An Roinn Coimirce Sóisialaí
Department of Social Protection

Department of Social Protection's Privacy Statement

Among other things, this Privacy Statement relates to the processing of personal data in respect of identity authentication (SAFE 2 registration) and the Public Services Card (PSC)

10 December 2021

Change Control Notice

December 2021
Updated to include the text "Among other things, this Privacy Statement relates to the processing of personal data in respect of identity authentication (SAFE 2 registration) and the Public Services Card (PSC)", immediately below the heading to the Privacy Statement on the cover page.

Updated with minor edits to ensure corporate information is up to date and accurate - for example, updated name of the Department, contact numbers, and updated information on the latest department statistics in Section 1.1.

February 2020
Update of Privacy Statement to present information in an expanded set of headings and to provide additional information to address the deficiencies in the previous Privacy Statement as identified by the Data Protection Commissioner (DPC) in respect of the processing of personal data including in respect of identity authentication (SAFE 2 registration) and the Public Services Card (PSC).

This Privacy Statement replaces the previous version of the Privacy Statement which is available here.

The deficiencies identified by the DPC in that statement are set out in an Addendum to that statement. The purpose of the revisions included in this updated version of the Privacy Statement is to:

i. Present information in a format with an expanded set of headings which is intended to aid readers in identifying and finding particular sections that are of particular interest to them;

ii. Provide information on the functions of the Department (Section 1);

iii. Provide additional information with respect to the collection of Public Service Identity Data from other public bodies (Section 2);

iv. Provide additional information with respect to updating of data and the possible consequences for data subjects of any failure of data subjects to inform the Department of any changes that impact their entitlement to a benefit or service (Section 3);

v. Provide additional information on the types of personal data collected and information with respect to updating of personal data provided for the purposes of identity authentication (SAFE 2/ PSC) and the possible consequences for data subjects of any failure of data subjects to inform the Department of changes to this personal data (Section 3);

vi. Provide further information about whom personal data is processed (Section 4);

vii. Provide information on how we collect personal data (Section 5);

viii. Provide additional information on the legal basis under both the GDPR and Law Enforcement Directive that provide for the processing undertaken (Section 6);

ix. Provide further information on the purposes of processing carried out including profiling (Section 7);

x. Provide additional information on data shared with other organisations (Section 9);

xi. Provide further detail on the transfers of data to third countries (Section 10);

Change Control Notice

xii. Provide additional information with respect to data retention policies and the rationale for data retention periods (Section 11);

xiii. Provide additional information with respect to the additional processing of personal data performed by the Department. (Section 12);

xiv. Provide additional information regarding data subjects' rights (Section 13).

Table of Contents

Introduction: What is GDPR

GDPR is the European Union General Data Protection Regulation. It came into effect on 25 May 2018. It sets out a series of EU rules concerning how data can be processed and used by organisations. The objective of the Regulation is to strengthen and standardise data protection laws for all EU citizens. This Regulation applies to any organisation that determines the purposes and means of the processing of personal data (a Data Controller) and also any other organisation processing data on behalf of the Data Controller (a Data Processor). Those responsible for adhering to this Regulation include employees of the relevant organisation, contractors, consultants, agents and third parties who have access to data either directly or indirectly.

The key principles relating to the processing of personal data under the GDPR are lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability (Article 5 of the GDPR). Further information on GDPR and the steps to take in ensuring compliance is available on the website of the Data Protection Commission (DPC) at GDPRandYou.ie or dataprotection.ie.

The Law Enforcement Directive (LED)

The Law Enforcement Directive (Directive (EU) 2016/680) also took effect from May 2018. It deals with the processing of personal data by data controllers where the processing is for 'law enforcement purposes', which fall outside the scope of the GDPR.

The LED was transposed into Irish law primarily by Part 5 of the Data Protection Act 2018.

Section 1: Who we are

Section 1: Who we are

1.1 The Data Controller

The Department supports the Minister for Social Protection in the discharge of governmental, parliamentary and departmental duties.

The main functions of the Department include:

- advising the Government and formulating appropriate policies in respect of employment law, labour market interventions, social protection and social inclusion,
- designing, developing and delivering effective and cost-efficient income supports, activation and employment services,
- contributing to the seamless delivery of services in conjunction with other Departments, agencies and bodies, **and**
- controlling suspected fraud and abuse in relation to employment and social protection services.

The Department of Social Protection (DSP) is the Data Controller for all personal data collected for the purpose of its business. The Department decides what personal data we need to collect from you, and others, to allow us to operate our schemes and services. Our data processes are documented.

Each week, some 1.61 million people receive a social welfare payment. In the region of 633,000 families receive child benefit payments in respect of over 1.2 million children each month. There are approx. 6,000 staff members directly employed in the Department. Operational guidelines for all our schemes are available on our website www.gov.ie/dsp

You can contact the Department in any of the following ways:

By post: The Department of Social Protection,
Aras Mhic Dhiarmada,
Store Street, Dublin 1.
By email: info@welfare.ie
By phone: 071 9193302 or 0818 66 22 44 (LoCall)

Note: Calls to 0818 Standard Rate numbers are included in bundles that include calls to landlines. Out of bundle, 0818 calls are charged at the "Standard Rate" which is no more than calling a landline.

1.2 The Data Protection Officer

In accordance with Article 37 of the GDPR, the Department has appointed a Data Protection Officer (DPO) who heads a dedicated Data Protection Unit (DPU).
If you wish to contact our Data Protection Officer (DPO) you can do so in any of the following ways:

By post: Data Protection Officer,
Department of Social Protection,
Goldsmith House,
Pearse Street,
Dublin 2.
By email: dpo@welfare.ie

Section 2: When we collect your information

Section 2: When we collect your information

We collect information about you for a range of reasons and from a number of sources, as well as from yourself. The common situations where we collect personal data are as follows:

2.1 When you apply for a Personal Public Services Number (PPSN);

2.2 When you have your identity authenticated via a process called Standard Authentication Framework Environment (SAFE) registration, a Public Services Card (PSC) is issued as a token of the SAFE registration;

2.3 When you earn income – we collect data on your social insurance contributions and receive information about your income from the Revenue Commissioners;

2.4 When you make a claim for, or use, any of our schemes or services, either in person or online;

2.5 When you are in receipt of a payment and notify us of a change in your circumstances;

2.6 When we undertake a review of your claim;

2.7 When you have a child – with the child also being allocated a PPSN;

2.8 We also receive information from other Government Departments and agencies – see Section 9. As data controller for the Public Services Identity (PSI) dataset* we may collect identity information from the other specified bodies that may be used to update the PSI dataset. The list of specified bodies is set out in Schedule 5 of the Act which can be found on pages 542-544 here;

2.9 The Department also develops and provides services via contracted agencies/ bodies that may in turn collect information from you on behalf of the Department. These agencies/ bodies include, Branch Office providers of welfare services, medical practitioners (certifying eligibility to illness and disability schemes) and providers of employment and community services (including Community Employment Schemes, Local Employment Services, JobClubs, Tús and JobPath). The agencies/ bodies are all engaged under legally binding contracts that require adherence to GDPR rules;

2.10 We may also collect data from TDs or councillors acting on your behalf, or from other people, approved by you to act on your behalf.

***Public Service Identity information includes your name, date & place of birth, photograph, signature, address, and nationality.**

Section 3: What types of personal data do we collect?

Section 3: What types of personal data do we collect?

3.1 It is the Department's policy to only collect the information that is required for legitimate purposes, such as those outlined in Section 7. The information we collect about you depends on the nature of your transactions with us but we may use the information for any of our functions. An easy way to see what kind of information the Department processes for a particular income support or employment service is to look at the claim form for that support/service.

3.2 Personal data we collect can include the following:

- your name,
- your address,
- your date of birth,
- your place of birth,
- your gender,
- your former surnames (if any),
- the former surnames of your mother (if any),
- your Personal Public Services Number (PPSN),
- your nationality,
- your marital status,
- your family status and details,
- your phone number,
- your email address,
- certain financial information,
- PRSI paid and credited,
- employment, training and education details,
- supports or services provided to you, and
- photograph(s) and signature used for the purpose of identification.

3.3 At times, we may also need to collect 'special category' personal data as defined under Article 9 of the GDPR here. For example, this includes data relating to health, racial or ethnic origin, trade union membership, offences including alleged offences, criminal proceedings, outcomes and sentences.

3.4 If we ask you for personal information, you need to:

- give us accurate information,
- tell us as soon as possible if there are any changes, such as a new address, changes in your living arrangements, including cohabiting/ marriage, and changes in your employment status or earnings or any other factors that may affect your entitlement to a service or benefit (e.g. if you are in receipt of a disability or invalidity payment you need to advise the Department if your circumstances change such that you regain the capacity to work).

This helps us to:

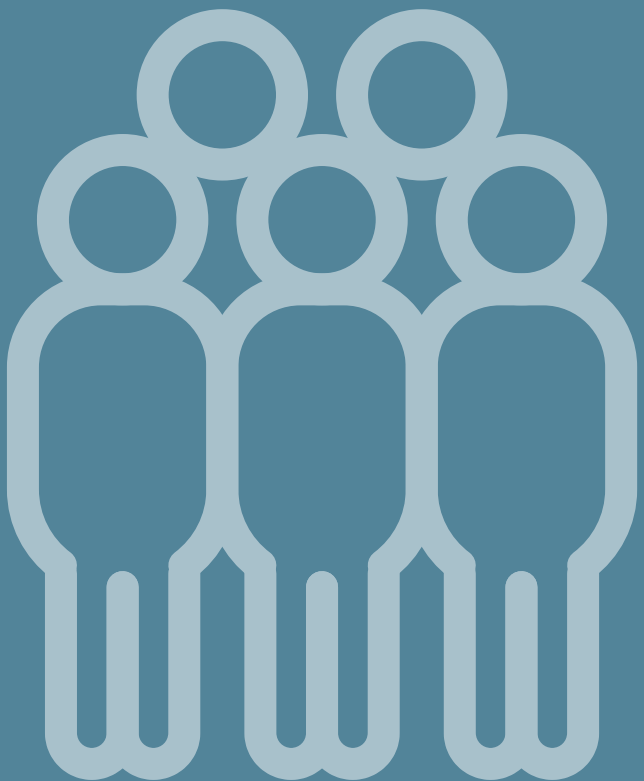
- keep your information accurate and up to date,
- pay you the right amount,
- provide you with the best possible service.

Failure to update the Department of any changes to information you previously provided, in particular in relation to your address, your living arrangements, including cohabiting/ marriage, and your employment status or earnings, or any other factors that may affect your entitlement to a service or benefit, may result in the incorrect delivery of services/benefits or a failure to provide services or benefits to which you are entitled. Any benefits/services delivered in error would then have to be withdrawn and any payments made incorrectly would have to be recovered. An investigation might also have to be commenced to determine if the failure to provide updated information was deliberate and if so if a prosecution for fraud is appropriate.

3.5 It is important that you update the Department with any changes to the data collected for identity authentication (SAFE/PSC) purposes as this information may be referred to by other specified bodies when they are transacting a service with you.

Failure to update the information may lead to delays in those bodies verifying your identity and/or processing applications

Section 4: About whom does the Department process information?



Section 4: About whom does the Department process information?

The Department processes personal data about:

- members of the public,
- people who use or have used our services (including income support services),
- people who live in the household of a person who has used, is using or is claiming access to our services,
- suppliers and services providers,
- advisers, consultants and other professional experts,
- complainants and enquirers,
- relatives, guardians or people who have used, are using or are claiming access to our services,
- its staff and employees, and,
- employers.

4.1 The Department sometimes needs information about people other than the person who has applied for income support or a service in order to assess and, if appropriate, calculate that person's entitlement to a service or benefit. For example, information about other members of the household may be needed to calculate the correct amount of a payment in cases where that payment is means–tested (e.g. Jobseeker's Allowance), where the amount of the payment may be dependent on the number of people in the household who are dependent on the income of the claimant (e.g. Pension payments) or where the entitlement to a payment depends on the circumstances of another person in the household (e.g. Carer's payments).

Children's personal data is required to process claims for Child Benefit and Guardian's Payment and all schemes where the rate of payment is affected by the number of qualifying children.

Section 5: How does the Department collect data?

Section 5: How does the Department collect data?

We may collect personal data in any of the following ways:

- Face to face discussions,
- Post,
- Email,
- Online via websites operated by or on behalf of the Department,
- Social Media,
- CCTV,
- Website,
- Phone,
- See Section 9 in respect of the collection of data from third parties,
- See Section 2.9 regarding contracted agencies/ bodies.

The following gives further detail on how we collect data in the ways listed above:

5.1 Claim forms and other correspondence received by post are usually scanned into the Department's computer systems, associated with the person's claim and dealt with by the relevant customer service unit. The original hard copy correspondence is destroyed securely. If correspondence is not scanned but is retained in hard copy, it is associated with the relevant file.

5.2 Emails from people accessing our services are associated with the relevant claim/service and dealt with by the relevant customer service unit.

5.3 Data collected through online services are processed by the relevant customer service unit in order to process a claim or provide the relevant service.

5.3.1 MyGovID (www.mygovid.ie) is an online Identity Service Portal that enables users to log in to and access government provided online services (for example Revenue MyAccount; MyWelfare.ie) in a safe and secure manner. The MyGovID website does not collect any personal data, apart from information that you volunteer (for example, when filling a form) and your IP address. The MyGovID identity portal enables people to create a MyGovID account to one of two levels of access – basic account access (which enables access to a limited range of services) and 'verified' account access (which enables access to a broader range of services including services that allow a person to apply for and view benefits and update their data); log-in and authenticate their identity using their MyGovID account; update their mobile phone number (mobile phone SMS is used as part of the login process for verified accounts); change their password; and recover their account.

As part of the process of authenticating a person's identity for access to service websites such as MyWelfare.ie and for example Revenue MyAccount the MyGovID identity portal may share your public service identity details such as PPSN and date of birth with other Government departments/agencies that use MyGovID, in accordance with law. Any data which is shared is data to which the relevant specified body is legally entitled and requires for the provision of it's service(s). Before a person logs in to MyGovID, they are advised that they are agreeing to share their personal details and contact information with the government body whose online services they intend to access. The information that is shared with other Government agencies is available at www.mygovid.ie

MyGovID may collect the following information from each user of the site:

- Statistical information (IP address and hostname, web browser version, pages visited etc.). This includes tagging for Google Analytics which is used to inform service design improvements.
- IP address information which is retained for a limited time for security reasons and to prevent misuse of the website.
- The previous website address from which you reached MyGovID.ie, including any search terms used.
- Registration details shared with MyGovID (email address, name and mobile number).
- Your language preference (English/Irish).
- Other information submitted in forms, for example if you submit your personal details when requesting or submitting an online form.
- The date and time you access the MyGovID portal.

5.3.2 MyWelfare (www.mywelfare.ie) is an online service channel for people wishing to access services of the Department. The MyWelfare website does not collect any personal data, apart from information that you volunteer (for example, when filling a form) and your IP address. Any information you provide in this way is used only for the purpose for which you provide it. Currently these purposes include: making an appointment to visit an office of the Department; applying for jobseeker, parent, child, and family support schemes; applying for a pension recalculation; requesting or viewing a statement of contributions and payments and refunds, accessing the benefit of work calculator; and checking eligibility for treatment benefits. Any information provided for the purposes of accessing the benefit of work calculators is deleted immediately once the session expires.

MyWelfare uses MyGovID as an identity and access management service and for authentication of users. It may collect the following information from each user of the site:

- Statistical information (IP address and hostname, web browser version, pages visited etc.). This includes tagging for Google Analytics which is used to inform service design improvements.
- IP address information which is retained for a limited time for security reasons and to prevent misuse of the website.
- The previous website address from which you reached us, including any search terms used.
- Registration details shared with MyGovID (email address, name and mobile phone number) as well as the PPSN and date of birth.
- Your language preference (English/Irish).
- Other information submitted in forms, for example if you submit your personal details when requesting or submitting an online form.
- The date and time you access the MyWelfare site.

5.3.3 WelfarePartners (www.welfarepartners.ie) is an online service channel for business partners of the Department. The website currently supports Community Employment and Wage Subsidy schemes to provide services on behalf of the Department. It also supports dentists, opticians, and audiologists in the provision of Treatment Benefit services. These business partners may provide information such as the client's PPSN, date of birth and address. Community Employment sponsors, in addition, may provide information relating to training and education and work experience undertaken by a client as part of their participation on the Community Employment scheme. This enables the Department to fund the provider so that the relevant service/payment is provided to the person concerned. In addition, Wage Subsidy Scheme Employers may provide information on a client's employment status, hours worked and gross

earnings. This enables the Department to provide the appropriate Wage Subsidy Payment to that employer.

WelfarePartners uses the Revenue ROS digital certificate infrastructure to authenticate business users and may collect the following information from each user of the site:

- Statistical information (IP address and hostname, web browser version, pages visited etc.). This includes tagging for Google Analytics which is used to inform service design improvements,
- IP address information which is retained for a limited time for security reasons and to prevent misuse of the website,
- The previous website address from which you reached us, including any search terms used,
- Registration details shared with ROS (email address and name),
- Your language preference (English/Irish),
- Other information submitted in forms, for example if you submit your personal details when requesting or submitting an online form,
- The date and time you access the WelfarePartners site.

5.3.4 JobsIreland.ie (www.jobsireland.ie) is an online job advertising and matching service that enables users to register as an employer and advertise job vacancies online or register as a jobseeker and place their profile online to help them search for and be matched to vacancies. Jobseekers access the jobsireland.ie website via the MyGovID website, which is a method of accessing government provided online services in a safe and secure manner. The JobsIreland.ie website does not collect any personal data, apart from information that you volunteer (for example, when filling a form) and your IP address.

The JobsIreland.ie website allows the user to create and populate their personal account, to log-in and authenticate their identity using a password; to update the personal data that is stored on their profile; to change their password; and to request deletion of their profile. As part of the process of authenticating a person's identity for access to Jobsireland.ie, the MyGovID identity portal may share your public service identity details such as PPSN and date of birth with other Government departments/agencies that use MyGovID, and the Department's servants and agents in accordance with law. Before a person logs in to JobsIreland.ie, they are advised that they are agreeing to share their personal details and contact information with the government body whose online services they intend to access.

The JobsIreland.ie website may collect the following information from each user of the site:

- Statistical information (IP address and hostname, web browser version, pages visited etc.). This includes tagging for Google Analytics which is used to inform service design improvements,
- IP address information which is retained for a limited time for security reasons and to prevent misuse of the website,
- The previous website address from which you reached us, including any search terms used,
- Registration details shared with MyGovID (email address, name and mobile number),
- Your language preference (English/Irish),
- Other information submitted in forms, for example if you submit your personal details or details of your company when completing your JobsIreland.ie profile,
- The date and time you access the Jobsireland.ie site.

5.4 The Department uses social media accounts to communicate with the people who use its services and with other stakeholders. Messages or posts received by the Department on these platforms are viewed and the data is further processed if, for example, a query is received in relation to a claim or application process. The query is either answered directly or sent to the relevant customer service unit for action.

5.5 Some of the Department's offices use closed-circuit television (CCTV) to help manage security and keep people safe. If the Department is a tenant in a building, CCTV services may be provided by the landlord from whom the premises is rented (or a management company), or by a company providing services for the office. For some buildings the Office of Public Works has the contract with the company providing CCTV services. Signs in our offices advise who you should contact on any matter relating to the use of CCTV. The legal basis for CCTV processing is Article 6(1(f) GDPR i.e. it must be necessary for the Department's legitimate interests. CCTV footage is normally retained for a period of 28 days. Where an incident occurs or an offence is suspected a copy of CCTV footage may be retained for a longer period, and may be provided to An Garda Síochána or other bodies with investigative powers, to allow for investigation and court proceedings.

5.6 The Department's websites use certain cookies. Our Cookie Statement can be viewed here.

5.7 The Department does not record customer phone calls. During the course of customer calls, personal data shared with the Department may be used to answer queries directly or may be referred to other customer service units to be dealt with as appropriate. Notes relating to the content of the phone conversation may be recorded on an electronic or paper file.

Section 6: The legal basis for processing

Section 6: The legal basis for processing

General Data Protection Regulation (GDPR)

The legal bases for the processing of personal data depends on the purpose for which the processing is being carried out.

6.1 The main legal basis under the GDPR upon which the Department relies for the purposes of processing personal data are Article 6 (1) (c) and/or 6 (1) (e): i.e.

Article 6 (1) (c): processing is necessary for compliance with a legal obligation to which the controller is subject.

Article 6 (1) (e): 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.

Most of the schemes and services the Department provides are set out in legislation which provides the Department with the authority, and the obligation, to provide the services concerned. The main legislation is the Social Welfare Consolidation Act 2005 (as amended).

In addition the following Articles of the GDPR are also relevant.

Article 6 (1) (a): where the data subject has given consent to the processing of his or her personal data for one or more specific purposes. An example of where consent applies is where Jobpath providers seek your consent to provide your employer with certain personal data belonging to you.

Article 6 (1) (b): processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of a data subject prior to entering into a contract. (e.g. data processed in respect of the operations of a Community Employment scheme).

Article 6 (1) (d): processing is necessary in order to protect the vital interests of the data subject or another natural person. (e.g. where the Department in the delivery of its services forms a concern about the wellbeing of a data subject it may refer the person concerned to another specialist service provider/agency).

Article 6 (1) (f): processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This legal basis does not apply to processing carried out by the Department in the performance of our tasks, where the Department forwards a letter to a client from a private pension provider who is seeking to contact the client for the purpose of paying a pension entitlement.

To the extent that the Department processes special categories of personal data including biometric data and data concerning a person's health, the legal bases upon which the Department mainly relies are:

Article 9 (2) (b): processing is necessary for the carrying out of obligations and specific rights in the field of employment and social security and social protection law;

Article 9 (2) (g): processing is necessary for reasons of substantial public interest

Article 9 (2) (h): processing is necessary for the assessment of working capacity and the provision and management of social care systems and services.

6.2 The Department operates under a number of Acts which provide that personal data may be legally processed. The main Act is the Social Welfare (Consolidation) Act, 2005, as amended. An administrative consolidation of the 2005 Act can be viewed here. There are also a number of other pieces of primary and secondary legislation that allow the Department to process personal data. Should you wish to know more about these, please see the list which is included in Appendix 1.

6.3 The Department is also entitled to process personal data under other legislative provisions that provide the basis for all Government Departments to administer services and supports and to share data for these purposes.

Law Enforcement Directive (LED)

6.4 The LED deals with the processing of personal data for 'law enforcement purposes' by data controllers which fall within the definition of being a 'competent authority' for the purposes of the LED, as transposed into Irish law, mainly by Part 5 of the Data Protection Act 2018.

6.5 Section 70 of the Data Protection Act 2018 defines the scope of processing of personal data which falls within that part of the Act. It states that Part 5 of the Act applies to the processing of personal data carried out

"for the purposes of (i) the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against, and the prevention of threats to public security, or (ii) the execution of criminal penalties…"

6.6 The term 'competent authority' is defined in Section 69 of the Data Protection Act 2018 as being, inter alia,

"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".

6.7 For certain processing activities which it carries out, the Department is a 'competent authority' for the purposes of Part 5 of the 2018 Act.

6.8 The legal basis for the Department to process personal data as a 'competent authority' is Section 71(2) of the Data Protection act 2018 which provides:

"The processing of personal data shall be lawful where, and to the extent that –

(a) The processing is necessary for the performance of a function of a controller for a purpose specified in section 70(1)(a) and the function has a legal basis in the law of the European Union or the law of the State…."

6.9 The Social Welfare (Consolidation) Act 2005 as amended, most notably Sections 250 – 279 of that Act, provide for the prevention, detection, investigation and prosecution of social welfare fraud. An administrative consolidation of the 2005 Act can be viewed here.

The Compliance and Anti-Fraud Strategy 2019 – 2023 gives detail on the type of control activities undertaken by the Department.

Section 7: The categories of processing undertaken by the Department

Section 7: The categories of processing undertaken by the Department

7.1 We process personal data for the following purposes:

7.1.1 To provide personal public service numbers (PPSNs).

7.1.2 To validate and authenticate identity, to conduct SAFE registrations and to provide Public Services Cards (PSCs) as a token of such registration. PSI data is also made available to support identity authentication by other specified bodies – further details can be found in the Comprehensive Guide to Safe Registration and the PSC.

7.1.3 To collect and associate social insurance contributions with specific identifiable individuals in order to properly record any entitlement to certain schemes and payments either now or in the future – for example the State Contributory Pension.

7.1.4 To check a person's eligibility for access to any working age or illness related schemes and if eligible, to arrange for the payment of the relevant amount to the person concerned.

7.1.5 To process applications for any of the range of employment or other supports that we provide and for related services.

7.1.6 To provide services and supports to employers.

7.1.7 To provide supports for people who lose their jobs due to redundancy or the insolvency of an employer.

7.1.8 To handle contracts with external service providers.

7.1.9 To deal with customer service complaints.

7.1.10 To respond to queries and service requests from people (e.g. to provide statements of contributions made and payments received).

7.1.11 To make payments to people.

7.1.12 To review and check continued entitlement of any person to receive income supports and services. For example, about every 18 months forms are sent to most Child Benefit claimants. The forms must be completed and returned to the Department because they help us to determine if payment should continue. If the forms are not completed the Department will suspend the Child Benefit payments.

7.1.13 To review the use of our schemes and services to inform the evaluation and development of policy.

7.1.14 To assist in the management of our schemes and services and to detect and remedy any fraud or error in the payment of benefits.

7.1.15 For internal human resources functions.

In certain situations, data may also be shared with other organisations, in accordance with legislation and as outlined in Section 9.

7.2 Automated Decision Making

An automated decision is a decision which is made entirely by a computer system, without the intervention of one of our officers.

The Department uses a number of automated decision making processes, but in all cases, the automated decision is limited to successful awards of a payment or service. A person will only receive an automated notification if they have been successful in their claim. This means, where a computer system indicates that a person may not qualify for a payment, the system will refer the application concerned to an officer of the Department. That officer reviews the application and determines entitlement and it is that officer who will correspond with the person concerned.

In this way, there is no situation where a person will be refused payment by a computer system. In addition, customers always have the right to appeal against a decision and/or seek a review of a decision made by the Department.

7.3 Profiling

Profiling involves the processing of personal and other data in order to inform business or customer service decisions. The Department uses profiling techniques in two areas – assessment of a person's employability and assessment of potential fraud and error risk.

7.3.1 As provided for in Section 244A of the Social Welfare (Consolidation) Act 2005 as amended and Statutory Instrument 373/2012, the Department uses personal data to assess an unemployed jobseekers likelihood of securing employment.

This assessment involves the completion of a questionnaire by the jobseeker concerned. This information in turn informs the approach taken by the Department in the provision of employment supports and service to the person concerned.

7.3.2 The Department also analyses trends and patterns in claimant payments in order to identify potential cases where there is a higher than normal risk of fraud and error. These cases are then selected for review, and action if appropriate.

Section 8: Where do we store your personal data?

Section 8: Where do we store your personal data?

8.1 Electronic Storage of Your Personal Data

Personal data stored by the Department is stored electronically on our internal ICT (Information and Communications Technologies) systems located in secure, Department owned and operated, data centres. These systems are fully protected by anti-virus and anti-malware software. Electronic data includes scanned copies of application forms, evidence of identity, contact information, financial information, family details, educational and training achievements, copies of electronic correspondence, social insurance contributions, employment history and claim history.

Access to personal data is restricted to those staff members who need the information to carry-out their official duties. Access is controlled by every staff member having a unique login username and password and with usernames being linked to the minimum permissions necessary to allow the staff member to work in a secure environment and to only access the personal data that they need for their jobs. In addition, our staff members are not allowed to deal with claims from relatives, close friends and colleagues/ex-colleagues known personally to them.

Some personal data provided by clients to contractors retained by the Department in order to provide services on its behalf (for example JobsIreland online jobsite, Local Employment or Community Employment Services) is stored in Ireland by third party contractors who are subject to GDPR and are required under contract with the Department to adhere to specified policies with respect to the collection, processing and storage of data.

8.2 Storage of Hard Copy (Paper) Files

Where the Department holds paper records containing a person's personal data, these are stored on individual files which are held in secure premises. Where personal files are held in storage by external providers only the staff of the provider can physically access the files. Retrieval of files is limited to named staff within the Department and will only be delivered to registered offices of the Department. Requested files are delivered to the requesting office by registered post or secure courier by a recorded delivery. Soft copies of files, if required, will only be supplied to pre-approved staff members of the Department.

This is achieved through physical security, where access to a Department office is by a swipe card or access card and where visitors are screened, signed in and accompanied by a member of staff, so that they cannot access any personal data stored by the Department.

Section 9: Sharing personal data

Section 9: Sharing personal data

9.1 The Department may share information with and receive information from other organisations. The Social Welfare Consolidation Act 2005 as amended allows for data sharing with public bodies including information concerning income and social welfare payments and public service identity details. The Department can share a person's public service identity details with a range of organisations that are listed in schedule 5 of that Act and can be found here on Pages 542 to 544. Legislation governing other bodies provides for sharing of personal information with the Department.

The Department works closely with other parts of government, non-governmental, and community organisations to help deliver many supports and services. These include services such as the provision of income supports, employment services, social security, services to employers, and other services for children, students, people at work, those with disabilities/illnesses or who have retired.

When acting as a public authority providing services and income supports the sharing of personal data conforms with the requirements of the GDPR. When sharing data for the purpose of preventing, detecting, investigating or prosecuting social welfare fraud, the Department is acting as a 'competent authority' and the appropriate legislative framework is the Law Enforcement Directive and Part 5 of the Data Protection Act 2018 (See Section 6).

9.2 The Department and the Revenue Commissioners work very closely together, and share information on a continuous basis. This is because social welfare entitlements are affected by how much a person earns and the PRSI a person pays. Benefits, pensions and other payments a person receives from the Department affect how much tax they may have to pay, or the tax credits that Revenue may allow.

Information is also shared between both organisations to prevent and detect suspected fraud or wrongful activity that could result in incorrect payments being made by the Department and/or tax payments to Revenue being avoided.

Personal information exchanged with Revenue includes identifying details, data relating to employers, PRSI contributions paid, earnings, income and social welfare payments made.

9.3 The categories of other organisations that the Department would normally share information with/ receive information from are as follows:

- **9.3.1** Government Departments to provide for a range of shared services, supports and statistical information. An example is the Department of Education and Skills where data in relation to participants on schemes co-funded by the European Social Fund(ESF)is given to the Department of Education and Skills who is the managing authority of ESF in Ireland to facilitate a claim for re-imbursement from the fund. Another example includes sharing income and identity information with the Department of Children and Youth Affairs for childcare application,

- **9.3.2** Other public sector bodies or agencies which provide services or supports to customers such as the HSE (PSI data for the purpose of the Individual Health Identifier project and the Primary Care Reimbursement Service, i.e. medical cards), Student Universal Support Ireland (grant applications for third level colleges). The Department also shares personal data with other Departments/

Agencies such as An Garda Síochána for the prevention, detection, investigation and prosecution of offences. Section 41(b) of the Data Protection Act 2018 allows us to do this,

- **9.3.3** Educational bodies and institutions,
- **9.3.4** Local Authorities: for example we share data in relation to Housing Assistance Payment (HAP) Tenancies,
- **9.3.5** Social Security organisations in other countries: Data can be made available to, or received from, any member state of the European Union/European Economic Area in respect of an individual customer to help ensure they receive the correct social welfare entitlements,
- **9.3.6** Employers: We record the employer engagement activity between the Department and Employers. This data can include information on upcoming vacancies that the employer may make available to jobseekers on the live register,
- **9.3.7** Community organisations providing activation supports, work placement schemes or training and education courses (such as Tús schemes, Community Employment Schemes, local training initiatives etc),
- **9.3.8** Private contractors providing key services and supports to customers, including Branch Managers, Local Employment Service companies, Jobs Clubs and JobPath providers,
- **9.3.9** Regulators or supervisory authorities: Customer data is shared with regulators where necessary to deal with complaints/ investigations,
- **9.3.10** Public representatives who make representations on behalf of constituents,
- **9.3.11** IT consultants and general contractors hired by the Department, where they may be working on enhancing the Department's data handling systems & processes,
- **9.3.12** Banking and Payment Service Providers used by the Department to make payments to clients.

Section 10: Will your personal data be transferred out of the European Economic Area i.e. to ‘Third Countries’?

Section 10: Will your personal data be transferred out of the European Economic Area i.e. to 'Third Countries'?

10.1 There may be occasions when personal data needs to be transferred outside the European Union or the European Economic Area or EEA (EU countries, plus Iceland, Norway, and Liechtenstein). Where we do transfer information outside the EEA to third countries, we will always take steps to ensure that any transfer of information is carefully managed to protect privacy rights under the GDPR.

10.2 The Department has bilateral agreements with some countries outside the EEA which are listed at Appendix 2. These are legally binding agreements, the main purpose of which is to protect the pension rights of people who have worked and paid social security contributions in Ireland and those countries. This is achieved by allowing reckonable social security contributions paid in one of these countries to be aggregated with Irish full-rate social insurance contributions for the purposes of qualifying for certain contributory payments in Ireland or in those other countries. The agreements also deal with the social security status of workers who are sent on temporary assignments from one country to the other. These agreements provide for a range of measures, including the exchange of information, required to implement their provisions.

Any transfer of data to third countries is safeguarded in accordance with Chapter V GDPR.

Section 11: How long will we keep your personal data?

Section 11: How long will we keep your personal data?

11.1 Social insurance contribution records, PPSN, past claim data and identity data are retained for the lifetime of the person concerned plus a period of ten years. This is required for a number of reasons:

First, in order that a person can claim entitlement to services and benefits – many of which may not fall due until the occurrence of a particular event during the lifetime of a person – the date of which cannot be known, for example illness, disability, caring responsibilities or widowhood.

Second, PPSN and identity data is critical to the prevention, detection and prosecution of identity fraud, which again can occur at an unknown time. It is also critical to the efficient administration of estate cases (i.e. payments made or refunded after a person dies). Estate cases can take a number of years to resolve.

Third, prior claim data is required because it can affect entitlement to future payments, because, under law, a person can request a review in respect of any claim decision at any time. Also it can be necessary to inform an investigation into a prior fraud or error which is detected on the occasion of a subsequent claim or life event.

11.2 Documents that support claim and identity data (e.g. documents evidencing income and identity) may be retained for so long as the claim and identity data is retained. This is necessary in order to support prosecution and resolution of any issue that may emerge relating to a person's entitlement to a service or benefit or to their identity. For example, even after a claim closes or a service ceases, issues can arise when a person's estate is being settled, when the person subsequently claims another benefit or service or when another person seeks to claim a service or benefit in the name of the first person. In addition the Department can be called upon at any time to verify the identity of any person to whom it has issued a PPSN.

11.3 Where data (other than social insurance contribution, PPSN, identity, and claim data) is collected or processed as part of an ongoing department/client relationship then it may be retained for the lifetime of that relationship plus ten years. (For example data relating to the provision of employment services to a person will be retained for so long as the person concerned is in receipt of employment services plus up to ten years). The retention of the data for up to a ten year period after the direct service relationship ends enables the Department to access prior service history in the event that the person concerned re-engages with the service at a future date.

11.4 Where other transactional data is collected it will be deleted as soon as its purpose has been served. An example of this is where the Department may generate customer lists for invitations to jobs fairs. These lists are deleted within six months of the conclusion of the relevant event.

11.5 The Department's retention policy can be found here.

Section 12: Additional processing of personal data

Section 12: Additional processing of personal data

12.1 **Will your personal data collected be used for any other purposes?**
As mentioned earlier, the Department is allowed by law to collect and process personal data for a range of reasons. We are also allowed to collect personal data for a specific reason and use it for another compatible purpose. This is because the Department provides a wide range of related services and it would be impractical for us, and inconvenient for the person, if we repeatedly asked the person for the same information repeatedly.

12.2 An example of this is the information that may be supplied by a person for a Jobseeker's claim, but this information may be used to later provide education or training supports or supports such as the Back to School Clothing and Footwear Allowance or the Fuel Allowance. In this way, we are better able to help the person with their income needs and to progress from dependency on a welfare payment into employment.

12.3 Another example is that information that may be provided by a person for a State Pension might be used to allow the customer to receive a free-travel pass or a household benefits package.

12.4 Another example is the biometric processing of photographs provided as part of the SAFE identity authentication process/issuing of PSCs. This biometric processing of the photograph produces an arithmetic template which allows precise comparison of the photograph in question with others held by the Department.

This in turn helps to identify cases where the same person has sought to register twice or more under different names. It also helps to identify cases where a person seeks to assume the identity of another person, so protecting against identity theft. This biometric processing is performed by the Department and the arithmetic template produced is not shared with any other specified body nor is it stored on the PSC.

12.5. As stated in Section 4 a person's personal data may be processed if it is needed to decide how much to pay someone related to you or in your household or for whom you are caring.

Section 13: Your rights as a data subject

Section 13: Your rights as a data subject

All our customers (data subjects) have certain rights under the GDPR and the Data Protection Acts:

13.1 The right to information

You have a right under Articles 13 and 14 of the GDPR to information on your personal data processed by the Department, including:

- the purposes of the processing,
- the legal basis for it,
- the categories of personal data held,
- the original source of the data,
- the recipient or categories of recipients of your data,
- the period for which it will be stored,
- whether your data has been or is intended to be transferred to a third country or international organisation.

This privacy statement serves to provide you with the above information.

13.2 The right to access your personal data (the information that we have on you)

You are entitled to ask us for copies of any of your personal data that we have collected and stored. Such requests can be submitted in writing to **Subject Access Requests Section, Social Welfare Services Office, Shannon Lodge, Carrick-on-Shannon, Co. Leitrim** or by e-mail at SARS@welfare.ie. We will need to verify your identity before we deal with any request for copies of your personal data. Under the GDPR, we have one month in which to process these requests.

13.3 The right to rectification

We always try to make sure that the information we have about you is accurate and up-to-date. Sometimes we may ask you to verify this information. If your information changes or you believe that we have information which is not up-to-date, please let us know. This can be information such as your address, when you start work, when you are earning more or when your family details change.

We cannot allow anyone else but yourself to update your personal data, unless you have fully authorised a personal representative.

13.4 The right to erasure of personal data

Each person in respect of whom the Department holds data has the right to ask the Department to delete any information held, subject to the provisions of the GDPR. As set out in Section 11, given the nature of the services and benefits the Department provides, it is necessary for the Department to retain some data for a lengthy period of time.

The Department processes personal data it collects because there is a statutory basis for the processing. Where the Department receives a request from you looking to exercise your right of erasure then the Department will carry out an assessment of whether the erasure of the data concerned is required under the GDPR. In so doing, it will take into account whether any such

erasure would reduce the ability of the Department to provide services to you, to assure the integrity of its services and payments, to protect the rights of other people to whom the Department provides services and to perform its statutory functions.

If you wish to avail of this right to erasure of personal data, you can contact us either in writing or by email. (See contact details below at Section 14).

13.5 The right to restriction of processing

In certain circumstances you have the right to request that we restrict processing of your personal data. This is provided for under Article 18 of the GDPR. The Department will assess whether a person's request to restrict the processing of their data can be implemented.

If you wish to avail of this right, you can contact us either in writing or by email (see contact details at Section 14).

13.6 The right to object

13.6.1 You have the right to object to the processing of your personal data where that processing is being carried out:

- for the performance of a task carried out in the public interest or under official authority of the data controller,
- for the purposes of legitimate interests pursued by the data controller or by a third party.

The processing of personal data for the above reasons can be stopped at your request unless there are compelling legitimate grounds for the processing which:

- override the interests, rights and freedoms of the data subject,
- are required for the establishment, exercise or defence of legal claims.

If you wish to avail of this right, you can contact us either in writing or by email. (See contact details at Section 14). You should set out clearly the personal data involved and the reasons why you consider processing should be restricted. We will either grant your request without undue delay or explain to you why we will not do so.

13.6.2 The right to object to automated decision making including profiling:

The GDPR gives you the right to object to automated decision making by the Department's computer systems, where there is a legal or significant impact on you as a customer. As stated in Section 7.2, there is no situation in the Department where a customer will be refused payment due to an automated decision.

13.7 The right to data portability

The Department processes personal data it collects usually because there is a statutory basis for the processing. Where the Department has collected your personal data by consent or by contract then you have a right to receive the data in electronic format to give to another data controller.

This right cannot be used to interfere with the Department's main functions – see Section 1

If you wish to avail of this right, you can contact us either in writing or by email setting out the data which you would like to receive and the format in which you wish it to be delivered. (See contact details below at Section 14).

13.8 The right to withdraw consent

In circumstances where the Department relies on your consent for the purposes of data processing you may withdraw this consent at any time. If you wish to withdraw consent please contact us in writing or by email setting out the data processing which you wish to have ceased. (See contact details below at Section 14). The Department will consider if its right to conduct this data processing is dependent on your consent and will advise you of its decision in writing.

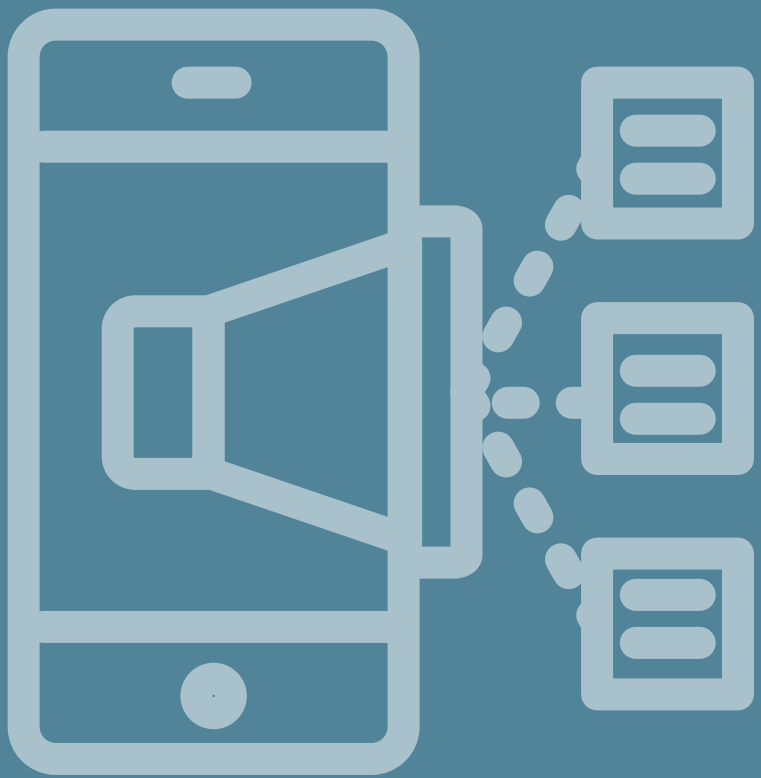
13.9 The right to be notified of a Data Breach

A personal data breach is defined as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed,"

In the unlikely event that your personal data is breached, the Department will notify the Data Protection Commission unless the breach is unlikely to result in a risk to your rights and freedoms. If it is considered that the breach results in a high risk to your rights and freedoms, we will also notify you of the breach.

Section 14: How can you exercise your rights and get in touch with us?



Section 14: How can you exercise your rights and get in touch with us?

We must allow you to exercise your rights as outlined in Section 13. You can make a request under any of these rights by contacting the Department's DPO at this address:

By post: Data Protection Officer,
Department of Social Protection,
Goldsmith House,
Pearse Street,
Dublin 2.
By email: dpo@welfare.ie

Subject Access Requests should be sent to Subject Access Requests Section, Social Welfare Services Office, Shannon Lodge, Carrick-on-Shannon, Co. Leitrim or by email to: SARS@welfare.ie

We may need you to confirm your identity first, as we cannot give your personal data to others.
Once we have verified your identity, we will seek to get the information that you have requested as soon as possible.

If you make an electronic request, we must respond to you electronically, unless you prefer otherwise.

Anything we do in response to your request and any information we provide will generally be performed free of charge. If you make excessive requests (e.g. make the same one repeatedly) or your requests have no basis in fact, we may either charge you a fee or refuse to act on it. We will not charge you a fee where you have made a mistake, but will not act on your request.

Depending on the detail provided we may ask you to clarify your request. You can help us to fulfil your request about personal data by being as specific as possible particularly about your dealing or contacts with us.

If you have any queries about this privacy statement, please contact the Data Protection Unit (DPU) at DPO@welfare.ie

The Department works hard to handle your data responsibly and we take our data protection responsibilities seriously. If you are unhappy about the way that we do this, please contact the Department's Data Protection Officer at the address set out above. In addition, you also have the right to complain to the Data Protection Commission (DPC). The DPC can be contacted:

By post : Data Protection Commission,
21 Fitzwilliam Square South,
D02 RD28
By email: info@dataprotection.ie
By phone: 01 765 0100 or lo call number 1800 437 737

Section 15: Further information - Operational Guidelines

Section 15: Further information - Operational Guidelines

If you would like any more information on how an area of the Department works and what is required to make a decision on a claim or service, then please go to our website at www.gov.ie/dsp. Information on each of our schemes includes operational guidelines.

Appendix 1 – List of primary and secondary legislation under which we have the authority to collect personal data

Primary legislation (all as amended)	
Social Welfare Consolidation Act 2005	The Comhairle Act 2000
The Protection of Employees (Employers' Insolvency) Act 1984	The Civil Registration Acts 2004 – 2014
The Pensions Act 1990	The Gender Recognition Act 2015
Citizens Information Acts 2000 - 2007	Redundancy Payments Act 1967

Key secondary legislation (statutory instruments)
S.I. No, 142 of 2007 - Social Welfare (Consolidated Claims, Payments and Control) Regulations 2007
S.I. No. 412 of 2007 - Social Welfare (Consolidated Supplementary Welfare Allowance) Regulations 2007
S.I. No. 102 of 2007 - Social Welfare (Consolidated Occupational Injuries) Regulations 2007
S.I. No. 312 of 1996 - Social Welfare (Consolidated Contributions and Insurability) Regulations 1996
S.I. No. 108 of 1998 – Social Welfare (Appeals) Regulations 1998
S.I. No. 188 of 1998 - Social Welfare (Rent Allowance) Regulations 1998

Appendix 2 – Bi-lateral agreements with countries outside the EEA

Country/province outside the EEA with whom DSP transfers personal data

Australia

S.I. No. 799/2005 - Social Welfare (Revised Agreement with Australia on Social Security Order, 2005)

Canada

S.I. No. 317/1991 - Social Welfare (Agreement with Canada on Social Security) Order, 1991.

Quebec

S.I. No. 120/1995 - Social Welfare (Understanding with Québec on Social Security) Order, 1995.

Japan

S.I. No. 527/2010 - Social Welfare (Agreement with the Government of Japan on Social Security) Order 2010.

Republic of Korea

S.I. No. 552/2008 - Social Welfare (Agreement with the Republic of Korea on Social Security) Order 2008.

New Zealand

S.I. No. 57/1994 - Social Welfare (Agreement with New Zealand on Social Security) Order 1994.

Switzerland

S.I. No. 206/1999 - Social Welfare (Agreement with The Swiss Confederation on Social Security) Order, 1999

United Kingdom (Isle of Man, Jersey and Guernsey)

S.I. No. 701/2007 - Social Welfare (Bilateral Agreement with the United Kingdom on Social Security) Order 2007.

United Kingdom
Following the end of the transition period of the UK's withdrawal from the EU the following legislation now applies:

Convention on Social Security between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of Ireland.

United States of America

S.I. No. 243/1993 - Social Welfare (Agreement with the United States of America on Social Security) Order 1991.