



**CROFTING COMMISSION
COIMISEAN NA CROITEARACHD**

CROFTING COMMISSION

**DATA PROTECTION POLICY
AND
SUBJECT ACCESS REQUESTS**

Guidance for Staff

VERSION 1.9

Last Review: December 2024

Next Review: December 2025

CONTENTS

PART 1: DATA PROTECTION POLICY 1

 BACKGROUND 1

 PERSONAL DATA 1

 WHAT IS DATA PROCESSING? 2

 GDPR PRINCIPLES 2

 INDIVIDUALS’ RIGHTS2

 Right to Be Informed 2

 Right of Access (SAR) 3

 Rectification 3

 Erasure (Right to Be Forgotten) 3

 Restriction 3

 Right to Object 3

 LAWFUL BASIS FOR PROCESSING 4

 SPECIAL CATEGORIES OF PERSONAL DATA AND CRIMINAL CONVICTIONS &
 OFFENCES DATA 5

 THE CROFTING ANNUAL NOTICE – *THE CROFTING CENSUS* 6

 Is The Annual Notice Information “Personal Data”? 6

 How Does FOISA/EIR Regulate The Release Of Such Data? 6

 How Does This Relate To The Annual Notice Data? 7

 DATA CONTROLLERS AND PROCESSORS 8

 DATA SHARING AGREEMENTS 9

 CONTRACTS 9

 INFORMATION MANAGEMENT 9

 RETENTION SCHEDULES 9

 PRIVACY IMPACT ASSESSMENTS / DATA PROTECTION IMPACT
 ASSESSMENTS 9

 DATA PROTECTION OFFICER (DPO) 10

 DATA BREACH INCIDENTS – HOW TO AVOID, RECOGNISE AND REPORT
 BREACHES 11

 POWERS OF THE UK INFORMATION COMMISSIONER 12

PART 2: PROCESSING A SUBJECT ACCESS REQUEST 13

 SUBJECT ACCESS REQUEST (SAR) RECEIVED 13

VERIFY REQUESTER'S ID	13
ACKNOWLEDGEMENT	14
ASSOCIATED COSTS	14
CLARIFICATION	14
LOCATING INFORMATION	15
REVIEW	15
EXEMPTIONS	15
THIRD PARTIES	15
What is Third Party Data?	15
Supplying Information to the Requester	16
APPLYING EXEMPTIONS – REDACTING INFORMATION	16
What Is Redaction?	16
How Should It Be Done?	16
RELEASING INFORMATION	17
TEMPLATES	18
APPENDIX 1.....	19
SUBJECT ACCESS REQUEST (SAR) TIMELINE	19
APPENDIX 2.....	20
PROCESSING CIS ATTACHMENTS	20
APPENDIX 3.....	23
BULK REQUESTS	23
APPENDIX 4.....	24
REPEATED OR UNREASONABLE REQUESTS	24
APPENDIX 5.....	25
SENSITIVE ITEMS NOT FOR SCANNING	25
APPENDIX 6.....	26
OUTLOOK 'OUT OF OFFICE'/AUTOMATIC REPLIES.....	26
APPENDIX 7.....	27
APPLYING EXEMPTIONS UNDER DATA PROTECTION & GDPR 2018	27
APPENDIX 8.....	30
CONDITIONS FOR PROCESSING SPECIAL CATEGORY PERSONAL DATA WITHOUT THE DATA SUBJECT'S CONSENT	30

PART 1: DATA PROTECTION POLICY

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 –

- a) Held electronically or manually
- b) Forms part of a relevant filing system
- c) Forms part of an accessible record
- d) 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:

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.

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](#))

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 6 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 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 (a list of the Information Asset Owners, can be found under CloudDocuments>Common>Governance>InformationAssetRegister or by [clicking here](#)).

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, 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.

THE CROFTING ANNUAL NOTICE – *THE CROFTING CENSUS*

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:

1. Consent – relevant only where consent has been freely given;
2. Performance of a contract;
3. Necessary for statutory compliance;
4. Necessary to protect the vital interests of the data subject;
5. Necessary for administration of justice;
6. 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:

1. Does the third party requester have a legitimate interest in obtaining the information?
2. If yes, is disclosure necessary for the purpose of those legitimate interests?
3. If yes, would disclosure cause prejudice to the data subject's rights and freedoms, including the right to privacy and family life?
4. 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.

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.

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

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. As well as this staff guidance document, the staff handbook and Induction Pack for new staff have been updated and 2 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 personal 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 individual's to take complaints to the ICO and increases the ICO's ability to instruct organisations to pay compensation.

ICO Powers Figure:



PART 2: PROCESSING A SUBJECT ACCESS REQUEST

SUBJECT ACCESS REQUEST (SAR) RECEIVED

The Commission can receive a SAR by letter, email, and social media or as a verbal request. Should an individual make a verbal request, write this down and read it back to them, to make sure you have all the information you need.

The Compliance Manager (Stacey Paton) will log the request on the intranet and then pass the details to the appropriate Head of Division for allocation.

If you are ever required to create the case yourself the following steps should be taken:

- *Create case on the Data Access Tracker located on the intranet under Focal Groups, Data Protection or by following:*

<https://croftingscotlandgovuk.sharepoint.com/sites/Intranet/DataProtection/Lists/Data%20Access%20Requests/AllItems.aspx?viewpath=%2Fsites%2FIntranet%2FDataProtection%2FLists%2FData%20Access%20Requests%2FAllItems%2Easpx>

- *Fill in the appropriate fields and attach your document(s).*
- *Copy the request and DPA number to compliancehub@crofting.gov.scot.*
- *Once a response has been sent update the Data Access Tracker.*

VERIFY REQUESTER'S ID

To avoid personal data about one individual being sent to another, either accidentally or as a result of deception, you need to be satisfied that you know the identity of the requester. You can ask for enough information to judge whether the person making the request is the individual to whom the personal data relates (or a person authorised to make a SAR on their behalf).

You should not request a lot more information if the identity of the person making the request is obvious to you. This is particularly the case when you have an ongoing correspondence with the individual.

However, you should not assume that, on every occasion, the person making a request is who they say they are. In some cases, it is reasonable to ask the person making the request to verify their identity before sending them information, especially if the request comes via email. You could, for instance, ask for a postal address and croft identifier, to verify identity.

ACKNOWLEDGEMENT

An acknowledgement of the SAR must be issued within 3 days confirming receipt and a response provided within a calendar month.

All staff should use the approved templates for acknowledging a SAR.

Postal Address:

If no postal address has been provided make sure to ask for this in the acknowledgment letter – *in case it is required to issue requested information by disc.*

N.B. Pseudonyms are not valid (e.g. Mickey Mouse). There is nothing to prevent a customer submitting a SAR via our Facebook page or Twitter but we cannot use social media to respond to the request.

See [Appendix 1](#) for SAR Timeline.

ASSOCIATED COSTS

There is not normally a fee for processing or providing this information. However if the request is a repeat request and/or if it is excessive and 'manifestly unfounded' we can charge an admin fee, which includes search time as well as the time spent getting the data ready for release. If you are concerned about this, ask the DPO.

CLARIFICATION

Data Protection law allows the Commission to clarify two things before we are obliged to respond to a request.

The **first** thing you can ask for is enough information to judge whether the person making the request is the individual to whom the personal data relates. This is to avoid personal data about one individual being sent to another, accidentally or as a result of deception.

The key point is that you must be reasonable about what you ask for. You should not request lots more information if the identity of the person making the request is obvious to you.

The **second** thing you are entitled to do before responding to a SAR is to ask for information that you reasonably need to find the personal data covered by the request. Again, you need not comply with the SAR until you have received this information. In some cases, personal data may be difficult to retrieve and collate. However, it is not acceptable for you to delay responding to a SAR unless you reasonably require more information to help you find the data in question.

You should not delay in asking for additional information, and ensure that you inform the requester what details you require in order to proceed with their request.

Please note that the calendar month for responding to the request does not begin until you have received any additional information that is necessary.

LOCATING INFORMATION

You should consider all types of information from every source. To do this, you need to check for any electronic files relating to your request **e.g. CIS, intranet, outlook, work folders etc.**; you need to check to see if any paper documents relate to your request **e.g. any paper filing system, Croft/Common Grazings/Apportionment files etc.** These types of files will be held at FileVault, so requests for them should be submitted with the date that you need them by, in an electronic format, should you need to redact them.

You must be able to provide evidence of the searches you have undertaken to locate the information. Information requested must not be destroyed before it can be released.

NB: Filevault require a 48 hour turnaround for files, so bear this in mind when requesting.

For more information on the processing of CIS attachments see [Appendix 2](#).

REVIEW

Unlike FOI & EIR there is no statutory right of review for a SAR. However, if a requester has a complaint about the way we have handled their personal information, they should contact the ICO on scotland@ico.org.uk or at 45 Melville Street, Edinburgh, EH3 7HL.

EXEMPTIONS

The Data Protection Act 2018 revises previous exemptions; further guidance to follow.

THIRD PARTIES

What is Third Party Data?

Third party data is any information collected by an entity that does not have a direct relationship with the user the data is being collected on e.g. a Report on a particular case from the RPID Area Office.

Supplying Information to the Requester

The Commission is not required to provide information to the requester (the data subject) if it contains information about other identifiable people, unless those other people mentioned have given their consent to the disclosure or we deem it reasonable, in the public interest, to supply the information without their consent.

If consent is needed, the requester should be advised of this prior to seeking it. The consent must be in writing and include sufficient information (full name, address, date of birth, for instance) to allow us to identify the subject.

If we decide not to disclose the other persons' information, we should still disclose as much as possible by redacting the references to them.

Example:

Where the information requested is part of an RPID report and includes the name of the reporting officer. It may be reasonable to include this if it is obvious who the officer is because the requester has already seen the report.

APPLYING EXEMPTIONS – REDACTING INFORMATION

Some requests may only be for specific pieces of information *e.g. statistics*. If this is the case you may not need to redact any information but rather use a different format like a table for releasing the information.

What Is Redaction?

In some instances only part of the information requested might be covered by an exemption, or releasing it in its entirety may result in a breach of the Data Protection Principles relating to third parties. You should still make efforts to release what information you can to the applicant. You may need to blank out certain sections (such as third party personal information) which is known as 'redacting'. This may be individual words, sentences, or whole sections of a document.

How Should It Be Done?

Redaction should always be carried out on a copy of the original document, not the original, whether paper or electronic. The end result must ensure that the redacted material cannot be seen or guessed by the applicant in any way.

To redact copies of original paper documents:

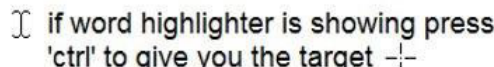

- Use a black marker pen or white correction fluid to block out the sensitive material.
- Then photocopy the redacted copy to provide the version to be released.
- Double check that the redacted information is not still visible before final release.

To redact copies of electronic documents:

- Never release redacted Word or similar versions of any documents - any redaction can be undone by the recipient, sometimes even if specialist software has been used.
- Delete information as required then insert "[redacted]" so that redaction is apparent.
- Use Adobe Acrobat DC in order to redact (black out) information
- All documents MUST be in a pdf format in order to redact them.
- Print the redacted version or provide a disc with a pdf and provide this to the enquirer.

Helpful tip:

It is easier to select an area for redacting using the target option rather than the word highlighter.

 if word highlighter is showing press 'ctrl' to give you the target 

RELEASING INFORMATION

All staff should use the approved templates in preparing their response so that all relevant information is included e.g. exemptions used.

The information can be released in different formats whether in an email or letter depicting a table of statistics or noting the information in the body of text. The requester can stipulate the format to use for the response and the Commission must try to use this, if it is practical.

Should you require to release the information by disc, be aware as there is only one external disc drive for use, which can be obtained from the IS Team.

When the files are ready for issuing, save a copy of the information and the response against the Data Protection case on the Data Access Tracker. Officers completing subject access requests should ensure that their Head of Team is satisfied with the response before it is released.

The Commission has a statutory duty to display information and statistics on its SAR requests. Once you have issued your response you **must** provide a copy of the letter/email to the Compliance Manager by complaincehub@crofting.gov.scot for recording.

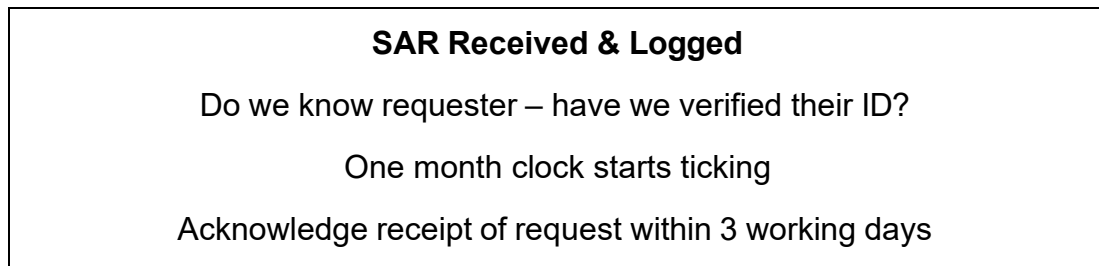
TEMPLATES

All templates are located on the intranet under Focal Groups > Data Protection > Staff Guidance > Templates or by following the link [Data Protection - Templates - All Documents \(sharepoint.com\)](#)

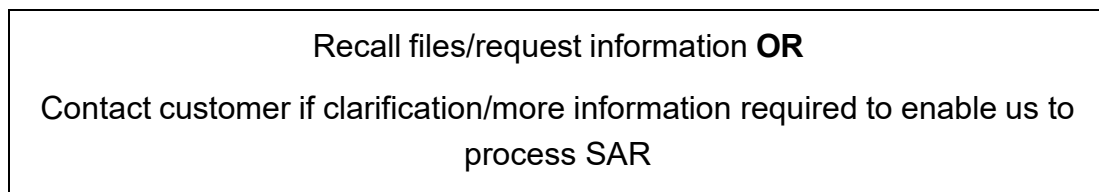
SUBJECT ACCESS REQUEST (SAR) TIMELINE

Use this timeline as an aid to organising and planning your SAR response.

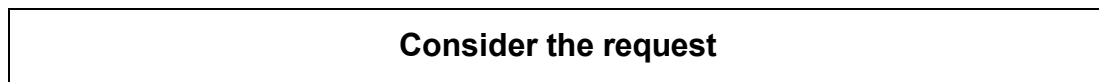
Day 1



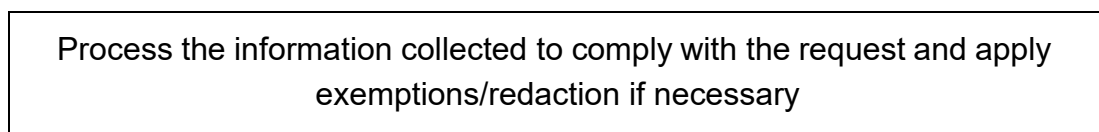
Day 2



Day 3



Days 4-29



End of Month



Please note there is an exception for cases of a complex nature. An additional 2 months may be allowed for processing such requests. See DPO for details.

PROCESSING CIS ATTACHMENTS

To locate documents / cases associated with your request from CIS, firstly you will need to open the appropriate holding record.

Holding Record
 Register Number: A1275 Name: 2 & 4 Mannal
 Holding ID: 14101
 Add to my list
 Close
 Holding Summary

Stakeholders Holding Summary Report Copy Entry Report RoC Online

Status Case Grazing Share Notes Consent to be absent **Documents** Land Allocation Conditions Reports Township Census Land Court Duties

Crofting Reg. No: C3750 Extent (Ha): 18.69170
 Main Location Code: 168/0165 Postcode:
 Authority: Agreement
 Area: NIA
 Parish: Tiree
 Township: Mannal, Tiree
 Council: Argyll And Bute
 Region: Strathclyde: Argyll And Bute
 Strathclyde: Argyll And Bute
 Croft Type: Owned
 Crofter Status: Owner-Occupier Crofter
 Croft Status: Crofted

Is a Croft
 Deemed
 Share Only
 Apportionment Only
 House Site Only
 Short term let
 Breach of Duties
 Consent to be Absent
 Tenancy Terminated
 Conditions of Let Varied
 Formal Letting Notice Issued

Service providers:

Provider Type	Name
Staff Lead	Christopher Gaff
Area	Argyll & Argyll Islands & Ayrshire
Newspaper	The Oban Times
Newspaper	An Tirisdeach
RPID Office	SGRPID (Oban)

R.O.S.
 Registration Date: 16/02/2017 Notification Date: 21/02/2017 Challenge Period End: 21/11/2017
 Rectification Date: Notification Date: Challenge Period End:

Locating CIS Holding Information

To find Holding information select the 'DOCUMENTS' tab, this will bring up a list of documents attached to the holding.

Holding Record
 Register Number: A1275 Name: 2 & 4 Mannal
 Holding ID: 14101
 Add to my list
 Close
 Holding Summary

Stakeholders Holding Summary Report Copy Entry Report RoC Online

Status Case Grazing Share Notes Consent to be absent **Documents** Land Allocation Conditions Reports Township Census Land Court Duties

Green Book B C D Rec'd Origin: Croft file number: 14356
 Croft File: B C D Public

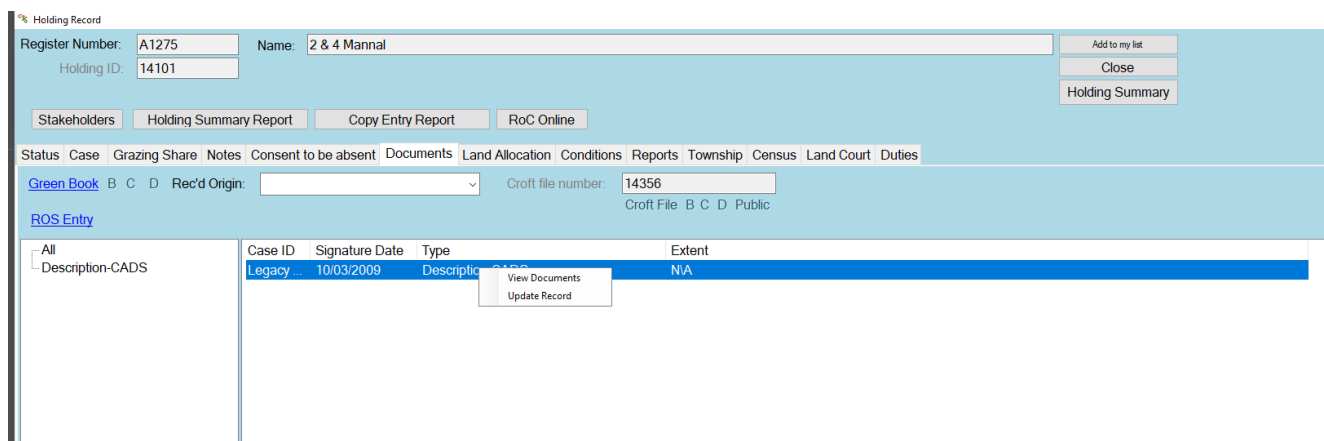
ROS Entry

All	Description-CADS	Case ID	Signature Date	Type	Extent
	Legacy ...		10/03/2009	Description-CADS	NA

All

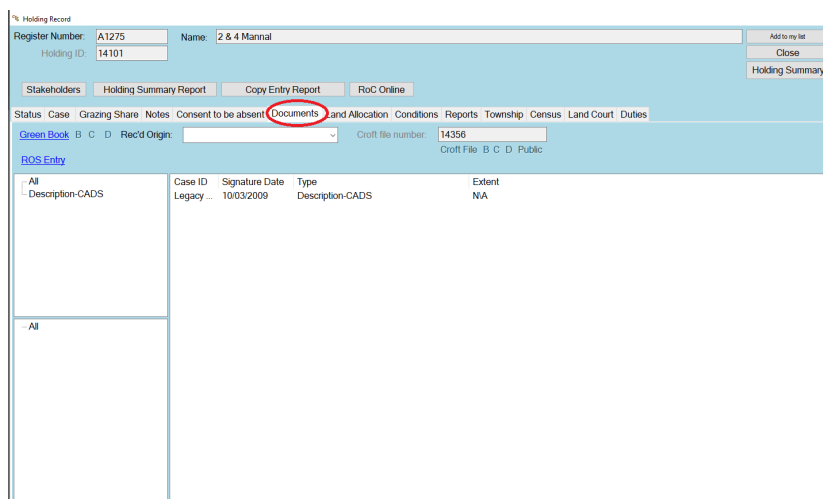
To save a document or documents it must be done on an individual basis

Select the document(s) required and right click on the document and select 'VIEW DOCUMENTS'. This will open the document and you can then save it to the appropriate location.



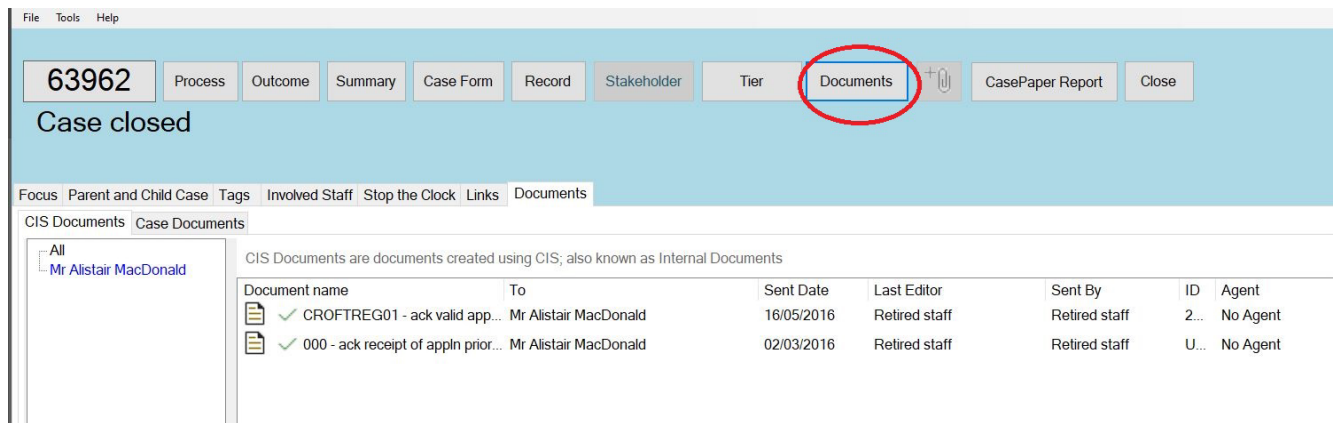
Locating CIS Cases and Attachments

To find case information select the 'Case' tab, this will bring up a list of cases associated with the holding.



Select and open the appropriate case by double clicking on it.

To locate the case documents select the 'DOCUMENTS' tab



To save a document or documents it must be done on an individual basis.

To do this you right click and select view. For documents that are internal and marked as 'Out' in the direction column you must click Reprint when the document opens in a new window. Then once you have clicked reprint, the document will open as a PDF in the browser. You can then save or print from there.

For Documents mark as 'In' in the direction column double click to view and they will open in a PDF browser and can be saved or print from there.

BULK REQUESTS

Dealing with Bulk Requests

The Commission may from time to time receive several SARs in a short period of time.

Each SAR within a bulk request must be considered individually and responded to appropriately. The following principles should be kept in mind when dealing with high volumes of SARs:

- a SAR that is made as part of a bulk request has the same legal status as a SAR that is made individually;
- the purpose for which a SAR is made does not affect its validity, or your duty to respond to it;
- if the request is made by a third party on behalf of the individual concerned, you are entitled to satisfy yourself that the third party is authorised to make the request;
- you are also entitled to satisfy yourself as to the identity of the individual concerned;
- you must respond to the request even if you hold no information about the individual. Your response may obviously be very brief in such cases; and
- you should be prepared to respond to peaks in the volume of SARs you receive.

REPEATED OR UNREASONABLE REQUESTS

Dealing with Repeated or Unreasonable Requests

Data Protection law does not limit the number of SARs an individual can make to any organisation. However, it does allow some discretion when dealing with requests that are made at unreasonable intervals.

The Crofting Commission is not obliged to comply with an identical or similar request to one that has already been dealt with, unless a reasonable period of time has elapsed between the first request and any subsequent ones.

Where it is unclear if a reasonable period of time has elapsed the following should be considered:

- The nature of the data – this could include considering whether it is particularly sensitive.
- The purposes of the processing – this could include whether the processing is likely to cause detriment (harm) to the requester.
- How often the data is altered – if information is unlikely to have changed between requests, you may decide that you need not respond to the same request twice.

Section 8(6) of the Data Protection Act 1998 states that the “information to be supplied pursuant to a request... must be supplied by reference to the data in question at the time when the request is received...”. If there has been a previous request or requests, and the information has been added to or amended since then, when answering a SAR a **full** response to the request is required: not merely supply information that is new or has been amended since the last request.

An attempt to negotiate with the requester to get them to restrict the scope of their SAR to the new or updated information is acceptable; but if they insist upon a **full** response then you would need to supply all the information.

Example

A library receives a SAR from an individual who made a similar request one month earlier. The information relates to when the individual joined the library and the items borrowed. None of the information has changed since the previous request. With this in mind, along with the fact that the individual is unlikely to suffer any disadvantage if the library does not send any personal data in response, you need not comply with this request. However, it would be good practice to respond explaining why it has not provided the information again.

APPENDIX 5

SENSITIVE ITEMS NOT FOR SCANNING

As you will all be aware, the Commission often receives sensitive documents from individuals usually as supporting evidence for their application / case / situation / issue / complaint. The type of document will dictate whether or not the Commission is able to retain this information for processing. See the below list for details on documentation that should not be retained by the Commission.

A note should be made on CIS to say that we have had sight of any documents, these documents should then be returned to sender.

Where staff need a file(s) to be deleted they are required to submit a CIS help desk ticket containing full details of the document(s) including the Post ID.

DOCUMENT LIST	
Succession	Death certificate
	Wills
	Certificate of Confirmation to a deceased tenant crofters estate
	Certificate of Confirmation of a deceased person's estate
Financial	Invoices for house improvements and travel to and from croft e.g. ferry receipts
	Bankruptcy Notice / Sequestration Petition
	Acquisition Reports
Domestic	Copies of council tax documents relating to residency
	Utility bills
	Info on electoral roll info e.g. if they are eligible to vote in the croft area
Employment	Employment contracts
Medical	Clinical Assessment of Mental Capacity
	Medical information, e.g. confirmation of hospital appointments, letters from doctors confirming a crofter's medical history, x-rays
	Medical certificates or information from medical professionals – this has in the past been received and may still be received in relation to duties/residency cases
Marriage/Birth	Birth certificate
	Marriage certificates
	Court documents relating to divorce and separation
Images	Photographs that include people that we haven't had consent from
Children	Letters from schools confirming children are attending a particular school

OUTLOOK 'OUT OF OFFICE'/AUTOMATIC REPLIES

FOI/FOISA, EIRs, Subject Access Requests under Data Protection law and formal Complaints are all cases that we must respond to within prescribed timescales.

Our ability to adhere to the prescribed timescales that are in place to investigate these types of cases is put at risk if emails received by a member of staff on annual leave lie un-actioned for any length of time.

As such, before you go on leave you **must** include a note in your Outlook 'Out of Office'/Automatic reply, informing customers when you are back in the office and if their email contains an FOI request or a request under Data Protection law or a formal Complaint, they should contact xxx in your absence.

APPLYING EXEMPTIONS UNDER DATA PROTECTION & 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. UK 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/UK 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 UK 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 UK 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 UK 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 UK GDPR Articles 12-22 and chapter 3 of part 4 of the DPA 2018.

CONDITIONS FOR PROCESSING SPECIAL CATEGORY PERSONAL DATA WITHOUT THE DATA SUBJECT'S CONSENT

The Crofting Commission will meet its obligations under UK 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 UK GDPR Documentation log, in accordance with Article 30 and has been disseminated to the staff of the organisation.