Data Protection Policy

21 April 2017

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 and 2003 confer rights on individuals as well as additional 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 new EU General Data Protection Regulation (GDPR) - Regulation 2016/679 which comes into effect in May 2018 and replaces the current Data Protection Directive 95/46/EC and the Irish Data Protection Act(s).
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 principles of the Data Protection Acts 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:
    - Details of convictions relating to fraud, tax offences and settlements, dishonesty, medical information

5 The Data Protection Officer

As part of the General Data Protection Regulation (GDPR), it is mandatory for the ISI to have a formally appointed DPO. The DPO's role facilitates compliance and ensures that in carrying out its "*core activities*" – the primary services provided by the ISI - all private individuals' data held and processed by the ISI, such as internal staff, ISI service users, and third parties, is appropriately protected in line with their regulatory rights.

The contact details of the DPO will be published to all data subjects (internal and external), and also communicated to the Office of the Data Protection Commissioner (ODPC. The latter is achieved by annually registering with the ODPC. The published details will include a postal address, a dedicated telephone number and a dedicated e-mail address. The name of the DPO does not need to be publically published.

The DPO will be included in any matters involving data protection at the earliest possible stage, including privacy impact assessments, data processing activities that may affect data subjects and incidents which effect the data of subjects. This may involve the DPO attending middle and senior management meetings. Where it is decided not to follow the DPO's advice, the matter of discussion, the discussion, the DPO recommendation, and the reasons for not adhering to the recommendation should be formally recorded.

Appointment of a DPO

In line with Article 37(5) of GDPR, the DPO "*shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39*".

Furthermore, the DPO role cannot be assigned to someone where his or her other role(s) and their DPO duties present a conflict of interest.

Management Facilitation of the DPO

By Article 38(2) of the GDPR, ISI management will support the DPO by providing:

- the necessary resources to carry out his / her tasks, including finance, infrastructure (premises, facilities, and equipment), and staff where appropriate
- access to personal data and processing operations
- the resources for him / her to maintain their expert data protection knowledge such as continuous training
- active support by senior management
- adequate time to fulfil their DPO duties. A specific percentage of their weekly time should be dedicated to data protection activities
- communication of the DPO role and their activities to employees within the ISI
- access to other services such as, but not limited to, HR, legal, IT, and security for support and information to fulfil their duties

The DPO will also not receive any instructions regarding the exercise of his / her tasks, and must be in a position to perform his / her duties and tasks in an independent manner. The DPO cannot "*be dismissed or penalised by the controller [ISI] or the processor for performing [his / her] tasks*".

Responsibilities of the DPO

The GDPR specifies that the DPO's role is to "*assist the controller or the processor to monitor internal compliance with this Regulation [GDPR]*". As such, the DPO must monitor the ongoing data processing and storage of personal data by the ISI via:

- collection of information to identify processing activities
    - The DPO must maintain the "record of processing operations", a document required by the GDPR which details all the personal data processing activities of the ISI

- analysis and checking the compliance of processing activities with GDPR, the Data Protection Acts, and internal policies
    - This will be accomplished via technical controls, reviews, assessments, and audits
    - This also involves assigning responsibility for raising awareness and continuous internal data protection training for staff and management, and ensuring they are carried out adequately
- informing, advising, and issuing recommendations to management and employees of their obligations under the GDPR and the Data Protection Acts

Although the DPO is bound by secrecy / confidentiality concerning their tasks, they are encouraged to contact and seek advice from the ODPC.

Data Protection Impact Assessments

Note that it is the task of the ISI, not the DPO, to carry out Data Protection Impact Assessments (DPIAs) as necessary; however, the DPO provides advice and guidance at each stage of the DPIA as follows:

- whether or not to carry out a DPIA
- what methodology to follow when carrying out a DPIA
- whether to carry out the DPIA in-house or whether to outsource it
- what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR

Again, where adherence is not paid to the DPO's advice, this should be formally recorded in the DPIA documentation.

Further information can be obtained from Guidelines on Data Protection Officers ('DPOs') Article 29 WP.

6 Policy Contents

Principles of Data Protection

The ISI performs its responsibilities under the Data Protection Act(s) in accordance with the following eight principles:

1. *Obtain and process information fairly*

The ISI is committed to collecting information fairly and ensuring that it is processed fairly. It is committed to only collecting personal data necessary to allow it to carry out its functions as set out in legislation. To comply with this rule, all forms whether electronic or paper

requesting information from a member of the public should only request information for which there is a specific business need and legislative basis.

2. Keep it only for specified, explicit and lawful purposes

The ISI will only keep personal data for purposes that are specific, lawful and clearly stated. It is unlawful to collect information about people routinely and indiscriminately without having a clear and legitimate purpose for doing so.

3. Use and disclose it only in ways compatible with these purposes

If personal data is obtained by the ISI for a particular purpose then, subject to limited exceptions, the data will not be used or disclosed for any other purpose other than that for which it was obtained.

Disclosures of personal data held by the ISI are detailed in the Data Protection registration that is available on the Data Protection Commissioner's website.

4. Keep it safe and secure

The ISI implements appropriate physical and technical security measures against unauthorised access to, or alteration, disclosure, destruction or unlawful processing of personal data and against the accidental loss or destruction of such data. Employee access to personal data that is held by the ISI is restricted on a need to know basis and is reviewed periodically.

5. Ensure that it is adequate, relevant and not excessive

Personal data should not be collected or retained if it is not needed and/or on the basis that it might be required in the future. The types of information about individuals that the ISI collects will be reviewed periodically to ensure compliance with this requirement.

6. Keep it accurate and up-to date

The ISI must ensure that all personal data it holds is accurate, complete and up to date. Any inaccuracies will be remedied as soon as possible.

7. Retain it for no longer than is necessary

Personal data should be retained for no longer than necessary for the purpose(s) for which it is acquired. Personal data may not be retained indefinitely.

Personal and personal sensitive data is stored and retained in compliance with the Data Protection Act(s) and in keeping with the ISIs' Data Retention Policy.

8. Right of access to personal data

Section 4 of the Data Protection Act(s) provide individuals with a right of access to personal data relating to them which is held by the ISI, and the response is to be given no later than

40 days from receipt of the request. Procedures for complying with an individual's data protection access request are outlined in this document.

It should be noted that there are exceptions and limitations on the right of access to personal data. The right of access does not apply in some cases where the needs of civil society may be jeopardised, such as the need to investigate crime effectively, or the need to protect the international relations of the state.

The right of access to medical data and social worker's data can also be restricted in limited circumstances where the contents could result in physical, mental, or emotional harm to the requestor.

Where an expression of opinion has been given in confidence, such an opinion shall not be given to the individual making the access request.

The right of access does not include a right to see personal data about other individuals without that other person's consent, to protect their personal rights.

7 Data Protection Access Requests (DAR) and Data Rectification or Deletion Requests (DRDR) - Procedures

Detailed Procedure in relation to Individual Data Access Requests

1. All data access requests directed to the ISI must be in writing. On receipt of a query or access request by telephone, please ask the caller to put their request in writing and to address it to the DPO.
2. If an access request is sent to a division, ensure that the letter is date stamped on the day it is received as the ISI must reply to the request within 40 days of receipt and ensure the DPO receives the access request as soon as possible.
3. The DPO will check the validity of the access request. The request must be in writing and include sufficient identification and details to definitively identify the data subject.
4. Where the access request is relevant to a number of divisions, the DPO will contact the relevant divisions and request them, in writing, to conduct a search of all data held by them. Such searches should be conducted in accordance with guidance provided by the DPO and all steps taken to locate and collate data should be noted and documented.
5. Divisions need to satisfy themselves that sufficient material has been supplied to definitively identify the individual. This is most important. Criteria on what is sufficient to prove identity for your division must be followed. This may be the signature, an ID number in combination with name and address or date of birth. It should not be possible for a third party to provide the material to lodge a false access request.

6. Check that sufficient information to locate the data has been supplied. If it is not clear what kind of data is being requested, the DPO will ask the data subject for more information.
    - This could involve identifying the databases, locations or files to be searched or giving a description of the interactions the individual has had with the ISI.
7. The DPO will log the date of receipt of the valid request. This is the date from which the 40 day legal timeframe begins and can be the original date the access request was received, or the date where the request was validated with the requestor.
8. A search of all electronic files, no matter the format, and all manual files stored on a relevant filing system(s) should be undertaken in the division. All data identified should be reviewed by the relevant division.
9. Once this review is completed the personal data that is recommended for disclosure / deletion should be forwarded to the DPO for consideration. This step should also include an analysis of the relevant exemptions being relied upon and a description of the purpose in processing the relevant personal data, to whom the data may have been disclosed and the source of the data (unless revealing the source would be contrary to the public interest).
10. If data relating to a third party is involved, it should not be disclosed / deleted without the consent of the third party, or anonymised if this would conceal the identity of the third party. An opinion given by a third party may be disclosed unless it is an opinion which was given in confidence on the clear understanding that it would be treated as confidential.
11. A final decision on disclosure / deletion of the requested information will be taken by the DPO, in conjunction with the head of the relevant division(s) as required.

If DAR:

12. The extracted data is collated into an intelligible form (including an explanation of terms and abbreviations if necessary) and sent via registered posted to the requester.

If DRDR:

13. The identified information is deleted from each of the systems on which it is located, including shredding of hardcopy documents by the appropriate system administrator. Additionally, the IT administrator for each system should be informed that the information should be fully deleted from the system(s).

Both DAR and DRDR:

14. The DPO will keep copies of all DAR / DRDR correspondence on a registered file.

8 Data Protection Breach

Any loss of personal data in paper or digital format will be responded to and managed in accordance with the ISI's Data Security Breach Procedures and in compliance with the provisions set out in the Data Protection Commissioner's Personal Data Security Breach Code of Practice (the "Code of Practice").

In order for the ISI to be able to comply with the Code of Practice, it is essential that all incidents (including suspected incidents) which give rise to the risk of unauthorised disclosure, loss, destruction or alteration of personal data are reported without delay to the DPO.

Incidents can include:

- Minor incidents which do not actually result in unauthorised disclosure, loss, destruction or alteration of personal data,
- Major incidents for example: loss or theft of devices such as laptops; unauthorised access to ISI environment.

A data protection breach can happen for a number of reasons, including:

- Loss or theft of data or equipment on which data is stored (including break-in to an organisation's premises)
- Loss or theft of documents
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a flood or fire
- A hacking attack
- Obtaining information from the organisation by deception
- Misaddressing of e-mails
- Improper dissemination of information

In the event of a data breach happening, the DPO must be notified immediately. It must not be assumed that someone else has already notified the breach.

The breach should be notified using a Personal Data Security Breach Form set out in Appendix 1 of the Personal Data Security Breach Procedures.

The DPO will assess the breach and make a decision on the next steps to be taken.

After review of the breach by the DPO, if the data breached affects the rights and freedoms of a data subject, the DPO will inform the ODPC of the breach within 72 hours of the ISI becoming aware of the breach.

A summary of any data breach that occurs, containing the facts relating to the personal data breach, its effects and the remedial action taken, will be recorded in the ISI Log of Data Breaches that is maintained by the DPO.

9 Training

Data Protection Training will be provided through staff presentations and will be augmented by online material and information notices. The DPO is responsible for this training but can assign creation of, and providing of the training to another party.

Further information and guidance can be obtained on the Data Protection Commissioner's website www.dataprotection.ie

10 Registration with the Office of the Data Protection Commissioner

The ISI is registered with the Office of the Data Protection Commissioner as a Data Controller. This is renewed on a yearly basis by the ISI. A list of the data holdings and disclosees for the ISI can be found on the Data Commissioners Offices website.

If Divisions hold data that is not included in this description, the DPO should be contact by email to dp@isi.gov.ie to have the description amended.