

# DATA SHARING AGREEMENT

Sharing of personal data between the Department of Employment  
Affairs and Social Protection and Central Statistics Office

---

---

## **1. Agreement and Parties to the Agreement**

This Data Sharing Agreement governs the sharing of data between the Department of Employment Affairs and Social Protection (hereafter 'the Department') and the Central Statistics Office (CSO) in relation to the management, administration and/or operation of INFOSYS access within the CSO.

This Data Sharing Agreement is between the Department with its principal office at Aras Mhic Dhiarmada, Store St, Dublin 1 and the CSO with its principal office at Shehard Road, Cork (together 'the Parties').

## **2. Scope of the Data Sharing Agreement and Governance**

The Parties will ensure that the Data Sharing Agreement remains fit for purpose, accurate and up to date. This Data Sharing Agreement will lapse 3 years from the date of signature. This time period may be altered by the Department or CSO and is subject to review in the light of any future legislative changes. Any amendments to the Data Sharing Agreement will be signed by the Parties.

The Parties shall ensure that all relevant staff are aware of and act in compliance with the Data Sharing Agreement.

The Parties will actively monitor and periodically review the data sharing arrangement to ensure that it continues to be compliant with data protection law, that it continues to meet its objective, that safeguards continue to match any risks posed, that records are accurate and up to date, that there is

---

---

adherence to the data retention period in para 7.13, and in particular to ensure that an appropriate level of security is maintained.

### **3. Roles of The Parties**

**Department:** Data Controller (as defined in the Data Protection Acts 1988 and 2003 - DPA) as the owner of the data and as the body providing approval for access to the INFOSYS system.

**CSO:** Data Controller as the body receiving access to the INFOSYS system and using it for its own purposes as set out in para no. 4 of this Data Sharing Agreement.

### **4. Purpose of Data Transfer**

The Central Statistics Office has requested The Minister to provide access to the computerised records of her Department insofar as they are necessary for the efficient discharge of their functions in relation to the administration of the following schemes.

- **Survey on Income and Living Conditions (SILC),**
- **the Household Budget Survey (HBS) and**
- **the Household Finance and Consumption Survey (HFCS)**

The Central Statistics Office (CSO) has requested access to INFOSYS for the purpose of gathering and verifying PPSNs relating to respondents that participate in the Survey. In order to reduce the burden on respondents (an important factor given the lengthy nature of the questionnaires) SILC, HBS and HFCS collect the PPS number of survey respondents and will use this number to link to administrative data, for example social transfer payments etc held on file in the CSO's Administrative Data Centre. After the interview is completed in the field, the encrypted data is returned to the CSO office. The PPS number is then used to access administrative data. This will significantly reduce the time taken by respondents and households to answer the SILC, HBS and HFCS questionnaires as otherwise the CSO would have to ask respondents about all the individual payment schemes that they are eligible for. It will also allow the CSO to access the exact payments made to respondents during the reference period of both surveys (i.e. the 12 month period prior to the date of interview), thus improving the accuracy of the data.

The PPS number will be used to access:

- 
- 
- (1) CS - Client Search : Used to search for or verify the PPS number of Survey respondents by name or address.

## **5. Type of Data Being Requested:**

The Department agrees to provide personal data which expression shall have the meaning ascribed to it by the DPA and will only be accessed in connection with the purposes for which it has been provided.

The personal data sought is sufficient to enable CSO to achieve the stated purposes and no more.

## **6. Legislative Basis for Data Sharing**

### **6.1 Department Legislation As Basis For Sharing Data**

**The Social Welfare Consolidation Act 2005** provides a legislative basis for the provision of INFOSYS as follows:

#### **Exchange of Information**

261. (2) Information held by the Minister for the purposes of this Act or the control of schemes administered by or on behalf of the Minister or the Department of Social and Family Affairs may be transferred by the Minister to another Minister of the Government or a specified body, and information held by another Minister of the Government or a specified body which is required for those purposes or the control of any such scheme administered by another Minister of the Government or a specified body may be transferred by that Minister of the Government or the specified body to the Minister.

## **7. Obligations of CSO**

The Department agrees to provide access to INFOSYS for the specific purpose outlined in para no. 4 of this Data Sharing Agreement subject to the following



---

---

terms and conditions and CSO unreservedly accepts these terms and conditions:

7.1 Information which originates from the Department will be processed by CSO as a data controller;

7.2 CSO will fully comply with the requirements of the DPA, and any legislation amending or extending same, in relation to its use of and the manner by which it processes any and all data supplied by the Department;

7.3 CSO shall adhere to the procedures at para no. 9 regarding the granting of access to INFOSYS;

7.4 CSO acknowledges the duty of care it owes to citizens in respect of whom any data has been received from the Department. Accordingly, CSO shall keep the personal data secure and shall take such measures as may be necessary to ensure no unauthorised access, alteration, disclosure, deletion or disposal of the data whether it is held in electronic or written format;

7.5 CSO will take appropriate technical and organisational measures to comply with all their obligations under the DPA. This includes, but is not limited to, the following:

- Policies, guidelines and procedures governing information security.
- Password protection for computer access.
- Automatic locking of idle PCs.
- Appropriate virus-checking software and firewalls used to protect integrity and security of electronically processed data.

- Unique identifiers for every user with access to data.
- Employees have access only to personal data required for them to do their jobs.
- Adequate security where remote access is allowed.
- Encryption of data held on portable devices.
- Logs of data accesses.
- Data breach procedures.
- Adequate physical security.
- Staff training and awareness.
- Monitoring of staff accessing data.
- Controlling physical access to IT systems and areas where paper-based data are stored.
- Adopting a clear desk policy.
- Appropriate techniques for destruction of data.
- Having back-ups of data off-site.

7.7 CSO shall not request or process personal data from the Department for any purpose other than in connection with purposes set out in para no. 4 of the Data Sharing Agreement or in accordance with the law;

7.8 CSO will fully comply with the requirements of the Social Welfare Consolidation Act 2005 in relation to the use of the Personal Public Service Number / Public Service Identity data, and any legislation amending same;

7.9 CSO will not reveal personal data to any unauthorised person;

7.10 CSO shall obtain from each of its employees having access to the data a signed declaration warranting personal compliance with the terms of the DPA (and any amending legislation) and with this Data Sharing Agreement;

7.11 CSO shall ensure that employees having access to the data are properly trained and aware of their data protection responsibilities in respect of that data;

7.12 Access to the data supplied by the Department will be restricted to persons on the basis of least privilege, sufficient to allow such persons carry out their role;

7.13 Data will be retained by CSO for a **period of 5 years** and will be destroyed in an appropriate, secure manner;

7.14 In so far as the data shared is processed by CSO as a data controller, CSO will deal with data subjects in their exercising of rights, including but not limited to, the right to be informed of the existence of personal data, the right of access, the right of rectification, blocking, erasure and destruction.

7.15 If a breach of the data supplied by the Department is caused by CSO or its agents, CSO will act in accordance with the Office of the Data Protection Commisisoner's data security breach Code of Practice;

7.16 CSO will notify data subjects whose data is received from the Department of the following:

- CSO role as data controller of the data
- the purpose of the processing of the data by CSO



- the categories of data processed
- the identity of the Department as the supplier of the data
- how the data subject may exercise their data protection rights
- other relevant information as set out in Section 2D of the DPA and the Data Sharing in the Public Sector guidelines produced by the Office of the Data Protection Commissioner.

At a practical level, the expectation is that where application forms or standard documentation in signing up new customers or clients are used, CSO should explain the purpose/uses on such forms or documentation. This information should also be displayed on the Council's Privacy Statement and Data Protection Notice.

7.17 CSO shall indemnify and keep indemnified the Department in full from and against all claims, proceedings, actions, damages, losses, penalties, fines, levies, costs and expenses, whether direct or indirect and all consequential or indirect loss howsoever arising out of, in respect of or in connection with any breach by CSO including their servants with data protection requirements;

7.18 CSO agrees that its Compliance Officer shall be responsible for the administration and control of Infosys accounts issued to staff within CSO functional areas. Such administration will include, but not limited to, notifying the Minister of all staff commencements, movements and cessations in those cases where access to personal data is to be commenced, modified or terminated. It should also be noted that transferring of accounts is not permitted



## Compliance Officer

Name	Location
Anne Grimes	Household Survey Processing CSO

7.19 CSO will confirm to the Department in writing when asked that it is complying with the terms of this Data Sharing Agreement.

## 8. Obligations of the Department

8.1 The Department will fully comply with the requirements of the DPA and any legislation amending or extending same, in relation to the data supplied to CSO;

8.2 The Department shall, in respect of Shared Personal Data, ensure that their privacy notices are clear and provide sufficient information to Data Subjects in order for them to understand what of their Personal Data the Parties are sharing, the circumstances in which it will be shared, the purposes for the data sharing and either the identity with whom the data is shared or a description of the type of organisation that will receive the Personal Data.

8.3 The Department reserves the right to terminate, without notice, access to personal data where the Department has reason to believe any of the conditions of this Data Sharing Agreement are not being observed. Where a service is so terminated, the Department shall provide to CSO the

---

---

Department's reasons for terminating the service as soon as is practicable following termination. Where the Department is subsequently satisfied that the conditions of this Data Sharing Agreement are being observed, access will be restored forthwith. The Department will accept no responsibility for any consequences arising from the exercise of this right

8.5 The Department agrees that the Officer who signs this Data Sharing Agreement, shall oversee the adherence to terms and conditions of this Data Sharing Agreement.

## **9. Procedures for granting access Infosys to CSO**

Access to the Department's customer information systems (Infosys) (which is permitted under Section 261 of the Social Welfare Consolidation Act 2005 for the purpose of performing their public functions) is managed by CIS Division. Before authorising access to Infosys, a business case has to be made by and accepted from a nominated compliance officer in the agency concerned. Access is granted strictly on the basis of a business need and is restricted to named individuals. The level of access is determined by business requirement which in turn determines the User Group that the organisation is assigned to by CIS. The protocol involved in granting such access includes ensuring CSO is aware of its responsibilities under both social welfare and data protection legislation. Each user is required to sign a data protection agreement to state that s/he is aware of her/his data protection obligations.

Signature: Edel McGloin

Date: 16/5/18

Name: EDEL MC GLOIN

Position: AP., CTS.

For and on behalf of Department of Department of Employment Affairs and  
Social Protection

In the presence of

Signature: Anne Marie Freeman

Date: 16/5/18

Name: Anne Marie Freeman

Department of Employment Affairs and Social Protection

---

Signature: Caitiona O'Brien

Date: 16/5/18

Name: CAITIONA O'BRIEN

Position: STATISTICIAN

For and on behalf of CSO

In the presence of

Signature: Anne Grimes

Date: 16/5/18

Name: ANNE GRIMES

CSO



