An Roinn Cosanta
Department of Defence

Department of Defence

Data Protection Policy

May 2018

Table of Contents

1. Introduction

As a central Government Department, the high-level goal of the Department of Defence is:

To provide for the military defence of the State, contribute to national and international peace and security and fulfil all other roles assigned by Government.

The Department's main functions are:

- Provision of timely and relevant policy and military advice;
- Contribute to national and international security and defence policy;
- Enhance cross-cutting policy collaboration;
- Administration matters for the Department of Defence and the Defence Forces
- Implement the White Paper on Defence 2015.

The Department needs to collect and use certain personal data that it collects about individuals including but not limited to:

- Customers and citizens
- Business contacts
- Suppliers
- Employees

Data protection legislation confers rights on individuals as well as responsibilities on those persons processing personal data. This policy sets out how the Department of Defence seeks to process personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work.

The EU General Data Protection Regulation (GDPR EU 2016/679) replaces the Data Protection Directive 95/46/EC and was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organisations across the region approach data privacy. The GDPR will be enforced from the 25th of May 2018. This version of the policy has been updated to reflect the GDPR.

2. Purpose

This policy should be read in conjunction with other relevant Departmental policies and procedures. We may supplement or amend this policy by additional policies and guidelines from time to time.

This data protection policy is a statement of the Department's commitment to protect the data protection rights of individuals in accordance with Irish data protection and GDPR requirements.

3. Scope

The policy applies to all of the Department's personal data processing functions in relation to identified or identifiable natural persons.

Personal data is defined as 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 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.

Special categories of personal data is defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4. Data Protection Principles

All processing of personal data must be conducted in accordance with the data protection principles set out in relevant legislation. Our policies and procedures are designed to ensure compliance with the following principles:

4.1 Personal data shall be processed **lawfully, fairly and in a transparent manner** in relation to the data subject ('lawfulness, fairness and transparency);

4.2 Personal data shall be collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

4.3 Personal data shall be **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation');

4.4 Personal data shall be **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

4.5 Personal data shall be 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

4.6 Personal data shall be processed in a manner that ensures **appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

5. Rights of data subjects

The Department will implement policies as appropriate to ensure the following rights of data subjects:

5.1 **Right of access by the data subject**

The Department will implement procedures to ensure that requests from data subjects for access to their personal data will be identified and fulfilled in accordance with the legislation

5.2 **Right to rectification**

The Department is committed to holding accurate data about data subjects and will implement processes and procedures to ensure that data subjects can rectify their data where inaccuracies have been identified.

5.3 **Right to erasure (right to be forgotten)**

The Department processes personal data it collects because there is a statutory basis for the processing. Where we receive requests from data subjects looking to exercise their right of erasure, we will carry out an assessment of whether the data can be erased without affecting the ability of the Department to provide future benefits and services to the data subject.

5.4 **Right to restriction of processing**

The Department will implement and maintain appropriate procedures to assess whether a data subjects request to restrict the processing of their data can be implemented. Where the request for restriction of processing is carried out then we will write to the data subject to confirm the restriction has been implemented and when the restriction is lifted.

5.5 **Right to data portability**

The Department processes personal data its collects because there is a statutory basis for the processing. Where we have collected personal data on data subjects by consent or by contract then the data subjects have a right to receive the data in electronic format to give to another data controller.

5.6 **Right to object**

Data subjects have a right to object to the processing of his or her personal data in specific circumstances. Where such an objection is received the Department will assess each case in its merits.

5.7 **Right not to be subject to automated decision making**

Data subjects have the right not to be subject to a decision based solely on automated processing, where such decisions would have a legal or significant effect concerning him or her. The Department ensures that where systems or processes are implemented that calculate benefits or services then an appropriate right of appeal is available to the data subject.

5.8 **Right to complain**

The Department will implement and maintain a complaints process whereby data subjects will be able to contact the Data Protection Officer. The Data Protection Officer will work

with the data subject to bring the complaint to a satisfactory conclusion for both parties. The data subject will be informed of their right to bring their complaint to the Data Protection Commissioner and their contact details.

6. Responsibility for this policy

The Department is committed to compliance with all relevant EU and Irish laws in respect of personal data, and the protection of the rights and freedoms of individuals whose information we control and process.

All staff working in the Department and third parties of the Department who separately collect and or control the content and use of personal data have responsibility for ensuring personal data is collected, stored and handled appropriately. Each Branch that handles personal data must ensure it is handled and processed in line with this Policy, best practice and data protection legislation.

7. Responsibilities of the Department of Defence

The Department has responsibility for the following:

7.1 Maintaining a record of data processing

The Department will maintain a record of data processing activities in the manner prescribed by the General Data Protection Regulation. The record will be reviewed and signed off by Senior Management on an annual basis.

7.2 Ensuring appropriate technical and organisational measures

The Department will implement appropriate technical and organisational measures to ensure and be able to evidence that personal data is protected.

7.3 Implementing appropriate agreements with third parties

The Department will implement appropriate agreements and contracts with all third parties with whom personal data is shared. The term 'third parties' includes other departments and agencies of the Irish Government. All such agreement shall be implemented in writing prior to the commencement of the transfer of the data. The agreement shall specify the purpose of the transfer, the requirement for adequate security, right to terminate processing, restrict further transfer to other parties, ensure that response will be given to requests for information and the right to audit.

7.4 Transfers of personal data outside of the European Economic Area (EEA)

The Department will not transfer the personal data of its data subjects outside of the EEA unless appropriate safeguards are in place.

7.5 Data protection by design and default

The Department will implement processes, both prior to the time of determining the means of processing as well as during the processing, to ensure the appropriate technical and organisational measures and safeguards are integrated into the process and that they to adhere to the data protection principles.

7.6 Data protection impact assessments

The Department will implement procedures whereby all new types of processing, in particular using new technologies, that result in a high risk to the rights and freedoms of its data subjects shall carry out a data protection impact assessment. As part of this process, a copy of the impact assessment shall be shared with the Department's Data Protection Officer. Where the Department is unable to identify measures that mitigate the high risks identified we will consult with the Data Protection Commissioner prior to the commencement of processing.

7.7 Personal data breaches

The Department defines a 'personal data breach' as meaning 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. The Department deems any loss of personal data in paper or digital format to be a personal data breach.

The Department will develop and maintain a protocol for dealing with personal data breaches which will establish the methodology for handling a personal data breach and for notification to the DPC and data subjects where necessary.

7.8 Governance

The Department will monitor compliance with relevant legislation through the Data Protection Working Group. The working group of staff, nominated by Heads of Branches from branches within the Department, and designated to assist the Data Protection Officer with a range of data protection matters on an ongoing basis.

8. Responsibilities of the Data Protection Officer

The Data Protection Officer will report to the Management Board concerning the tasks allocated to them. The responsibilities of the Data Protection Officer will include the following;

(i) Keeping the Management Board and Data Protection Working Group updated about data protection responsibilities, risks and issues

(ii) Act as an advocate for data protection within the Department

(iii) Monitoring compliance with the relevant data protection legislation.

(iv) Monitoring that all data protection policies are reviewed and updated on a regular basis

(v) Monitoring that the Department provides appropriate data protection training and advice for all staff members and those included in this policy

(vi) Providing advice where requested as regards the data protection impact assessments and monitoring that such assessments are completed to an appropriate standard

(vii) Provide advice on data protection matters to staff, board members and other stakeholders

(viii) Responding to individuals such as clients and employees who wish to exercise their data protection rights

(ix) Monitoring that appropriate data processing agreement are put in place with third parties that handle the Department's data and ensuring that reviews of third parties are carried out on a regular basis

(x) Monitoring that the record of data processing is updated as necessary

(xi) Acting as a contact point and providing cooperation with the Data Protection Commissioner

9. Responsibilities of staff

All staff that process personal data on behalf of the Department have a responsibility to comply with this data protection policy.

9.1 Training and Awareness

All staff will receive data protection training. New staff will receive training as part of the induction process.

All staff will be kept aware of data protection obligations through regular notifications from the Data Protection Office and poster campaigns.

9.2 Failure to comply with the data protection policy

All staff have a duty to ensure compliance with the principles of data protection and undertake to follow the provisions of this policy. All staff are charged with the responsibility to ensure that all data processed by them as part of their daily duties, is done in accordance with the Data Protection Act and this policy. Breaches of this policy may result in disciplinary action.

10. Queries about the data protection policy

The Department has appointed a Data Protection Officer for you to contact if you have any questions or concerns about the Department's personal data policies. Contact details for the Data Protection Officer are as follows:

Data Protection Officer
Department of Defence
Station Road
Newbridge
Co. Kildare
W12 AD93

Email: dataprotection@defence.ie

Telephone: +353 45 492190