pirc people plan

DATA PROTECTION POLICY

pirc

Police Investigations & Review Commissioner

CONTENTS

1. Introduction

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

The GDPR operates in a number of ways. Firstly, it provides that anyone handling personal information must comply with the six data protection principles laid down in the GDPR. 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 GDPR.

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

In addition, the PIRC is a named competent body in the Data Protection Bill as being subject to the Law Enforcement Directive (LED). The additional requirements for compliance with the LED are incorporated in this policy.

2. GDPR Principles and Definitions

We endorse and adhere to the seven principles of the 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.

3. Types of Data

The 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 GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The 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 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. Handling of Personal/Sensitive Information

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

5. Individual Rights

Right to be Informed

A key transparency requirement of the 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 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 passed in the first instance to the Information Officer who is responsible for responding to Subject Access Requests. The PIRC has one calendar month from the day after receipt to respond to subject access requests under the GDPR, so such requests should be forwarded without delay.

Some information requested by individuals may be exempt from release. The 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 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 individual have this right, there are no circumstances where this is relevant to the PIRC.

6. Employee Responsibilities

All employees must ensure that, in carrying out their duties, the PIRC is able to comply with obligations under the 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 enquirer/applicants 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.

7. 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.

8. Offences under the GDPR

The ICO have powers to administer fines of up to €20M depending on the severity of the offence.

9. Publication of Information

Information that is 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 HR & Corporate Services.

10. Subject Consent

The need to process data for normal purposes will be communicated to all data subjects as appropriate.

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.

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.

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 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 the Law Enforcement Directive (LED). 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.

11. Retention and Disposal of Data

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

Information will be kept in line with our Records Management Policy. 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.

12. Registration

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

The 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.

The Data Processing Officer has overall responsibility for ensuring compliance with the GDPR, for notifying and updating the Information Commissioner of our processing of personal data, and for the monitoring and implementation of this policy on behalf of PIRC.

13. Implementation, Monitoring and Review of this Policy

The Head of HR and Corporate Services (HHRCS) has overall responsibility for implementing and monitoring this policy, which will be reviewed on a regular basis following its implementation and additionally whenever there are relevant changes in legislation or to our working practices.

Any queries or comments about this policy should be addressed to the HHRCS.

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 HHRCS.

14. Communication & Contacts

This policy will be shared with all PIRC staff and may be published for access by prospective candidates on our website.

Queries should be addressed to:

Head of HR & Corporate Services
Hamilton House
Hamilton Business Park
Hamilton
ML3 0QA

Phone: 01698 542900

Email: enquiries@pirc.gov.scot

15. Benchmarks Used in Policy Formulation

- None – new Regulation

16. Review of Policy

This Policy is a formal PIRC policy and will be reviewed by the Head of Department Group on an annual basis.

Version Control Data

Title:	Data Protection Policy
Author:	Janice Carter, Information Officer
Approver:	Sharon Smit, Head of HR & Corporate Services
Version Number:	Version 1.1
Date of Approval:	April 2019
Summary of last modification:	Change to PIRC email address
Next review date:	April 2020