POLICY DOCUMENT	ervia
ERVIA/PD/64	

Data Protection Policy

Document Classification: ***Internal Use***

	REVISION NO.	APPROVAL	DATE
Page 1 of 13	8	M. M & Nicholas	02.02.2017

Table of Contents

1. Introduction

Ervia is committed to protecting the rights and privacy of individuals in accordance with the following:

- The Data Protection Acts 1988 and 2003 and all statutory instruments made under these Acts
- S.I. No.336 of 2011: The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011

This legislation is together referred to in this document as the "DP Acts".

As a service provider and an employer, Ervia is required to collect, use and keep personal data for a variety of purposes relating to its employees, customers and other individuals who come in contact with the organisation**.** These purposes include:

- For the provision of services to its customers, Ervia collects and uses personal data for the purposes of account administration, customer service and to facilitate operational activities including construction and maintenance at customer premises. In addition, data relating to customers may be used for health and safety, risk assessment, marketing and credit checking purposes.

- For the purpose of processing data concerning employees and other individuals with whom Ervia has dealings including the recruitment and payment of staff/contractors, compliance with statutory obligations and compliance with legal obligations to government bodies.

Ervia is classified as a Data Controller in certain circumstances. Under the Data Protection Act 1988 (Section 16(1)) Regulations 2007, however, which came into effect on 1st October 2007, as a commercial semi—state, Ervia falls within an exemption and is no longer required to register as a Data Controller with the Office of the Data Protection Commissioner (the **"**DPC"). As such, although Ervia does not appear on the DPC's public register, the organisation is still obliged to comply with the general provisions of the DP Acts relating to Data Controllers and Processors. Ervia is classified as Data Processor in instances where personally identifiable information is processed by Ervia, but is controlled by a third party.

2. Related Policies and Procedures

- PD 69 - Information Security Policy
- PD 82 - IT Acceptable Usage Policy
- ISDP P06 Data Handling Procedures
- ISDP P07 Data Protection Procedures
- ISDP P21 Third Party Management Procedures

3. Purpose and Scope

This policy is a statement of Ervia's commitment to protect the rights and privacy of individuals in accordance with the DP Acts. Data protection obligations outlined relate to personal data of Ervia employees, contractors, third parties and external parties, customers and prospective customers.

All references to "Ervia" in this policy shall be deemed to include its subsidiaries, including Gas Networks Ireland and Irish Water.

This Policy applies to all employees, part-time staff, contractors, and any third parties authorised to use Ervia systems and/or to process data on its behalf. They are collectively referred to as "Users" from this point.

4. Data Protection Principles

As a Data Controller, Ervia must comply with eight data protection principles which are set out in the DP Acts. Ervia will administer its responsibilities under the legislation in accordance with these stated principles as follows:

(i) **Obtain and process information fairly**
Ervia will obtain and process personal data fairly in accordance with the DP Acts.

This means that Ervia must ensure that, in so far as practicable, the Data Subject (e.g. the employee or customer) has been provided with details relating to the uses and disclosures that will be made of their data and is informed of their access and amendment rights (see section 6 below). Compliance with this obligation is achieved through the publication of the *Ervia Data Protection Notice, Gas Networks Ireland Data Protection Notice* and the *Irish Water Data Protection Notice*, on the Ervia, Gas Networks Ireland and Irish Water websites and in the policies communicated to employees. Please refer to the *Ervia Data Protection Procedures* for further information.

Ervia must process *personal data* and *sensitive personal data* in accordance with its legal obligations. This includes an obligation under the DP Acts to legitimise the processing of personal data. In respect of regular personal data, processing must be legitimised on the basis of consent or that processing is necessary for certain purposes specified in the DP Acts including:

- the legitimate interests of Ervia or third parties to whom the data is disclosed;
- the performance of a contract to which the Data Subject is party;
- the performance of a statutory function;
- the performance of a legal obligation (provided it does not arise under contract); or
- the prevention of injury or damage to the health of the Data Subject or another person, damage to property or to otherwise protect a person's vital interests.

Additional criteria must be satisfied to legitimise the processing of sensitive personal data with the result that explicit consent to processing is usually required. There are a number of limited alternatives to explicit consent set out in the DP Acts including scenarios where the processing is necessary for:

- preventing injury or property damage or protecting the vital interests of the Data Subject (where consent cannot reasonably be obtained);
- the exercise or performance of any right or obligation conferred or imposed by law on Ervia in connection with employment;
- obtaining legal advice or in connection with legal proceedings; and
- certain other grounds which are limited in their application (please refer to the *ISDP P07 Ervia Data Protection Procedures*).

(ii) **Keep data only for one or more specified, explicit and lawful purposes**
Ervia will keep data for purposes that are specific, lawful and clearly stated. Personal data will only be processed in a manner compatible with these purposes. Ervia will create and maintain an inventory of personal data held within the organisation.

(iii) **Process data only in ways compatible with these purposes**
Ervia will only process personal data that is necessary for the purpose(s) or compatible with the purpose(s) for which it collects and keeps personal data. This means that if Ervia obtains personal data for a particular purpose, it may not use the data for any other purpose (unless the consent of the Data Subject is obtained).

(iv) **Keep data safe and secure**
Ervia and its Data Processors (e.g. third parties) will take appropriate security measures against unauthorised access to, or alteration, disclosure, destruction or unlawful processing of the data and against their accidental loss or destruction. In determining what security measurements should be put in place, 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.

(v) **Keep data accurate, complete and, where necessary, up-to-date**
Ervia will operate procedures that ensure high levels of data accuracy, completeness and consistency**.** This will include Ervia reminding individuals on a periodical basis to inform Ervia of any changes to their details or Ervia amending inaccurate data which is revealed as a result of a subject access request.

(vi) **Ensure that data is adequate, relevant and not excessive**
Personal data held by Ervia will be adequate, relevant and not excessive in relation to the purpose(s) for which it is collected and kept. This means that Ervia should only collect the minimum amount of personal data from individuals that is necessary to carry out the processing referred to in its Data Protection Notice(s).

(vii) **Retain data for no longer than is necessary for the purpose or purposes**
Ervia has defined practices and processes on the retention of personal data which reflects guidance issued by the DPC**.**

(viii) **Provide a copy of his/her personal data to that individual, on request, and correct the data or, in certain cases as defined in the DP Acts, block or erase the data where that individual so requests**
Ervia has formal procedures in place to ensure that Data Subjects can exercise their access and amendment rights under the DP Acts (see section 6).

Note: Ervia will always be regarded as the Data Controller in relation to personal data of which it controls the contents and use (e.g. in relation to customers and employees). All third parties and external parties acting as Data Processors must comply with Principle IV (i.e. keep data safe and secure) and process the data solely in accordance with the instructions of Ervia. In this regard, Ervia must continue to provide guidance to third parties and external parties on all other principles such as data retention and destruction. As the Data Controller, Ervia is ultimately responsible for ensuring that all 8 principles are complied with and is required as a matter of

law to ensure that a written contract (the "Data Processor Agreement") is put in place particularly stipulating, as a minimum, that the Data Processor must:

a) process the data solely in accordance with the instructions of Ervia; and
b) comply with the data security obligations set out in the DP Acts.

Further optional/recommended clauses would include the right for Ervia to audit the Data Processor's security measures and an obligation for the Data Processor to assist where Ervia receives a subject access request.

Ervia will always be regarded as the Data Processor in relation to personal data which is controlled by third parties but processed by Ervia (e.g. customer name, customer address etc). While acting as a Data Processor, Ervia must comply with Principle IV (i.e. keep data safe and secure) and process the data solely in accordance with the instructions of the Data Controller.

5. Roles/Responsibilities

Ervia has overall responsibility for ensuring that the organisation as a whole complies with its obligations under the DP Acts. However, all Users working on behalf of Ervia who, as part of their responsibilities, process personal data about identifiable individuals, either in an automated or manual form, must comply with this policy and the associated Data Protection Procedures. Ervia will provide support, assistance, advice, and in special circumstances, training to appropriate individuals who are handling such data in order to ensure that they are in a position to comply with the legislation.

It is the responsibility of the Ervia Data Protection Officer ("DPO") to formulate data protection policies and procedures and provide direction in matters concerning data protection.

Managers at all levels are responsible for ensuring that Users and third parties adhere to this policy and the associated Procedures. Information Security and Data Protection ("ISDP") will provide direction and guidance to departments in the fulfilment of these obligations.

As the Data Controller, Ervia is ultimately responsible for the protection of all personal data which it obtains. In this regard, if Ervia outsources personal data to a third party, Ervia is responsible for ensuring that the third party is providing adequate security over this data.

Where personal data has been outsourced to a third party, data protection clauses must, as a matter of law, be put in place between Ervia and the third party in question in order to ensure that such data is afforded appropriate protection. The Business Information Owner, in conjunction with ISDP, is responsible for ensuring that the third party is providing adequate security over the data in line with the *Ervia Information Security Policy*. This compliance must be validated throughout the duration of the contract via active management and monitoring.

Where Ervia is engaging third parties to process personal data on their behalf, the Business Information Owner, ,with the assistance of ISDP, has a responsibility to know where all the data flows are and where the data will reside while in the possession of the third party. There is a responsibility to ensure that these are recorded in the Ervia Third Party Register (see *ISDP P21 Ervia Third Party Management Procedures*).

ISDP are responsible for addressing all Data Subject access requests received by Ervia or any third party or external party, from customers, employees, An Garda Síochána, the Revenue Commissioner, the DPC, Local Authorities, Health Boards or other State agencies. All correspondence from the DPC must be forwarded to the DPO immediately and/or other parties which the DPO has nominated to process these requests on their behalf.

Confidentiality

Ervia has defined classes of information in terms of its sensitivity, from a data protection perspective and its criticality to business operations. Confidentiality obligations will arise in circumstances where information which is not in the public domain is disclosed to the recipient for a limited purpose and the recipient knows (or should reasonably know) that the information needs to be treated as confidential. Therefore, unlike the DP Acts (which only govern the use of personal data), confidentiality obligations apply in respect of all data (including in relation to corporate bodies) which has the necessary quality of confidence (i.e. it is not in public domain) and which is disclosed on the mutual understanding it would only be used for a limited purpose.

Ervia has a significant amount of confidential information to protect (both relating to itself and third parties). As such:

- Confidential information, whether personal data, sensitive personal data or commercially sensitive, relating to Ervia and its activities should be protected by being clearly marked as such (to the extent reasonably practicable) and, more importantly, by entering into non-disclosure agreements with parties to whom the information is disclosed. For the avoidance of doubt, this confidential information should only be given to such persons engaged by Ervia where it is essential to the carrying out of their work on behalf of Ervia.

- Confidential information relating to customers, third parties and others must not be subject to misuse and/or unauthorised disclosure. Ervia is required to preserve the confidentiality of all commercially sensitive information obtained in the course of carrying out its business unless it is under a legal obligation to disclose this information (*Gas (Interim) (Regulation) Act, 2002).*

- Any improper disclosure of confidential or strictly confidential information may result in disciplinary action for employees and legal redress in the case of other persons or companies engaged by Ervia.

6. Right to Access Personal Data

Employees and other Data Subjects have the right to access any personal data that is being kept about them by Ervia on computer systems and in relevant filing systems. This right is subject to certain exemptions which are set out in the DP Acts. Any person who wishes to exercise this right should make the request in writing at the published address**.** The relevant ISDP Data Protection Manager will coordinate the request with DPO as appropriate.

Ervia reserves the right to charge the maximum fee payable for each subject access request. If personal details are inaccurate, they can be amended upon request.

All Data Subject requests received from customers, whether verbal or written should be referred without delay at the published address**.** There are strict deadlines within which the organisation must respond to any such request.

Any queries, written or verbal, from An Garda Síochána, the Revenue Commissioners, Local Authorities Health Boards or any other State Agency seeking access to any personal data held by Ervia should be referred **immediately** to the relevant Data Protection Manager.

7. Marketing

The DP Acts confer rights on individuals and on corporate entities in respect of the use of their data for marketing purposes. Rights vary according to the means of communication used**,** whether the party is an individual or a corporate entity and whether or not the party is a customer of Ervia. Opt-In or Opt-Out measures are applied for the purposes of marketing and these are detailed in the *Ervia Data Protection Procedures*.

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

All data transfers that include personal data should be approved by ISDP.

Ervia policy is to minimise the transfer of personal data outside the EEA.

Additional DP Act rules apply in respect of the transfer of personal data to countries outside of the EEA (EU members plus Switzerland, Norway, Iceland and Liechtenstein) which the European Commission does not regard as conferring an adequate level of data protection.

Where personal data must be transferred outside the EEA, one of the following conditions must be met by the Data Controller:

- consented to by the data subject; or
- required or authorised under an enactment, convention or other instrument imposing an international obligation on this State; or
- necessary for the performance of a contract between the data controller and the data subject; or
- necessary for the taking of steps at the request of the data subject with a view to his or her entering into a contract with the data controller; or
- necessary for the conclusion of a contract between the data controller and a third party, that is entered into at the request of the data subject and is in the interests of the data subject, or for the performance of such a contract; or
- necessary for the purpose of obtaining legal advice; or
- necessary to urgently prevent injury or damage to the health of a data subject; or
- part of the personal data held on a public register; or

- authorised by the Data Protection Commissioner, which is normally the approval of a contract which is based on EU model contracts

In addition, the Data Controller must ensure that individuals have been made aware that their data may be transferred outside the EEA to a country which does not confer adequate protection and this transfer must be legitimised by obtaining the data subjects consent. Alternative to this, the Data Controller must be able to rely on the fact that the transfer is necessary for its own legitimate business interests or for one of the other grounds for legitimising processing in the DP Acts (see section 3(i) above). Where the data being transferred is sensitive personal data it will usually be necessary to obtain the Data Subject's explicit consent to any form of processing, including transfers abroad.

Note: the transfer of data outside the EEA may include situations where a third party provides remote access or transfers Ervia data to another geographical location outside the EEA The situation may also arise where a third party provides remote access or transfers Ervia data to an external party outside the EEA to whom it outsources particular functions. Ervia as the Data Controller is ultimately responsible for the data within the remit of these external parties and, must satisfy one of the exceptions above**.**

Compliance with these rules will be addressed by Ervia in the event of any proposed transfer of data beyond the European Economic Area. The DPO should be contacted in the event that a transfer of data outside of the EEA is necessary.

9. Data Protection Procedures

This policy supports the provision of a structure to assist in Ervia's compliance with the DP Acts, including the provision of best practice guidelines and procedures in relation to all aspects of data protection. Procedures are set out in the *ISDP P07 Ervia Data Protection Procedures* document and are added to and revised on an on-going basis as required.

10. Document Ownership

The owner of this document is the Ervia Data Protection Officer.

11. Maintenance

This *Data Protection Policy* is reviewed on an annual basis or in light of any legislative or other relevant developments.

12. Enforcement

Violation of this policy may result in disciplinary action, up to and including termination of employment for employees and, in the case of others engaged in Ervia business, may result in legal redress. Violation of this policy may also result in action by judicial and regulatory authorities. Any person who is aware of, or observes,

a suspected violation of this policy is responsible for reporting the incident to the relevant ISDP Data Protection Manager.

The DP Acts impose a variety of penalties, ranging from criminal to civil, for failures to comply and may be directed at organisations or at individuals. The DPC oversees national compliance with the terms of the legislation. The DPC has a wide range of enforcement powers, including investigation of an organisation's records and record keeping practices. There is also a risk that Data Controllers in breach of the DP Acts will be named in the DPC's Annual Report which can reflect badly on the organisation in question. A Data Controller may be found guilty of an offence under the DP Acts for failure to comply with an information or enforcement notice issued by the DPC.

Summary proceedings for an offence under the DP Acts may be brought and prosecuted by the DPC. Under section 31 of the DP Acts the maximum fine on summary convictions of such an offence is set at €3,000. On conviction or indictment, the maximum penalty carries a fine of €100,000. A Data Controller found guilty of an offence can, in addition to the fine, be ordered to delete data.

In relation to unsolicited marketing by electronic means, summary proceedings for an offence under S.I. No. 336 of 2011 may be brought and prosecuted by the Commissioner.

Each call or message can attract a fine of up to €5,000 on summary conviction. If convicted on indictment, the fines range from €50,000 for a natural person to €250,000 or 10% of turnover if the offender is a corporate body.

13. References

For further details relating to the following legislation please refer to the DPC's website www.dataprotection.ie:

- The Data Protection Acts 1988 and 2003
- Statutory Instrument –= S.I. No.336 of 2011 The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011

14. Definitions

For the purpose of this document and the associated Procedures the following definitions apply:

Business Information Owner	A Senior Manager with overall accountability within Ervia for managing an information type e.g. Customer or Employee data processed by Ervia - irrespective of actual legal ownership.
Commercially Sensitive Data	Relates to any information held by Ervia that if disclosed to an unauthorised party could: • Result in loss or material financial damage to Ervia. • Confer unfair commercial advantage or disadvantage. • Result in reputational damage to Ervia.

Data Protection	Data protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data, in both paper and electronic format.
Data	Data refers to both automated and manual data. Automated data means any information held on a computer, or information recorded with the intention that it will be processed by computer. Manual data means information that is recorded as part of a "Relevant Filing System" (defined below) or with the intention that the data forms part of a system.
Data Controller	A Data Controller is a body that, either alone or with others, controls the contents and use of personal data. For the purposes of this policy, the Data Controller is Ervia. As such, Ervia is ultimately responsible for ensuring that any third party or external party, to which the processing of personal data is outsourced, comply with the DP Acts.
Data Processor	A data processor refers to a person or third party who processes personal data on behalf of a Data Controller. It does not include an employee of a Data Controller who processes such data in the course of his/her employment. All Data Processors who process personal data on behalf of Ervia must only process the data in accordance with the instructions of Ervia and must ensure that the data is kept safe and secure at all times.
Third Party	A third party refers to an organisation that holds a contract with Ervia and is a direct supplier of services and/or software to Ervia.
External Party	An external party refers to an organisation that does not have a contract with Ervia but provides services to a third party which involves the processing of Ervia personal data on behalf of the third party.
Users	Users refer to Ervia personnel, contract and agency staff, consultants, advisors and agents, who process personal data in either paper or electronic format on behalf of Ervia.
Data Subject	Data Subject means an individual who is the subject of personal data (e.g. Ervia's employees and customers).
Personal Data*	Personal data means 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. This is commonly referred to as Personally Identifiable Information or PII.
Sensitive Personal Data	Relates to specific categories of personal data. Indicators used by Ervia to identify priority or special services customers are considered sensitive personal data. Sensitive personal data is afforded a higher level of protection under the DP Acts. It means personal data which relates to: • The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the Data Subject; • Whether the Data Subject is a member of a trade union; • The physical or mental health or condition or sexual life of the Data Subject;

	• The commission or alleged commission of any offence by the Data Subject; or • Any proceedings for an offence committed or alleged to have been committed by the Data Subject, the disposal of such proceedings or the sentence of any court in such proceedings.
Relevant Filing System	With regard to manual data, a relevant filing system is one that is structured in such a way that specific information in relation to an identifiable individual is readily accessible. This would include a file with a person's name on the front or a file containing alphabetical sub-divisions which allows personal data relating to particular individual to be located readily. A relevant filing system would not include miscellaneous collections of paper in which it is difficult to find data relating to individuals.
Processing	Processing means performing any operation or set of operations on the information or data, whether or not by automatic means, including: • Obtaining, recording or keeping the information, • Collecting, recording organising, storing, altering or adapting the information or data, • Retrieving, consulting or using the information or data • Disclosing the information or data by transmitting, disseminating or otherwise making them available, or • Aligning, combining, blocking, erasing or destroying the information or data.

* **Note:** *'Personal data'*, unless otherwise stated, refers to both *'personal data'* and *'sensitive personal data'* as defined above.

15. Document Control

Revision History

Version	Date	Change Notice	Remarks	Changed by
0.1	05 March 2010	Draft	Revised 1st Draft Data Protection Policy for Ervia Steering Committee following review by McCann Fitzgerald & BGE Legal.	Ivan O'Brien
0.2	19 March 2010	Draft	Revised 2nd Policy following feedback from Steering Committee members	Ivan O'Brien
0.3	15 April 2010	Draft	Sent to Legal, HR & Procurement for final review.	Ivan O'Brien
0.4	06 May 2010	Final Draft	Version sent to Legal & HR following feedback.	Ivan O'Brien
0.5	24 May 2010	Final Draft	Version sent to Ervia Executive for feedback	Ivan O'Brien
1.0	29 June 2010	Final	Version following Ervia Executive review	Ivan O'Brien
2	26 September 2011	Annual Review	Version following annual revision	Frank O'Reilly
2.1	16 November 2012	Annual Review	Version sent to BGE Executive for feedback	David Whelan
2.2	26 November 2013	Annual Review	Version following annual revision	Frank O'Reilly
2.3	29 November 2013	Annual Review	Version sent to Ervia Executive for feedback.	David Whelan
2.4	11 December 2014	Ànnual Review	Version sent to Chief Legal Officer and Company Secretary for review.	Noeleen McHenry
Rev 7	03 December 2015	Ànnual Review	Version sent to Chief Information Officer for feedback.	Martin Ward
Rev 8	30/11/2016	Ànnual Review	Version sent to Chief Information Officer for feedback.	Joanne Connolly