# DEASP Data Protection Policy

An Roinn Gnóthaí Fostaíochta
agus Coimirce Sóisialaí
Department of Employment Affairs
and Social Protection

# DEASP Data Protection Policy

## Table of Contents

# 1. Introduction

The Department of Employment Affairs and Social Protection (DEASP) is tasked with providing employment services and administering Ireland's social protection system. The Department's mission is:

*"To promote active participation and inclusion in society through the provision of income supports, employment services and other services."*

The Department's main functions are to:

- advise Government and formulate appropriate social protection and social inclusion policies;
- design, develop and deliver effective and cost-efficient income supports, activation and employment services, advice to customers and other related services;
- work towards providing seamless delivery of services in conjunction with other Government Departments, Agencies and Bodies; and
- control fraud and abuse within the social protection system.

The Department is committed to protecting the rights and privacy of individuals in accordance with both European Union and Irish data protection legislation. The Department is required to lawfully & fairly process personal data about employees, customers, suppliers and other individuals in order to achieve its mission and functions.

The data protection legislation confers rights on individuals as well as responsibilities on those persons processing personal data. This policy sets out how the Department 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 organizations across the region approach data privacy. The GDPR will be enforced from 25th May 2018. This version of the Department policy has been updated to reflect the GDPR.

# 2. Scope & purpose

This policy applies to all of the Department's personal data processing functions in relation to identified or identifiable natural persons, including those performed on customers, employees, suppliers and any other personal data the Department processes from any source.

Personal data is defined as any information relating to an identified or identifiable natural person ('customer'); 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 – 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.

# 3. Responsibility for this policy

Overall responsibility for this policy rests with the Data Controller, the Secretary General. The Minister, Junior Ministers, Secretary General, Deputy Secretary, Senior Officers and Assistant Secretaries of the Department are 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 Department collects and processes.

Senior Officers, Assistant Secretaries and Principal Officers are responsible for ensuring that this policy is implemented in their respective Divisions. Managers at all levels are accountable for being to demonstrate that this policy has been implemented.

All members of staff have a responsibility to comply with Department's data protection policies.

# 4. Data protection principles

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

## *4.1 Personal data must be processed lawfully, fairly and transparently*

Lawfully – the legal basis for processing personal data is normally based on relevant legislation. The Department administers both statutory schemes and administrative schemes. The legal basis for statutory schemes is the relevant section of the Social Welfare Consolidation Act 2005 and in the relevant legislation for each statutory scheme.

The Department is permitted by law to process information to administer its schemes and core functions. Specific legislation is contained in the Social Welfare Consolidation Act, 2005 (as amended) where provisions for the Department's main schemes are outlined separately. In addition, Bunreacht na hÉireann (article 28(2)) and the Ministers & Secretaries Acts 1924 to 2017 bestow overall powers on the Government to collect and process data

Fairly – in order for processing to be fair, the Department has to make certain information available to the customers. This applies whether the personal data was obtained directly from the customers or from other sources.

Transparently – the Department provides the required information to customers at the time personal data is collected. The Department ensures that the information provided is detailed and specific, and that such notices are understandable and accessible, using clear and plain language. In order to balance the requirements above, the Department implements appropriate policies to make information available on its website. The information provided must include information about personal data collected both directly from the customer and from other sources. The Department may adopt standardised icons in the future.

## *4.2 Personal data can only be collected for specific, explicit and legitimate purposes*

The Department collects and processes personal data only for the purposes for which it is collected, and related purposes

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

The Department ensures that in designing methods of data collection, whether online, forms or offices, that only the personal data required to identify the customer(s), and provide the benefit or service, will be processed. The Department undertakes regular reviews of the data requested to ensure that the amount of personal data collected is minimised.

### *4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay*

All customers have a right to ensure that their data is accurate and complete. The Department needs accurate and up-to-date data about customers in order to ensure that the correct benefits and services are provided to the correct recipients. All data collection procedures are designed to ensure that reasonable steps are taken to update personal data where new data has been provided. All changes to personal data should be shared with each third party with whom the previous data had been shared, unless this is impossible or requires disproportionate effort.

### *4.5 Personal data must be kept in a form such that the customer can be identified only as long as is necessary for processing*

The Department implements appropriate policies and procedures to ensure that personal data is retained only for the minimum period required to provide the benefit or services requested. This may be done by destroying the personal data, by anonymization or any other appropriate method.

### *4.6 Personal data must be processed in a manner that ensures appropriate security*

The Department implements appropriate technical and organisation measures to ensure that appropriate security of the processing of personal data is implemented.

### *4.7 Accountability for demonstrating compliance*

The Department ensures that it maintains adequate records of its processing and evidence that it has complied with this policy and related policies and procedures, in accordance with Article 30 of GDPR ('Record of Processing Activities').

# 5. **Rights of individuals whose data is collected**

The Department designs and maintains appropriate policies, procedures and training to implement the following data rights of customers.

### *5.1 Right of access by the customer*

The Department implements procedures to ensure that requests from customers 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 customers and implements processes and procedures to ensure that customers 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 the Department receives requests from customers looking to exercise their right of erasure then the Department 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 customer.

### *5.4 Right to restriction of processing*

The Department will assess whether a customer's request to restrict the processing of their data can be implemented.

### *5.5 Right to data portability*

The Department processes personal data it collects because there is a statutory basis for the processing. Where the Department has collected personal data on customers by consent or by contract then the customers have a right to receive the data in electronic format to give to another data controller. It is expected that this right will apply only to a small number of customers.

### *5.6 Right to object*

Customers have a right to object to the processing of their personal data in specific circumstances. Where such an objection is received, the Department will assess each case on its merits.

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

Customers 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 customer.

### *5.8 Right to complain*

The Department implements and maintains a complaints process whereby customers will be able to contact the Data Protection Officer (DPO). The DPO will work with the customer to bring the complaint to a satisfactory conclusion for both parties. The customer will be informed of their right to bring their complaint to the Data Protection Commissioner.

# 6. Responsibilities of the Department

The Department has responsibility for the following

## *6.1 Ensuring appropriate technical and organisational measures*

The Department implements appropriate technical and organisational measures to ensure and be able to evidence that it protected personal data always.

## *6.2 Maintaining a record of data processing*

The Department maintains a record of its data processing activities in the manner prescribed by Regulation.

## *6.3 Implementing appropriate agreements with third parties*

The Department implements appropriate agreements, bilateral agreements, memoranda of understanding and contracts (collectively "agreements") with all third parties with whom it shares personal data. The term 'third parties' is meant to include other agencies, departments, and data processors acting on behalf of the Department. The agreement shall specify the purpose of the transfer, the requirement for adequate security, the review period, the right to terminate processing, the right to restrict further transfer to other parties, and to ensure that responses will be provided to requests for information and the right to audit, in the case of data processors.

## *6.4 Transfers of personal data outside of the European Economic Area*

The Department will not transfer the personal data of its customers outside of the European Economic Area unless an adequate level of protection is ensured.

## *6.5 Data protection by design and by default*

The Department implements processes, prior to the time of determining the means of processing as well as when actually processing, to implement appropriate technical and organisational measures to implement the data protection principles set out in Section 4 and integrate necessary safeguards into the processing to meet GDPR requirements.

## *6.6 Data protection impact assessments*

The Department implements procedures and documentation whereby all new types of processing, in particular using new technologies, that result in a high risk to the rights and freedoms of its customers 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 then the Department will consult with the Data Protection Commissioner prior to the commencement of processing.

## *6.7 Personal data breaches*

The GDPR 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. (e.g. the most common breach incidents that can occur are correspondence issuing to an unauthorised third party). The Department deems any loss of personal data in paper or digital format to be a personal data breach.

The Department develops and maintains a protocol for dealing with personal data breaches. This protocol sets out the methodology for handling a personal data breach and for notification of the breach to the Data Protection Commissioner and to customers where this is deemed necessary.

## *6.8 Freedom of Information*

The Freedom of Information Act 2014 (FOI) obliges the Department to publish information on their activities and to make the information held, including personal information, available to citizens and customers.

The Department maintains a separate policy to ensure compliance with FOI. The Department maintains procedures to ensure that requests for personal data are correctly fulfilled under either data protection legislation or FOI legislation.

## *6.9 Governance*

The Department monitors compliance with relevant legislation through the Data Management Programme Board. The Board:

- Receives regular reports of data protection activities from Department Divisions
- Receives regular reports from the Data Protection Officer
- Reviews data protection impact assessments and approve or not the design of data protection elements of projects
- Arranges internal audits, or similar, of Department units for compliance with this policy
- Reviews requests to share data, and data sharing arrangements and agreements
- Oversees any other such activities relating to the Department's compliance with EU & Irish Law in the area of data protection.

# 7. The Data Protection Officer's Responsibilities

The Department has appointed a Data Protection Officer (DPO). The DPO reports to the Secretary-General and the Data Management Project Board. The responsibilities of the DPO include the following

i. Keeping the Board updated about data protection responsibilities, risks and issues

ii. Acting as an advocate for data protection within Department

iii. Monitoring compliance with the relevant data protection legislation

iv. Monitoring that all data protection policies and 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 from staff, board members and other stakeholders

viii. Responding to individuals such as customers and employees who wish to know which data is being held on them by the Department

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

x. Monitoring that the Record Of Data Processing is updated regularly.

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

# 8. Responsibilities of staff and similar parties

Anyone who processes personal data on behalf of the Department has a responsibility to comply with this data protection policy.

## *8.1 Training and awareness*

New joiners will receive awareness raising as part of the induction process. Completion of the e-learning module is compulsory for all new staff.

All staff are continuously reminded of data protection obligations through annual data protection obligations for signing; regular poster campaigns; e-mails to staff from Business Information Security Unit (BISU); e-mails to staff from the Sec-Gen; resources on the BISU intranet site; corporate video and e-learning module; GDPR and BISU newsletters; regular awareness weeks; annual obligations notice.

## *8.2 Consequences of failing to comply*

The Department takes compliance with this policy very seriously. Failure to comply puts both you and the Department at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under the Civil Service Disciplinary Code, which may result in sanction up to and including dismissal.

# 9. Where to go if you have queries about the data protection policy

The Department has resources on its website and you should refer to these in the first instance.

If you cannot find the answer to your query on the website then do not hesitate to contact

Business Information Security Unit (BISU)
Goldsmith House
Dublin 2
E-mail: bisu@welfare.ie

The Data Protection Officer
Goldsmith House
Dublin 2
E-mail: dpo@welfare.ie