An Roinn Dlí agus Cirt
Department of Justice

DEPARTMENT OF JUSTICE

Data Protection Policy

V2.0
June 2020

Contents **Page**

1. Introduction

The Department of Justice (hereinafter referred to as DoJ) works to make Ireland a safe, fair and inclusive place to live and work.

As the Government Department whose responsibilities include:

- the security of the State
- the protection of life and property
- the prevention and detection of crime
- maintaining and promoting fairness and equality
- managing inward migration to the State
- updating our criminal and civil laws
- various other regulatory services

DoJ necessarily collects, processes and stores significant volumes of personal data from our customers, staff and service providers.

In accordance with the EU General Data Protection Regulation, 2016/679 (GDPR) as given further effect in Part 3 of the Data Protection Act 2018, DoJ is a 'Data Controller' and, as such, has significant responsibilities for ensuring the privacy of data subjects and the protection of personal data processed.

In parallel with GDPR the EU Law Enforcement Directive (LED) deals with the processing of personal data by data controllers for 'law enforcement purposes' – such data falls outside of the scope of the GDPR. This Directive has been given effect primarily through Part 5 of the Data Protection Act 2018 on the Processing of Personal Data for Law Enforcement purposes and DoJ has responsibilities for the processing of such personal data.

Personal data is defined as

"any information relating to an identified or identifiable natural person (data subject)"

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number (e.g. PPSN), location data or online identifier and covers all electronic, manual and image data which may be held on computer or on manual files.

The key definitions used in the GDPR and the LED are set out in Appendix A.

2. Scope

This policy applies to DoJ and is available to all DoJ agencies and executive offices to apply to data processing for which they act as 'Data Controller'.

This policy applies to all personal data collected, processed and stored by DoJ in respect of all individuals, (i.e. staff, customers and service providers) by whatever means including paper and electronic records.

This policy takes account of best practice in the area of data protection using resources available on the website of the Data Protection Commission and the European Commission.

3. Data Protection Principles

The six principles[1] of the General Data Protection Regulation (GDPR) require that personal data are:

1. Processed in a way that is lawful, fair and transparent;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary;
4. Accurate and kept up to date;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
6. Processed in a manner that ensures appropriate security of the data.

Article 5(2) of the GDPR also obliges DoJ to "*be responsible for, and be able to demonstrate, compliance with the principles*".

Very similar principles of data protection apply in cases where personal data are processed for 'law enforcement purposes' under the Law Enforcement Directive (LED). Those principles, which apply to processing for law enforcement purposes, can be found in Section 71 of the Data Protection Act, 2018.

Application of Data Protection Principles in the Department of Justice
GDPR requires that the processing of personal data is conducted in accordance with the data protection principles set out above. DoJ's policies and procedures are designed to ensure compliance with these principles.

[1] Article 5

3.1 Personal data must be processed in a way that is lawful, fair and transparent[2]

Article 6 of the GDPR sets grounds on which personal data processing is lawful. These grounds include:

'*processing is necessary for compliance with a legal obligation …….. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller …….*

Section 38(1) of the Data Protection Act, 2018 further states that processing is lawful where it is required for:

'…… the performance of a function of a controller conferred by or under an enactment or by the Constitution…….'

Much of the personal data processing by DoJ is carried out for the performance of the Minister's functions or in the public interest. The functions of the Minister for Justice, underpinned by Bunreacht na hEireann Article 28.12 and the Ministers & Secretaries Act 1924 (as amended), are included in Appendix B, Table 1 to this document. Table 2 lists tasks carried out in the public interest in DoJ, for which personal data may also be processed.

In addition, personal data are processed by DoJ in compliance with certain legal obligations to which DoJ is subject or for certain law enforcement purposes.

DoJ may also process personal data in accordance with contracts it has put in place and, in limited circumstances, where it has a legitimate interest in processing specified personal data.

DoJ is aware that if it seeks to rely on the legal basis of 'consent' it must ensure that the consent was 'freely given'. It recognises that this can be difficult to establish where there is a significant imbalance of power between the data subject and the controller. Therefore in very limited circumstances, DoJ may request the consent of the data subject to process their data. In such cases, consent will be sought at the time that the data are collected and the data subject will be advised that they can withdraw their consent at any stage during processing.

DoJ will be fully transparent in relation to how personal data collected is used, in particular ensuring that it is not used in a way that a data subject would not expect. DoJ will provide the required information to data subjects when the personal data are collected. DoJ will ensure that the information is provided in an intelligible form using clear and plain language. In order to ensure that the information provided is comprehensive and always accessible, DoJ may make detailed information available on its website.

[2] Article 6 of the GDPR and Section 34 of the Data Protection Act, 2018 refer.

3.2 Personal data can only be collected for specific, explicit and legitimate purposes

DoJ processes personal data only for the purposes for which it is collected. Where it processes personal data for archiving purposes in the public interest; scientific or historical research purposes or statistical purposes it will put measures in place to ensure the principle of minimisation. Data subjects will not be identifiable and appropriate safeguards will be put in place with regard to information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Should there be a need for any further proposed processing of personal data (regardless of apparent compatibility with original purpose) it will be the subject of a preliminary risk assessment to ascertain if it poses a high risk to the rights and freedoms of the data subject. This assessment may take the form of a data protection impact assessment (see Section 5.5 below).

3.3 Personal data must be adequate, relevant and limited to what is necessary for processing (data minimisation)

DoJ will ensure that the data collected and held is the minimum amount required for the specified purpose. DoJ will not collect personal data unnecessary to the business purpose. All personal data requests issued by DoJ will clearly state the business purpose for the collection of such data.

3.4 Personal data must be accurate and kept up to date

In order to ensure that the functions of the Minister for Justice are delivered efficiently and effectively, DoJ will ensure that, where possible, all personal data held is kept accurate and up to date. All areas in DoJ that hold personal data are responsible for ensuring that all manual/computer procedures are adequately maintained and that, where notified of inaccuracies, the personal data will be corrected in a timely manner unless it requires disproportionate effort[3].

3.5 Personal data is only held for as long as is necessary

DoJ will establish the length of time that personal data is required to be retained and the purpose(s) of its retention. Subject to the requirements of the National Archives Act, 1988, where the retention period expires DoJ will ensure that the personal data is properly destroyed/deleted. Where personal data must be retained in accordance with the National Archives Act, DoJ will ensure that the data is held securely and inaccessible for normal processing.

[3] It should be noted that the correction of data is not an absolute right – it depends on the circumstances of each individual case. This was the ruling of the Data Protection Commission (DPC) in the complaint brought by Ciaran O'Cofagh against the Health Service Executive (HSE).

3.6 Personal data are processed in a manner that ensures appropriate security of the data

DoJ maintains the highest standards of technical, organisational and physical security measures to ensure that personal data held/processed is secure at all times. Security systems, measures and policies are constantly reviewed and, where necessary, updated. DoJ staff avail of ongoing training in relation to their personal responsibilities for the protection of personal data.

4.0 Rights of 'data subjects'

Subject to Section 60 of the Data Protection Act, 2018 and any associated Regulations, the GDPR specifies the following rights for data subjects:

- right to be informed/right of access
- right to rectification
- right to erasure
- right to restrict processing
- right to data portability
- right to object to processing
- rights in relation to automated decision making and profiling.

Where personal data are processed for law enforcement purposes under the LED, data subjects have similar rights, found in Sections 89-95 of the Data Protection Act 2018, which are subject to a range of restrictions. These rights include the right to information, right of access, and rights to rectification, erasure, and restriction. Data Subjects may contact the DoJ Data Protection Officer with regard to all issues related to processing of their personal data and to the exercise of their rights. dataprotectioncompliance@justice.ie

4.1 Right to be informed and right of access

As noted previously data subjects have the right to be informed by DoJ about the collection and use of their personal data. In addition, they have the right to access their personal data and other supplementary information, as appropriate.

DoJ has implemented procedures to ensure that all Subject Access Requests (SARs) are responded to within the one month period as required under Article 12 of the GDPR.

Further information on making a Subject Access Request can be found on our website at http://www.justice.ie/en/JELR/Pages/Data_Protection

4.2 Right to rectification

Data subjects have the right to have inaccurate personal data held by DoJ rectified and to have incomplete personal data updated so that it is complete.

On receipt of a request from a data subject for rectification of their personal data, DoJ will take reasonable steps to ensure that the data held are accurate and will ensure that data are rectified, where necessary and appropriate.

4.3 Right to erasure

Article 17 of the GDPR provides for the right of data subjects in certain circumstances to have their personal data erased ('right to be forgotten'). These circumstances include:

- the personal data are no longer necessary in relation to the purposes for which they were collected or processed;
- the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation.

DoJ will notify the recipients of that particular data so that it can be erased unless this requires disproportionate effort.

The right to erasure is not an absolute right and does not apply in circumstances where DoJ's processing of personal data is necessary in particular:

- for the performance of a function of the Minister or a task carried out in the public interest (Appendix B Tables 1 & 2)
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
- where the data are required for the establishment, exercise or defense of legal claims.

Where a data subject is of the opinion that elements of personal data held by DoJ are incorrect, they may make a request in writing to have such data permanently erased. DoJ will review all such requests and, where appropriate, will erase the data in question.

4.4 Right to restriction of processing[4]

A data subject has the right to obtain a restriction in relation to the processing of their personal data where any one of the following applies:

- the data subject contests the accuracy of their data. The restriction will apply for a period enabling DoJ to verify the accuracy of the personal data;
- the processing is unlawful and the data subject does not wish to have the data erased, but rather wishes to restrict its' use;
- DoJ no longer requires the data in question but the data subject seeks its' retention in order to establish, exercise or defend a legal claim; or
- the data subject has objected to the processing of their data by DoJ. The restriction will apply pending verification on whether DoJ's legitimate grounds for processing overrides the data subjects concerns.

As a matter of good practice, DoJ will restrict the processing of personal data to 'strictly necessary processing' whilst a review of the accuracy of the data and/or the legitimate grounds for processing the data is carried out.

4.5 Right to data portability

The collection of a significant proportion of personal data by DoJ is lawful in accordance with Article 6.1(c) or 6.1(e) of the GDPR i.e. *'necessary for compliance with a legal obligation*' or '*necessary for a task carried out in the public interest or in the exercise of official authority vested in the controller'*.

In cases where DoJ has collected personal data from a data subject by consent (in exceptional circumstances) or by contract, that data subject can request DoJ to provide the data in electronic format in order to provide it to another Data Controller. DoJ will comply with all such legitimate requests.

It should be noted that this right does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4.6 Right to object to processing

Under Article 21 of the GDPR, data subjects have a right to object to the processing of their personal data in specific circumstances. Where such an objection is received, DoJ will assess each case on its' individual merits.

4.7 Right not to be subjected to automated decision making[5]

Data subjects have the right not to be subjected to a decision based solely on automatic processing, including profiling, that have a legal or similarly significant effect on them.

[4] Article 18
[5] Article 22

DoJ will ensure that no decision issued to a data subject is based on automatic processing alone.

4.8 Complaints

Data subjects who may be concerned that their rights under the GDPR are not upheld by DoJ can contact the DoJ's Data Protection Officer (DPO). The DPO will engage with the data subject in order to bring their complaint to a satisfactory conclusion.

The DPO can be contacted at dataprotectioncompliance@justice.ie.

Where the complaint to the DPO cannot be resolved, the data subject will be informed in writing and will be further informed of their right to bring their complaint to the Data Protection Commission.

5.0 Responsibilities of DoJ

DoJ is responsible for the following:

5.1 Implementing and maintaining appropriate technical and organisational measures for the protection of personal data.

DoJ has implemented appropriate technical and organisational measures to ensure that all data held under its control is secure and is not at risk from unauthorised access, either internal or external. Measures for the protection of personal data are reviewed and upgraded, where appropriate, on an ongoing basis.

5.2 Maintaining a record of data processing activities

DoJ maintains a written record of all categories of processing activities for which it is responsible in accordance with GDPR Article 30 and the Data Protection Act 2018 section 81..

5.3 Data Protection agreements with personal data recipients

On an ongoing basis, DoJ puts in place appropriate contracts (agreements /arrangements/memoranda of understanding/bilateral agreements) with third parties where personal data are shared. This includes state agencies and other government departments. The agreements specify the purpose of sharing the data, the manner in which data subject rights are upheld, the requirements for security of the data, the requirements for termination of the agreement and the steps necessary for the return/deletion of the data shared.

5.4 Data Protection by design and default

In accordance with Article 25 of the GDPR, DoJ implements technical and organisational measures to give effect to the principles of the protection of personal data and to ensure that, by default, only personal data necessary for each specific purpose of the processing are processed.

Such measures include the introduction of organisational policies and procedures such as Acceptable Usage Policy and Digital Communications Policy and the implementation of security measures to secure the data.

5.5 Data Protection Impact Assessment (DPIA)

Where DoJ considers that proposed processing (in particular processing that involves new technology), poses a high risk to the rights and freedoms of the data subjects involved, DoJ will carry out a DPIA.

DoJ's Data Protection Officer will be consulted in relation to each DPIA completed. Where technical and/or organisational measures proposed will not mitigate the high risks previously identified, the Data Protection Commission will be consulted as appropriate.

5.6 Transfer of personal data outside of the European Union[6]

DoJ will ensure that appropriate safeguards are in place prior to transferring any personal data outside of the European Union.

5.7 Personal data breaches

The GDPR defines a personal data breach as

'*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*'.

Staff in DoJ will notify DoJ's Data Protection Officer where they identify or suspect a breach of personal data. The DPO will notify the Data Protection Commission without undue delay[7] where a breach is likely to result in a risk to the rights and freedoms of the data subject(s) involved.

The DPO will also assess if the breach is likely to result in a high risk to the data subject(s) involved. Where a high risk is identified, the DPO will arrange for the data subjects to be notified.

[6] Chapter 5 of GDPR and Chapter 5, Part 5 of the Data P

[7] In accordance with Article 33 of the GDPR this will be no later than 72 hours after having become aware of the breach.

5.8 Data Protection Governance

Compliance with the GDPR is a key requirement for DoJ. DoJ's Corporate Governance Framework (Data Protection Steering Group) will detail the arrangements in place to oversee, monitor and ensure compliance with data protection legislation.

5.9 Data Protection Officer

In compliance with Article 37.1(a) of GDPR and Data Protection Act (section 88), DoJ has a designated Data Protection Officer (DPO). DoJ will involve the DPO in a timely manner in all issues which relate to the protection of personal data and will support the DPO in performing their tasks as set out in the legislation. The tasks assigned to DoJ's Data Protection Officer include the following:

- Informing and advising DoJ and staff who process personal data, of their obligations under data protection legislation;
- Monitoring compliance with the GDPR and the Data Protection Act, 2018 and the policies of DoJ in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff and the related audits;
- Providing advice where requested as regards the data protection impact assessment and monitoring its performance;
- Cooperating with the Data Protection Commission;
- Acting as a contact point for the Data Protection Commission on issues relating to processing and prior consultation.

6.0 Data Protection Contacts

Data Protection Officer
Ms Eileen Tully
Data Protection Support and Compliance Office
Department of Justice
51 St. Stephen's Green
Dublin 2.

Email: dataprotectioncompliance@justice.ie

The contact information for DoJ's Data Protection Officer is published on DoJ's website and has been notified to the Data Protection Commission.

If you have a query, concern or complaint regarding a data protection matter, you can also engage with the Data Protection Commission in the following ways:

- DPC Website; https://www.dataprotection.ie/en/contact/how-contact-us

- By post.
  Data Protection Commission
  21 Fitzwilliam Square South
  Dublin 2
  D02 RD28
  Ireland.

APPENDIX A

GDPR Key Definitions

Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Subject is an individual whose personal data are processed.

Processing means any operation or set of operations which is performed on personal data, by manual or automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special categories of data means any data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor means a person, public authority, agency or other body who processes personal data on behalf of the controller.

LED Key Definitions

Below are definitions of the key terminology used in the LED:

Competent authority means

(a) a public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the State, including the safeguarding against, and the prevention of, threats to public security, or

(b) any other body or entity authorised by law to exercise public authority and public powers for the purposes of the prevention,

investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the State, including the safeguarding against, and the prevention of, threats to public security.

Controller means

(a) a competent authority that, whether alone or jointly with others, determines the purposes and means of the processing of personal data, or

(b) where the purposes and means of the processing of personal data are determined by the law of the European Union or otherwise by the law of the State, a controller nominated -

i. by that law, or
ii. in accordance with criteria specified in that law.

APPENDIX B

Table 1 - Functions of Minister for Justice
Provision of a Courts Service
Management of inward migration to the State (Immigration)
Ensuring the security of the State
Protection of life and property (Policing)
Provision of a Prison Service
Updating of criminal and civil laws (Law Reform)
Maintaining and promoting fairness
Preventing and detecting crime
Ensuring access to justice
Administration of the Good Friday Agreement

Table 2 – Department of Justice - Public Interest Tasks
Communication with Citizens
Communication with Members of the Oireachtas
Internal Government Communications
Administration of Official Duties