AN tÚDARÁS PÓILÍNEACHTA
POLICING AUTHORITY

Data Protection Policy

25 May 2018

Contents

Foreword

The objective of this policy is to provide information regarding the Authority's obligations under Data Protection legislation. There are related legal obligations arising from the legislation covering Freedom of Information, the National Archives and Official Secrets.

A data breach may have serious consequences for the person whose data is breached, for the organisation responsible for the breach, and, in some circumstances, for individuals who may be responsible for the breach. Breaches can be due to systems failures, individual error, or deliberate breaches by internal or external people using a range of techniques.

The Policing Authority is responsible for having a policy and systems in place to support it, and to audit for compliance.

All Members and staff of the Authority have personal responsibility to make themselves aware of this policy, and, if handling personal information, to ensure compliance with it.

The Data Protection Rules

The Office for the Data Protection Commissioner outlines eight data protection rules which describe the requirements and responsibilities of the Authority under Data Protection legislation with regard to personal information:

1. Obtain and process the information fairly;
2. Keep it only for one or more specified and lawful purposes;
3. Process it only in ways which are compatible with the purposes for which it was given;
4. Keep it safe and secure;
5. Keep it accurate and up-to-date;
6. Ensure it is adequate, relevant and not excessive;
7. Retain it no longer than is necessary for the specified purpose or purposes; and
8. Give a copy of his/her personal data to that individual, upon request.

Members and staff are responsible to ensure that they are familiar with these rules and comply with them.

On becoming aware of any issue, potential or actual, staff must raise it with their manager and with the Data Protection Compliance Officer.

The Authority's primary and most important aim is to prevent data breaches and to have a prompt system for reporting any breaches that occur within the 72 hour deadline.

1. Introduction

The Policing Authority is committed to protecting the rights and privacy of individuals in accordance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), the Data Protection Acts 1988, 2003 and 2018. These Acts give effect to the Council of Europe Data Protection Conventions.

Data Protection is the manner in which the privacy rights of individuals are safeguarded in relation to processing their personal data. Personal data covers **any** information that relates to an identifiable, living individual. The data may be in electronic or manual format, or exist as images, and may be held on computers or in manual files.

The policy applies to all Data Subjects whose personal data is held by the Authority, including staff details and data relating to clients and members of the public.

This policy applies to the Policing Authority. Its development took account of best practice using resources made available by the Data Protection Commission.

This policy applies to all data held by the Policing Authority. This includes:

- all electronic and paper records;
- CCTV images in the premises occupied by the Authority;
- logs or registers in relation to access through controlled doors by staff, visitors, contractors and others; and
- footage of meetings in public.

2. Key definitions used in the Data Protection legislation

The following are definitions of the key terminology in the legislation and which are used in this policy

Automated Data means any information stored on computer or information recorded with the intention of putting it on computer. It includes not only structured databases but also emails, office documents or CCTV images.

Data means information in a form which can be processed. It includes both automated data and manual data.

Data Controllers are those who either alone or with others control the contents and use of personal data. Data Controllers can either be legal entities such as companies, Government Departments or voluntary organizations, or they can be individuals such as GPs, Pharmacists or Sole Traders.

Data Processor is a person who processes personal data on behalf of a Data Controller, but does not include an employee of the data controller who processes such data in the course of his/her employment. Again, individuals such as GPs, Pharmacists or Sole Traders are considered to be legal entities.

In the context of the Authority, this means information that is being processed for the Authority by the Department of Justice and Equality, the National Shared Service Office (including Peoplepoint and PSSC) and Financial Shared Services (FSS), for example, when a new staff member joins.

Data Retention refers to the continued storage of personal data by the organisation for compliance or business reasons.

Data Subject is an individual who is the subject of personal data.

Manual Data means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system – this includes temporary folders.

Personal Data means data relating to a living individual who is or can be identified either from the data or in conjunction with other information that is in, or is likely to come into the possession of the data controller. This can be a very wide definition depending on the circumstances.

Processing means performing any operation or set of operations on data, including:

- Obtaining, recording or keeping data;
- Collecting, organizing, storing, altering or adapting the data;
- Retrieving, consulting or using the data;
- Disclosing the information or data by transmitting, disseminating or otherwise making it available;
- Aligning, combining, blocking, erasing or destroying the data.

Relevant Filing System means any set of information that, while not computerized, is structured by reference to individuals, or by reference to criteria relating to individuals so that specific information is accessible.

Sensitive Personal Data refers to specific categories of data which are defined as data relating to a person's racial origin, political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

3. The Eight Rules of Data Protection

All personal data held by the Authority must be treated in compliance with the following eight rules.

Rule 1 – Obtain and Process information fairly.

The Policing Authority is committed to collecting information fairly and ensuring that it is processed fairly. We are committed to only collecting personal data necessary to allow us to carry out our functions as set out in legislation. To comply with this rule, all forms whether electronic or paper requesting information from any data subject, including for example a member of the public, should only request information for which there is a specific business need and legislative basis.

Rule 2 – Keep it only for one or more specified, explicit and lawful purposes.

The Authority will only keep data for purposes that are specific, lawful and clearly stated and data will only be processed in a manner compatible with that purpose.

In order to comply fully with the rule, the Authority must let the person know the reason why we are collecting and retaining their data. . If data collected is to be used for statistical purposes, this should also be stated. The purpose for which data is being collected must be a lawful one.

Rule 3 – Use and disclose it only in ways compatible with these purposes.

The Authority will ensure that personal information collected for a particular purpose will not be used for any other purpose. The Authority must also ensure that personal data is not divulged to any third party, except in ways that are specifically allowed for the stated purpose. If contact details of a data subject are collected these details can only be used for the purpose for which the information was collected. The Authority's email distribution list includes a description on each tab for this purpose to ensure that the purpose of each category of information is clear and transparent.

To comply with this rule we must ensure that data is only transferred to another department or body on the basis of a statutory requirement where there is a legal basis for this sharing. When data sharing is being considered the following principles should also be considered:

Transfers of personal data to agents of the Authority, who are carrying out operations upon the data on behalf of the Authority and not retaining it for their own purposes, do not constitute "disclosures" of data for the purposes of the Act. (Examples of such transfers would include the transfer of staff data to an outsourced provider for payroll administration purposes, Even though such transfers would not involve "disclosure" of personal data, the data controller might also have to consider whether the data has been "fairly obtained" for these purposes.

The restriction on processing of personal data (including disclosure to a third party) is lifted in a limited number of circumstances, specified in section 8 of the Data Protection Acts, where the right to privacy must be balanced against other needs of civil society, or where the processing is in the interests of the individual.

Transferring Personal Data Abroad

Where data is being transferred abroad it must always be done in accordance with specified international agreements. Specific guidance on the *Safe Harbour* countries is available from the Authority's Data Protection Officer.

There are special conditions that have to be met before transferring personal data outside the European Economic Area (all EU countries plus Norway, Iceland and Liechtenstein), where the importing country does not have an EU approved level of data protection law. This is termed a finding of adequacy. In such a case, one of the following conditions must be met if a transfer is to take place. Either the transfer must be:

- consented to by the data subject;
- required or authorised under an enactment, convention or other instrument imposing an international obligation on this State;
- necessary for the performance of a contract between the data controller and the data subject;
- necessary for the taking of steps at the request of the data subject with a view to his or her entering into a contract with the data controller;

- necessary for the conclusion of a contract between the data controller and a third party, that is entered into at the request of the data subject and is in the interests of the data subject, or for the performance of such a contract;
- necessary for the purpose of obtaining legal advice;
- necessary to urgently prevent injury or damage to the health of a data subject;
- part of the personal data held on a public register; or
- authorised by the Data Protection Commissioner, which is normally the approval of a contract which is based on EU model contracts.

As the legislation on the transfer of data abroad is complex, the Data Protection Officer must be consulted prior entering into any arrangement to send personal data abroad.

Consideration in relation to any potential transfers abroad of personal data should be considered during the impact analysis of any new project or during any procurement process that could involve such transfers, for example where a service may be provided by a company based outside the jurisdiction or where a service provider may have reason to store personal data in another country or on the cloud.

Rule 4 – Keep it safe and secure.

The Authority will maintain the highest standards of technical and physical security to ensure that we protect confidential personal data while we hold and process it. This responsibility is discharged in structural terms by the IT Division of the Department of Justice and Equality on the Authority's behalf but primarily by the actions of staff members. This will be done by ensuring:

- Access to the information is given to staff at the appropriate authorised level and this is done in accordance with an outlined ICT policy;
- All computer systems are password protected: passwords must never be disclosed to any individual including other employees in the Authority or the Department;
- All portable devices used to transport data are password protected and encrypted;
- Where sensitive personal data is being sent via email measures are taken to ensure that it is sent securely – such as a password protected attachment – in accordance with the Acceptable Usage Policy or in consultation with the ICT Division of the Department of Justice and Equality or other ICT service provider as applicable;
- All premises will be kept secure, in particular when they are unoccupied;
- Regular awareness sessions are arranged for staff to ensure that they are aware of their responsibilities under the Data Protection Acts;
- Individual staff members have a key role in keeping data safe and secure through this policy in conjunction with the Acceptable Usage Policy;
- In the event of theft of a mobile device while not password secured the ICT section of the Department should be immediately contacted by the user and asked to remotely wipe the phone urgently.

Rule 5 – Keep it accurate, complete and up to date.

The Authority must ensure that all personal data is kept fully up to date and accurate.

The Authority must ensure that all clerical and computer procedures are adequate to ensure the highest levels of data accuracy. It is the right of every individual to have any inaccurate data held by the Department updated or erased as appropriate.

Procedures/Systems in Divisions will be reviewed by the Data Protection Compliance Officer or by Internal Audit. A catalogue of systems is under development which will, among other reasons, identify the holding of personal information.

Controller processor agreements

Controller / Processor agreements must be put in place with any organisation with whom the Authority shares personal data. This agreement should form part of the contract entered into with service providers arising from any procurement process. Agreements must describe the subject and duration of processing, the purposes of processing, the types of personal data and data subjects and the controller's rights and obligations.

Rule 6 – Ensure that it is adequate, relevant and not excessive.

In order to comply with this rule the Authority will put measures in place to ensure that the data sought and held is the minimum amount required for the specified purpose. The data held must be adequate, relevant and not excessive in relation to the purpose for which it is sought. All requests for data must clearly state the Authority's business need for the collection of such data.

Rule 7 – Retain it no longer than is necessary

Data must not be retained for longer than necessary and must not be retained once the initial purpose has ceased. As long as personal data is retained by the Authority, the full obligations under the Data Protection Acts are attached to it.

The Authority's Policy in relation to data retention is as follows:

- A set of agreed data retention periods have been put in place for the Authority following consultation with each division. The Authority's Register of Data Subjects specifies the approved retention periods for each data category. This ensures clarity in regard to the length of time data is kept and why it is being retained. As the Authority is subject to the National Archives Act 1986 and the Freedom of information Act 2014 the requirements of these Acts has also been taken into account when considering the agreed retention periods;
- This formal Data Retention Policy for the Authority has been put in place following consultation with divisions within the Authority;
- It is the responsibility of each Head of Division to ensure that personal data in their area is permanently deleted in compliance with the approved retention periods. The relevant Head of Division should be consulted by staff prior to deleting any such records;
- On rare occasions personal data that is not appropriate to the Authority's business requirements may be received from the Garda Síochána in response to a request from the Authority. The staff member responsible for monitoring receipt of such information should review all material received pursuant to such requests for the existence of any such personal data and bring the it to the attention of their line manager and ensure it is deleted. At the

earliest opportunity a response should be sent to the Garda Síochána requesting that the personal data be redacted and the material re-sent.

- On rare occasions personal data that is not appropriate to the Authority's business requirements may be received from a member of the public. The staff member responsible for monitoring external correspondence should review all correspondence received for the existence of any personal data and should bring it to the attention of their line manager or the Data Protection Officer following which an appropriate response should be sent to the sender. For example where the material was intended for another recipient the sender should be advised accordingly and the email or letter deleted from the system and any paper copies of the letter or email should be shredded.

Rule 8: Give a copy of his/her personal data to that individual on request

Under the Data Protection Act, the Authority has a responsibility, on receipt of a written request, to provide an individual with the following:

- A copy of the data being kept about him/her;
  - A description of the purpose for which it may be held;
  - A description of those third parties to whom the data may be disclosed; and
  - The source of the data unless this would be contrary to the public interest.

Please note that a Data Protection Request does not need to refer to the Data Protection Acts in order to be a valid request.

4. Roles and Responsibilities

Table 1 sets out the roles and responsibilities for data protection in the Authority:

Table 1 Roles and Responsibilities for Data Protection

Role	Responsibility
All employees and Authority Members	• All employees and Authority Members have personal responsibility for ensuring compliance with the principles of the Data Protection Acts and for adhering to the Authority's Data Protection Policy. • All employees and Authority members are responsible for ensuring that they are fully aware of and complying with the contents of this policy on a daily basis.
Line Managers	Responsibility for ensuring compliance with the Authority's Data Protection Policy within their Division. They are also responsible for ensuring that staff in their area are aware of the policy and have received Data Protection Awareness Training as part of their Performance Management and Development System

Data Protection Officer	• The development of and implementation of, and support arrangements for, the Authority's Data Protection Policy. • Dealing with any data protection queries that arise and being available to provide guidance to divisions on how to comply with data protection rules and to advise where specific issues arise. • Responsible for reporting data breaches (if any occur) to the Office of the Data Protection Commissioner. • Promoting data protection awareness across the Authority.
Internal Audit	The Internal Audit function is responsible for providing reasonable assurance that the accounting systems, procedures and controls operated by the Authority are adequate and are being complied with. It is not the primary role of Internal Audit to ensure that divisions are data protection compliant; however as part of its audit work it may carry out periodic data protection audits in relation to the Authority as a whole or to specific areas within the Authority.
Human Resources	Data protection training will be provided to new staff as part of their induction programme.
Audit and Risk Management Committee	The Charter of the Audit and Risk Management Committee provides that the Committee shall: • Advise on the scope and effectiveness of the Authority's internal control frameworks implemented by management, including information technology security and control; • Assess whether internal control recommendations made by the internal and external auditors have been implemented by management; and • Advise on the controls and processes implemented by management to ensure that the financial statements derive from the underlying financial systems, comply with relevant standards and requirements and are subject to appropriate management review.
Chief Executive	The Chief Executive in her role as Accounting Officer has overall responsibility for the Authority's data and implementation of the policy in terms of data protection.

5. Training, Awareness and Resources

Data protection training and information sessions have been held for staff of the Authority. All staff involved in handling personal information must attend one of these sessions and familiarise themselves with this policy. In addition, the Data Protection Commissioner's website is an invaluable resource. It can be accessed at www.dataprotection.ie. Another useful website for GDPR is http://gdprandyou.ie/.

The Department of Justice and Equality has established a network of Data Protection Officers in the Department's offices and agencies. The key objective of this is to provide an opportunity to keep up

to date and share experiences within the Justice sector. This will be progressed in parallel with arrangements being put in place to implement the new Data Protection Regulation and Directive.

6. Audits of Data Protection

The work programme for Internal Audit will include periodic reviews of the Authority's data protection procedures as part of their ongoing internal audit review process. The office of the Data Protection Commissioner may also carry out audits and inspections on a periodic basis.

7. What to do in the event of a breach

A data protection breach can occur for a number of reasons:

- Failure of protective systems or equipment;
- Theft or loss of data/equipment/paper that data is stored on;
- Human error;
- Authority systems being hacked or by outsiders wrongly getting access by technical means or by fraud or misplaced curiosity to personal information;
- Fire or flood; or
- Access levels to systems or buildings not being properly monitored and controlled.

In the event of a data breach the Data Protection Officer must be immediately notified. The Data Protection Officer will contact the CEO and the Head of Communications when advised that a breach has occurred.

In all relevant cases, the Office of the Data Protection Commissioner will be contacted, and also if necessary, the data subjects affected by the breach.

Remedying breaches has significant cost in terms of time, money and reputation. **Prevention is always better.**

8. Office of the Data Protection Commissioner

The Office of the Data Protection Commissioner is responsible for upholding the rights of individuals as set out in the Acts and ensuring that the data controllers comply with their obligations. The Office is an independent body and has full rights of audit.

The Policing Authority is registered with the Office of the Data Protection Commissioner as a Data Controller under the Data Protection Acts 1988 & 2003. Up until 25 May 2018 this registration has been renewed annually by the Policing Authority. From the 25 May 2018 a register of personal data subjects has been in place.

Managers and staff should routinely check if their areas hold data that is not included in this register of personal data and if necessary contact the Authority's Data Protection Officer to have the description amended.

9. Useful contacts

Data Protection Officer:

The Authority's Data Protection Officer is: Clare Kelly

Contact details:

Email: DPO@policingauthority.ie

Phone: 01 8589090

Any queries regarding data protection related matters can be addressed to the Data Protection Officer who can seek wider assistance and advice as required. Awareness training is also provided to ensure staff are aware of their requirements and of the contents of this policy document and are in a position to comply with the legislation.

As always, further information is available from the website of the Office of the Data Protection Commissioner at www.dataprotection.ie.

Personal data requests under the Data Protection Acts, can be obtained by request from:

The Data Protection Officer
The Policing Authority
90 King Street North
Dublin 7
D07 N7CV

Or by email at DPO@policingauthority.ie

See Appendix 1 for further details on how to make a request.

Appendix 1: Requesting Personal Data under the Data Protection Acts

A request for a copy of Personal Data under the Data Protection Acts is called a **Subject Access Request (SAR).**

This applies to all manual and electronic records held at the time the access request was received regardless of when the record was created.

The information must be provided in permanent form unless otherwise agreed by the Data Subject.

Please be aware of these key points when responding to Subject Access requests under the Data Protection Acts:

- The request must be received in writing, however it does not need to state that the request is being made under the Data Protection Acts;
- The Data Subject must provide sufficient information to enable the Data Controller to clearly identify them and to locate the relevant data or information;
- The Data Subject must also provide proof of identity, such as a copy of a drivers licence or passport;
- In the normal course of events, an organisation will be obliged to respond to an access request within **one month** of receiving the request. In certain limited circumstances, the one month period may be extended by two months (taking into account the complexity of the request and the number of requests). Where an organisation is extending the period for replying to your request, it must inform the requestor of any extension, and the reason(s) for the delay in responding, within one month of receiving the request.
- There is no fee payable by the data subject to make an access request - the organisation must deal with the request free of charge. However, where the organisation believes a request is manifestly unfounded or excessive (for example where an individual makes repeated unnecessary access requests), the organisation may either charge a fee taking into account its administrative costs in dealing with the request(s), or refuse to act on the request(s). The burden of demonstrating why a request is manifestly unfounded or excessive rests on the organisation.

What must be disclosed in an access request?

- Personal Data Held;
- Outline the purposes for processing data;
- The persons to whom the data has been disclosed;
- The source of the data – while taking account of any confidentiality safeguards; and
- The logic involved in any automated decisions.

For details on exemptions under the Data Protection Acts see the website of the Office of the Data Protection Commissioner at: https://www.dataprotection.ie/docs/Exceptions-to-the-Right-of-Access/r/78.htm which includes details regarding exceptions.

If the Data subject is enquiring as to whether or not an organisation holds data on them, and a description of what data is held, they must receive a response within 21 days.

Appendix 2: Closed Circuit Television

Purpose of the CCTV systems in the Policing Authority

The Policing Authority has CCTV in its offices at 90 King Street North. There is also CCTV in the reception of the building which is operated by the building managers and to which the Authority has no access or control of records.

The primary purpose for the use of CCTV cameras in the Policing Authority is for security and health and safety. As an ancillary use, the Policing Authority may have regard to CCTV footage where it is reasonably required to assist with establishing facts in an investigation, be it a security event, a trip and fall or any other safety concern. In the event that the Authority needs to investigate an incident involving a member of staff, either as a result of a complaint being brought by that employee or another party, CCTV may be used where reasonably necessary to assist in the investigation and resolution of any such issue.

Under the Data Protection Acts 1988 and 2003, the eight rules apply to CCTV images as to all the Data held within the Policing Authority.

Employee personal data

CCTV is not used for remote management of employees. Recorded images may be viewed in exceptional circumstances including but not limited to a security breach, or incidents relating to employee personal protection and health and safety.

Appendix 3: Good Practices to comply with Data Protection Rules

- Keep your work area clear of confidential data when not in use;
- Do not walk away from the printer when you have a document printing as this could be picked up by another staff member and it may contain personal data;
- Ensure that you never leave documents/files/notebooks behind in a meeting room or other office following a meeting;
- Always keep paperwork together and on relevant files;
- Ensure that files are registered and are placed in relevant cabinets/filing areas when not in use;
- Follow computer security procedures – Acceptable usage Policy;
- If you need to send sensitive personal data by email, please use an attachment and password protect it. Please ensure you transmit the password in a separate email or by phone to the recipient. It should also be noted that where a document is password protected it is unlikely that ICT Division of the Department of Justice and Equality will be able to unlock it should the password go missing. If you need further information on other options available, contact ICT;
- Be sure that you have established the identity of an enquirer prior to disclosing any personal data and make sure that the enquirer has the right to the information (The requester should always submit ID with their request for data);
- Discuss it with your supervisor if you are unsure about giving the information out;
- Keep a record of the disclosure on the relevant file;
- If there are difficulties locating a record/file carry out an exhaustive search; and
- Ensure mobile devices are never left unattended and that they are secured by a strong password.