Scottish Government
Riaghaltas na h-Alba
gov.scot

Scottish Government Data Protection training course

Scottish Government
Riaghaltas na h-Alba
gov.scot

Contents

Must Read 3

1. What is personal data? 4

2. What are our legal obligations under the GDPR? 8

3. Handling personal data 14

4. How should the Scottish Government handle a request for personal data? 19

5. How do I handle data in certain circumstances and where can I find further information? 21

Must Read

⚠ You need to use the e-Learning platform for the assessment

The Scottish Government's Data Protection training course consists of 5 sections of information and a Mandatory Assessment.

- The 5 sections of information are available on the e-Learning platform *and* in this document. The content is the same across both formats.
- The assessment is *only* available on the e-Learning platform.

You have to do the assessment as part of the training. If you are using this document for the 5 sections of information, you still need to use the e-Learning platform to complete the assessment.

1. What is personal data?

1.1 Overview of Data Protection

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 regulates the processing of information relating to living individuals. This includes the obtaining, holding, use or disclosure of such information held, or likely to be held, by an organisation. The Scottish Government processes personal information and therefore is governed by these laws.

It gives individuals a legal right over how information about them is collected and used and it requires the Scottish Government to handle the information fairly and lawfully.

1.2 What is personal data?

The GDPR defines personal data as **information held by an organisation**, for example, the Scottish Government:

1) relating to a living individual
2) that identifies or is likely to identify an individual
3) in any physical format, such as paper, electronic format, audio, video or image.

The Freedom of Information (Scotland) Act 2002 has an exception under section 38 which may be applied to protect individuals from their personal data being released to the public.

Typical examples of records containing personal data are:

1) personnel files
2) interview notes, questionnaires, surveys
3) payroll system, access swipe cards, CCTV
4) medical, social, housing and education records

1.3 Recognising personal data

Here is a sample range of data found in the Scottish Government.

Personal data ✓

1) Case worker Grant Applications that include details of living individuals
2) Personal details, such as dates of birth, about current staff in personnel database records
3) Housing records and tenants records
4) CCTV footage
5) Names and addresses on invitation lists for events

***Not* personal data** ✗

1) Personnel files where you can ascertain that the person is no longer living. If it is difficult to ascertain whether a person is still alive, assume 84 years from date of data. Otherwise their death can be assumed to be 100 years after their birth, if known. See Section 3 below for more information
2) Aggregate statistical information about groups of the Scottish population
3) IT supplier contact information
4) Anonymous comments on visitor comment books/cards i.e. Historic Scotland sites that have visitor books
5) Census information from the 1800s

Be aware that while, in general, information about dead people does not fall under data protection law, any confidentiality agreements that limit disclosure should be reviewed with the person's heirs where applicable.

1.4 What are special categories of personal data?

Some categories of personal information are identified in the GDPR as requiring extra protection. These are called special categories of personal data, which was previously known as sensitive personal data. Any information in the following categories should be handled with particular care:

1) race/ethnic origin
2) political opinions
3) religious or other beliefs
4) trade union membership
5) physical or mental health
6) sex life and sexual orientation
7) criminal offences
8) current criminal proceedings
9) genetic data, and biometric data where processed to uniquely identify an individual (for example fingerprints, retina scans)

2. What are our legal obligations under the GDPR?

2.1 What does the GDPR say we must do?

The GDPR protects personal data in two ways:

1) it gives people the right to find out about whatever information is held on them and to be given that information;
2) it requires organisations (and their employees) who process personal data to comply with the Data Protection Principles (see subsection 2.3 below).

An organisation can be fined up to £18 million for a breach of the GDPR by the Information Commissioner's Office (ICO), the regulator for data protection in the UK.

There are two important roles in data protection: data controller; and data processor.

1) The **data controller** is the organisation who determines the purposes for, and manner in which, personal data is processed. They own the personal data and are responsible for, and must be able to demonstrate, compliance with the data protection principles.
2) The **data processor** is an organisation or person (apart from a person who is a direct employee of the organisation) who processes the personal data on behalf of the data controller.

If you are working on a project, program, or any activity that involves personal data being processed on your behalf, for instance by a third party supplier,

you must ensure there is a legally binding contract with that supplier that includes certain mandatory terms from the GDPR as to the roles and responsibilities of each party for data protection.

The Scottish Government Procurement Directorate can provide information about the contract terms.

2.2 Processing personal data

What do we mean by ‘processing’?

The GDPR defines ‘processing’ as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as",

1) collecting, recording, storing, organising, adapting or altering of the information or data
2) retrieving, consulting or using the information or data
3) disclosing the information or data by transmission, dissemination or otherwise making available
4) aligning, combining, blocking, erasing or destroying the information data
5) sharing data or linking data

2.3 The Data Protection Principles are:

2.3.1 Processed lawfully, fairly and in a transparent manner

From a practical perspective, this means that you must be able to meet a condition for processing, which is also known as the legal basis.

You must inform the data subject of the processing, and their rights. This is done through a privacy notice, which provides information on the purposes of the processing, the legal basis and lets them know about their rights and who to contact.

The legal basis is also called the "condition for processing", and you must be sure that the processing is necessary for one of the following:

1) a public task
2) contractual reasons
3) legal obligations
4) legitimate interests
5) the vital interests of the data subject (person).

Different conditions apply to special category personal data (see subsection 1.4 above).

If you are using consent as your legal basis, this must be freely given, able to be withdrawn, and explicit. This means that it must be indicated by a positive action by the data subject such as ticking a box or signing a form. You cannot rely on implied consent, for example a failure to respond indicating that a person does consent.

Consent is unlikely to be the correct legal basis to use in the Scottish Government due to the imbalance of power between the data controller and the data subject (person). For example, if you are applying for a social security benefit you have no choice about providing your personal data if you want to receive the benefit, so your consent would not be freely given.

You can read more about legal bases, privacy notices and consent on the data protection pages on Saltire. Links are included on the final page of this training module.

2.3.2 Collected for specified, explicit and legitimate purposes

If you are going to use the information for a purpose that is not the one you told the individual about when collecting their data, your new purpose should be compatible with the original purpose so that you are meeting the reasonable expectations of the individual.

For example, if you are gathering addresses in order to update an HR database, you cannot send the same people fund-raising brochures.

2.3.3 Adequate, relevant and limited

When you gather personal data, make sure that the information is relevant for your purpose and not excessive.

For example, if you have a web form people can use to sign up for regular 'SG News' emails, you will need to know their email address, but not their marital status.

2.3.4 Accurate and up to date

The individual has the right to have correct personal data held about them. Therefore, when someone updates their details, you must change, erase or rectify them without delay.

2.3.5 Kept for no longer than necessary

You must not keep data for longer than necessary for its specified purpose, although bear in mind that there is a provision in the Regulation for retaining data research, statistical and archiving in the public interest.

For example, if you hold CVs for students who volunteered on a project, you should destroy the CVs in a secure manner (e.g. shredding) once the project has finished. Whereas criminal records may be kept for longer periods.

2.3.6 **Processed in a manner that ensures appropriate security of the personal data**

When handling personal data, it is vital that you ensure the security of that data from loss or theft. Make sure that nobody unauthorised can gain access to the data, and that you are only disclosing personal data to the data subject (person) or their authorised representative. In practice this means checking that you are sending information to the correct person – getting it wrong is one of the most common incidents involving personal data.

In paper filing systems this can be a matter of locking the cabinet with the personnel files and making sure that only those who need access to these files for their work can get hold of the key. In an electronic environment this means that files need to be password protected, and access needs to be limited to those who need it in order to do their job. At all times check and double check details before sending personal data.

Any serious breach of security involving personal data must be reported by the Scottish Government to the Information Commissioner's Office (ICO) within 72 hours of us becoming aware of the breach. Tell the Data Protection and Information Assets team immediately about any incident so that it can be assessed, contained, and the ICO informed quickly if required.

Use the security incident reporting tool available via Saltire to make the report. You can also find out more about how to recognise an incident involving personal data on the data protection Saltire pages. Links are included on the final page of this training module.

2.3.7 **The controller shall be responsible for, and be able to demonstrate, compliance**

This means we have to be able to demonstrate that we comply with the GDPR. We do this through staff training (this e-learning module), internal audits, use of data protection impact assessments and through you registering your information assets on the information asset register and undertaking regular reviews.

Data protection impact assessments (previously known as privacy impact assessments) are a means to demonstrate this compliance and build public trust, and in some circumstances are a mandatory requirement of the GDPR. It is important that you start your data protection impact assessment early, and get your Information Asset Owner (IAO) involved, as they are responsible for managing information risk and must sign off the required assessments.

You can find out when, why and how to undertake a data protection impact assessment on the data protection Saltire pages. Links are included on the final page of this training module.

3. Handling personal data

3.1 How should I handle personal data?

The GDPR builds on an established framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to process personal data for business purposes with the rights of individuals in the protection of their personal data.

For the public, the GDPR gives individuals:

1) the right to ask an organisation for all information it holds on them
2) the right to be informed in writing whether personal data about them is held by the organisation and to have that information supplied to them
3) the right to have their data updated promptly
4) the right to ask the organisation to stop processing their data

For the Scottish Government, the GDPR:

1) requires it to keep records of certain details of the personal data which it processes, including the purpose that the data is processed under, and who it is shared with
2) requires it to protect the personal data the SG processes by ensuring that it is accurate and up-to-date; held only for the time it is needed for business purposes; held securely; and that it is restricted and only accessible to the persons who process the personal data
3) requires it to undertake data protection impact assessments

4) requires it to comply with the Data Protection Principles (outlined in Section Two of this tool)
5) requires it to respond to subject access requests (SARs) within one calendar month and
6) allows it to apply certain exceptions, such as information kept for research purposes

You can find out more about data sharing on the data protection pages and on the analytic profession data sharing, access and linkage pages on Saltire. Links are included on the final page of this training module.

3.2 Good practice in handling personal data

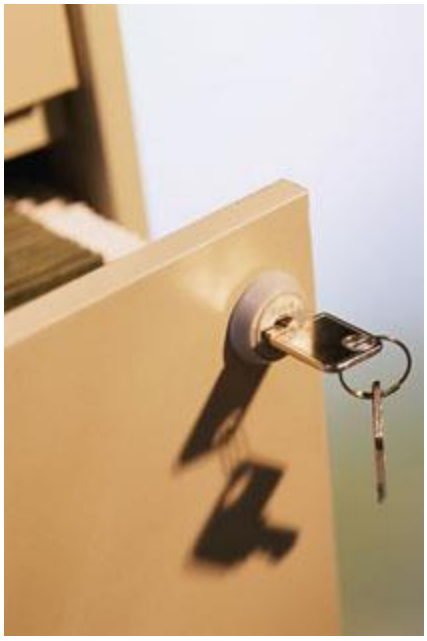
Before processing any personal data, you should consider the following issues:

1) Do you really need the information?
2) Is the information 'special category' personal data?
3) If there is a legal basis, are you able to justify processing the data?
4) Has the data subject been told that this type of data will be processed?
5) Where necessary, have you checked with the data subject that the data is accurate?

Are you satisfied that:

1) There is a business requirement for the Scottish Government to collect and retain the data.
2) Does processing meet one of the relevant conditions for processing?

3.3 How should I *store* personal data?



1) Make sure that the data is secure and in line with data handling procedures such as encryption
2) Ensure that the data you process is up to date and accurate
3) Securely dispose of any personal data you no longer need for its intended purpose, following the records management disposal schedules and the security procedures for the destruction of protectively marked material
4) If you transfer personal data, do it in a secure manner (e.g. encrypt electronic files) and ensure it is stored securely by the recipient

3.4 How do I *securely dispose of* personal data?

1) When personal data is no longer needed for the purpose it has been gathered for, it needs to be destroyed securely
2) Personal data on paper, CDs, hard drives, or film records should be disposed of by shredding or other means of permanent physical destruction
3) When deleting database records or other electronic records including personal data, see your IT support team for guidance on secure and authorised destruction. Remember that until all relevant back-ups have been overwritten, you will still hold personal data
4) You should document the fact that you are disposing of personal data (amount or volume, media, date and authorised person). If outsourcing to a shredding service or other disposal contract, ensure that they will handle and dispose of the data securely
5) Some records of enduring value may merit or require permanent preservation in the archives. The GDPR allows personal data gathered for other purposes to be further processed for archiving purposes in the public interest

3.5 Disclosure of personal data

Exemptions of the GDPR include the following.

You do not have to provide data to a subject if disclosure would:

1) threaten national security
2) prejudice the prevention or detection of crime
3) reveal another person's personal data without their informed consent, unless you have reasonable grounds for doing so
4) cause substantial harm or distress

You do not have to have the subject's consent to disclose personal data for the following uses:

1) law enforcement
2) taxation purposes
3) statistical or historical research if certain conditions intended to protect the interests of the subject are met
4) to obtain legal advice or for the purposes of legal proceedings

Note: Exemptions are usually applied on a case by case basis and must be carefully explained to the individual requesting subject access. Where personal data is kept solely for statistical, historical or research purposes, such as in an archive, and where the date of death of the individual is not clear, we must undertake reasonable efforts to confirm the death of that person or else assume death occurs at 100 years of age where the birth date is known. If birth dates of individuals are unknown, reasonable efforts should be made to ascertain the age of the person.

See Section Five for further guidance.

4. How should the Scottish Government handle a request for personal data?

4.1 What are subject access requests (SARs)?

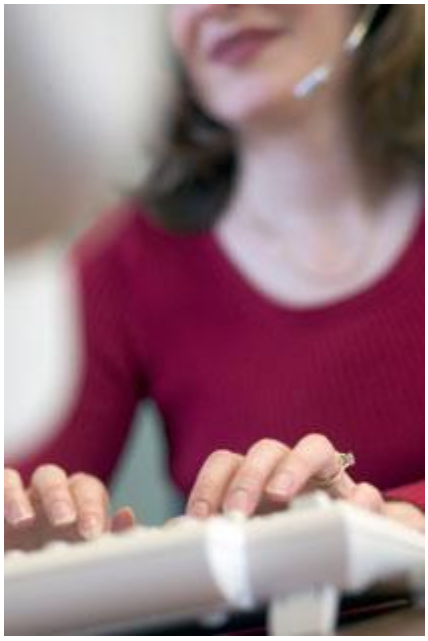
Under the GDPR, the data subject has the right to find out what information is kept about them. The data controller (organisation) must respond within one calendar month. These requests are called subject access requests. A SAR can come in any format, and in order for the organisation to respond to it, the request must:

1) include the name and address of the data subject
2) describe the information requested; if there is a need for further details to find the information, this can be asked of the person making the request
3) come from the data subject, or their authorised representative, to whom it pertains once proof of identity has been confirmed.

If you receive a SAR it is worth bearing in mind that:

1) no fee can be charged (unless under very specific circumstances). This is a change from the Data Protection Act, where an organisation could ask for a £10 fee
2) all subject access requests (SARs) should be sent to the Data Protection and Information Assets (DPIA) team. The DPIA team acts as a liaison between business areas and data subjects.

4.2 How do we respond to a data subject access request (SAR)?



1) As an organisation we cannot charge for subject access requests
2) The DPIA team verify the identity of the data subject (with assistance from the business when appropriate)
3) If necessary, further clarification from the data subject can be asked for
4) The DPIA team inform the appropriate business areas of the request, once they are certain that the enquirer has the right to obtain the data. The SG then has one calendar month to respond to the request

5. How do I handle data in certain circumstances and where can I find further information?

5.1 Case studies

5.1.1 **A customer of an internet mail order company has been the subject of a security breach. All his information, including his credit card details, was freely available on the internet for almost 24 hours before the site was taken down. He has had to freeze his credit card account and is worried that he will be a victim of identify fraud.**

- He does not trust the company not to do this again. They had been the cause of a previous security breach, and at that time he had asked to have his details removed from their customer list. He asks the court to award him compensation. The court may do so if the individual can show that he has suffered financial loss because of the breach of the Regulation.

5.1.2 **How long should the Scottish Government keep job applications from unsuccessful applicants?**

- Recruitment files for unsuccessful applicants should only be kept until the relevant appeal process is over (usually about 6 months) or until any external audit has been completed. Your HR or Personnel officer can confirm how long the appeal process lasts and when audit takes place.

5.1.3 **Under the Freedom of Information (Scotland) Act 2002 (FOISA), a member of the public asks for all of the personal data held on people who attended a particular event at the Scottish Government. Should you disclose that information?**

- You should withhold it under the exemption at section 38(1)(b) (3rd party personal data) of FOISA. For more guidance see Step 3 of the Step-by-Step Guide to Handling FOI/EIRs Requests.

5.1.4 **An academic has requested access to personal individual level data from an education survey run by SG statisticians, as they would like to do some research into educational attainment. They are going to publish a report which would not identify any individuals but have asked for some variables that do not appear to be required for the research topic. Should you provide the data requested?**

- You should take into account what people were told regarding what would happen to their data and whether they would expect their data to be shared. You must establish how the requested data will be stored, transferred, accessed and destroyed when made available to the researcher. If those who completed the survey would expect their data to be shared and the security criteria is met for personal data, the data can be shared, although variables that do not appear to be required for the specific project should not be shared.

5.1.5 **An academic has requested access to personal individual level data from an education survey and a housing survey run by SG statisticians, and they wish to link the two datasets. They are going to publish a report which would not identify any individuals. Should you provide the data requested and allow them to be linked?**

- You should take into account what people were told regarding what would happen to their data and whether they would expect their data to be shared and linked. You must establish how the requested data will be stored, transferred, accessed and destroyed for the duration of the project. You must also determine whether the datasets can be linked and how they plan to do this. If those who completed the survey would expect their data to be shared/linked, and the security criteria is met for personal data and the linked dataset, the data can be shared, although variables that do not appear to be required for the specific project should not be shared.

5.1.6 **If a colleague asks you for the contact details of someone who attended an event or with whom you are in regular contact, should you share that information?**

- You can share the information if the use that your colleague will make of it is compatible with your use of it. You should take into consideration what expectations the person would have had as to how the information about them would be used.

5.1.7 **Is it a problem if I accidentally leave copies or originals containing personal data in or near the photocopier?**

- Yes! You must protect personal data such as case files, names and addresses or HR-related information at all times. Be vigilant when copying!

5.1.8 **An individual's name is entered onto an employee fraud database without justification**

- The individual is understandably distressed to discover the implication that he is a fraudster. However, the information about him is removed from the database before he applies for a new job, and so he suffers no damage as a result of the error. The employee has no entitlement to compensation for distress alone.

5.2 Where do I go for further information on the Data Protection Act?

- Ask the Data Protection & Information Assets Team who are located in V Spur, Saughton House, Edinburgh, EH11 3XD.
- Further guidance is available on Saltire - My Workplace under "IT and information management".