CPF distribution list legitimate interests assessment (LIA)
Created: 10 September 2019
Shared with Data Protection, SGLD, IMSO and Information Asset Owner (IAO): 10 September 2019
Date of next review: 10 September 2020. Review public task advice A25722852

✓ **We have checked that legitimate interests is the most appropriate basis.**
Data Protection colleagues offered two options.

1. Obtain consent of people involved
2. Use the legitimate interests basis

In reviewing these, legitimate interest seems the most appropriate. Reasoning is set out within responses to questions below.

✓ **We understand our responsibility to protect the individual's interests.**

We have developed a privacy notice, instructions for C&F team members to follow when updating and using the distribution list and a standard privacy summary email signature to include when emailing stakeholders as part of any distribution list communication.

These set out our understanding of responsibilities to protect individuals interest.

✓ **We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.**

This LIA was completed on 10 September 2019 and is stored on the Creating Positive Futures Administration folder, within ERDM.

✓ **We have identified the relevant legitimate interests.**

ICO says: "The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits." And "You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests."

The policy area supports helping individuals and in doing so it has societal benefits.

We anticipate that the people who we contact would reasonably expect to engage with us – we wish to contact them as people who hold key posts within organisations that have a direct interest in this policy area. This is a business-to-business contact list rather than communicating directly with private individuals.

ICO says: "*The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply."*

Our stakeholders are directly affected by policy developments and we anticipate they would expect to be involved in shaping its development. To seek consent would

involve an extra layer of communication with stakeholders and it risks not all of them responding – not necessarily because they wouldn't consent but because it's an action we're asking them to take which may get low priority, people will be on leave etc. Legitimate interest is a less intrusive way of meeting their information needs.

- ✓ **We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.**

Maintaining and updating a distribution list is vital if we are to involve and update organisations that have an interest in Creating Positive Futures policies.

This is a straightforward business-to-business communication and there isn't a less intrusive way to update and involve these key stakeholders.

This list also reduces the need for teams to keep separate lists thus removing duplication and minimising contacting stakeholders multiple times (for example a stakeholder who has changed post).

- ✓ **We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.**

This distribution list supports business-to-business communication and it supports our need to engage stakeholders as well as their need to be kept up-to-date and have the opportunity to be involved where appropriate.

Individuals are only interested, and therefore contacted, in that context. We have also organised the list so that we can tailor communications to particular sectors or meetings to avoid over-burdening anyone with irrelevant communication.

If an individual notifies us they have changed posts and our communications are no longer relevant we will remove them from the distribution lists.

- ✓ **We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.**

The individuals we communicate with are post holders within children and family-related stakeholders. It is important that we:

- share policy updates
- invite partnership working through meetings, policy development activity and input to publicity development
- invite stakeholders to update their networks, staff and public audiences about relevant Creating Positive Future policy

- ✓ **We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.**

We will communicate when there reasons to do so as set out within the response above.

- ✓ **If we process children's data, we take extra care to make sure we protect their interests.**

It is not anticipated that the distribution list will include contact details for anyone under 18.

If children's data is knowingly added it will most likely be because the individual, with their parent's permission, has agreed to support us as part of a group dedicated to informing policy development and communicating it to networks.

We will not store details on the distribution list beyond what is necessary to involve the individuals in these activities.

- ✓ **We have considered safeguards to reduce the impact where possible.**

The distribution list is stored securely on ERDM. Back-up copies will not be kept. We will only communicate when there is a clear reason to do so.

- ✓ **We have considered whether we can offer an opt out.**

Our privacy notice and the email signature block which will be included on emails that use the distribution list will invite stakeholders to let us know if they want to be removed. They may wish to do so if they have changed posts.

- ✓ **If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.**

We have not identified a significant privacy impact

- ✓ **We keep our LIA under review, and repeat it if circumstances change.**

We will review in a year's time.

- ✓ **We include information about our legitimate interests in our privacy information.**

Legitimate interest is reflected within our Privacy Notice which is contained within our team's distribution list handling instructions. Link below.

CPF Distribution List Procedures.obr

Sample LIA template

This legitimate interests assessment (LIA) template is designed to help you to decide whether or not the legitimate interests basis is likely to apply to your processing. It should be used alongside our legitimate interests guidance.

Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

• Why do you want to process the data? • What benefit do you expect to get from the processing? • Do any third parties benefit from the processing? • Are there any wider public benefits to the processing? • How important are the benefits that you have identified? • What would the impact be if you couldn't go ahead with the processing? • Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)? • Are you complying with other relevant laws? • Are you complying with industry guidelines or codes of practice? • Are there any other ethical issues with the processing?
We want to process contact details for people working within asylum and refugee integration policy and/or volunteers who have an interest in this policy area so that we maintain networks and contacts to enable the implementation of the New Scots refugee integration strategy and associated policy work of the Scottish Government. All contacts will be professionals/employees of organisations or will have provided their contact details to Scottish Government officials for the purposes of engaging with this Scottish Government policy. This will include processing data by updating the contact list and using the list to make contact with relevant contacts as part of our policy work. Benefits from processing will be the continued collaborative working which has enabled the establishment, development and implementation of the New Scots refugee integration strategy and enabling wider networks within the sector to be involved in Scottish Government policy in this area. Third parties on the contact list will benefit from the processing because we will be able to contact them when there are developments relevant to their interests. This will include New Scots conferences or other relevant events and other opportunities to engage with Scottish Government policy which impacts refugees, asylum seekers and the communities they live in. Wider public benefits include: enabling sharing of good practice and information relevant to supporting asylum and refugee integration across Scotland which will be of benefit to refugees, asylum seekers and communities.

In line with GDPR, any contact can request to be removed from the list at any time and we will make them aware of this in any general contact. We will take steps to maintain privacy of contacts (for example, obtaining specific consent before sharing contact details with third parties and only sharing contact details for specific, relevant purpose). We will also update the contact list as staff at relevant organisations change.

These steps are being taken to comply with GDPR and other relevant laws or policies. We will review this LIA periodically to ensure continuing compliance with reference to any changes in law or policy.

Only minor ethical issues have been identified and all are considered to be mitigated. These include:

- the contact list being limited to contacts policy officials have met and therefore potentially exclusive to a narrow group of contacts who will benefit from information or opportunities. This is mitigated by the encouragement of contacts on the list to communicate any general information or opportunities further through their networks, and being open to adding and updating contacts on the list.
- The contact list will identify people and link them with an interest in asylum and refugee integration. This is mitigated because anyone on the list will be working in this field or actively engaging in supporting refugees and asylum seekers – this is therefore likely to be information generally publicly available and does not identify sensitive personal data.
- The list will enable individuals to be identified and linked to their contact details, however the information kept will be proportionate for the purpose as set out above and will not include sensitive personal data as this will not be gathered or processed.

Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

• Will this processing actually help you achieve your purpose? • Is the processing proportionate to that purpose? • Can you achieve the same purpose without the processing? • Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?
The processing is necessary to maintain a contact list which enables the implementation of the New Scots refugee integration strategy, including the promotion of the New Scots approach and communicating updates on progress of policy implementation. It is also necessary to enable policy officials to make contact with the most relevant person at partner organisations and key stakeholders for the purposes of preparing briefing for Ministers and progressing policy development and implementation. The processing is proportionate to the purpose set out above. The same purpose could not be achieved without the processing as contact details would not be available to policy officials and as a result policy would be less informed and developed in a less collaborative manner. Data processed will be only what is required for the purpose outlined, this will be done in an unobtrusive manner.

Part 3: Balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

Nature of the personal data
• Is it special category data or criminal offence data? • Is it data which people are likely to consider particularly 'private'? • Are you processing children's data or data relating to other vulnerable people? • Is the data about people in their personal or professional capacity?
Due to the intention to process data without issuing a privacy notice to the individual, the need for a DPIA has also been considered. The conclusion is that impact and risk are minimal as the processes proposed are low risk, mitigated as appropriate and reasonable to achieve the purpose of processing. No significant changes are being made to the way we process personal data. No special category data or criminal offence data will be processed. Data is unlikely to be considered particularly 'private' by individuals as the majority of contact details will be those associated with employment or in the individual's professional capacity. Data about people is predominantly in their professional capacity; in some cases, individual's may use a personal email account or phone number – for example volunteers at community groups or small charities – however this type of contact detail will be processed proportionately and only when the individual uses it for purposes relevant for the policy contact and where they have freely provided that information. The contact list will not include children's data or data relating to other vulnerable people.
Reasonable expectations
• Do you have an existing relationship with the individual? • What's the nature of the relationship and how have you used data in the past? • Did you collect the data directly from the individual? What did you tell them at the time? • If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you? • How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations? • Is your intended purpose and method widely understood? • Are you intending to do anything new or innovative?

• Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation? • Are there any other factors in the particular circumstances that mean they would or would not expect the processing?
All contacts on the list have some form of existing relationship with policy officials or the work of the Scottish Government. Including: direct involvement in policy work; they have made contact with the policy area; they receive funding following an application; or they responded to engagement or a call to note interest in an opportunity or receiving information. Prior to processing contact details (by adding to the list), some contacts may have initially been referred by third parties. However, their details will not be held unless there is a reason to do so, for example because of their direct involvement in work relating to a policy. The nature of the relationship of contacts on the list is professional. In the past the data has been used to make contact in relation to specific policy matters, including to enable preparation of briefing for Ministers, or to provide general updates on policy and invite people to register to attend events associated with policy area. Data has been collected directly from the individual or from their employer/organisation (for example, when informed of a change of postholder or another relevant contact within an organisation for a specific enquiry). At the point of obtaining data of this type it has been volunteered by the individual or their organisation. In some circumstances, contact details may have been provided by a third party – in these circumstances the individual has been contacted for a specific purpose, they will have been informed where their contact details were sourced from and invited to respond/engage and their data only processed for the purpose set out above following their positive response or active engagement in relation to policy work. Data has not been a systematic single sourcing and evolves over time as professional contacts and networks develop, change and become apparent. As a result it has been collected at various times. There have been no changes in context or technology since the data was collected. Data will be regularly reviewed and updated (for example when postholders change) with data which is no longer relevant for the purpose set out above deleted. Contacts can also request to have their contact details removed at any time and will be informed of this for any general updates which are issued. We would consider the intended purpose and method to be widely understood – our policy contacts expect relevant policy officials to be able to contact them and to provide them with relevant policy updates. Our contacts have asked us to communicate information to our contacts previously – if doing so we have always explained that we will not share contact details without prior consent of the individual but where information is relevant we will be willing to inform our

contacts. This has established a pattern which our stakeholders are comfortable with. We have received requests to add individuals to our contact list previously – indicating an expectation that we would process this type of data and that it is considered reasonable for us to do so. We are not intending to do anything new or innovative with the data.
Likely impact
• What are the possible impacts of the processing on people? • Will individuals lose any control over the use of their personal data? • What is the likelihood and severity of any potential impact? • Are some people likely to object to the processing or find it intrusive? • Would you be happy to explain the processing to individuals? • Can you adopt any safeguards to minimise the impact?
Possible impacts are people receiving information that they had not anticipated or specifically requested. It will also impact people when they are contacted about specific policy matters which enables them to provide further information or engage in policy development. Individuals will not lose any control over the use of their personal data. They can request that the data be deleted at any time, they will always be consulted before contact details are shared with third parties outside the Scottish Government. Likelihood and severity of any potential impact is minimal. We would not expect any individuals on the contact list to object to the processing or find it intrusive. We would be happy to explain the processing to individuals and to provide them with privacy information. Safeguards to minimise impact include: any general policy updates being issued without displaying contact details to recipients and giving an option for individuals to have their contact details removed from the contact list. The contact lists will be stored securely in eRDM.

Can you offer individuals an opt-out?	Yes

Making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.

Can you rely on legitimate interests for this processing?	Yes
Do you have any comments to justify your answer? (optional)	

There is a clear purpose to processing this data and which there would be reasonable expectation for: to enable Scottish Government asylum and refugee integration policy to be informed by stakeholders and to engage with stakeholders about policy developments which are relevant to their interests. The processing of data is necessary to achieve the purpose and is minimally obtrusive. The processing is done in a way which is balanced against the individual's interests, rights and freedoms.

LIA completed by	[REDACTED]
Date	24 May 2018

What's next?

Keep a record of this LIA, and keep it under review.

Do a DPIA if necessary.

Include details of your purposes and lawful basis for processing in your privacy information, including an outline of your legitimate interests.

Data Protection Policy

Information Assurance and Data Protection Branch

Document Control

Date	Version	Name	Role	Reason For Change
2017	0.1	Iain Mackintosh	Author	First draft
2018		Ann Robertson	Reviewer	Approve draft
2018	1.0	Ann Robertson Head of IA&R	Approver	First release
2022	2.0	Nicholas Reid	Reviewer	Update
2022	2.0	Stuart Gardner	Approver	Update

1. Introduction

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018 impose obligations on the use of all personal data held by the Scottish Government, whether it relates to data subjects and their families, employees, complainants, contractors or any other individual who comes into contact with the organisation, defined as data subjects.

This policy sets out how the Scottish Government meets its legal obligations and requirements under data protection law. It will be reviewed annually, or as appropriate to take into account changes to legislation that may occur. Any breach of this policy may result in the Scottish Government being liable for the consequences of the breach.

2. Roles and responsibilities

The Permanent Secretary, as **Accountable Officer (AO),** has overall responsibility for data protection within the Scottish Government.

The Director General of Corporate is designated as the Scottish Government's **Senior Information Risk Owner (SIRO).**

The Data Protection Officer (DPO) is responsible for data protection assurance and compliance, and reports key findings and recommendations to the Executive Team.

Information Asset Owners (IAO) are responsible for maintaining, registering and safeguarding information assets. IAOs also have a responsibility to ensure compliance with data protection law within their business area.

Deputy Information Asset Owners (DIAOs) are responsible for supporting IAOs in their role and helping to encourage, develop and maintain good information and records management practices within their business area.

The **Information Assurance and Data Protection Branch** provide advice and guidance and training to the staff of the Scottish Government and Executive Agencies.

3. The data protection principles

Article 5 of the UK General Data Protection Regulation outlines the six data protection principles (detailed below) which must be adhered to when processing personal data.

Principle	Key considerations
3.1 Lawfulness, fairness and transparency *Processed lawfully, fairly and in a transparent manner in relation to individuals;*	Have you identified your lawful basis? To process personal data at least one of the conditions at Article 6 must be met, and when using: • special category data one of the conditions in Article 9 must be met. • Criminal offence data you must do so in line with Article 10.

Principle	Key considerations
	• Personal data for law enforcement purposes, this must be carried out under Part 3 of the DPA 2018. It is vital to consider your lawful basis on a case-by-case basis, and ensure you have established one, with input from the IADP Branch, before processing begins. In most cases the Scottish Government will be operating under the bases of public task or legal obligation, in that there is legislation giving us a power or responsibility and it is necessary for us to use personal data when acting on those powers. As a public sector organisation, where there may be an imbalance of power between us and a data subject, it is often inappropriate or unnecessary for us to rely on the basis of consent – the use of this should be strongly considered before consent is sought from individuals to process their data. Your SGLD legal team will be able to assist you to identify these conditions for processing. How will individuals be told about the use of their personal data? Do you need to create or amend your privacy notice?
3.2 Purpose limitation *Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;*	Have you clearly considered the purpose or purposes that are requiring you to collect personal data before you start processing? Have you demonstrated that the use of the data is justified and proportionate to your stated purposes? How would you meet data protection law if you identify any new purpose for processing personal data? Do you need to create or amend your privacy notice?

Principle	Key considerations
3.3 Data minimisation *Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;*	Data minimisation. Do you collect personal data that you do not need? If so do you need to keep it? You should also consider whether you can cut down on the amount of personal data held as your project continues.
3.4 Accuracy *Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;*	How are you ensuring that personal data obtained from individuals or other organisations is accurate? You should also consider whether you need to maintain accurate records (such as when you are providing a service or making decisions about people using their data); or whether you can rely on a 'snap-shot' of data at a certain time (such as for a research project).
3.5 Storage limitation *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject 'storage limitation'*	Do your systems allow you to amend or delete data where necessary? What are your retention schedules? These can be based on legal requirements, or on identified business needs if there is no specific legislative guide. Have you considered anonymization/ Pseudonymisation?
3.6 Integrity and Confidentiality *Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using*	Personal data must be protected from unauthorised access at all times, during collection, storage and transmission. This includes both IT security and physical security. When processing personal data you should use already assessed SG systems, or where that is not possible undertaken a data protection impact assessment and security and cyber assessments before using.

Principle	Key considerations
appropriate technical or organisational measures	As a controller, we are also responsible who we transfer data to. Has a data protection impact assessment been undertaken for your project?
3.7 Accountability *the controller shall be responsible for, and be able to demonstrate, compliance with the principles.*	The overarching requirement of accountability requires us to maintain adequate records of our data processing activities, and keep evidence of how we comply with the data protection principles. These documents include: • **Data protection impact assessment**, which details what data is being processing, the justification and risks and mitigations applied. This is legally required where processing poses a high risk to individuals and their rights, and is Scottish Government Policy to undertake a DPIA where the Scottish Government is acting as data controller. • **Data sharing agreement**, which documents the transfer of data between two or more data controllers • **Privacy notice**, which informs the data subjects of how we are using their data • **Legally binding contracts**, which set out how a third party processor appointed by Scottish Government can use personal data. These are legally required under Article 28(3) of the UK GDPR. The Scottish Government also maintains an **Information Asset Register** which catalogues which information (not exclusively personal data) each area of the Scottish Government holds, and which IAO is responsible for it. IAOs and their deputies must ensure they maintain their register entries, and update and remove assets as necessary.

4. Reporting incidents

All data protection and information security related incidents should be reported via the Security Incident Reporting Tool and properly investigated according to the Scottish Government's Security Breach Policy. In the main, correspondence with the

Information Commissioner's Office (ICO) on data protection matters will be dealt with by the DPO.

Further information can be found here

5. Staff awareness and training

All staff must be trained before they can handle personal information in any form in the course of their job.

The Scottish Government has a mandatory training programme which includes maintaining awareness of data protection and information handling for all staff. This is carried out by annual completion of elearning as follows:

- Data Protection elearning package;
- Pathways learning modules on Information Management

Advice and guidance regarding this policy or the data protection law in general is available on Saltire here or by emailing the data protection and information assets team.

6. Disciplinary issues

A deliberate or reckless breach of data protection law can result in a member of staff facing disciplinary action. Managers must ensure that all staff familiarise themselves with the content of this policy.

All personal data recorded in any format must be handled securely and appropriately in line with the data protection law, and staff must not disclose information for any purpose outside their normal work role. Any deliberate or reckless disclosure of information by a member of staff will be considered as a disciplinary issue.

Employees should be aware that it is a criminal offence to deliberately or recklessly disclose personal data without the authority of the Scottish Government (the data controller).

7. Associated documents and guidance

For ease of reference some of the key documents and guidance are included below.

Link	Document type
Data protection impact assessment	Guidance
Privacy notice checklist	Document
Data sharing agreements(personal data)	Template
Subject access request guidance	Guidance
Information Asset Register	System
Security Incident Reporting Tool	System

Subject Access Request Procedure

Purpose

The purpose of this procedure is to provide clear and consistent instructions for the handling of a subject access request (SAR) throughout its' end-to-end lifecycle from request through to closure.

Scope

The scope of this procedure covers all SARs as defined in the Data Protection Act (2018).

This procedure is to be used by members of the Information Assurance and Data Protection (IADP) branch members

This procedure is applicable to all the core Scottish Government Directors General (DG), Directorates, Divisions and Branches.

Prerequisites

This procedure is based upon the guidelines for Subject Access Requests provided by the Information Commissioner's Office (ICO). These guidelines can be found on the ICO website, www.ico.org.co.uk.

It is expected that IADP branch members are familiar with the guidance provided by the ICO.

Responsibilities & Third Party Involvement

This procedure provides instructions for the responsibilities of the following:

- SAR requester
- IADP branch
- Relevant Scottish Government Divisions and Branches

Procedure Steps

The procedure has been broken down into various steps. Each step will have associated work instructions.

The identified steps are listed:

- Request
- Validation, clarification & acknowledgement
- Request(s) to search
- Management of request(s) to search
- Redaction
- Collation
- Release

This procedure is supported by the use of eRDM Connect. In the appendix, there are the links to how to use eRDM, IADP team guidance and an overall process map for eRDM Connect. Links are also contained in the following steps to support the existing use of eRDM connect.

1. Request

1.1 The following are the main channels used to receive a SAR:

- External email
- Online request from the Scottish government website Request personal data: form - gov.scot (www.gov.scot)
- Internal email from a Scottish Government resource (employee, contractor, etc.)
- Phone
- Social media or a verbal request

1.2 There may be occasions when the requester is acting on behalf of a data subject. In these circumstances, we should seek to ensure that the appropriate approval has been provided by the data subject, i.e. legal representation.

2. Validation, clarification & acknowledgement

2.1 There are two main elements of the validation process:

- Validate the nature of the request, e.g. is it a SAR?
- Validate the identity of the requester

2.2 SAR Validation

Before taking any further actions, it is essential to determine the precise nature of the request. The following activities will assist you:

- Is it a request for personal data?
- Is the data held by the Scottish Government or an Executive Agency (EA) or another public body, e.g. Police, Prison service, NHS or a local authority? A list can be found in the appendix. If this is the case, we should provide assistance and guidance to direct the requester to the correct body
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 01b - request is for another organisation details - Objective ECM (scotland.gov.uk)

2.3 Requester not data subject

There are occasions when a is made by a data subject's friend, family or legal representative. In such circumstances, it is expected that we establish that there is current mandate in place before proceeding with a SAR.

2.4 ID Validation (Data Subject)

It is essential that the identity of the requester is validated. If the request is made by the actual data subject then we need to confirm their identity. This can be done by:

- Photo ID, e.g. current passport or driving licence
- Pre-existing business relationship (this can be determined by checking with the relevant branch)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 01 - request for proof of identity details - Objective ECM (scotland.gov.uk)

2.5 ID Validation Follow-up

If the requester does not respond within a reasonable timeframe with proof of identity, e.g. 2 weeks. It is recommended that we follow-up the original request.

- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 05 - letter chasing proof of ID details - Objective ECM (scotland.gov.uk)

2.6 Request related to a child

If the request for data is related to a child, there are specific guidelines on the ICO website that can be consulted to determine the appropriate steps to take. The following templates have been created within eRDM Connect

- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 09 - requesting proof that a parent can act on behalf of their child over 12 details - Objective ECM (scotland.gov.uk)

- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 10 - requesting proof that a parent can act on behalf of their child under 12 details - Objective ECM (scotland.gov.uk)

2.7 Clarification

There are occasions when a SAR is for specific dates or timeframes or about a specific topic. Any items related to a clarification should be addressed in a timely manner with the data requester.

- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 04 - request for clarification details - Objective ECM (scotland.gov.uk)

2.8 Once, we have satisfied all the earlier points an acknowledgement letter with a deadline date is sent to the data requester

- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 02 - acknowledgement letter giving deadline date details - Objective ECM (scotland.gov.uk)

3. Request(s) to Search

3.1 If the SAR contains any specific named contact names or branch details these should be used when requesting data

3.2 When using the eRDM global search, it is recommended to search by either the named individual or the branch name.

3.3 A good source of information is the MiCase system

3.4 A list of internal contacts to request data is contained within the appendix section. The following template is used:

- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 03 - email to business area to conduct a search for information details - Objective ECM (scotland.gov.uk)

4. Management of request(s) to search

4.1 A request(s) to search should be no longer than 10 working days (2 calendar weeks).

4.2 A reminder to be sent after 5 working days (1 calendar week).

4.3 the SAR spreadsheet should be updated to manage the request to search requests.

4.4 If there is no response from a business area the appropriate escalation steps should be discussed.

5. Redaction

This is a key step to ensure that any response provided by the data requester does not compromise the data privacy of another data subject.

The majority of data redaction will be performed by the relevant branch.

5.1 Redaction guidelines

General redactions guidelines can be found on Saltire Redacting information

The IADP branch should provide advice and guidance to

- Business area to perform redaction

5.2 Redaction tools

The main redaction tool is Adobe Acrobat Pro. However, it is expected that redaction functionality within eRDM will be made available within the Scottish Government.

5.3 Quality Assurance Checks

It is expected that any quality assurance checks are performed by the relevant branch before responding to the IADP branch. This would require some review and approval by the relevant manager(s) before returning to the IADP branch.

5.4 The four areas that need to be considered are:

- Un redacted personal data
- Over redaction
- Exemptions
- Redacted text cannot be made visible

6. Collation

6.1 All the responses are collated in the ERDM Connect folder.

6.2 A check should be made to ensure that all the relevant documents are in the folder before moving to the next step.

7. Release

7.1 The following template is sent to the data subject once all quality checks have been performed:

- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 15 - invitation to Objective Connect details - Objective ECM (scotland.gov.uk)

7.2 In the rare instances that all documentation is to be provided as hard copies, the IADP branch will need to make the necessary arrangements for printing and secure delivery.

There is no legal obligation to provide hard copies, but this can be done in situations such as: requester has accessibility issues; or has originally written to us by post and does not have internet access.

If working remotely release can be arranged by contacting the Atlantic Quay house team: AccHouseTeamEBAQHH@gov.scot. We should provide the Cost Centre – 311446 – and request the document is sent first class and signed for on delivery.

If working in the office documents can be printed and hand-delivered to that building's mailroom, again including the Cost Centre.

The following template is to be included in the delivery package with the documents:

- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 14 - send with disclosed document details - Objective ECM (scotland.gov.uk)

7.3 Advise the area(s) that submitted the documents of the retention plan for the released items (as below), and that this does not affect their own retention schedules. Use template document 16 if necessary.

8. Retention of documents

8.1 After discussion with the team it was decided that documents will be retained on the following schedule:

- Accessible to the data subject for one calendar month in the Objective Connect folder
- Following that month expiring, retained for a further 3 calendar months to allow review or handling of a complaint.
- This does not impact on or reflect the retention periods of the areas which originally held the data, who should maintain their own retention schedules.

8.2 Once the first month of access has expired, remove the requester and rename the document 'Retained prior to deletion – SAR 2021-XX'

8.3 After the subsequent 3 months have expired delete all documents, run an audit report on the Workspace, and save report to the main SAR folder.

Troubleshooting and Frequently Asked Questions (FAQ)

To be developed

Procedure Review(s)

It is recommended that this procedure is reviewed on an annual basis or whenever there is a major change in one of the steps, e.g. introduction of a new tool or significant organisational change

Appendix

1. 1 General Guidance on eRDM Connect

http://saltire/my-workplace/it-and-information-management/it-services/Pages/erdm.aspx?pageid=12b5f49b-e504-4965-ab4d-4139e01c7d56

1.2 IADP templates for eRDM Connect

Data protection (DP) - Team guidance for eRDM and Objective Connect details - Objective ECM (scotland.gov.uk)

Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - process map for SARs details - Objective ECM (scotland.gov.uk)

- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 01 - request for proof of identity details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 01b - request is for another organisation details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 02 - acknowledgement letter giving deadline date details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 03 - email to business area to conduct a search for information details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 04 - request for clarification details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 05 - letter chasing proof of ID details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 06 - acknowledgement of request for second search details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 07 - to requester advising we hold no data details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 08 - to requester advising we hold no more data, complaints procedure details - Objective ECM (scotland.gov.uk)

- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 09 - requesting proof that a parent can act on behalf of their child over 12 details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 10 - requesting proof that a parent can act on behalf of their child under 12 details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 11 - template inventory details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 12 - invitation to data subject to view documents details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 13 - to third party asking for consent to release details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 14 - send with disclosed document details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - 0000 - Template - 15 - invitation to Objective Connect details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) - Subject Access Request (SAR) - Template - 0000 - 16 - retention information for business area details - Objective ECM (scotland.gov.uk)
- Data Protection (DP) – Subject Access Request (SAR) – Template – 0000 – 17 – applying exemption and complaints procedure
- Data Protection (DP) - Subject Access Request (SAR) - template letter - applicant refusing to provide further information details - Objective ECM (scotland.gov.uk)

Internal contacts for SAR responses

SAR Topic	SG Area	Individual contacts	Staff directory area	Team mailbox
HR, disciplinary/ performance issues	People Advice and Wellbeing	[REDACTED]	Staff Directory - Branch Details	
Payroll	HR Shared Services	[REDACTED]	Staff Directory - Branch Details	
Recruitment	Resourcing Policy and Operations	[REDACTED]	Staff Directory - Branch Details	recruitment@gov.scot
Public appointments	Public Appointments Team	[REDACTED]	Staff Directory - Branch Details	Public.appointments@gov.scot
First Minister	Ministerial Private Offices (mailbox)	Each office is run by a separate team	Organisation Hierarchy	FirstMinister@gov.scot
Deputy First Minister/ Cabinet Secretary	Ministerial Private Offices (mailbox)	Each office is run by a separate team	Organisation Hierarchy	DFMCSF@gov.scot
Government minister	Ministerial Private Offices	Each office is run by a separate team	Organisation Hierarchy	
Chief Nursing Officer				CNO@gov.scot
Chief Medical Officer				CMO@gov.scot
CCTV footage	Physical Security	[REDACTED]	Staff Directory - Branch Details	
Children	Child related (Improving Lives for people with Care Experience Unit)	[REDACTED]	Staff Directory - Branch Details	Looked_After_Children@gov.scot
Survivor Relations	Survivor Relations and Advance Payment Scheme	[REDACTED]	Staff Directory - Branch Details	

Contacts for EAs/other public bodies

External body	Contact page

Police Scotland	Data Protection - Police Scotland
Local authority	Each local authority is a separate controller, DPO contacts are easily found on their website
Executive agencies	• Accountant in Bankruptcy • Disclosure Scotland • Education Scotland • Forestry and Land Scotland • Scottish Forestry • Scottish Prison Service • Scottish Public Pensions Agency • Social Security Scotland • Student Awards Agency Scotland • Transport Scotland
NHS Scotland/ healthcare data	• Each NHS Scotland Health board is responsible for its own data processing and SAR responses: Organisations – Scotland's Health on the Web • Each doctor's surgery is a data controller in their own right
MSPs, MPs, political parties	Each Member of Scottish Parliament and Member of Parliament (Westminster) are data controllers in their own right. Political parties are data controllers in their own right, separate from SG and MSPs/MPs who are members of them. Requests for councillors are typically held by local authorities. In all cases DPO details are available on the respective websites.

The process map (PDF version) can be viewed in https://erdm.scotland.gov.uk:8443/documents/A33486177/details

1. Complying with GDPR

This privacy notice complies with the General Data Protection Regulation (GDPR) which came into effect European Union wide from 25 May 2018. We have not changed the way we use, share or keep your data.

2. Why we gather data

Data is collected to administer and deliver services across the organisation. Processing is necessary so that we comply with our legal obligations as an employer or as part of our statutory duties. Read more details of our record retention and disposal schedule.

No data is transmitted outside of the European Union, with the exception of Survey Monkey which stores European customer data on its servers in the US. This is under the EU-US Privacy Shield Programme which is a means of legalising the transfer of personal data from Europe to the US. Survey Monkey is certified under, and complies with, the EU-US Privacy Shield Program and its principles regarding the collection, use, and retention of personal data from EU member states.

3. Who we collect data from

The People Directorate collect and retain personal data from:

- candidates for employment (including senior civil servants (SCS), non-executive directors and public appointments)
- employees, including ex-employees and retired staff
- employees of shared services customers
- contractors and agency workers
- candidates for public appointments and public appointees
- non-executive directors
- inward secondees
- special advisers
- children under 16 years of age coming in on a work placement

4. Candidates for employment

We collect data from candidates for employment. This includes senior civil servants (SCS), non-executive directors and public appointments.

Vacancies Online is hosted by Peoplesolutions who have a data protection regime in place along with the Scottish Government to oversee the effective and secure processing of your personal data. All personal data is processed and stored securely within the UK by Peoplesolutions and their subcontractors.

We undertake identity and pre-employment checks for all new entrants, employing third party suppliers to provide services, including utilising a credit reference agency. These services are used to verify identity information and to complete pre-employment checks, but do not include credit reference checks.

Recruitment campaigns that involve psychometric and other testing, for example those run by Capita, involve the sharing of data. Data is processed only in connection with the services provided to the Scottish Government and for business necessity. No third parties have access to your personal data unless the law allows them to do so.

Personal data held includes special types of sensitive information. This includes an identifier, name, email addresses, work and personal contact information. It also includes diversity monitoring information provided to Peoplesolutions by the Scottish Government in addition to the IP address you use to connect to the service.

Completed application forms and diversity monitoring information are stored on the HR system. This includes name, date of birth, address, contact information, CVs, supporting statements and references. Unsuccessful applicants' details are destroyed after two years. How long successful candidates' details are kept for are shown in Annex A.

5. Employees, ex-employees and retired staff

Data is collected from employees, ex-employees and retired staff from our eHR systems such as iExpenses, iFix/HR Help, excess fares, relocation data, eOvertime, flexible working hours, and records systems. Paper based pay files are held for all staff including senior civil service (SCS) staff. This includes:

- name, title, date of birth, address, contact telephone numbers, National Insurance (NI) number, bank details, tax code, emergency contact/next of kin, payslip data, pensions data, marital status and occupational health reports. Baseline Personnel Security Standard ID checks information is held (copies of passport, driving licence, utility bill and Disclosure Scotland certificate)

- current job information, employee contract, employment history, disciplinary records, performance management and training information, gifts/hospitality, outside interests/activities for conflict of interest purposes
- annual leave records, flexi records and sick leave records, performance review forms (and 9 box grid placings for SCS)
- disability information, diversity monitoring including ethnicity, nationality, gender, religious beliefs and sexual orientation
- SCS pay data
- voluntary/compulsory exit details and compromise agreements are retained
- for iFix/HR Help, personal information provided by employees seeking assistance

For staff administrative purposes data may be shared with the Department of Work and Pensions (DWP), Cabinet Office, Her Majesty's Revenue and Customs (HMRC), National Fraud Initiative (NFI) and the pensions administrator.
See contact details for the pensions administrator.

The above is shown in the contracts of employment.

6. Employees who join internal diversity networks

These are voluntary associations and include:

- Alternative Working Pattern
- Carers Network
- LGBTI Allies Network
- LGBTI Network
- Disabled Staff Network
- ME - Chronic Fatigue Syndrome Network
- Mental Health Network
- Race Equality Network
- EU Nationals Network

Network membership lists may be held electronically by network members and the diversity and inclusion team.

Personal data held can infer special types of sensitive information and includes an identifier such as name, work or personal email addresses. In the case of the LGBTI network, identifying as lesbian, gay, bisexual, transgender or intersex is a requirement for membership. Although no specific information is gathered in

relation to a member's actual sexual orientation or gender identity, it can be inferred that a person identified as LGBT or I by virtue of being a member.

Members' lists are used to keep members up-to-date on network activity, or for members to connect with each other. They are used in the course of Scottish Government policy development, to gain insights and assist in the development of policies that are free from bias and discrimination.

For networks which are open to any employee to join, the membership lists may be shared with policy teams who wish to engage network members in the course of policy development. The LGBTI network membership is never shared outwith network members.

7. Employees of shared services customers

People Directorate provide a number of other bodies with a range of HR services. Data held and processed is as outlined above and is set out in contracts of employment for staff of those bodies. It is also referenced in the overarching Memorandum of Understanding between the body and Scottish Government People Directorate for the delivery of the service.

Bodies include Revenue Scotland, Food Standards Scotland, Scottish Fiscal Commission, National Records Scotland, Office of the Scottish Charity Regulator, Scottish Housing regulator, Community Justice Scotland, Education Scotland, HM Inspectorate of Prisons for Scotland, HM Inspectorate of Constabulary, HM Fire Service Inspectorate and non-departmental public bodies.

A number of senior civil servants work within public bodies and their career files and other data as noted under employees is processed centrally and retained within HR.

8. Contractors and agency workers

Data is gathered and shared between People Directorate and the various contractors and agency workers undertaking work on behalf of the Scottish Government and its other bodies. It is retained by the Scottish Government and processed in line with our guidelines.

9. Candidates for public appointments and public appointees

People Directorate have a function to support the public appointment process. While candidates for public appointment and successful appointees are not employees, the information gathered to facilitate the recruitment process and the payment of fees is similar to that outlined in the other pages of the guidance.

10. Non-executive directors - candidate information

Data collected is as per the details outlined in candidates for employment (including senior civil servants (SCS), non-executive directors and public appointments).

11. Non-executive directors - appointed

Data collected is as per the details outlined for employees.

12. Inward secondees, special advisers and children

13. Inward secondees

We collect the following data for inward secondees:

- name, title, Baseline Personnel Security Standard ID checks information, secondee agreement, outside interests/activities for conflict of interest purposes declaration

For staff administrative purposes, data may be shared with the Department of Work and Pensions (DWP), His Majesty's Revenue and Customs (HMRC) and National Fraud Initiative (NFI).

14. Special advisers

We collect the following data for special advisers (SPADs):

- name, title, date of birth, address, contact telephone numbers, National Insurance (NI) number, bank details, tax code, emergency contact/next of kin, payslip data, pensions data, marital status and occupational health reports. Baseline Personnel Security Standard ID checks information is

held (copies of passport, driving licence, utility bill and Disclosure Scotland certificate)
- current job information, employee contract, employment history, outside interests/ activities for conflict of interest purposes, gifts and hospitality returns

For staff administrative purposes data may be shared with the Department of Work and Pensions (DWP), Her Majesty's Revenue and Customs (HMRC) and National Fraud Initiative (NFI).

15. Children under 16 years of age

Data is stored for children under 16 years of age coming in on a work placement. This includes name, contact details of next of kin, address and school information as appropriate, as well as parental/guardian content forms.

16. Processing not for employment purposes

When we process personal data which is not for employment purposes, we may need specific consent to do so.

17. When consent is required for processing

In addition to the processing which is done on the basis of employment purposes, we also ask colleagues and staff of shared service bodies to consent to processing if they wish to access other employee benefits. These benefits are ancillary to the employment purposes such as our benefits provider (currently Edenred).

Where colleagues/staff of shared service bodies are asked to provide sensitive personal data (for example health information in the context of occupational health referral) explicit consent is obtained and held on file.

18. When consent is not required for processing

This is generally disclosures required by law. As such personal data is exempt from the non-disclosure provisions if the Scottish Government are required to disclose it:

- by or under any UK enactment
- by any rule of common law, or
- by an order of a court or tribunal in any jurisdiction

Examples include:

Schedule 2 and 3, Data Protection Act (DPA)

- prevention and detection of crime and/or the apprehension or prosecution of offenders

Schedule 2 and 3, DPA

- to protect vital interests of the data subject; serious harm or matter of life or death
- for the administration of justice (usually bringing perpetrators to justice)
- for the exercise of functions conferred on any person by or under any enactment (police/social services)

Human Rights Act, Articles 2 and 3

- right to life
- right to be free from torture or inhuman or degrading treatment

19. Your data and your rights

Only specific People Directorate Human Resources staff and managers can access your data held in Scottish Government records and systems. Employees are entitled to review/update their personal information held on HR systems.

If you wish to request additional information about your data and our privacy policy, contact HR Shared Services on x48500.

Under the Data Protection Act 1998, you are entitled to request a copy of your HR records, known as a subject access request (SAR). The Data Protection Officer for the Scottish Government can be contacted by emailing the data protection and information assets team.

20. What are your rights?

If at any point you believe the information we process on you is incorrect you can request to see this information through a subject access request.

You may have a right to have this information corrected, deleted and to object to or restrict the processing of the information held.

You may also have a right to receive the information in a structured, commonly used and machine readable format and transfer or have this information transferred to another data controller.

If you wish to raise a complaint on how your personal data is handled, you can contact the Scottish Government Data Protection Officer who will investigate the matter.

If you're not satisfied with the response or believe we are not processing your personal data in accordance with the law you can complain to the Information Commissioner's Office (ICO).

The Information Commissioner's Office - Scotland
45 Melville Street
Edinburgh
EH3 7HL

Phone: 0303 123 1115

Email: Scotland@ico.org.uk

Candidate Privacy Notice
Scottish Government
December 2021

As part of any recruitment process, Scottish Government and associated public bodies collects and processes personal data relating to job applicants and applicants for public appointments.

This privacy notice explains how we collect, use and store your personal information in the context of applying for employment or a public appointment and for use in our recruitment processes. It also sets out the situations where we may share your personal data. The privacy notice also explains your rights and how to contact us. We may collect, process and store different personal data from you depending on what stage you are at in the recruitment process and whether you are applying for employment or you are applying for a public appointment.
The personal data we may collect from you includes:

- contact details such as name, title, addresses, telephone numbers, and personal email addresses
- copies of driving licence, passport, birth certificates and proof of current address, such as bank statements and council tax bills
- evidence of how you meet the requirements of the role, including CVs and references
- evidence of how you meet the Civil Service nationality rules and confirmation of your security clearance – this can include nationality details and information about any convictions, allegations and offences as part of Baseline Personnel Security Standard checks
- evidence of your right to work in the UK and immigration status
- diversity and equal opportunities monitoring information – this can include information about your race or ethnicity, religious beliefs, sexual orientation, disability and other 'special category data'
- information about your health, including any medical needs or conditions
- other information required for some applications, for example verification of qualifications
- if you contact us regarding your application, a record of that correspondence
- details of your use of our recruitment tools and services, such as your candidate profile and alerts for vacancies
- the status of your application and updates on how it moves forward

1. **Our lawful basis for using your data**

We process personal data throughout the application on different lawful bases.

For Employment and Public Appointments:
Contract Processing your data is necessary to move your application forward before signing a contract of work. This concerns employment or pre-employment checks.
Legal obligation The law requires Scottish Government to check that candidates are entitled to work in the UK.

Public task When we carry out National Security vetting for some roles, we have to process personal data to perform a task that's in the public interest or in the exercise of our official authority.
Processing criminal convictions and sensitive information We collect, use and hold sensitive information such as criminal convictions on the lawful bases of contract, legal obligation and public task.
Public Task When the selection panel requires to discuss with you any issues raised concerning conflicts of interest and time commitment. Processing your data is necessary to check your identity and credentials prior to taking up a public appointment
Legal obligation For anonymised reporting in line with the Equality Act 2010 and reporting to the Ethical Standards Commissioner
For the appointment letter Processing your data will be necessary to provide you with the terms of appointment.

2. **Processing special category data**

Personal data is defined as 'special category' when it reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. It includes:

- data concerning health
- data concerning someone's sex life or sexual orientation

We process this data when it's necessary for reasons of substantial public interest for the exercise of our functions. This applies to information about criminal convictions, allegations and offences during baseline security clearance checks.

3. **Why we need your data**

We need your data in order to:

- move your application forward
- check that you're the right candidate for the role
- get in contact with you
- send you notifications for vacancy roles or job or public appointment alerts

4. **How your personal information is collected**

We usually collect your personal information when you enter it in iCIMS. We might also collect information from third parties.
These include:

- former employers and people named by candidates as references
- Disclosure Scotland

5. **Employment Reserve lists**

We maintain a reserve list of candidates who met our requirements but were not successful in securing the specific post they applied for. We'll ask for your consent to be added to this list. We will refer to the list when other roles are advertised and will contact you if you match the role. We will ask for your consent before putting you forward for the role.

6. **Data sharing**

Personal information you provide in the recruitment process will be made available to Scottish Government and our additional data processors, Capita and Amiqus. The following information will be shared with our additional data processors depending on their role:

- contact details such as name, title, addresses, telephone numbers, and personal email addresses
- copies of driving licence, passport, birth certificates and proof of current address, such as bank statements and council tax bills
- evidence of how you meet the requirements of the role, including CVs and references
- evidence of how you meet the Civil Service nationality rules and confirmation of your security clearance – this can include nationality details and information about any convictions, allegations and offences as part of Baseline Personnel Security Standard checks
- evidence of your right to work in the UK and immigration status
- other information required for some applications, for example verification of qualifications
- if you contact us regarding your application, a record of that correspondence
- details of your use of our recruitment tools and services, such as your candidate profile and alerts for vacancies
- the status of your application and updates on how it moves forward

If you are successfully recruited for employment or a public appointment, we will upload your details to our HR system.
Employees will sign a contract of employment and agree to additional terms on how your data is handled and stored.
We will also share your data for statistical analysis (it will be anonymised first) if we are required to do so by law – for example, for public interest, by court order, or to prevent fraud or other crime.
Where Scottish Government is managing the recruitment of employees or of public appointees on behalf of a public body or, we will share your information with that public body, who will be the data controller.

7. **Transferring information to iCIMS outside the UK**

Our data processor, iCIMS, is based outside the UK, so your data might be transferred and stored securely outside the UK however will remain within the EU. Where that is the case it will be protected through the use of Model Contract Clauses. The following information will be shared with iCIMS:

- contact details such as name, title, addresses, telephone numbers, and personal email addresses
- evidence of how you meet the requirements of the role, including CVs and references
- evidence of how you meet the Civil Service nationality rules and confirmation of your security clearance – this can include nationality details and information about any convictions, allegations and offences as part of Baseline Personnel Security Standard checks
- other information required for some applications, for example verification of qualifications
- if you contact us regarding your application, a record of that correspondence
- details of your use of our recruitment tools and services, such as your candidate profile and alerts for vacancies
- the status of your application and updates on how it moves forward

8. **Data security**

We have put in place measures to protect the security of your information.
Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.
We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we only give access to your personal information to those employees, agents, contractors and other third parties are involved in the recruitment process.
We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

9. **Data retention**

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for - including legal, accounting, or reporting requirements. This will depend on:

- the amount, nature, and sensitivity of the personal data
- the potential risk of harm from unauthorised use or disclosure of your personal data
- the purposes for which we process it
- whether we can achieve those purposes in other ways

For recruitment to employment the retention period for documents supporting recruitment, application and sifting the retention period is 2 years.
For recruitment to public appointments the retention period for documents supporting the public appointments process is 5 years.
If you are unsuccessful, personally identifiable data is removed 2 years after your most recent application. You can request the deletion of your personal information by contacting us at ScottishGovernmentrecruitment@gov.scot.

10. **Your rights**

You have the right to:

- request access to your personal information (known as a 'data subject access request') - you'll receive a copy of the personal information we hold about you, so you can check that we are lawfully processing it. It also allows you to request an electronic copy of any data you have provided in a structured, commonly used and machine-readable format
- request that we correct incomplete or inaccurate personal information that we hold about you
- request we delete or remove your personal information - you can do this when there is no good reason for us to keep it - you can ask us to delete or remove your personal information where you have exercised your right to object to processing (see below)
- withdraw your consent for any data processed under the lawful basis of consent (see below)
- object to the processing of your personal information where we are relying on the legal basis that we are carrying out our public task (see legal bases above)
- request we restrict the processing of your personal information - you can ask us to stop processing your personal information, for example if you want us to establish its accuracy or the reason for processing it

To make any of these requests or to ask us to transfer a copy of your personal information to another party, contact the Scottish Government Resourcing team at ScottishGovernmentrecruitment@gov.scot. Please note that these rights are not absolute and will be processed on a case by case basis.

11. **Accessing your data**

You will not have to pay a fee to access your personal information or to exercise any of the other rights. However, if your request for access is clearly unfounded or excessive we may refuse the request.
In some cases we will need some information to confirm your identity. This is to ensure that your personal information is not disclosed to someone who has no right to access it.

12. **Questions and complaints**

If you have concerns about the way we process and handle your personal information, in the first instance you should raise your concerns to the People Directorate:

Resourcing Team
People Directorate
Scottish Government
Saughton House
Broomhouse Drive
Edinburgh
EH11 3XD

If you are not satisfied with the response, you can escalate to Scottish Government Data Protection Officer by email to DataProtectionOfficer@gov.scot

If you are not satisfied with the response or believe we are not processing your personal data in accordance with the law you may make a complaint to the Information Commissioner's Office (ICO):

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

13. **Changes to this privacy notice**

We may change this privacy notice. When we make changes to this notice, the 'last updated' date at the top of this page will also change. Any changes to this privacy notice will apply to you and your data immediately. If these changes affect how your personal data is processed, we will take reasonable steps to let you know.

14. **National Fraud Initiative in Scotland**

National Fraud Initiative in Scotland: Privacy notice (audit-scotland.gov.uk)

1. Redacting information

Redaction is the process of blanking out information on a document before it is released. This applies to individual words, sentences or whole sections of a document. Redaction should be done by a person who has knowledge of the subject matter to decide which material should be exempt.

When redaction is used on Freedom of Information requests (FOI) or Environmental Information Regulation requests (EIR) you need to explain to the applicant which exemptions have been applied and why. Redaction may also be needed when dealing with subject access requests.

2. Redaction guidance

You should always carry out redaction on a copy of the document, leaving the original intact. Never redact the master or original version of an electronic record – make a copy.

Delete any intermediate versions and only keep the original and redacted version of the document.

Spacing should not indicate the missing information. Words should not be visible or be able to be guessed due to incomplete redaction. Hold the paper up to the light to check.

3. Hard copy

Photocopy the original and block out the sensitive material using a black marker pen or quality correction fluid.

Photocopy the document again for release.

4. Electronic documents

Make a copy, remove all sensitive information and replace it with **[redacted]**. Print the redacted version. If an electronic version is needed, scan in the printed version as a pdf.

In Microsoft Office (Word, Excel, PowerPoint), you **must not** use the highlighter tool to highlight the text in black to 'hide' it. The highlighter tool does not properly redact information.

If the highlighter tool has been used, copying and pasting can reveal the sensitive information even if the document has been converted to a PDF.

5. PDFs

You can redact from PDFs if you have Adobe Acrobat Pro.

Make an electronic copy using Adobe Acrobat. Use the text touch-up tool to replace the redacted information with a redaction marker **[redacted]**.

For help, see the Adobe Acrobat redaction guidance or email the central scanning unit.

6. Word documents

Make an electronic copy and remove all sensitive information. Replace it with **[redacted]**. Print the document as a pdf – this is the redacted document.

7. Spreadsheets

Make an electronic copy by exporting the document as a .csv format file and remove all sensitive information. Replace it with **[redacted]**.

The redacted version can be reimported to the spreadsheet.

8. Help and support

Contact the data protection and information assets team for further advice on data protection.

Scottish Procurement

Data Processor - Contract Assurance Assessment

Service Provider Name (Data Processor)	
Contract / Framework Agreement Title	
Duration of Contract/Framework Agreement (Dates)	

Introduction

The purpose of this document is for the supplier, when they are acting as a Data Processor for the Scottish Ministers (as Data Controller) to provide assurance that they are handling personal data in compliance with the General Data Protection Regulation (GDPR) and other relevant data protection legislation.

All questions should be answered from the context of your company operating as a Data Processor under the Contract/ Framework Agreement. Further information on GDPR can be found on the Information Commissioner's website :

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/data-processors/

1. Please confirm that your business has registered with the Information Commissioner's Office**.**
[enter yes/no]

2. Please confirm that your business has an **information security policy** supported by appropriate security measures.
[enter yes/no and provide brief details]

3. Please confirm that your business has an appropriate **data protection policy.**
[enter yes/no and provide brief details]

4. Please confirm that your business has nominated a data protection lead or Data Protection Officer (DPO).
[enter yes/no and provide details]

5. Please confirm that your business manages information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively.
[confirm yes/no and provide brief details]

6. Please confirm that your business has implemented appropriate technical and organisational measures to show you have considered and integrated data protection into your processing activities.
[enter yes/no and provide high level details]

7. Please confirm that your business has conducted an information audit to map data flows.
[enter yes/no]

8. Please confirm that your business has processes to ensure that the personal data you hold remains accurate and up to date.
[enter yes/no and provide high level details]

9. Please provide high level details of how you ensure persons authorised to handle personal data are properly trained, fully aware of their obligations in maintaining confidentiality of personal data, and that this awareness is maintained?
[provide brief details]

10. Please provide high level details of how you ensure that only staff who have a need to access or handle personal data do so and explain how you prevent unauthorised access by staff and contractors that are not authorised to access the data?
[provide brief details]

11. Please detail your security measures in place for storing personal data. *This could include back-up procedures, encryption, secure file storage, levels of security etc.* Please include the actual tools/formats/storage types used to hold each aspect of electronic data.
[provide brief details]

12. Please confirm where, geographically, any physical/paper and electronic personal data will be both processed and stored and (where applicable) backed up to? What security measures are in place in these locations?
[provide brief details]

13. Please confirm that your business has a process to routinely and securely dispose of personal data that is no longer required in line with agreed timescales as stated within your contract with the data controller.
[enter yes/no and provide brief details]

14. If you intend to use or are using third parties to process personal data in the delivery of services under the contract/ framework, you must seek prior written authorisation from the data controller. Please confirm that you have the written consent of the Scottish Ministers to use a sub-processor for the processing of personal data in relation to the contract/ framework agreement. What processes are in place to safeguard data processed by any third parties?
[enter yes/no and provide brief details]

15. Please provide high level details of your process for identifying, reporting, managing and resolving any personal data breaches and in particular how you would interact with the purchasing authority where their personal data has, or may have been, breached.
[provide brief details]

16. Please confirm that your business has procedures to respond to a data controllers' request to suppress the processing of specific personal data.
[enter yes/no and provide brief details]

17. Please confirm that your business can respond to a request from the data controller for the supply of the personal data you process in an electronic format? Please also confirm that your business has a process to respond to a data controller's request for information (following an individual's request to access their personal data).
[enter yes/no and provide brief details]

18. Please confirm that your business has documented what personal data you hold in relation to the contract/ framework agreement, where it came from, who you share it with and what you do with it.
[enter yes/no and provide brief details]

19. Please provide high level details of your process for advising the purchasing authority of any material changes to the information set out above?
[enter information here]

This document should be read and applied alongside the terms and conditions of contract and in particular, the clauses that relate to personal data protection. The document should be signed by a senior manager within the company qualified and empowered to understand the matters concerned and with the authority to sign this document on behalf of the Service Provider.

I hereby confirm on behalf of my company that I am authorised to complete this information and that the information provided is accurate and complete.

For and on behalf of:	[enter supplier name]
Name:	
Position:	
Date:	