

Data Protection Policy

November 2023



Contents

1. Introduction
2. UK GDPR Principles and Definitions
3. Types of Data
4. Law Enforcement Processing
5. Handling of Personal/Sensitive Information
6. Individual Rights
7. Employee Responsibilities
8. Data Security
9. Working From Home
10. Offences under the UK GDPR
11. Publication of Information
12. Subject Consent
13. Retention and Disposal of Data
14. Registration
15. Review of Policy
16. Communication & Contacts
17. Benchmarks Used in Policy Formulation

Appendix A : Data Breach Notification Procedures

1. Introduction

The Police Investigations & Review Commissioner (PIRC) is a data controller in terms of the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA). As a registered data controller, the PIRC has a statutory duty to comply with these provisions.

The UK GDPR and DPA 2018 operates in a number of ways. Firstly, it provides that anyone handling personal information must comply with the data protection principles. Secondly, it provides individuals with rights in relation to information which relates to them and places duties on data controllers to uphold these rights.

We are required to maintain personal data about individuals for the purposes of satisfying our operational and legal obligations. We recognise the importance of correct and lawful treatment of personal data as it helps to maintain confidence in our organisation and to ensure efficient and successful outcomes when using this data.

The types of personal data that we may process include information about current, past and prospective employees; applicants and enquirers; police officers and witnesses; suppliers and other organisations with which we have dealings.

Personal data may consist of data kept on paper, computer or other electronic media; all of which is protected under the UK GDPR/ DPA 2018. As a named authority within the Scottish Biometrics Commissioner Act 2020, the PIRC is obliged to process this type of information in accordance with the Commissioner's code of conduct. Therefore any information of this nature processed in accordance with the PIRC's role must be held in accordance with the Records Management Policy.

This policy summarises the key concepts contained in the UK GDPR/DPA 2018 and the responsibilities of the PIRC as a data controller.

In addition, the PIRC is a named competent body in the Data Protection Act 2018 as being likely to process personal information for Law Enforcement purposes. The additional requirements for compliance for this are incorporated in this policy.

2. UK GDPR Principles and Definitions

We must and do comply with the seven principles of the UK GDPR which are summarised below. Data must:

1. Be processed fairly and lawfully processed
2. Be obtained for a specified, explicit and legitimate purposes
3. Be adequate, relevant and limited to what is necessary.
4. Be accurate and kept up to date
5. Only be kept for as long as is necessary for the purpose for which it is processed.
6. Personal data must be secure
7. Accountability

Employees of PIRC who obtain, handle, process, transport and store personal data for us must adhere to these principles at all times.

Personal data

Personal data only includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information.

Controller

Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data.

Processor

Processors act on behalf of, and only on the instructions of, the relevant controller.

Processing

The term "processing" is very broad. It essentially means anything that is done to, or with, personal data (including simply collecting, storing or deleting those data). This definition is significant because it clarifies the fact that EU data protection law is likely to apply wherever an organisation does anything that involves or affects personal data.

Data Subject

an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Law Enforcement Processing

This strengthens the rights of data subjects, whilst ensuring that criminal justice agencies and others can continue to use and share personal data to prevent and investigate crime, bring offenders to justice and keep communities safe.

Special Category Data

Special category data is personal data that needs more protection because it is sensitive. Examples of Special Category Data include race, political opinions and health.

Biometric Data

Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images.

3. Types of Data

The UK GDPR lays down conditions for the processing of any personal data, and makes a distinction between personal data and "special categories of personal data".

The UK GDPR applies to ‘personal data’ meaning any information relating to an identifiable person. This definition provides for a wide range of information to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The UK GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

4. Law Enforcement Processing

As previously mentioned, the PIRC is a named competent body in the DPA 2018 and as such is subject to Part 3, Law Enforcement Processing when processing personal data for this purpose.

The six data protection principles set out in Part 3 differ from the six data processing principles in the GDPR in only one significant way: there is no requirement for personal data to be processed transparently, because of the risk of prejudicing criminal investigations.

Competent authorities or their processors must be able to distinguish between different categories of data subjects, such as suspects, convicts, victims and witnesses.

Data subjects have some of the same rights that they do under the GDPR, however the rights to rectification, erasure and restrict processing do not apply to “the processing of relevant personal data in the course of a criminal investigation or criminal proceedings”.

Moreover, certain rights under the GDPR, as outlined later in section 6 – such as the right to object and the right to data portability – do not exist under Part 3.

5. Handling of Personal/Sensitive Information

All staff should be aware that the PIRC is a data controller under the UK GDPR, understand the key provisions of the UK GDPR and the PIRC’s responsibilities as a data controller, and should take responsibility for ensuring that their actions are in compliance with the UK GDPR in their handling of personal information. As a data

controller, the PIRC will be processing special categories of personal data as part of its functions.

The PIRC will, through appropriate management and the use of strict criteria and controls:

- specify the purpose for which information is used and ensure consent is freely given and recorded
- collect and process information only to the extent that it is needed to fulfil operational needs or legal requirements
- endeavour always to ensure the quality of information used
- not keep information for longer than required operationally or legally
- always endeavour to safeguard personal information by physical and technical means
- protect personal data held on computers and computer systems by the use of secure passwords, which where possible, are changed periodically
- allow only designated users to access software and databases
- wherever possible restrict staff access to printers to secure printing
- ensure that personal information is not transferred abroad without suitable safeguards
- ensure that the lawful rights of people about whom the information is held can be fully exercised

In addition, the PIRC will ensure that:

- there is a designated Data Protection Officer with specific responsibility for data protection
- all employees understand that they are contractually responsible for following good data protection practice and all employees are appropriately trained to do so
- methods of handling personal information are regularly assessed and evaluated
- data sharing is carried out under a written agreement, setting out the scope and limits of the sharing, any disclosure of personal data will be in compliance with approved procedures

6. Individual Rights

Data protection legislation provides individual data subjects with a number of rights.

Right to be Informed

A key transparency requirement of the UK GDPR is for individuals to have the right to be informed about the collection and use of their personal data. Therefore the PIRC will provide individuals with information explaining how we will use any personal information we collect and process, including who we will share this with.

Right of Access

The UK GDPR gives individuals the right to make a request, in writing, for a copy of the personal data which the PIRC holds about them. This is known as a 'subject access request'.

If any staff receive what appears to be a subject access request, the request should be forwarded in the first instance to the mailbox informationrequests@pirc.gov.scot to be addressed by staff who are responsible for responding to Subject Access Requests. The PIRC has one calendar month from the day of receipt to respond to subject access requests under the UK GDPR, so such requests should be forwarded without delay.

Some information requested by individuals may be exempt from release. The UK GDPR contains a number of clearly defined exemptions, for example personal data processed for the prevention and detection of crime or the apprehension of prosecution of offenders.

Right of Rectification

The UK GDPR gives individuals the right to have personal data rectified. Personal data can be rectified if it is inaccurate or incomplete. Requests for rectification must be responded to within one month, whether action is being taken or not, following a request.

Right to Erasure

This right enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances.

Right to Restricted Processing

Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, PIRC is permitted to store the personal data, but not further process it. In some circumstances the PIRC's statutory obligations will not permit individuals this right, for example when undertaking an investigation at the request of Police Scotland or COPFS.

Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Right to Object

Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority. In some circumstances, however the PIRC will demonstrate legitimate grounds for the processing of personal information, and will explain to individuals where this applies.

Rights relating to automated decision making including profiling

Whilst individuals have this right, there are no current circumstances where this is relevant to the PIRC.

7. Employee Responsibilities

All employees must ensure that, in carrying out their duties, the PIRC is able to comply with obligations under the UK GDPR. In addition, each employee is responsible for:

- checking that any personal data that he/she provides is accurate and up to date
- informing of any changes to information previously provided, e.g. change of address
- checking any information that we may send out from time to time, giving details of information that is being kept and processed

Information stored on enquirers/applicants/employees should be reviewed regularly to ensure it is accurate and up to date. All documents, whether hand written or stored in emails (current or deleted) are potentially disclosable in the event of a subject access request.

8. Data Security

Personal data held by the PIRC which relates to others should be kept in accordance with an appropriate level of security, taking into account the nature of the information and the harm that might result from unauthorised disclosure.

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and both access and disclosure must be restricted.

All employees are responsible for ensuring that any personal data which they hold is kept securely and that personal information is not disclosed either orally, in writing or otherwise to any unauthorised third party.

All staff are required to ensure the security of documents or other material / productions when travelling away from the office. Documents relating to investigations must not be left unattended, in cars, unless absolutely necessary, and only where this can be stored safely. When leaving documents in a hotel room staff must ensure they are secured in the room safe where available.

It is appreciated that staff may have to take documents with them for the purposes of conducting interviews or undertaking investigations, however as the UK GDPR carries heavy penalties for loss of documents containing personal information, staff should take cognisance of security requirements.

When travelling away overnight, it may be best for staff to take laptops with them and access documents online, as laptops contain the ability to restrict access via encryption and other security measures such as password protection.

9. Working From Home

Many organisations continue to have staff to work from home, which was introduced during the pandemic. While Working From Home was once a legal requirement, staff are reminded to ensure that data protection principles are applied to home working using whatever means possible. As the organisation progressed to a hybrid model allowing a combination of working between home and office, the need to ensure the security of information remains crucial. Staff can be provided with resources such as lockable cases should they require them to protect the information they hold at home to carry out their duties. In addition, staff are also reminded to take care to restrict access to work information, ensuring that family members are protected in not viewing the information we process, which may be upsetting or distressing to them if they were to view it. Staff must also not permit others to use the laptop or other equipment provided to them for work purposes, and this can lead to the installation of malware which has the potential to infect the entire network.

10. Offences under the UK GDPR

The ICO have powers to administer fines of up to €20M depending on the severity of the offence. Offences relating to the breaching of the Act by failing to comply with one or more of the principles listed at 2 above. The PIRC's Data Breach Notification Procedures are outlined at Appendix A.

11. Publication of Information

Information already in the public domain is exempt from the Regulation. This would include, for example, information on employees contained within externally circulated publications.

Anyone wishing their details to remain confidential in such publications should contact the Head of Corporate Services (HoCS).

12. Subject Consent

Processing personal data relating to a living individual requires us to notify data subjects as appropriate, in most instances.

In some cases, explicit consent is required to process the data which will be recorded. Such processing may be necessary to carry out the functions of the PIRC and to comply with some of our policies, such as health and safety and equality and diversity, in which case our legitimate interests will apply.

Contracts of employment provide us with a lawful requirement to process personal data for the purposes of administering, managing and employing our employees. This includes: payroll, benefits, medical records, absence records, sick leave/pay information, performance reviews, disciplinary and grievance matters, pension provision, recruitment, family policies (maternity, paternity, adoption etc) and equal opportunities monitoring.

Information about an individual will only be processed for the purpose for which it was originally given. Employees and managers must not collect or store data which is not necessary or which is to be used for another purpose.

Members of the public requesting a Complaint Handling Review from us will be asked to provide their consent in order to allow us to provide the service they require. Whilst applicants have a range of rights outlined earlier, including the right to erasure, in some instances we may continue to retain personal information pertaining to an individual where there is ongoing activity and we require to limit this right in order to provide additional information in defence of our decisions.

Activities relating to Investigations we undertake are subject to the same UK GDPR, however any information which relates to processing personal information for the prevention, investigation, detection or prosecution of all criminal offences will be subject to Part 3 of the Data Protection Act 2018, Law Enforcement Processing. In general terms, we will be unable to oblige a request for erasure made by a data subject due to the purpose for which we are processing their information. In any case, we will inform the individual concerned and explain our legal basis for processing. Depending on the nature of an individual's involvement with the PIRC investigation, we may restrict some of the individual's rights if we consider this will prejudice the investigation.

13. Retention and Disposal of Data

Personal data must not be retained by the PIRC for longer than is required for the purposes for which it was collected.

Information will be kept in accordance with our Records Management Policy Retention Schedule. All staff are responsible for ensuring that information is not kept for longer than necessary. The Information Officer will carry out regular audits to ensure that the retention schedule is being adhered to.

Documents containing any personal information will be disposed of securely, and paper copies will be shredded.

14. Registration

The PIRC is registered in the Information Commissioner's public register of data controllers.

The UK GDPR requires every data controller who is processing personal data to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

15. Role of the Data Protection Officer

The UK GDPR introduces a duty for organisations to appoint a data protection officer (DPO) if they are a public authority or body, or if they carry out certain types of

processing activities. Further details on the role of the DPO can be found on the Information Commissioner Officer's web site, or by following [this link](#).

The Information Officer, as PIRC's Data Protection Officer has overall responsibility for ensuring compliance with the UK GDPR, for notifying and updating the Information Commissioner (or Scottish Biometrics Commissioner if this involves biometric information) of our processing of personal data, and for the monitoring and implementation of this policy on behalf of PIRC. The DPO can be contacted by emailing informationrequests@pirc.gov.scot.

16. Review of Policy

This policy indicates how the PIRC intends to meet its legal responsibilities for data protection. Any breach will be taken seriously and may result in formal disciplinary action. Any employee who considers that the policy has been breached in any way should raise the matter with his/her line manager or the HoCS.

This Policy is a formal PIRC policy and will be reviewed by the PIRC Senior Management Team regularly, or at least biannually to ensure compliance with statutory requirements. Any queries regarding this policy, or comments, should be addressed to the employee's line manager.

17. Implementation, Monitoring and Review of this Procedure

The Head of Corporate Services has overall responsibility for implementing and monitoring this procedure, which will be reviewed on a regular basis by the policy owner following its implementation and may be changed from time to time.

Any queries or comments about this procedure should be addressed to the HR@pirc.gov.scot

18. Benchmarks Used in Policy Formulation

- Previous PIRC Policy
- ICO Guidance

Version Control Data

Title:	Data Protection Policy
Version Number:	V7
Publish Internet/Pulse:	Both
Date of Approval:	November 2023
Summary of last modification:	Change GDPR to UK GDPR, further details and explanations added
Next Review Date:	November 2025

APPENDIX A – PIRC Data Breach Notification Procedures

The UK GDPR introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioners Office (ICO). This must be done within 72 hours of becoming aware of the breach, where feasible.

Failing to notify the ICO of a breach, when required to do so, can result in a significant fine of up to 10 million euros. The fine can be combined with the ICO's other corrective powers. It is therefore important to make sure there is a robust breach-reporting process in place to ensure the PIRC can detect and notify the ICO of a breach, on time; and to provide the necessary details.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the PIRC must also inform those individuals without undue delay.

We are also required keep a record of any personal data breaches, regardless of whether there is a requirement to notify.

Employees are reminded that personal information relating to individuals must not be disclosed to other people, either internally within the PIRC or externally unless we have the written consent of the individual, or we have a legal basis to do so.

What is a Data Breach ?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example:

Personal data breaches can include:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal data.

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk, then we must notify the ICO; if it is unlikely then we do not have to report it. However, even in cases which we decide we do not need to report the breach, we need to be able to justify this decision, and record it on our Breach Register.

Reporting a Breach

Any and all breaches of personal data must be reported to the Information Officer who is the PIRC's designated Data Protection Officer (DPO) under the UK GDPR. In the absence of the IO, the Information Coordinator should be approached. Under UK GDPR all data breaches of a sufficiently serious nature must be notified to the ICO within 72 hours of us becoming aware of the breach. Therefore there should be no delay in making this notification.

Low Level Breaches

Where the breach is considered to be a low level breach, for example an email sent to the wrong contact in Police Scotland, it is generally considered to be contained within the police IT system and therefore not at risk from unauthorised disclosure to a member of the public. This also applies to emails sent to an incorrect email address within the SCOTS email system. Nevertheless, in both examples, steps must be taken to both report this breach internally and provide all necessary evidence, in the format of the email sent in error. The incorrect recipient of the information must also be asked to delete the email from their email account. In some instances, an email response indicating the incorrectly sent email was undeliverable will suffice.

The Breach Register will be updated by the DPO, or Information Coordinator. This will include justification of why the breach does not require to be reported to the ICO.

Serious Breaches

For more serious breaches, we will need to assess both the severity of the potential or actual impact on individuals as a result of a breach, for example the loss of documentation, the loss of a USB memory stick containing personal information or emails sent to the wrong individual. These cases must be investigated more thoroughly.

The DPO will complete a Breach Report which documents how the breach occurred, what has been done to mitigate the risk and what steps will be taken to prevent a reoccurrence of the breach. The DPO will then notify the Information Commissioner and remain the main point of contact with her office. The ICO will want to know the following:

- What happened?
- When it happened?
- How it happened?
- How many people could be affected?
- What sort of data has been breached?
- What did you have in place that could have stopped it?
- What have you done to help the people this affects?
- What have you learned?
- How can you stop similar breaches in the future?

In addition to reporting serious breaches to the ICO, breaches are reported quarterly to the Audit and Accountability Committee as it has a role in providing robust scrutiny of the governance processes deployed by the PIRC

In the absence of the Data Protection Officer and Information Co-ordinator, the breach will be recorded by another qualified PIRC Data Protection Practitioner.

The individual(s) affected must also be notified where the breach is sufficiently significant as to be reported to the ICO. The DPO will liaise with management to consider the best way for this to be done and this is likely to differ in each case.

Further Action

As with any security incident, we will investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps. The DPO will agree the next steps with the Head of Service(s) affected. This will vary depending on how the breach occurred and the effect it has had on the individual and the organisation. This may involve changing procedures and/or providing additional training. However in some cases, it may result in disciplinary action.

If information has been deleted in error, early intervention is required to determine if this information can be reinstated from any backup system.

Partner Organisations

In circumstances where the PIRC uses another organisation to process personal data on our behalf, for example, payroll and pensions, that other organisation must inform us without undue delay as soon as it is aware of the breach.

This requirement allows us to take steps to address the breach and meet our breach-reporting obligations under the UK GDPR.

Where we use a processor, the requirements on breach reporting must be detailed in the contract between us and the processor.