CROFTING COMMISSION

DATA PROTECTION POLICY

VERSION 0.3

Last Review: 23 August 2019
Next Review: 20 September 2020

CONTENTS

Background

The General Data Protection Regulation (GDPR) came into force on 25 May 2018. Despite 'Brexit', the new Regulation will remain in place and is augmented by the Data Protection Act 2018 for the UK.

This Guidance document is designed to explain the Crofting Commission's approach to GDPR and explains the Commission's Policy on Data Protection. It will be kept under review as the changes in practice become embedded across the organisation.

Personal Data

Under Article 5 of the GDPR, personal data is any information relating to an identifiable living person who can be directly or indirectly identified, in particular by reference to an identifier.

This definition provides for a wide range of identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. It also means that if pieces of data could be put together, they could create data which identifies a person.

This applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria. When deciding whether a document contains personal data, we will take the context into account – some things are obvious but others are not, until they are put together.

What Is Data Processing?

We are processing data if it is –

a) Held electronically or manually

b) Forms part of a relevant filing system

c) Forms part of an accessible record

d) Recorded by a public authority.

GDPR Principles

GDPR is based around six principles of 'good information handling':

1. Process Lawfully, Fairly and Transparently – treating everyone the same
2. Limit the processing to a specific purpose
3. Data Minimisation – process only the data needed, not anything extra
4. Accuracy – keep information up to date
5. Storage Limitation – retain personal data for only as long as is necessary for the processing
6. Integrity and Confidentiality – keep it secure.

These principles form the core of the Regulation and give individuals rights in relation to their personal data and place obligations on organisations responsible for processing it.

Individuals' Rights

Under Data Protection law data subjects (individuals) have eight rights. Of these, six apply to the Crofting Commission:

Right to Be Informed

– Individuals have a right to be informed about how and what personal data we process. You have the right to know who we are and how to contact us; the reason why we are processing your data and our lawful basis for doing so. You have the right to know the type of personal data we are processing, who we are sharing it with, how long we are keeping it and that you have other rights relating to the use of your personal data. You must know that you can complain to us if you think we are misusing your data and we must tell you how to complain to the Information Commissioner, who oversees the GDPR and DPA (Data Protection Act 2018).

  We must also be clear to you if you are under an obligation to provide us with your personal data (meaning that you cannot object to the processing). And this information has to be provided at the first point of contact, when the data is obtained or, where the data is obtained from a third party, within a month of us having received it.

  The Commission largely complies with the 'Right to be Informed' by creating Privacy Notices for all of our various processes and also displaying a general Privacy Notice on the website, so that anyone can see our approach before they contact us. Where it is not practical to issue a Privacy Notice, we have created various amended letter templates and revised information for emails.

Right of Access (SAR)

– To personal data processed by the Commission. Subject access enables people to find out what information is held about them and who it is disclosed to. This right can be exercised by making a written subject access request (SAR).

  Subject access allows individuals to verify the accuracy of personal data and the lawfulness of the processing.

  The Commission can receive a SAR by letter or email. The identity of the requester should be verified. Generally the requests will be completed free of charge within one calendar month.

Rectification

– Correcting any inaccuracies relating to personal data.

Erasure (Right to Be Forgotten)

– Where data is no longer relevant, unlawfully processed or the individual would like to withdraw their consent; if consent is relied on.

Restriction

– For a period where data is contested or processing is unlawful. This means the data cannot be processed further and it cannot be deleted. It has the effect of 'freezing' the data.

Right to Object

– To processing (e.g. marketing). Only on rare occasions will the data subject be able to object to the Commission processing personal data obtained, if the lawful basis is 'legal obligation'.

For more information on the rights of data subjects, please see **ICO guidance**.

Lawful Basis for Processing

To comply with the first principle of GDPR, we must have a lawful basis for processing personal data. There are six available:

Legal Obligation	Consent	Contract
Vital Interest	**Public Task**	**Legitimate Interest**

It is unlikely that the Commission will ever use the 'Vital Interests' lawful basis, as this is to cover 'life or death' situations.

Of the other lawful bases, the Commission will most often rely on 'legal obligation' to process personal data. This is because we are under a legal obligation to receive the data, as we are subject to the Crofting Acts and the data subjects in regulatory, duties, grazings and registration cases are obliged to provide us with the information.

To a lesser extent, we rely on Consent (for instance, when cookies are used on the website or we wish to use photographs for the Annual Report), legitimate interests (for instance, to monitor staff internet use) and public task (for instance, to carry out our obligations under FOISA).

Processing is only lawful if we can rely on a lawful basis, as set out in Article 6 of GDPR and we must demonstrate the reason why the particular lawful basis applies to the specific piece of processing – if we cannot show this, the processing will be unlawful and the Commission will be in breach of Data Protection law. We must inform data subjects of the lawful basis for processing their data in the Privacy Notice or relevant contact correspondence. It will be up to the Chief Executive, as Accountable Officer, or the SIRO (Senior Information Risk Owner) or the IAOs (Information Asset Owners) to decide which lawful basis applies to each kind of processing carried out by the Commission.

GDPR recognises that some organisations will need to retain personal data to archive it for historical research (Article 89). This does not mean the Commission can keep everything that is old – we still have to have a lawful basis for processing any personal data but it means that, in situations where we need to retain minimal personal data to enable us to 'read' the history of the croft, it is legitimate to do so.

Special Categories of Personal Data and Criminal Convictions & Offences Data

Under Articles 9 & 10 of GDPR this personal data (as described below) is more sensitive, requiring more protection before it can be processed. Keeping this type of data could create more significant risks to a person's fundamental rights and freedoms.

- Race
- Ethnic origin
- Political affiliation
- Religion/philosophical beliefs
- Trade union membership

- Genetics
- Biometrics (where used for id purposes)
- Health
- Sex life
- Sexual orientation
- Criminal Convictions & Offences (including allegations).

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, it needs to be treated with greater care than other personal data.

If the Commission needs to process special category personal data, in order to complete a function it is obliged to complete, explicit written consent **MUST** be obtained from the data subject, before the processing is concluded. Only that personal data explicitly required should be processed. Anything additional or not required, should not be retained. It should either be returned or deleted.

Personal data relating to crime, criminal convictions or allegations of criminal activity is covered by a new Law Enforcement Directive and Article 10 of GDPR. The Commission has no authority to process personal data relating to criminal activity, unless it was itself reporting a crofter to the Procurator Fiscal for non-return of the Annual Notice and should return any correspondence received which contains such information to the sender, as it cannot be processed.

Data Controllers and Processors

- A “data controller” determines the purposes for which and the manner in which any personal data is to be processed.
- Controllers must ensure that any processing of personal data for which they are responsible complies with legislation. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals. There are further obligations on data controllers to ensure any contracts with processors comply with Data Protection law.
- A “data processor” is responsible for processing personal data on behalf of a controller.
- Data Protection law places legal obligations on processors, e.g. the requirement to maintain records of personal data and processing activities. The processor has legal liability if they are responsible for a personal data breach.
- In most of our transactions, the Commission is the Data Controller.

Data Sharing Agreements

A Data Controller may share data with another organisation or other specified parties, if this is a necessary part of the processing, which conforms to the lawful basis on which we rely. If it is essential to share the personal data in order to complete the processing, the terms under which this is managed should be set out in a data sharing agreement between the parties. The data subjects must be aware that data sharing is taking place.

Contracts

The Commission holds several contracts. Where the Commission is the data controller, we must ensure the contract has been brought up to date to comply with GDPR. Where the Commission shares a contract, we must ensure the lead party has confirmed the contract is GDPR compliant.

Retention Schedules

In order to comply with GDPR Principle 5, it is important for an organisation to agree schedules which detail how long information, including personal data, will be kept. The Commission has a series of retention schedules. These are kept under review.

Privacy Impact Assessments/Data Protection Impact Assessments

The Information Commissioner wants to see organisations embedding data protection and individual's privacy rights into its processes. One way to provide evidence that the Commission is serious about protecting the rights of data subjects is to carry out Privacy Impact Assessments or Data Protection Impact Assessments for all projects involving personal data.

These can be large or small and include:

- Any new initiatives, policies or processes
- Procurement/contracts
- New IT systems
- Forms/guidance notes

The Data Protection Officer should be informed of plans early in the development stage, so that advice can be given to mitigate any risks associated with processing personal data.

Completing a Privacy Impact Assessment will make a project more transparent and help people understand how personal data is used. It will help to identify risks and what actions can be taken to reduce those risks. It will also ensure all relevant parties have been made aware of the proposals and the risks added to the Risk Register, if necessary and authorised at the appropriate level, either by the Information Asset Owner or the SIRO.

Data Protection Officer (DPO)

A DPO is responsible for providing advice and guidance to the Crofting Commission, to help it to meet its obligations under Data Protection law.

The DPO should:

- Provide advice & guidance to the Commission and its employees on the requirements under Data Protection, including staff training
- Monitor the Commission's compliance
- Be consulted and provide advice during Data Protection Impact Assessments
- Be the point of contact for individual 'data subjects' and cooperate and consult with the Information Commissioner's Office.

DPOs are responsible for carrying out data audits and overseeing the implementation of compliance tools. The DPO must be able to act independently of senior management, as well as reporting directly to the Board, the Audit & Finance committee and the Accountable Officer to raise any concerns.

Data Breach Incidents – How to Avoid, Recognise & Report Breaches

GDPR requires the Commission to process personal data in a manner that ensures its security (Principle 6). We are required to take appropriate technical and organisational measures to protect personal data. We do this by having a robust IT policy on security, which is kept under review, by ensuring staff adhere to security measures such as the clear desk policy and by training staff on cyber security and on keeping information safe.

Direct training on GDPR has been delivered to all staff, the members of the Audit & Finance committee and the Board. This includes an explanation of what constitutes a data breach, how to avoid breaches and how to report an incident. As well as a detailed staff guidance document, the staff handbook and Induction Pack for new staff have been updated and two new online mandatory training modules developed; one specifically dealing with personal data security.

Personal data breaches can include:

- Access by an unauthorised third party (for instance, someone in an employees' household, if personal data is taken home)
- Deliberate or accidental action
- Sending information to the wrong person
- Losing information, in a paper file or a computer
- Alteration of personal data without permission
- Loss of access/availability of persona data.

There will be a data breach whenever personal data is lost, destroyed without authorisation, corrupted, disclosed unlawfully, accessed unlawfully, distributed without authorisation or if the data is made unavailable and this has a significant negative impact on the data subject.

All data breach incidents, however minor, must be reported to the DPO, who will record them in an Incident Log. When a breach has occurred and there is a significant risk to the data subject's rights and freedoms (so harm could be caused by the breach) or where the breach has a severe impact on the organisation (such as prolonged loss of access to personal data records), the DPO must inform the Information Commissioner, within 72 hours of the breach occurring. If there is a concern about harm to the individual, then they too must be informed of the breach.

Failure to notify a breach when required to do so could result in a significant fine to the organisation.

Powers of the UK Information Commissioner

The Information Commissioner's Office (ICO) can take enforcement action if they find an organisation in breach of the requirements in the Data Protection law. This could include a monetary penalty of up to 4% of global annual turnover or €20,000, 000 or an enforcement notice ordering an organisation to improve its privacy notice or stop the processing if the notice is not improved.

Individuals can complain to the ICO if they think an organisation is not handling their data correctly and the ICO can award compensation.

APPENDIX 1

Applying Exemptions under Data Protection and GDPR 2018

BACKGROUND

Under Schedule 2 of the Data Protection Act 2018, a limited number of Exemptions may be applied to the processing of personal data. Only 2 are likely to apply, under certain circumstances, to the work of the Crofting Commission.

The main data protection exemptions staff may come across relate to:

1. GDPR Article 89 and DPA 2018 Schedule 2, Part 6 (27) and (28) – processing for the purposes of archiving historical data in the public interest for research or statistical purposes. Article 89 of GDPR and section 19 of the DPA 2018 extend safeguarding conditions for citizens that must be in place before the exemption can be applied.

   Public Authorities that hold records of public interest, with a legal obligation to acquire, describe, communicate and provide access to records of enduring value in the public interest (in the case of the Commission, this will cover the Register of Crofts) have the right to process personal data for archiving purposes.

2. DPA 2018 Chapter 2, section 15(a) and (b), and Schedule 2, Part 1 section 5(3) – which is (a) information in respect of which a claim to legal professional privilege or confidentiality of communications, could be maintained in legal proceedings, or (b) information in respect of which a duty of confidentiality is owed by a professional legal adviser to a client of the advisor. This was known as the section 35 legal privilege exemption under the 1998 DPA and operates in the same way.

APPLYING AN EXEMPTION

When applying an exemption, you should be aware that:

- All of the principles of data protection/GDPR that are not explicitly contained in the exemption must be complied with.
- Everything not contained in the exemption must be fairly and lawfully processed.
- If an exemption is being applied, it must be documented.
- Extra care needs to be taken if the processing involves special category data.

THE KEY EXEMPTIONS

The exemptions to GDPR are set out in the Data Protection Act 2018. The table below shows the main exemptions that you may come across in your work. You can find more guidance on the Information Commissioners' website at www.ico.org.uk. If in doubt, please consult the Compliance Hub.

Key Exemption 1

Processing data for archiving purposes in the public interest for historical research or statistical purposes

What this means

Example: Retaining historic data after initial processing, for the purpose of 'reading' the history of the croft unit

Exempts the Commission from GDPR principles on:

- Purpose limitation – the data can be used for reasons beyond the original lawful purpose, if safeguards are followed and it is needed for historic research/statistical purposes, in the public interest.
- Retention period – if the conditions are met, no limit needs to be placed on the retention period
- Requests from data subjects, including access to and alteration of personal data and restriction of data are exempted if conditions for applying the exemption are met.

Which part of the regulations applies?

GDPR Article 89 and DPA 2018 Schedule 2, Part 6 (27) and (28)

Safeguarding Conditions

GDPR and DPA 2018 introduce extra safeguarding conditions that must be met before the exemption can be applied.

- Technical and organisational measures must be in place to ensure only the minimum amount of data is kept
- The Information Asset Owner should confirm that data minimisation measures have been applied
- Wherever possible the data to be retained for research/statistical purposes should no longer permit the identification of data subjects.

Key Exemption 2

a) Exemption for information regarding confidentiality of communications, which could be maintained in legal proceedings, or

b) Information in respect of which a duty of confidentiality is owed by a professional legal advisor to a client of the advisor

What this means

Example:

This would be used to protect lawyer-client confidentiality, such as during a Subject Access request.

Exempts controllers from GDPR principles on:

- all of the principles at Article 5 and chapter 2 of part 4 of DPA 2018 (purpose limitation, data minimisation, accuracy, storage limitation, integrity and security) except principle 1 (fair, lawful, transparent)
- All of the data subject Rights in GDPR Articles 12-22 and chapter 3 of part 4 of the DPA 2018.

APPENDIX 2

Conditions for processing special category personal data without the data subject's consent

The Crofting Commission will meet its obligations under GDPR and the DPA (2018). There may be certain unusual circumstances which may prevail when the organisation will have to rely on one of the Conditions in Schedule 1 Part 2 of the Data Protection Act 2018.

It may retain special category personal data, if relevant to an enquiry, without relying on consent, if it has evidence that its **Anti-Fraud policy** has been breached, as per Condition 10 (1) and (2) of Schedule 1 of the DPA, Part 2. The Commission's Anti-Fraud policy is reviewed annually. Any personal data processed as a result of a serious suspected breach of the policy would be retained in line with the retention period set out below.

This will be limited to circumstances where it is suspected that an unlawful act may have taken place, as per the following:

"Schedule 1 Part 2, Substantial Public Interest

Preventing or detecting unlawful acts

10(1) This condition is met if the processing –

- *a) Is necessary for the purposes of the prevention or detection of an unlawful act,*
- *b) Must be carried out without the consent of the data subject so as not to prejudice those purposes, and*
- *c) Is necessary for reasons of substantial public interest."*

Likewise, the Commission may, in cases where serious concerns are raised and evidence provided which require investigation by the proper authorities, process special category personal data without the consent of the data subject, if relevant to the investigation, in order to protect the public from **dishonesty and serious maladministration**, as set out in 11 (1) and (2) of Schedule 1, Part 2 of the DPA (2018). Again, the data would be retained only as long as was necessary to gather evidence to forward to the proper authorities for investigation.

Exceptionally, where the Commission is involved in for example a **whistleblowing investigation** in connection with dishonesty, malpractice or seriously improper conduct, it may rely on condition 12 of Schedule 1 Part 2 of the DPA 2018 if processing is necessary for reasons of substantial public interest and the controller cannot reasonably obtain the consent of the data subject.

The Commission may on occasion be asked to forward details of a case, including personal details, as a result of **requests from elected members** (MSP's and MP's) covered by Schedule 1 Part 2 section 23 of the DPA (2018). Under section 24, the special category personal data may be released to the representative if the conditions in 24 (1) (a) (b) and (c) are met. If the request to the elected representative comes from a third party, the Commission will take care that the conditions set out in section 24 (2) are met, before disclosing personal data without consent.

The retention period for MP/MSP correspondence is 5 years and for complaints of maladministration investigated by the Standards Commission, the retention period is 6 years.

To the extent that the **Commission is acting as a tribunal** in any particular case in terms of the Tribunals and Inquiries Act 1992, the publication of the Commission's decision when acting in such a capacity may process special category data if it is necessary for the purposes of publishing such a decision in terms of conditions 26 of Schedule 1 Part 2 of the DPA 2018. The majority of the Commission's functions are administrative.

Exceptionally, the Commission may process special category data in terms of condition 6 of Schedule 1 Part 2 of the DPA where the processing is necessary in order to **exercise a function conferred on the Crofting Commission by any enactment or rule of law** and it is necessary for reasons of substantial public interest. The Commission does not envisage having to call upon this condition in any but rare and exceptional cases.

This policy forms part of the Commission's GDPR Documentation log, in accordance with Article 30 and has been disseminated to the staff of the organisation.