 How to make a request relating to personal data

Requests relating to personal data held by the Commission can be made by:

Email: dp@equalityhumanrights.com

or

Letter sent to the following address:

Data Protection Officer
Equality and Human Rights Commission
3rd floor Arndale House
The Arndale Centre
Manchester
M4 3AQ

If you would like to make your request verbally you can do so by calling 0161 829 8327

Requests can also be made via the sign video service.

Once the Commission receives a request it will send an acknowledgement letter to the requester. Once full details of a request have been confirmed and necessary ID provided, the Commission will provide a full response within one month, but this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject will be informed of the need for the extension.

The Commission does not need to comply with a request where it has received an identical or similar request from the same individual, unless a reasonable interval has elapsed between compliance with the original request and the current request.

1.24 Identity

The Commission must take steps to confirm the identity of the individual before responding to a request. The checks made will be reasonable and proportionate.

1.25 Complaints

If the requester is not happy with the response that they receive following any of the above, they should first complain to the Commission in writing to the Correspondence Unit at the above postal address.

If someone is unable to contact the Commission in writing and requires a reasonable adjustment because they are disabled, they may contact the Commission on 0161 829 8327 or alternatively, via the sign video service.

Complaints will be acknowledged within five working days of receipt and a response will be provided within 20 working days of receipt. Requesters who remain dissatisfied may complain to the Information Commissioner at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

The Information Commissioner will not normally deal with a complaint unless the Commission's internal complaints process has been exhausted.

Part 5: Transferring personal data outside the European Economic Area (EEA)

The Commission may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA only if:

- the transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data
- one of the following appropriate safeguards is in place:
  a) binding corporate rules
  b) standard data protection clauses adopted by the European Commission
  c) compliance with an approved code of conduct approved by the ICO
  d) certification under an approved certification, or
  e) a legally binding agreement between public authorities or bodies, or
- there is a mechanism, or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

The Commission will not transfer data outside the EEA without one of the above safeguards unless:

- The transfer is made with the informed consent of the relevant data subject(s).
- The transfer is necessary for the performance or conclusion of a contract between the data subject and the Commission, or for pre-contractual steps taken at the request of the data subject.
- The transfer is necessary for important public interest reasons.

- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent.
- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public, in general or otherwise, to those who are able to show a legitimate interest in accessing the register.

Part 6: Disclosure and sharing of personal information

The Commission sometimes needs to share information with other organisations, for example, if it is under a duty to disclose or share a data subject's personal data in order to comply with any legal or regulatory requirements to protect rights, property or safety of staff, Commissioners, committee members, stakeholders, suppliers or others (including those that it works with, advises or supports).

Where necessary or required, the Commission may also share information with:

- family, associates and representatives of the person whose personal data it is processing
- professional advisers and consultants
- service providers/suppliers
- police forces
- examining bodies
- central government
- financial organisations
- persons making an enquiry or complaint
- organisations subject to a complaint or assessment
- prosecuting authorities
- courts, and
- ombudsman or regulatory authorities.

1.26 Restrictions on disclosing certain information

Some legislation restricts disclosure of information, for example, the Gender Recognition Act 2004 and the Equality Act 2010.

Gender Recognition Act 2004

The Gender Recognition Act makes it an offence for a person who has acquired protected information in an official capacity to disclose that information to any other person. The legislation does permit disclosure in certain circumstances.

The Equality Act 2006

The Equality Act limits information that can be shared externally where the Commission has obtained it by undertaking its functions, in particular where information has been gathered in the course of an inquiry under section 16, an investigation under section 20, an assessment under section 31, an agreement under section 23 or a notice under section 32. The legislation does permit disclosure in certain circumstances.

Glossary of terms

The following definitions are used in this policy and will mean the following:

Anonymisation: the process of irreversibly de-identifying personal data so that an individual cannot be identified from the data.

Consent: freely given, specific, informed and unambiguous indication of wishes by a statement or clear affirmative action signifying agreement.

Data: information which is stored electronically, on a computer or in certain paper-based filing systems.

Data controller: the legal entity (organisation) that determines the purposes, conditions and means of the processing of personal data.

Data processor: the legal entity (or organisation) that processes data on behalf of the data controller.

Data protection officer: an expert on data protection who works independently to advise an organisation on their compliance with data protection laws.

Data subject: a living individual whose personal data is processed by a controller or processor.

Personal data: any information related to a natural person (normally called data subjects) that can be used to directly or indirectly identify the person.

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

Data protection by design: a principle that calls for data protection to be considered at the start of, and throughout, any new project including systems, services, products or processes.

Data protection by default: a principle that calls for the default position to restrict or limit processing, for example, access is set to the minimum necessary.

Data protection impact assessments: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing: any operation or set of operations performed on personal data, whether or not by automated means, including, for example, collection, use, recording, storing, disclosing and erasing.

Pseudonymisation: the processing of personal data so that it can no longer be attributed to a single data subject without the use of additional data, so long as the additional data stays separate to ensure non-attribution.

Alternative formats

For information on accessing one of our publications in an alternative format, please contact: correspondence@equalityhumanrights.com.

Changes to the policy

The Commission reserves the right to change this policy at any time. Where appropriate, it will notify the data subject.

Contacts

This publication and related equality and human rights resources are available from our website.

Questions and comments regarding this publication may be addressed to: correspondence@equalityhumanrights.com. We welcome your feedback.

For information on accessing one of our publications in an alternative format, please contact: correspondence@equalityhumanrights.com.

Keep up to date with our latest news, events and publications by signing up to our e-newsletter.

EASS

For advice, information or guidance on equality, discrimination or human rights issues, please contact the Equality Advisory and Support Service, a free and independent service.

Telephone	0808 800 0082
Textphone	0808 800 0084
Hours	09:00 to 19:00 (Monday to Friday) 10:00 to 14:00 (Saturday)
Post	FREEPOST EASS HELPLINE FPN6521

© 2018 Equality and Human Rights Commission

Published November 2018

You can download this publication from

www.equalityhumanrights.com

© 2018 Equality and Human Rights Commission

Published: November 2018

Equality and
Human Rights
Commission