Data Protection Policy

May 2018

ISI

Tackling problem debt, together

Insolvency Service of Ireland
Data Protection Policy

1. Contents

1 Introduction

The Insolvency Service of Ireland (the ISI) collects, processes and stores significant volumes of sensitive and personal sensitive data on an ongoing basis. The Data Protection Acts 1988 to 2018 together with the EU General Data Protection Regulation (GDPR) confer rights on individuals as well as responsibilities on those persons and organisations processing personal data.

This policy applies to all data held by the ISI. This includes electronic and paper records; it also includes all CCTV images in the ISI.

2 Ownership

The Data Protection Policy is maintained by the ISI's Data Protection Officer (DPO) and is approved by the Senior Management Team. The policy will be reviewed at least annually by the DPO to ensure alignment to appropriate risk management requirements and its continued relevance to current and planned operations, or legal developments and legislative obligations.

Further comments or questions on the content of this policy should be directed to the DPO. Any material changes to this policy will require approval by the Senior Management Team.

3 Glossary

The following table identifies some of the terms referred to within this policy.

Term	Definition
Data	Information in a form that can be processed. It includes both automated data and manual data.
Automated data	Any information on computer or information recorded with the intention of putting it on computer. It includes not only structured databases but also emails, office documents or CCTV images.
Manual data	Information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system – this includes temporary folders.
Data Controller	A person who (either alone or with others) controls the contents and use of personal data. A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.
Data Processor	A person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment. If an organisation or person holds or processes personal data, but does not exercise responsibility for or control over the personal data, then they are deemed to be a "data processor".

Term	Definition
Data Protection Officer (DPO)	An ISI appointed officer with responsibility for the Data Protection compliance of the organisation.
Data Subject	A data subject is an individual who is the subject of personal data that is held by a data controller or processed by a data processor.
GDPR	The EU General Data Protection Regulation (GDPR) - Regulation 2016/679 came into effect on 25 May 2018.
Personal Data	Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller
Processing	Processing means performing any operation or set of operations on data, including: • Obtaining, recording or keeping data; • Collecting, organising, storing, altering or adapting the data; • Retrieving, consulting or using the data; • Disclosing the information or data by transmitting; • Disseminating or otherwise making it available; • Aligning, combining, blocking, erasing or destroying the data.
Sensitive Personal Data	Any personal data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

4 Scope of Policy Document

This policy has been drawn up by the ISI and as such is applicable to all ISI personnel (i.e. staff and contractors) and relevant third party providers.

All staff have a personal responsibility to ensure compliance with the data protection principles and to adhere to the ISI's Data Protection Policy.

Line Managers are responsible for ensuring compliance with the ISI's Data Protection Policy within their division. They are also responsible for ensuring that staff in their area are aware of the policy.

The ISI's Data Protection Policy applies to data records of all types regardless of the medium on which they are held. The functions of the ISI are set out in section 9 of the Personal Insolvency Act 2012. In carrying out these functions the ISI collects and uses information in order to:

- Monitor the operation of the arrangements relating to personal insolvency
- Consider applications for debt relief notices
- Process applications for protective certificates

- Maintain public registers in relation to protective certificates; debt relief notices; debt settlements arrangements; personal insolvency arrangements; approved intermediaries and personal insolvency practitioners
- Authorise persons to perform the functions of an approved intermediary
- Supervise and regulate persons or classes of persons authorised to perform the functions of an approved intermediary
- Authorise individuals to carry on practice as personal insolvency practitioners
- Supervise and regulate persons practising as personal insolvency practitioners
- Prepare and issue guidelines as to what constitutes a reasonable standard of living and reasonable living expenses
- Administer the functions of the Official Assignee
- Manage the estates of bankrupt individuals
- Comply with legal obligations

As part of its role as a data processor, the ISI is responsible for securing the personal data it obtains, transmits, stores or processes. The following list highlights the type of data that is processed by the ISI and is covered by the Data Protection legislation (this list in indicative only, and is not intended to be exhaustive):

- Personal data including:
    - Name, date of birth, PPSN, private address, employer, business address, qualifications, work experience, contact details, marital/family status, employer information/self-employed information, bank details, income, creditors details, benefits, details of assets and property, investments, liabilities
- Sensitive personal data including:
    - Data concerning health, that is, medical information and details of convictions relating to fraud, etc.

5 Data Protection Principles

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

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

[1] Article 5

Article 5(2) of the GDPR also obliges the ISI to "be responsible for, and be able to demonstrate, compliance with the principles" GDPR requires that the processing of personal data is conducted in accordance with the data protection principles set out above. The ISI's policies and procedures are designed to ensure compliance with these principles.

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

Article 6 of the GDPR sets grounds on which personal data processing is lawful. These grounds include '*processing is necessary for compliance with a legal obligation…….. …processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller…….*. Section 37(1) of the Data Protection Act 2018 further states that processing is lawful where it is required for *'……the performance of a function of a controller conferred by or under an enactment or by the Constitution…….'*

The majority of personal data is processed by the ISI in compliance with its functions conferred under the Bankruptcy Act 1988 and the Insolvency Act 2012. Personal data is also processed in the performance of functions in the public interest. The ISI may also process personal data in accordance with certain contracts it has put in place and, in limited circumstances, where it has a legitimate interest in processing specified personal data. In very limited circumstances the ISI may request the consent of the data subject to process their data. In such cases, consent will be sought at the time that the data is collected and the data subject will be advised that they can withdraw their consent at any stage during processing.

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

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

The ISI processes personal data only for the purposes for which it is collected.

Any further proposed processing of data (regardless of apparent compatibility with original purpose) will be the subject of an impact assessment to ascertain if it poses a risk to the rights and freedoms of the data subject. This assessment may take the format of a data protection impact assessment (see below).

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

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

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

5.4 Personal data must be accurate and kept up to date

In order to ensure that the functions of the ISI are delivered efficiently and effectively, the ISI will ensure that, where possible, all personal data held is kept accurate and up to date. ISI Divisions holding personal data are responsible for ensuring that all manual/computer procedures are adequately maintained and that, where notified of inaccuracies, the personal data will be corrected in a timely manner. Data subjects have the right to have inaccurate data held by the isi updated or erased, as appropriate.

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

The ISI will ensure that a data retention policy is in place, which establishes the length of time that personal data is retained and the purpose(s) of its retention. The ISI will ensure that data is not be retained for longer than it is required and will be properly destroyed/deleted when it is no longer needed. In this regard, it is important to note that the ISI has limited control in relation to record destruction due to obligations which arise under the National Archives Act, 1986 and the Freedom of Information Act, 2014.

5.6 Personal data is processed in a manner that ensures appropriate security of the data

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

6 GDPR – Rights of 'data subjects'

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

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

6.1 Right to be informed and right of access

As noted previously data subjects have the right to be informed by the ISI about the collection and use of their personal data. In addition, they have the right to access their personal data and other supplementary information, as appropriate. The ISI has implemented procedures to ensure that all such Subject Access Requests (SAR) are responded to within the one month period as required under Article 12 of the GDPR. Further information on making a Subject Access Request can be found on the ISI website.

6.2 Right to rectification

Data subjects have the right to have inaccurate personal data held by the ISI rectified and to have incomplete personal data updated so that it is complete. On receipt of a request from a data subject for rectification of their personal data, the ISI will take reasonable steps to ensure that the data held is accurate and will ensure that data is rectified, where necessary.

6.3 Right to erasure

Article 17 of the GDPR provides for the right of data subjects in certain circumstances to have their personal data erased ('right to be forgotten'). The right to erasure is not an absolute right and does not apply in circumstances where the ISI's processing of personal data is necessary in particular:

- for the performance of a function of conferred on the ISI by enactment;
- for archiving purposes in the public interest or statistical purposes; or
- where the data is required for the establishment, exercise or defence of legal claims.

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

6.4 Right to restriction of processing[3]

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

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

[3] Article 18

As a matter of good practice, the ISI will restrict the processing of personal data whilst a review of the accuracy of the data and/or the legitimate grounds for processing the data is carried out. This restriction of processing will take into account any Regulations made under Section 60 of the Data Protection Act, 2018.

6.5 Right to data portability

The collection of a significant proportion of personal data by the ISI is lawful in accordance with Article 6.1(c) or 6.1(e) of the GDPR i.e. *'necessary for compliance with a legal obligation*' or '*necessary for a task carried out in the public interest or in the exercise of official authority vested in the controller'*. In cases where the ISI has collected personal data from a data subject by consent or by contract, that data subject can request the ISI to provide the data in electronic format in order to provide it to another Data Controller. The ISI will comply with all such legitimate requests.

6.6 Right to object to processing

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

6.7 Right not to be subjected to automated decision making[4]

Data subjects have the right not to be subjected to a decision based solely on automatic processing, including profiling, that have a legal or similarly significant effect on them. The ISI will ensure that no decision issued to a data subject is based on automatic processing alone.

6.8 Complaints

Data subjects who may be concerned that their rights under the GDPR are not upheld by the ISI can contact the Data Protection Officer (DPO). The DPO will engage with the data subject in order to bring their complaint to a satisfactory conclusion. The DPO's contact details are below. Where the complaint to the DPO cannot be resolved, the data subject will be informed in writing and will be further informed of their right to bring their complaint to the Data Protection Commission.

[4] Article 22

7 Responsibilities of the ISI

The ISI is responsible for the following:

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

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

7.2 Maintaining a record of data processing activities

The ISI maintains a written record of all categories of processing activities for which it is responsible in accordance with GDPR Article 30

7.3 Data Protection agreements with personal data recipients

On an ongoing basis, the ISI puts in place appropriate contracts, memoranda of understanding and bilateral agreements with third parties where personal data is shared. This includes state agencies and other government departments. The agreements specify the purpose of sharing the data, the requirements for security of the data and the requirements for termination of the agreement and the return or deletion of the data shared.

7.4 Data Protection by design and default

In accordance with Article 25 of the GDPR, the ISI implements technical and organisational measures to give effect to the principles of the protection of personal data and to ensure that, by default, only personal data necessary for each specific purpose of the processing are processed. Such measures include the development of organisational policies and procedures such as Acceptable Usage Policy and Digital Communications Policy and the implementation of security measures to secure the data.

7.5 Data Protection Impact Assessment (DPIA)

Where the ISI considers that proposed processing (in particular processing that involves new technology), poses a high risk to the rights and freedoms of the data subjects involved, the ISI will carry out a DPIA. The ISI's Data Protection Officer will be consulted in relation to each DPIA completed. Where technical and/or organisational measures proposed will not mitigate the high risks previously identified, the Data Protection Commission will be consulted as appropriate.

7.6 Transfer of personal data outside of the European Union

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

7.7 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*'.

ISI staff will notify its Data Protection Officer where they identify or suspect a breach of personal data. In accordance with GDPR, the DPO will notify the Data Protection Commission without undue delay where a breach is likely to result in a risk to the rights and freedoms of the data subject(s) involved.

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

7.8 Data Protection Governance

Compliance with the GDPR is a key requirement for the ISI. The ISI will oversee, monitor and ensure compliance with data protection legislation through its Risk and Control Framework.

7.9 Data Protection Officer

In compliance with GDPR Article 37.1(a) of GDPR, the ISI has a designated Data Protection Officer (DPO). In accordance with Article 38, the ISI will involve the DPO in a timely manner in all issues which relate to the protection of personal data and will support the DPO in performing the tasks referred to in Article 39 *Tasks of the Data Protection Officer*. The tasks assigned to the ISI Data Protection Officer in Article 39 include the following;

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

8 Data Protection Contacts

Data Protection Officer
Mr John Farrell
Principal Officer
The Insolvency Service of Ireland
Phoenix House
Conyngham Road, Dublin 8 D08 T3CK.

Phone: (076) 1064200
Email: dp@isi.gov.ie

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

Data Protection Commission
21 Fitzwilliam Square
Dublin 2.

and

Canal House
Station Road
Portarlington
Co Laois.

Phone: (0761) 104 800
Email: info@dataprotection.ie