Data Protection Policy
09 February 2021

ISI

Tackling problem debt, together

Revision History

Version	Date	Revision Author	Summary of Changes
1	09.02.21	John Phelan	Approved at SMT 15.12.20
2			

Approval

Name	Position	Signature	Date

Insolvency Service of Ireland
Data Protection Policy

Table of Contents

1 Purpose of the Policy

1.1. This Data Protection Policy (this "**Policy"**) is a statement reflecting the commitment of the Insolvency Service of Ireland ("**ISI**") to respect the privacy of individuals and to comply with applicable data protection laws including the General Data Protection Regulation (Regulation 2016/679) ("**GDPR**"), the Data Protection Acts 1988 to 2018 and any subsequent implementing legislation and amendments.

1.2. The GDPR imposes obligations on entities, such as the ISI, regarding how they collect and use Personal Data about identifiable individuals. In the course of exercising its functions, the ISI is required to process Personal Data and Special Categories of Personal Data (collectively referred to as "**Personal Data**" hereafter) relating to debtors, creditors, Personal Insolvency Practitioners, Approved Intermediaries ("**Responsible Persons**"), current, past and prospective employees[1], users of its website, suppliers and other third parties. The ISI is committed to ensuring that such Personal Data is at all times dealt with in accordance with the ISI's obligations under the GDPR.

1.3. The following ISI policies and procedures are relevant to this Policy:

1.3.1. Data Subject Rights Policy;

1.3.2. Security Incident and Data Breach Policy;

1.3.3. General Privacy Notice;

1.3.4. Cookies Policy;

1.3.5. Data Retention and Destruction Policy;

1.3.6. Data Protection Impact Assessment Policy;

1.3.7. Breach Register; and

1.3.8. Employee/Contractor Privacy Notice.

1.4 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

[1] Employees, staff, contractors, consultants, trainees and temporary or agency workers (collectively the "**employee**(s)").

staff have a personal responsibility to ensure compliance with the data protection principles and to adhere to this Policy.

1.5 Line Managers are responsible for ensuring compliance with this Policy within their division. They are also responsible for ensuring that staff in their area are aware of this Policy.

1.6 This Policy applies to data records of all types regardless of the medium on which they are held. In carrying out its 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

1.7 DEFINITIONS

There are a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this Policy are set out at **Appendix 1.**

2 Data Protection Principles

2.1. There are a number of fundamental principles upon which GDPR is based. Subject to and in accordance with applicable law, the ISI – in its capacity as a Controller – will comply with its obligations under the GDPR by adhering to the following six data protection principles. It should be noted that the restrictions imposed by the GDPR on the processing of Personal Data are subject to a number of exemptions set out in Article 23 of the GDPR which stipulates certain limitations that can be placed on Data Subjects' rights.

2.1.1. LAWFULNESS, FAIRNESS AND TRANSPARENCY

The ISI will obtain and process Personal Data lawfully, fairly and transparently in relation to the Data Subject.

The vast majority of Personal Data is processed by the ISI in compliance with its functions conferred under the Bankruptcy Act 1988 and the Personal Insolvency Act 2012. Personal Data is also processed in the performance of functions in the public interest or in the exercise of official authority vested in the ISI as controller. 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 some 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 provide the required information to data subjects when the Personal Data is collected. 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.

2.2. PURPOSE LIMITATION

Personal Data will be collected for specified, explicit and legitimate purposes and it will not be further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public

interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) of the GDPR, not be considered to be incompatible with the initial purposes. In circumstances where the ISI intend to use the Personal Data for another purpose, a lawful basis for processing the Personal Data must be identified prior to doing so.

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.

2.3. DATA MINIMISATION

The ISI will only hold Personal Data to the extent that it is adequate, relevant and not excessive. Prior to obtaining Personal Data, the ISI will ensure that the information sought is limited to what is necessary for the purpose for which it is being collected and not excessive.

2.4. ACCURACY

The ISI adopts procedures that ensure high levels of data accuracy and completeness, and that ensure data is up-to-date. Checks are carried out at regular intervals to verify the accuracy of any Personal Data held. Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

2.5. STORAGE LIMITATION

The ISI will ensure that Personal Data is 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. Personal Data is retained for a period of time in order to meet various legal obligations (e.g. the National Archives Act 1986 or the Freedom of Information Act 2014). The ISI's policy in relation to retention of records is set out in its Data Retention and Destruction Policy.

2.6. INTEGRITY AND CONFIDENTIALITY

The ISI will take appropriate security measures against unlawful processing or unauthorised access to Personal Data. The ISI will also ensure appropriate

security against alteration, disclosure, accidental loss, destruction or damage of Personal Data.

3 Types of Personal Data Processed or capable of being processed by the ISI

3.1 Personal Data processed or capable of being processed by the ISI includes, but is not limited to, the following: name, date of birth, PPSN, private address, employer, business address, qualifications, work experience, contact details, marital/family status, dependent's details, employer information/self-employed information, bank details, income, creditors details, benefits, details of assets and property, investments, liabilities) and special category Personal Data including data concerning health, that is, medical information and details of convictions relating to fraud, etc.)

An overview of some of the types of Personal Data processed or capable of being processed by the ISI is set out in Appendix 1.

4 Lawfulness of Processing

4.1 In order to process Personal Data a valid legal basis must be established for doing so. There are six alternative ways in which the lawfulness of a specific case of processing of Personal Data may be established under the GDPR. It is the ISI's policy to identify the appropriate basis for processing and to document it in the ISI's Article 30 Record of Processing ("**RoPA**"), in accordance with the GDPR. The options are described in brief in the following sections.

4.1.1 CONSENT

Where the sole legal basis for processing particular Personal Data is consent, the ISI will always obtain GDPR threshold consent from a Data Subject to collect and process their Personal Data. Transparent information about our usage of their Personal Data will be provided to Data Subjects at the time that consent is obtained and their rights with regard to their Personal Data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge (i.e. by way of the ISI's General Privacy Notice or Employee Privacy Notice).

4.1.2 PERFORMANCE OF A CONTRACT

Where the Personal Data collected and processed are required to fulfil a contract with the Data Subject this legal basis will apply. This will often be the case where the contract cannot be completed without the Personal Data in question e.g. a delivery cannot be made without an address to deliver to.

4.1.3 LEGAL OBLIGATION

If the Personal Data is required to be collected and processed in order to comply with the law, this legal basis will apply. It will usually be appropriate for the ISI to rely in such cases upon compliance with a legal obligation to which the ISI is subject, as the lawful basis for its processing activities.

4.1.4 VITAL INTERESTS OF THE DATA SUBJECT

In a case where the processing of Personal Data is necessary in order to protect the vital interests of the Data Subject or of another natural person, then this may be used as the lawful basis of the processing. The ISI will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of Personal Data.

4.1.5 TASK CARRIED OUT IN THE PUBLIC INTEREST

In a case where the processing of Personal Data is necessary for the performance of a task carried out by the ISI in the public interest or in the exercise of official authority vested in the ISI then this may be used as the lawful basis of the processing. The assessment of the public interest or official duty will be documented in the RoPA and made available as evidence where required.

4.1.6 LEGITIMATE INTERESTS

In a case where the processing of Personal Data is necessary for the purposes of the legitimate interests pursued by the ISI or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject this legal basis will apply. Note that as a statutory body this legal basis will not apply where the ISI processes Personal Data in the performance of its functions (instead task carried out in the public interest/exercise of official authority will apply).

5 Data Protection Roles

5.1 One of the key attributes of an effective approach to data protection is a clear allocation of roles, each with defined responsibilities. Each of these roles needs to be allocated to specific individuals or groups within the ISI.

5.2 It is vital that everyone within the ISI understands the part they must play in keeping the Personal Data/Special Categories of Data we hold and process about individuals safe. By ensuring that roles and responsibilities are clearly defined we will be in a good position to prevent many data protection incidents affecting Personal Data from happening and to react effectively and appropriately if and when they do.

5.3 Within the data protection framework relevant to our compliance with the GDPR, there are data protection responsibilities that must be carried out by existing internal roles within the organisation, as follows:

5.3.1 DATA PROTECTION OFFICER

The Data Protection Officer ("**DPO**") is a required appointment in line with the GDPR and has specific responsibilities for the protection of the Personal Data of Data Subjects. The ISI's designated DPO is John Phelan. The DPO has the following responsibilities:

- Demonstrate compliance with the Data Protection Principles.
- Inform and advise the Controller or the Processor and the employees who carry out processing of their obligations under applicable data protection law;
- Monitor compliance with data protection law and with the policies and procedures of the Controller or Processor in relation to the protection of Personal Data;
- Assignment of responsibilities, awareness-raising and training of staff involved in the processing of Personal Data, and the related audits;
- Provide advice where requested regarding data protection impact assessments and monitor their performance;
- Cooperate with all relevant supervisory authorities for data protection; and
- Act as the contact point for supervisory authorities on issues relating to Personal Data processing and to consult, where appropriate, with regard to any other matter.

5.3.2 DATA STEWARD

The Data Steward is required to assist in helping the ISI meet its data protection obligations. The Data Steward has the following responsibilities:

- assist the DPO with their responsibilities; and
- be a first point of contact when a Data Subject requests to exercise their rights.

5.3.3 DIVISIONAL MANAGEMENT (i.e. Data Protection Champions)

Divisional Management may be Directors, Heads of Division or other managers within the ISI. These persons have the following responsibilities:

- Review and manage employee competencies and training needs to enable them to perform their role effectively within the data protection area;
- Ensure that employees are aware of the relevance and importance of their activities and how they contribute to the achievement of data protection objectives;
- Participate in, and contribute to, data protection impact assessments affecting their business area by following the DPIA Policy and using the relevant templates;
- Immediately notify the DPO in the event of a suspected or actual Personal Data Breach; and
- Notify the DPO of any changes to the processing of Personal Data that may need to be reflected in the ISI's Record of Processing Activities (**RoPA**).

5.3.4 EMPLOYEES

An employee has the following main responsibilities:

- Ensure they are aware of and comply with all data protection policies of the ISI relevant to their role;
- Report any actual or potential security breaches to their line manager; and
- Contribute to data protection impact assessments where required.

6 Disclosure of Personal Data by the ISI

6.1. Personal Data will not be disclosed by the ISI other than in accordance with this Policy and with applicable law. Disclosure of Personal Data to a third party is a type of processing, and therefore the purposes and conditions of such disclosure need to be carefully assessed by the ISI. Even where the ISI is subject to a legal obligation requiring it to disclose certain data (for example under Freedom of Information legislation), data protection requirements still need to be considered. The ISI procedure for sharing data with third parties includes consideration of:

- whether to inform individuals of the relevant disclosure and whether consent is required. These considerations will be particularly important where the relevant disclosure or its purpose was not envisaged at the time the Personal Data was obtained by the ISI (or its predecessors). Reminders or specific notifications to individuals may also assist in ensuring the disclosure is fair and transparent;
- the extent of Personal Data disclosed and ensuring it is relevant to and required for a specified purpose;
- the identity, authority and location of the recipient;
- the security of the method of communication; and
- the ISI's relationship with the relevant third party, and whether a data sharing agreement is needed.

DISCLOSURE OF PERSONAL DATA TO DATA PROCESSORS

6.2. In the course of its activities, the ISI may appoint third parties to provide a service which involves handling Personal Data on behalf of the ISI (i.e. third parties who will act as Processors on behalf of the ISI). This may include, but is not limited to, third party call centres and website providers. The ISI may also benefit from shared services provided across several Government departments, such as technology and payroll services.

6.3. The ISI will ensure that all relationships it enters into that involve the processing of Personal Data are subject to a documented contract that includes the specific information and terms required by the GDPR.

6.4. The ISI remains responsible for ensuring that such Processors comply with data protection laws and with this Policy in their handling of the ISI's Personal Data. The ISI procedure for appointing Processors includes:

- assessing data protection guarantees and measures prior to the appointment of a Processor;
- imposing contractual obligations on the Processor (with particular emphasis on data security); and
- monitoring compliance by the Processor throughout the course of its relationship with the ISI.

DISCLOSURE OF PERSONAL DATA TO OTHER THIRD PARTIES

6.5. In order to provide our services, carry out our activities and to comply with legal obligations, we may share Personal Data with certain third parties such as:

- service providers, agents and advisors appointed by us;
- analytics and search engine providers who assist us in the improvement and optimization of our website;
- business partners, suppliers and sub-contractors for the performance of any contract we enter into with them or a data subject;
- creditors and debtors, or other third parties, involved in personal insolvency or bankruptcy arrangements;
- An Gardaí Síochána, local authorities, the Revenue Commissioners, the courts and any other central or local government bodies where they request it and we may lawfully disclose it, for example for the prevention and detection of crime or in the performance of a task carried out in the public interest or in the exercise of an official authority vested in us; and
- others who work for us in connection with the provision of products and/or services to data subjects.

TRANSFER OF PERSONAL DATA OUTSIDE OF THE EEA

6.6. Personal Data may be transferred, stored and processed in one or more countries outside the European Economic Area ("**EEA**"), for example, when one of our third party service providers use employees or equipment based outside the EEA. For transfers of Personal Data to third parties outside of the EEA, the ISI will take additional steps in line with the GDPR and the Data Protection Acts 1988 to 2018. We will put in place adequate safeguards with respect to the protection of privacy, fundamental rights and freedoms, and the exercise of data protection rights, e.g. we will establish an adequate level of data protection through EU Standard Contractual Clauses based on the EU Commission's model clauses.

7 Direct Marketing

7.1 No Personal Data obtained by the ISI is released for the purposes of direct marketing.

8 Monitoring of Staff

8.1 The Department of Justice provides email, internet and intranet facilities to employees, secondees, assignees, interns, and temporary and contract employees, primarily for the purposes of ISI business-related activity. While the ISI does not routinely monitor an individual's use of the ICT resources provided, the ISI reserves the right to do so for the purpose of the following: (i) maintaining and protecting network and system security; (ii) ensuring the privacy and integrity of any information stored on the ISI network; (iii) investigating security incidents; (iv) resolving technical faults; (v) ensuring compliance with the ISI policies and current legislation and (vi) ensuring compliance with Civil Service Policies and Codes.

8.2 A small number of CCTV cameras are in operation within the ISI offices, in addition to those cameras located at the entry and exit doors to the building and at reception. This is necessary for the security of staff and of ISI property and to protect against theft or vandalism. Access to the recorded material is strictly managed. For further information, please see the Department of Justice's CCTV Policy.

8.3 The ISI will act at all times in a fair and reasonable manner and will respect the user's rights under the GDPR and the Data Protection Acts 1988 to 2018. Any information collected through monitoring will be used only for the purpose for which the monitoring was introduced and will be deleted when no longer required.

9 Staff use of ICT Resources

9.1. Employees, secondees, assignees, interns, temporary and contract employees, ISI contractors and ISI agents are granted access only to information systems, services and networks which are necessary to carry out the responsibilities of their role or function. Each user must respect and

protect the privacy and confidentiality of the information systems and network they access and the Personal Data processed by those systems or networks. When an individual's role or responsibilities change, he or she may be denied access to systems relating to his or her previous position.

10 Data Subject Rights

10.1 Rights of the Individual

The Data Subject also has rights under the GDPR:

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

10.2 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 and in the Data Subject Rights Policy.

10.3 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.

10.4 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 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.

10.5 Right to restriction of processing

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.

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.

10.6 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 Controller. The ISI will comply with all such legitimate requests.

10.7 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.

10.8 Right not to be subjected to automated decision making

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.

10.9 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.

10.10 Each of these rights stated in the GDPR. are supported by appropriate procedures within the ISI These timescales are shown in Table 1 below. Please see our Data Subject Rights Policy for further information.

Data Subject Request	Timescale
The right to be informed	When Personal Data is collected (if supplied by Data Subject) or within one month (if not supplied by Data Subject)
The right of access	Without undue delay and in any event within one month of receipt of request
The right to rectification	Without undue delay and in any event within one month of receipt of request
The right to erasure	Without undue delay and in any event within one month of receipt of request
The right to restrict processing	Without undue delay and in any event within one month of receipt of request
The right to data portability	Without undue delay and in any event within one month of receipt of request
The right to object	Without undue delay and in any event within one month of receipt of objection
Rights in relation to automated decision making and profiling.	Without undue delay and in any event within one month of receipt of request

Table 1 - Timescales for Data Subject requests

11 Data Breach Notification

11.1 It is ISI's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of Personal Data.

11.2 In line with the GDPR, where a Personal Data Breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the Data Protection Commission will be informed **within 72 hours**. This will be managed in accordance with our Security Incident Data Breach Policy which sets out the overall process of handling information security incidents.

12 Procedures and Guidelines

12.1 The ISI is firmly committed to protecting the privacy of individuals and to ensuring compliance with data protection legislation, including the implementation of best practice guidelines and procedures in relation to all aspects of data protection.

12.2 All staff should familiarise themselves with the provisions of the GDPR. Further information is available on the website of the Data Protection Commission at www.dataprotection.ie

13 Review of ISI Data Protection Policy

13.1 The Data Protection Policy is maintained by the ISI's 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.

13.2 Any material changes to this Policy will require approval by the Senior Management Team.

Contact Us

Data Protection Officer

Address: John Phelan, Principal Officer, The Insolvency Service of Ireland, Phoenix House Conyngham Road, Dublin 8, D08 T3CK.

Phone: (076) 106 4200

Email: dp@isi.gov.ie

Data Protection Commission

Address: 21 Fitzwilliam Square South, Dublin 2, D02 RD28.

Phone: (076) 110 4800 or Locall 1890 252 231

Email: info@dataprotection.ie

Appendix 1

Article 1: MEANING OF KEY TERMS USED IN THIS POLICY

"Controller"	means the ISI and anyone else who (either alone or jointly with others) determines the purposes and means of the processing of Personal Data;
"Processor"	means anyone who processes Personal Data on behalf of a Controller. These purposes may include: IT software providers with maintenance services and the hosts of its servers, payroll providers etc.;
"EEA"	means the European Economic Area (i.e. the EU member countries plus Iceland, Norway and Liechtenstein);
"General Data Protection Regulation/GDPR"	means Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data. It applies from 25 May 2018. The GDPR applies directly in all member states without the need for any implementing legislation;
"Data Protection Commission/DPC (i.e. Supervisory Authority)"	means the Irish data protection authority for the purposes of the GDPR. It is empowered to take enforcement action in the event of non-compliance with the GDPR and/or other privacy laws. In addition, it is empowered to issue guidance and codes of practice about this. Its guidance and codes do not have the force of law but it is expected by the DPC that Controllers (including the ISI) will adhere to them;
"Personal Data"	means information held by an organisation (or advisers or service providers) from which individuals can be identified (referred to as a "**Data Subject**"). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;
"Personal Data Breach"	means 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;
"Processing"	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. In effect, it includes any activity involving Personal Data;

"Special Categories of Personal Data"	means information about an individual which relates to certain sensitive issues including their health, sexual orientation/sex life or whether they have been convicted of any criminal offence. This also includes information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person (i.e. an individual).
"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 Protection Officer (DPO)	An ISI appointed officer with responsibility for the Data Protection compliance of the ISI.