Data Protection Policy

CROFTING COMMISSION
COIMISEAN NA CROITEARACHD

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. Please note that the GDPR is now known as the UK GDPR.

This Guidance document is designed to help staff comply with the new law and explains the Crofting Commission's Policy on Data Protection. It will be kept under review as the changes in practice become embedded across the organisation and a formal review will take place each year.

Personal Data

Under Article 5 of the UK 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, staff should take the context into account – some things are obvious, but others are not, until they are put together.

It is important to note, where personal data has been pseudonymised – e.g. key-coded to remove names– it may still fall within the scope of Data Protection law, depending on how difficult it is to attribute the pseudonym to a particular individual. However, pseudonymising or anonymising personal data is good practice, where there may be a reason to continue to hold information (as evidence of trends in crofting, for instance) but where there is no longer a lawful basis to retain individual personal data.

What Is Data Processing?

We are processing data if it is –

- Held electronically or manually
- Forms part of a relevant filing system
- Forms part of an accessible record
- Is recorded by a public authority.

UK GDPR Principles

UK 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:

1. Right to Be Informed

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

We must also be clear to data subjects if they are under an obligation to provide us with their personal data (meaning that they cannot object to the processing). And this information has to be provided at the first point of contact, when the data are obtained or, where the data are 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.

2. 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 be aware of the personal data we hold on them and also to verify its accuracy and the lawfulness of the processing. (For details on how to complete a Subject Access Request, please see Part 2)

3. 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.

4. 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.

5. 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'.

6. Lawful Basis for Processing

To comply with the first principle of GDPR, we must have a lawful basis for processing personal data. There are 7 available:

1. Legal Obligation
2. Consent
3. Contract
4. Vital Interest
5. Public Task
6. Legitimate Interest
7. Recognised Legitimate Interest

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.

CROFTING COMMISSION
COIMISEAN NA CROITEARACHD

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).

In 2025 a new lawful basis was added under the Data Use and Access Act. For information on the changes most relevant to the Commission's processing, please see the notes in Appendix 9.

Processing is only lawful if we can rely on a lawful basis, as set out in Article 6 of UK 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.

The Regulation 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 UK 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, careful consideration needs to be given to the lawful basis for processing. 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.

The Commission does not intentionally request special category personal data. If such unsolicited personal data is supplied by a data subject or a third party, the first recourse would be to process none of the data which falls under Article 9 of UK GDPR. Only by exception and with a clear lawful basis should any special category data be retained and only with authorisation from a senior manager. The advice of the Data Protection Officer should be sought, to establish the lawful basis, which in most cases will reflect Article 9 2(g).

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.

CROFTING COMMISSION
COIMISEAN NA CROITEARACHD

The Crofting Annual Notice

Is The Annual Notice Information "Personal Data"?

The data comprising the annual notice received in terms of section 40A of the Crofters (Scotland) Act 1993 is personal data within the meaning of UK GDPR in so far as an individual can be identified from the data and in so far as the data "relates" to that individual.

Where the data relates to compliance or non-compliance with statutory duties by an individual, such data is likely to be sufficiently linked and connected to the individual to constitute personal data. It is less likely that such data comprises special category personal data within the meaning of Article 9 and 10.

How Does FOISA/EIR Regulate the Release of Such Data?

In terms of section 38 of the Freedom of Information (Scotland) Act 2002 ("FOISA"), information is exempt if it constitutes personal data and satisfies the condition that the information falls within the meaning of "data" in the DPA (and now UK GDPR) and the release of the information would contravene any of the data protection principles and was likely to cause damage or distress). Any information that is exempted under one or more of the data protection principles qualifies for absolute exemption and so the public interest test need not be applied, when dealing with a FOISA/EIR request.

Processing (in this case, disclosing) of the data would have to be "fair" and "lawful". If one of these conditions is satisfied, the information can be disclosed:

- Consent – relevant only where consent has been freely given;
- Performance of a contract;
- Necessary for statutory compliance;
- Necessary to protect the vital interests of the data subject;
- Necessary for administration of justice;
- Necessary for the legitimate interests of the data controller or a third party.

The issue is whether any third-party requester has any "legitimate interest" in obtaining the information he or she is requesting. In order to assess this matter, the data controller must balance the "legitimate interests" of the requester with the interests of the data subject to keep any personal data confidential. The following factors are relevant considerations:

How private is the information? Does it relate to the data subject's home, family life or social life, financial situation? There is an interrelationship here between data protection law and human rights law, as Article 8 of the ECHR provides that every individual has the right to respect for his or her private and family life, his home and correspondence.

Would disclosure of the information cause distress or harm to the data subject? For instance, disclosure that a person is not "ordinarily resident" at a particular address could pose a security risk to the individual's property; equally, it could be argued that disclosure could lead to "harm" in the sense that it is more likely that duties action would be taken against the data subject, thereby harming the data subject's interests, but this would have to be balanced against the argument that it is not legitimate in any way to protect or conceal a failure to comply with a statutory duty.

A "legitimate interest" could be the scrutiny of the exercise of a public body's official functions and activities. The Information Commissioner has suggested that the data controller asks the following questions:

- Does the third-party requester have a legitimate interest in obtaining the information?
- If yes, is disclosure necessary for the purpose of those legitimate interests?
- If yes, would disclosure cause prejudice to the data subject's rights and freedoms, including the right to privacy and family life?

If no, is the processing fair and lawful?

If the answer to questions 1, 2 and 4 are "no" and the answer to question 3 is "yes", the information is exempt from disclosure in terms of section 38(1)(b) of FOISA. Otherwise, it is not exempt.

CROFTING COMMISSION
COIMISEAN NA CROITEARACHD

How Does This Relate to The Annual Notice Data?

The Commission could seek the consent of the data subject for the release of the personal data contained on the crofting census return. The data subject would have to be aware of the specific personal data that is being considered for release. Where there are a large number of data subjects, this option is likely to be impractical. How practical would it be to seek consent of the data subject?

It is likely that the requester has a legitimate interest, if they are a crofter, to information relating to whether other crofters in a township are complying with their statutory duties. This is because the Commission has a duty to investigate whether a breach of a statutory crofting duty has taken place at the behest of various people, including a member of the crofting community (section 26A of the Crofters (Scotland) Act 1993).

There could also be said to be a wider public interest in ensuring that the Commission carries out investigations in respect of individual crofters or owner-occupier crofters who are not complying with their duties.

If the Commission considers that there is legitimate interest, is disclosure necessary? For instance, could there be other ways that the interests of the requester could be met without releasing the personal data? The concept of proportionality is important in this respect. If the data controller could satisfy, or go some way to satisfying, these interests in a way that is less intrusive of the data subject's rights of privacy, the data controller must consider such options.

The Commission must also consider carefully harm caused to the data subject. The biggest concern could be disclosure of information as to whether an individual is ordinarily resident at a residential address, as this could lead (if the information comes into the wrong hands) to a risk of damage or theft of private property. The Commission must balance this against the fundamental purpose of the annual notice, which is to provide the Commission with information that enables it to take regulatory action – in the public interest – in respect of crofters who are not complying with their statutory duties.

For more information on the section 38 Exemption on disclosure of personal information under FOISA please see this guidance note from the Scottish Information Commissioner's office.

Data Controllers and Processors

A "data controller" determines the purposes for which and the manner in which any personal data are 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 – but not for all e.g. Croft Registration.

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 you 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. The Commission's data sharing agreements should be logged in the Information Asset Register.

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.

CROFTING COMMISSION
COIMISEAN NA CROITEARACHD

Information Management

As part of its Records Management obligations, the Commission keeps an Information Asset Register. This is used to record the location, format and types of information held. It identifies the Information Asset Owner with responsibility for the data held.

Retention Schedules

In order to comply with UK 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. For more information please contact the Records Manager.

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 (PIA) or Data Protection Impact Assessments (DPIA) 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 DPO 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 PIA or DPIA (a template can be found here) 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 and Report Breaches

CROFTING COMMISSION
COIMISEAN NA CROITEARACHD

UK 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 UK 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.

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 or 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.

Organisations are more likely to find the ICO awarding data subjects' compensation if they uphold a complaint, rather than the ICO imposing fines on the organisation. This is because UK GDPR makes it easier for individuals to take complaints to the ICO and increases the ICO's ability to instruct organisations to pay compensation.

Appendix 1

Conditions For Processing Special Category Personal Data Without The Data Subject's Consent

CROFTING COMMISSION
COIMISEAN NA CROITEARACHD

The Crofting Commission will meet its obligations under UK GDPR and the DPA (2018). There maybe 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 –

1. Is necessary for the purposes of the prevention or detection of an unlawful act,
2. Must be carried out without the consent of the data subject so as not to prejudice those purposes, and
3. 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 UK GDPR Documentation log, in accordance with Article 30 and has been disseminated to the staff of the organisation.