

**POLICY
DOCUMENT**



ERVIA/PD/64

DATA PROTECTION POLICY

	REVISION NO.	APPROVAL	DATE
Page 1 of 19	10		29.01.2021

ERVIA/PD/64

Table of Contents

1 INTRODUCTION..... 4

2 POLICY STATEMENT 4

3 PURPOSE..... 5

4 SCOPE 5

 In Scope 5

 Policy Exclusions 5

5 POLICY 5

 Principles 6

6 DEALING WITH THIRD PARTIES 8

 Engaging Processors 8

 Controller to Controller Transfers 9

 Transfer of Personal Data Outside of the European Economic Area (EEA)..... 10

7 DOCUMENTING AND MONITORING COMPLIANCE 10

 Ervia Records of Processing activities (“ROPA” or “Article 30 Documentation”)..... 10

 Privacy by Design and Default 11

 Data Protection Assessment Impacts 12

 Accuracy 13

 Training 13

 Storage Limitation 13

8 MARKETING 14

 Compliance with Data Protection Law 14

 Consent 14

 Privacy Notice..... 14

9 DATA SECURITY..... 14

10 COMPLIANCE AND ENFORCEMENT..... 15

 Data Protection Officer (DPO) 15

 Supervisory Authority 15

 Enforcement, Sanctions and Penalties 15

	REVISION NO.	APPROVAL	DATE
Page 2 of 19	10		29.01.2021

ERVIA/PD/64

11 ROLES AND RESPONSIBILITIES..... 16
 Ervia Employee 16
 Business Owner 16
 Data Protection Officer..... 16
 Information Security..... 16
12 OWNERSHIP..... 17
13 GOVERNANCE..... 17
14 REVISION..... 17
15 APPENDIX
 Definitions 18

	REVISION NO.	APPROVAL	DATE
Page 3 of 19	10		29.01.2021

ERVIA/PD/64

1 INTRODUCTION

For the purpose of the Policy the term “Ervia” should be construed as including Ervia and its subsidiary companies in any geographic region (e.g. Gas Networks Ireland, Irish Water and GNI (UK) Ltd). Ervia may incorporate further subsidiaries from time to time and this Policy shall apply to all subsidiaries notwithstanding that they may not be in existence at the time this Policy was put in place. We are committed to conducting our business with honesty and integrity and we expect all personnel working on behalf of Ervia to maintain high standards.

Data Protection is an EU fundamental right for all individuals. Ervia, as an organisation that collects, controls and processes Personal Data, is required under law to make sure that the data collected is obtained fairly, for specific purpose, is no more than is necessary, is stored securely and is retained for no longer than is necessary.

Ervia is committed to protecting the rights and privacy of Data Subjects in accordance with the General Data Protection Regulation ((EU) 2016/679) (“**GDPR**”) and the Data Protection Acts 1988 to 2018, known collectively as the “Data Protection Laws”.

This Policy seeks to provide clarity on how Data Protection is governed within Ervia, and outlines the various roles and responsibilities of Ervia and Ervia Employees in relation to the collection and processing of Personal Data.

This Policy is supported by:

- Ervia Statutory Request for Information Policy (PD96);
- Ervia Acceptable Usage Policy (PD 82);
- Ervia Data Management Policy (PD 97);
- Retention Schedule
- Ervia Information Security Policy (PD69);
- Ervia HR Policies
- Article 30 Data Inventory
- Data Protection Procedures
- Corporate and Employee Privacy Notices

2 POLICY STATEMENT

This policy sets out the practices to be adopted in relation to collection and processing of Personal Data to ensure that Ervia complies with its commitment to protect the rights and privacy of Data Subjects. Personal Data is, broadly speaking, information relating to an identified or identifiable natural person (such as a name or an identification number). Personal Data does not include contact

	REVISION NO.	APPROVAL	DATE
Page 4 of 19	10		29.01.2021

ERVIA/PD/64

details for corporate entities that happen to relate to an employee or other representative of that corporate entity (e.g. names, email addresses and telephone numbers of contacts in corporate bodies) as long as those details are used only for business purposes. Capitalised terms used in this Policy are defined in the Appendix.

This policy aims to:

- a) Give effect to the obligations and provisions of Data Protection Laws; and
- b) Set out the requirements for all Ervia Employees (as defined in Section 11 of this document) with regards to data protection.

3 PURPOSE

This policy is a statement of Ervia's commitment to protect the rights and privacy of individuals in accordance with Data Protection Laws. The data protection obligations outlined relate to any Personal Data of a Data Subject which is processed by Ervia.

Ervia aims to adhere to these obligations in all aspects of its business and employees should strive to respect the data protection rights of individuals in carrying out their role.

4 SCOPE

In Scope

This Policy applies to all current and former employees of Ervia, which includes consultants, contractors, volunteers, trainees, work experience students, interns, part-time, full-time, casual workers and agency workers who directly or indirectly have access to data held by, or provide services to Ervia (collectively referred to as “**Ervia Employees**”).

Policy Exclusions

There are no exceptions to this policy.

5 POLICY

Ervia must comply with the data protection principles which are set out in Data Protection Laws. It is the duty of all Ervia employees to have regard to the data protection principles as part of their role as an employee. Ervia will administer its responsibilities under legislation in accordance with these stated principles as follows:

	REVISION NO.	APPROVAL	DATE
Page 5 of 19	10		29.01.2021

ERVIA/PD/64

Principles

1 Obtain and process Personal Data lawfully, fairly and in a transparent manner

Ervia will obtain and process Personal Data lawfully and fairly in accordance with Data Protection Laws. Ervia will ensure that Data Subjects are provided with details relating to the processing of their Personal Data, and are informed of their rights under Data Protection Laws by means of a data protection notice. This should be provided, where possible, at the time that the Personal Data is collected or as soon as possible thereafter. Further guidance can be provided by the Group Data Protection Team

For Personal Data to be processed fairly, Ervia must ensure that it is in a position to rely on one of a range of ‘legitimising conditions’ set out under Data Protection Law. The majority of Ervia’s processing activities will be carried out on the basis that these activities are necessary for the performance of a task carried out in the exercise of official authority vested in Ervia or a legal obligation to which Ervia is bound.

Ervia will also ensure that it does not process Special Categories of Personal Data without ensuring that it meets a ‘special legitimising condition’ as set out under Data Protection Law. In order for Special Categories of Personal Data (such as data relating to an individual’s health) to be processed fairly, Ervia must ensure that at least one legitimising condition in respect of Special Categories of Personal Data is met (unless exemptions which are set out under Data Protection Law apply). The main legitimising condition for Special Categories of Personal Data (outside the employment context) is that the processing is necessary and proportionate for the performance of a function conferred on Ervia by or under an enactment, subject to respecting the essence of the right to data protection.

2 Process Personal Data for only specified, explicit and legitimate purposes

Ervia will collect Personal Data only for purposes that are specific, lawful and clearly stated. Personal Data will be processed only in a manner compatible with these purposes. Ervia will create and maintain an inventory of Personal Data held within the organisation.

3 Ensure that Personal Data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

Ervia will collect the minimum amount of Personal Data necessary to carry out the required processing. Personal Data held by Ervia will be adequate, relevant and limited to what is necessary for the purpose(s) for which it is collected and kept. The types of information about individuals which Ervia collects and keeps are reviewed periodically to ensure compliance with this requirement. Information that is no longer needed is deleted in accordance with the Ervia Data Management Policy and the Retention Schedule.

	REVISION NO.	APPROVAL	DATE
Page 6 of 19	10		29.01.2021

ERVIA/PD/64

4 Keep Personal Data accurate, complete and up-to-date

Ervia will operate procedures that ensure high levels of data accuracy, completeness and consistency. Ervia will provide mechanisms for Data Subjects to access and rectify their Personal Data.

5 Retain Personal Data for no longer than necessary for the purpose(s) for which it is acquired

Ervia's practices and processes for retention of Personal Data are in line with Data Protection Law. Ervia has and will maintain the Retention Schedule, which applies to all Personal Data held within the Group.

6 Keep Personal Data safe and secure

Ervia will take appropriate security measures against unauthorised access to, alteration, disclosure, destruction or otherwise unlawful processing of Personal Data, and against their accidental loss or destruction. Ervia will take into consideration the state of technological developments, the cost of implementing the measures, the nature of the data concerned and the degree of harm that might result from unauthorised or unlawful processing. To the extent that any third party processes Personal Data on behalf of Ervia, Ervia will ensure that there is a written agreement in place which includes, among other things, appropriate security obligations regarding such Personal Data. Further details regarding the technical and security measures are set out in the Ervia Information Security Policy.

7 Be responsible for, and be able to demonstrate compliance with, obligations under Data Protection Law

Ervia takes its responsibility to comply with Data Protection Law seriously and maintains this Policy and the practices referred to in this Policy for this purpose. Ervia also ensures that it can demonstrate compliance with its obligations under Data Protection Law by maintaining the records, policies and procedures referred to in Section 1 (Introduction) as well as maintaining records including in relation to processing activities, requests by Data Subject, data protection notices, DPIAs, Personal Data breaches, and records of contracts with third parties who process Personal Data on Ervia's behalf.

8 Comply with requests from Data Subjects to exercise their data protection rights

Under Data Protection Law, Data Subjects (including Ervia Employees and customers) have the following rights in relation to the processing of their Personal Data (subject to limited exceptions):

- a) The right to access Personal Data. Data Subjects have the right to be provided with a copy of their Personal Data along with certain details in relation to the processing of their Personal Data.
- b) The right to information. Data Subjects have the right to be provided with certain

	REVISION NO.	APPROVAL	DATE
Page 7 of 19	10		29.01.2021

ERVIA/PD/64

information, generally at the time at which their Personal Data is obtained. Ervia complies with this obligation via its data protection notices.

- c) The right to rectification. Data Subjects have the right to have inaccurate Personal Data held by Ervia in relation to them rectified.
- d) The right to object to and restrict processing. In certain circumstances, Data Subjects have the right to: (i) require that Ervia restricts its processing of their data; and (ii) object to the processing of their data.
- e) Rights in relation to automated decision making. Data Subjects generally have the right not to be subjected to processing which: (i) is wholly automated; (ii) produces legal effects or otherwise significantly affects an individual; subject to certain limited exemptions.
- f) The right to erasure (“right to be forgotten”). In certain circumstances, a Data Subject has the right to request the erasure of their Personal Data.
- g) The right to data portability. In certain circumstances, Ervia is required to provide a Data Subject with a copy of their Personal Data in a structured, commonly used and machine readable format.
- h) Ervia will comply with any valid request by a Data Subject to exercise their rights within the timelines set out in Data Protection Law.

6 DEALING WITH THIRD PARTIES

Engaging Processors

If a third party has access to Personal Data that belongs to or is controlled by Ervia in order to provide a service to Ervia, then the third party is most likely to be acting as a Processor to Ervia. Prior to engaging a Processor, the Ervia Business Owner will:

- a) undertake due diligence to ensure that it is appropriate to engage the Processor; and
- b) ensure that it puts in place an agreement in writing with the Processor that complies with Data Protection Law.

For guidance on such relationships, please contact the Data Protection Team by emailing dataprotection@ervia.ie

	REVISION NO.	APPROVAL	DATE
Page 8 of 19	10		29.01.2021

ERVIA/PD/64

Details of arrangements that Ervia has in place with third party Processors will be kept by the Data Protection Officer.

It is the responsibility of each Ervia Employee to notify the Data Protection Team upon completion of the Data Processor Agreement, and to ensure that all relevant details of the processing are recorded on the Article 30 Record of Processing Activity which the Data Protection Team update. Any changes to the original agreement must also be immediately notified to the Data Protection Team.

Controller to Controller Transfers

In certain circumstances, Ervia will transfer Personal Data to third parties on a Controller to Controller basis. This means that the third party will process such Personal Data for their own purposes and not on behalf of Ervia. By way of example, this will occur in the following circumstances:

- a) Pensions – when Personal Data relating to Ervia Employees is provided to a pension service provider, the trustee(s) of the pension will be a Controller in relation to such Personal Data. The Personal Data is then processed by the pension trustee(s) (or the pension service provider, on their behalf) for the purposes of administering the pension;
- b) Health Insurance – when Ervia Employees are provided with health insurance, the health insurance provider will be a Controller in relation to the Personal Data that is used to administer the insurance;
- c) Audits – where a third party is granted a right to audit Ervia, and the audit is carried out on behalf of that third party (i.e. it is not an internal audit, or an audit by a third party that is requested by Ervia), any Personal Data (e.g. relating to Ervia Employees) that is processed in the context of such audits is processed by the auditing partner as a Controller; and
- d) Public Authorities or Bodies – Ervia is required by law to transfer certain Personal Data to other public authorities or bodies (e.g. the Commission for Regulation of Utilities), each of whom become a Controller in relation to any Personal Data it receives.

It is the responsibility of each Ervia Business Owner engaging with a Controller to notify the Data Protection Team upon completion of the Data Controller Agreement, and to ensure that all relevant details are recorded on the Article 30 Record of Processing Activity which the Data Protection Team update. Any changes to the original agreement must also be immediately notified to the Data Protection Team.

	REVISION NO.	APPROVAL	DATE
Page 9 of 19	10		29.01.2021

ERVIA/PD/64

Transfer of Personal Data Outside of the European Economic Area (EEA)

Under the Data Protection Laws, Ervia may not (subject to certain limited exemptions) transfer Personal Data to a country outside the EEA (including the UK), unless that country has been deemed by the European Commission to provide an adequate level of data protection.

While there are a number of exemptions, the following arrangements must be adhered to:

- a) the Data Subject has explicitly consented to the transfer, having been informed of the possible risks of such transfers due to an absence of an adequacy decision and appropriate safeguards;
- b) a data transfer agreement incorporating the model clauses in the form approved by the European Commission (or a data protection supervisory authority), has been executed by Ervia and the data importer (recipient) based outside the EEA; and
- c) the data importer is subject to a framework to facilitate transfers approved by the EU Commission.

Should a service provider outside of the EEA be considered by a Business Owner for services to Ervia, it is the responsibility of the Ervia Business Owners to ensure that the requirements of Chapter 5 of the GDPR are met. Since 2020 there is a requirement to conduct a Risk Assessment in respect of transfers of personal data outside of the EEA. It is the responsibility of the Business Owner to contact the DPO in respect of completing same and complying with this obligation.

If it is necessary for Ervia, as a Controller, to transfer Personal Data to another entity located in a country outside the EEA (which has not been found by the EU Commission to provide an adequate level of data protection), then Ervia will ensure it can rely on one of the relevant exemptions. This may arise in relation to transfers of Personal Data to third parties (e.g. external service providers).

7 DOCUMENTING AND MONITORING COMPLIANCE

Ervia Records of Processing activities (“ROPA” or “Article 30 Documentation”)

Ervia is required to maintain an inventory of the Personal Data that it holds (both as a Controller and a Processor). The ROPA / Article 30 Document must include the following details about Ervia’s processing of Personal Data:

- a) details of the Controller(s);

	REVISION NO.	APPROVAL	DATE
Page 10 of 19	10		29.01.2021

ERVIA/PD/64

- b) the purposes of the processing;
- c) a description of the categories of Data Subjects and the categories of Personal Data;
- d) the categories of recipients to whom Personal Data has been or will be disclosed, including recipients in third countries or international organisations;
- e) details of transfers of Personal Data to a third country, including the identification of that third country;
- f) where possible, time limits for retention; and
- g) where possible, a description of the technical and organisational security measures that are undertaken to protect the data.
- h) name of the Ervia person/ team responsible for supervising/ managing the data and who will operate as the internal point of contact in relation to queries on this data.

The Ervia ROPA/ Article 30 Document will be maintained by the DPO on an on-going basis. If Ervia Employees are planning any new activity or implementing any new initiative that will change the way that the Company processes Personal Data, they must contact the DPO so that such information can, if required, be added to the ROPA/ Article 30 Document.

Privacy by Design and Default

Implementation of data protection by design and default are additional obligations under Data Protection Law.

Data Protection by Design – Data protection by design is the concept that the means and purposes of the processing of Personal Data are designed with data protection security specifically in mind from the beginning. This principle requires Ervia to implement both technical and organisational measures that will strive to guarantee and protect the privacy of Data Subjects. Ervia Business Owners will seek, where possible, to implement and practice data minimisation (which could include, where feasible, the pseudonymisation of Personal Data). Other methods of data protection by design include, staff training and audit and policy reviews focused on data protection.

Data Protection by Default - Ervia will implement appropriate technical and organisational measures to ensure that, by default, only Personal Data as is necessary for the relevant purpose as set out in the Privacy Statement, is processed. This obligation applies to the amount of Personal Data collected, the extent of processing, the period of storage and accessibility. In particular, such

	REVISION NO.	APPROVAL	DATE
Page 11 of 19	10		29.01.2021

ERVIA/PD/64

measures ensure that, by default, Personal Data is not made accessible to an indefinite number of persons without the Data Subject's notice.

Data Protection Assessment Impacts

Ervia is obliged to ensure that a Data Protection Impact Assessment ("DPIA") is undertaken before commencing any processing which is likely to result in a 'high risk' to Data Subjects' rights and freedoms. The GDPR includes the 'large scale' processing of sensitive Personal Data or profiling activities as examples of high risk processing.

A DPIA must contain at least the following details:

- a) a description of the envisaged processing operations and the purposes of the processing;
- b) an assessment of the necessity and proportionality of the processing;
- c) an assessment of the risks to the rights and freedoms of Data Subjects; and
- d) the measures envisaged to address the risks that have been identified and to demonstrate compliance with the GDPR.

Ervia also considers whether a Privacy Impact Assessment ("PIA") is necessary when it engages in changes to its processing of Personal Data that do not require a DPIA. Where necessary, DPIAs and PIAs are carried out before the processing activity in question is commenced.

A DPIA or PIA is a mandatory requirement in advance of the introduction of for example, any new system, technology or business process. A DPIA or PIA may also be required if a business process is being revised or updated or if new category of personal data is being introduced to a processing activity.

It is the responsibility of the Business Owner to conduct the DPIA or PIA. The DPO can provide additional information on when a DPIA or PIA must be conducted.

Each DPIA and PIA that is carried out by an Ervia Employee is submitted to the DPO for review once it is completed, in advance of the processing beginning, and at regular intervals thereafter. The default period for such reviews is every 3 years, but shorter periods may be stipulated depending on the subject of the DPIA or PIA.

	REVISION NO.	APPROVAL	DATE
Page 12 of 19	10		29.01.2021

ERVIA/PD/64

Accuracy

Ervia ensures that Personal Data is accurate and kept up-to-date. Ervia will take every reasonable step to ensure that any Personal Data that is inaccurate or out of date, having regard to the purposes for which it is processed, is erased or rectified without delay in accordance with the Data Management Policy.

Training

Ervia will ensure that Ervia Employees who process Personal Data are made aware of and, when necessary, receive training in respect of data protection law and principles. Records of data protection training completed by Ervia Employees will be maintained as part of their personnel files.

Storage Limitation

Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the relevant purposes. Guidance from supervisory authorities has indicated that Personal Data should never be kept on a 'just in case' basis – it should be kept only where there are reasonable grounds for expecting that such information may be required.

To ensure compliance with the principles of Data Protection Law (and any applicable statutory requirements in respect of the retention of records), Ervia will:

- a) ensure that it collects and keeps only that Personal Data which is necessary for the purposes set out in its data protection notices. The types of information about individuals which Ervia collects and keeps will be periodically reviewed to ensure compliance with this requirement;
- b) retain such Personal Data only for as long as required for the purposes for which it is processed (or for any applicable statutory retention period) in accordance with the Retention Schedule;
- c) periodically review and update the Retention Schedule to ensure that it provides for retention periods that are relevant and appropriate having regard to statutory requirements, guidance from supervisory authorities etc.; and
- d) periodically carry out Group-wide audits to ensure that Ervia adheres to the retention periods set out in the Retention Schedule.

	REVISION NO.	APPROVAL	DATE
Page 13 of 19	10		29.01.2021

8 MARKETING

Compliance with Data Protection Law

Ervia engages in direct marketing to individuals from time to time. When undertaking direct marketing, Ervia must ensure that it processes any Personal Data in accordance with the general principles set out in Section 5 (Policy) above. Ervia must also ensure that any electronic direct marketing that it undertakes complies with the provisions of ePrivacy Law, which is currently set out in Directive 2002/58/EC (the “**ePrivacy Directive**”) as implemented into local law and which will, in the near future, be set out in a new EU Regulation (the “**ePrivacy Regulation**”).

Consent

In cases where Ervia relies on consent as the lawful basis for processing, they must be able to demonstrate and describe how they have received consent and that such consent was freely and unambiguously given for specific purposes and, further, that you can evidence an affirmative action on the part of the data subject to have indicated consent, such that data subjects can reasonably understand who is using their personal information, what information, and for what purposes, and using which communications channels.

Privacy Notice

Ervia strives to ensure that individuals are aware that their data is being processed, and that they understand:

- Who is processing their data
- What data is involved
- The purpose for processing that data
- The outcomes of data processing
- How to exercise their rights

To these ends the Ervia has a privacy statement, setting out how data relating to these individuals is used by the company. These statements are saved on all domain websites and the intranet (for employees). Privacy notices will be updated and review if there is a change in legislation or regulation.

9 DATA SECURITY

Ervia will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks to Personal Data that may arise in connection with the processing activities Ervia undertakes, e.g. from accidental or unlawful destruction, loss, alteration, unauthorised

	REVISION NO.	APPROVAL	DATE
Page 14 of 19	10		29.01.2021

ERVIA/PD/64

disclosure of, or access to Personal Data transmitted, stored or otherwise processed. Further details in relation to data security procedures, as well as the procedures to be adopted in the event of a data security breach, can be found in the Ervia Information Security Policy ([link](#)).

All Ervia Employees who have access to Ervia's IT systems are subject to the Ervia Information Security Policy and the Ervia Acceptable Usage Policy ([link](#)) which outline their responsibilities in using Ervia's IT Systems.

10 COMPLIANCE AND ENFORCEMENT

Data Protection Officer (DPO)

Certain Controllers and Processors are required under the Data Protection Laws to appoint a Data Protection Officer. As Ervia is a public authority, it is required to, and has, appointed a DPO, who can be contacted at dataprotection@ervia.ie or by phone at (01) 8230305.

Supervisory Authority

Each country in the EEA has a 'Supervisory Authority' that oversees compliance with Data Protection Law.

The lead supervisory authority for Ervia is the Irish Data Protection Commission (the "DPC").

Enforcement, Sanctions and Penalties

It is essential that all Ervia Employees comply with this policy and related policies and procedures, as a breach of Data Protection Law could result in serious consequences for Ervia and for the Data Subject(s). Such consequences could include:

- a) **Investigations, Audits and Criminal Penalties** - Supervisory Authorities have a wide range of investigation and enforcement powers, including the powers to investigate complaints, to carry out an audit of an organisation's compliance with Data Protection Law and the power to issue enforcement notices setting out steps which must be taken to rectify breaches of Data Protection Law. Failure to comply with enforcement actions by Supervisory Authorities may result in a criminal offence; and
- b) **Fines** - In addition to their investigation and enforcement powers, Supervisory Authorities have the ability to levy fines of up to the greater of 4% of annual worldwide turnover of the relevant undertaking or €20 million for certain breaches of the GDPR.

	REVISION NO.	APPROVAL	DATE
Page 15 of 19	10		29.01.2021

ERVIA/PD/64

- c) **Compensation for Loss** to a Data Subject of by way of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Any communication from a Supervisory Authority must be forwarded immediately to the DPO.

11 ROLES AND RESPONSIBILITIES

Ervia Employee

All Ervia Employees must comply with this policy and the associated Data Protection Procedures. Employees must seek guidance from the Data Protection Officer at dataprotection@ervia.ie, before the commencement of any new undertaking where the processing of Personal Data will occur at any stage within this undertaking.

All Ervia Employees must have regard to the Data Protection Principles and apply them in their roles.

It is the responsibility of all Ervia Employees to comply with this policy. Failure to comply with this policy may result in the defaulting Ervia Employee being subject to disciplinary action, up to and including summary dismissal or termination of contract.

Business Owner

Each Business Owner is responsible for the enforcement of this Data Protection Policy and adherence to the Data Protection Procedures within their business area. The Business Owner is responsible for ensuring the key Data Protection artefacts, including the Data Flow Diagrams, Data Protection Impact Assessments, and Record of Processing, are complete, accurate and up to date for their business area. Where the Business Owner manages the relationship with a third party, the Business Owner is responsible for ensuring the third party is compliant with Data Protection Law.

Data Protection Officer

The Ervia Data Protection Officer is responsible for managing the Data Protection Policy and associated procedures. The Data Protection Officer must provide guidance and direction to Ervia in matters concerning data protection, and must fulfil all other responsibilities outlined in Data Protection Law.

Information Security

The Information Security Team is responsible for protecting all Ervia data (both physical and electronic) from unauthorised/inappropriate access to data, or the unlawful use or disclosure of

	REVISION NO.	APPROVAL	DATE
Page 16 of 19	10		29.01.2021

ERVIA/PD/64

commercial and personal Ervia data.

12 OWNERSHIP

The owner of this Policy is the Data Protection Officer, who is responsible for the maintenance of this document and the associated procedure.

Any queries on this Policy can be directed to the Data Protection Officer.

13 GOVERNANCE

Each business area is required to cooperate and assist the DPO in conducting internal control checks to ensure compliance with this policy and its related procedures and with Data Protection Law generally and to document such checks as part of the audit reviews as required

The Chief Legal Officer and Data Protection Officer will provide advice and assistance to the business area in supporting how to comply with this policy and implementing oversight and monitoring procedures with each business unit.

Audit and Risk may independently conduct risk-based monitoring programmes and audits to assess compliance with Policy.

14 REVISION

This policy will be reviewed annually or more often as relevant law, regulation or practice dictates.

	REVISION NO.	APPROVAL	DATE
Page 17 of 19	10		29.01.2021

ERVIA/PD/64

APPENDIX

Definitions

Automated Means is, broadly speaking, processing using a computer or other electronic device.

Controller or Data Controller means any person who, either alone or with others, controls the purpose and means of the processing of Personal Data. Controllers can be either legal entities such as companies, government departments or voluntary organisations, or they can be individuals.

Data means information in a form which can be processed. It includes both data processed by Automated Means and Manual Data.

Data Processing means performing any operation or set of operations on Personal Data including: (a) collecting, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation; (b) use, disclosure by transmission, dissemination or otherwise making available; and (c) alignment or combination, restriction, erasure or destruction.

Data Protection Law means the General Data Protection Regulation (EU 2016/679) and any applicable national implementing or supplemental legislation, along with guidance published by competent regulatory authorities.

Data Subject means a natural person (an individual who is currently living) who's Personal Data is processed by or on behalf of Ervia.

Manual Data means information that is recorded as part of a 'filing system', or with the intention that it should form part of a 'filing system'. 'Filing system' means any structured set of Personal Data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographic basis.

Personal Data means any data relating to a living individual who is or can be identified either directly or indirectly, including by reference to an identifier (such as a name or identification number, e.g. WPRN, GPRN or Asset Identification Number). It also includes data specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.

Processor or Data Processor means a person who processes Personal Data on behalf of a Controller, but does not include an employee of a Controller who processes such data in the course of his/her employment.

	REVISION NO.	APPROVAL	DATE
Page 18 of 19	10		29.01.2021

ERVIA/PD/64

Special Categories of Personal Data means Personal Data relating to an individual's: racial or ethnic origin; political opinions or religious or philosophical beliefs; trade union membership; genetic or biometric data processed for the purpose of uniquely identifying a natural person; physical or mental health, including in relation to the provision of healthcare services; sex life or sexual orientation. Individuals have additional rights in relation to the processing of any such data.

Data Protection Team means the Data Protection Officer and dedicated team of supporting staff. They can be contacted by emailing dataprotection@ervia.ie or by telephone at (01) 823 0305.

Procedure

Please refer to the Data Protection team for copies of internal operational data protection procedures and additional subject right procedures.

	REVISION NO.	APPROVAL	DATE
Page 19 of 19	10		29.01.2021