Energy for generations

ESB Group Policy on Data Protection

Approved: April 2026

Version 1.0

Next review date: Q2 2028

Contents

1. Introduction

As a key public utility, ESB collects and processes large volumes of data about its customers, employees and a range of other business partners. Data that identifies or concerns individuals is known as Personal Data. Some of the data held may also be considered special purpose (sensitive) personal data. Under Irish and EU data protection laws and ePrivacy legislation, individuals have important rights, and ESB has extensive obligations, regarding the use and protection of that Personal Data.

ESB respects the rights and freedoms of our customers, employees and others who trust us with their Personal Data. Protecting the privacy and security of this information is a top priority. As the economy and society continues to digitize, we must ensure that the protection of Personal Data continues to be placed at the forefront of everything we do. This ESB Group Policy on Data Protection ("the Policy") will guide our approach to data protection.

2. Policy Purpose

The purpose of this Policy is to set out ESB's obligations in relation to the processing and protection of Personal Data and how we will achieve compliance with our obligations in the different jurisdictions in which we operate.

With the increased use of third-party providers for the provision of services using customer Personal Data, it is important to underline that ESB remains accountable for the security and protection of the information processed by third parties on our behalf. The principles set out in this Policy will also apply to our third-party processors.

3. Policy Scope

This Policy applies to all ESB personnel, whether directly or indirectly employed by ESB, or otherwise under its control, including contractors, agents and business partners. The Policy also applies to all information systems used by ESB, including all undertakings in which ESB has a controlling interest, wherever located and for whatever purpose used, and whether operated by ESB or by an outside body on its behalf. This includes all personal information:

- created, held or used on ESB's computer systems, corporate and OT networks, local area networks and standalone personal devices, including but not limited to, PCs, laptops, tablets, smartphones and other mobile computing and storage devices used for ESB business purposes and on 'cloud' based systems;
- on electronic mail, voicemail, telephone, videoconferencing, Office 365 suite of tools, CCTV, cameras, drones, dashboard or body cameras, Internet technologies and other facilities used both for voice, video and data transmission, either internal or external; and
- held in physical files and filing systems, i.e. manual records.

NIE Networks and SO Energy maintain their own company policies in accordance with local laws and regulations and aligned, as far as practical, to ESB Group policies. For application of this Policy to non-wholly owned subsidiaries, please refer to the Group Policy for Governance of Non-Wholly owned Entities.

4. Policy Statement

All handling of personal data in ESB must be conducted in a lawful manner in compliance with the EU GDPR, Irish Data Protection Acts 1988 to 2018, ePrivacy regulations and all other relevant data protection and privacy legislation. In non-EU countries the local jurisdictions privacy legislation must be complied with.

5. Key Principles

ESB will;

(i) comply with its obligations to process data fairly, lawfully, and transparently and will communicate privacy related matters to staff and customers in a clear, easily understood and unambiguous way (see Appendix A);

(ii) only store and process special category Personal Data under the explicit conditions outlined in the regulation as necessary for processing of such information (See Appendix B);

(iii) comply with its obligations to facilitate the timely fulfilment of data subjects requests (See Appendix C);

(iv) ensure personal data is stored in a safe and secure manner and dispose of personal data if the purpose for which it was obtained has ceased;

(v) report data breaches to the Supervisory Authorities when required to do so and in the timelines set out in the law;

(vi) have an identified data owner and documented record of processing for all ESB business processes which involve the processing of personal data;

(vii) conduct a Data Protection Impact Assessment (DPIA) for any new technology, business process or use of artificial intelligence, or any significant changes to existing technologies or processes, where personal data processing is involved;

(viii) have in place written contracts with third party providers to process personal data, instructing how the data will be processed, the minimum expected security measures to protect and, when required, destroy the data and the provision of guarantees by the third party in respect of these security measures;

(ix) be satisfied that adequate contractual arrangements, controls and risk mitigation is in place where personal data is to be processed outside of the EEA; and

(x) provide mandatory privacy and data protection awareness training to all staff. In addition, specific training is provided to key staff and third-party service providers who are involved in processing personal data or other data protection related activities.

Further information can be found on ESB website Data Protection.

6. Roles & Responsibilities

Business Unit Executive Directors are responsible for the management of data and data-related resources relating to their business unit including the ownership, stewardship and operational controls to ensure that data is managed as an asset.

Managers are responsible for making sure that their teams understand and comply with the policy and supporting procedures as well as complete any relevant training.

All employees must comply with the policy and supporting procedures and complete all relevant training.

The **ESB Data Protection Officer** promotes the objectives of this policy, provides support and guidance to the business in the fulfilment of their responsibilities, and undertake appropriate monitoring activities to provide assurance on compliance with this policy.

ESB Data Protection Office operates as a Second Line function. The Data Protection Officer is supported by a dedicated Data Protection team in addition to designated Data Owners and Data Stewards within each Business Unit.

7. Monitoring & Reporting

The ESB Board and Executive Committee are responsible for the oversight for this policy including the approval of any changes to the policy. This policy is reviewed on a three-year cycle or earlier if required.

Compliance with this policy is monitored by the ESB Data Protection Officer and Business Unit Data Owners on a quarterly basis by means of review of key performance indicators (such as the number of personal data breaches, fulfilment of Data Subject Requests, Data Protection Impact Assessments, and operational reviews).

The ESB Data Protection Officer reports half yearly to the Executive Committee and the Audit & Risk Committee on compliance with this policy and industry updates.

Appendix A : Principles of Data Protection

All handling of Personal Data in ESB must be conducted in a lawful manner and in compliance with data protection regulations and legislation. ESB will at all times operate in line with the principles of the GDPR which are that personal data is:

1. Processed lawfully, fairly and in a transparent manner in relation to the individuals.

2. Collected for specified, explicit and legitimate purposes not further processed in a manner that is incompatible with those purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accurate and, where necessary, kept up to date.

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

6. Processed in a manner that ensures appropriate security of the personal data.

7. The data controller is responsible for compliance with these principles and must be able to demonstrate such compliance.

Appendix B : Special Category Data

Certain types of sensitive personal data are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as “special categories” of personal data. The special categories are:

- Personal data revealing racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data and biometric data processed for the purpose of uniquely identifying a natural person.
- Data concerning health.
- Data concerning a natural person’s sex life or sexual orientation.

Processing of these special categories is prohibited, except in limited circumstances set out in Article 9 of the GDPR.

Appendix C : Rights of the Data Subject

The EU GDPR provides individuals with various rights for how their personal information is used and protected. ESB respects these rights and, while we must capture, store and process personal information in order to be able to carry out our business responsibilities, we will endeavour to minimise the amount of personal information that is processed and to ensure that it used in accordance with the owners instructions. The eight rights that the GDPR provides are:

1. **The right to be informed**

   Individuals should be informed about why their data is needed and how it will be used in a transparent and understandable way.

2. **The right of access**

   Individuals have the right to gain access to their personal data and supplementary information. They also have a right to be aware of and verify that their data is being lawfully processed.

3. **The right to rectification**

   Individuals have the right to have inaccurate or incomplete personal data rectified.

4. **The right to erase**

   Individuals have the right to expect and/or request that data about them is deleted as long as there is no compelling reason for that data to be retained for continued processing.

5. **The right to restrict processing**

   Individuals have the right to block or suppress processing of personal data in certain circumstances (e.g. if the data is inaccurate)

6. **The right to data portability**

   Individuals have the right to have data which they have provided presented back to them in electronic format so that they can reuse it for other services.

7. **The right to object**

   Individuals have the right to object to certain types of data processing (e.g. direct marketing, profiling).

8. **Rights in relation to automated decision making and profiling**

   Individuals have enhanced rights where their data is being processed for decision making without human involvement or where their data is being used for profiling purposes.

In addition, where data subjects have a concern with the lawfulness of how their data is being processed, they have a right to lodge a complaint to the relevant Supervisory Authority.

Appendix D : Glossary of Terms

"**Personal Data**" is any information relating to a living individual which allows the identification of that individual. Examples of personal Data include a name, address, email, phone number, date of birth, bank details, PPSN, account number, staff number, MPRN/GPRN, energy consumption, online browsing history, photograph, voice recordings.

"**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.

"**Data Controller**" means the entity (for example, ESB, ESB Networks DAC, ESB Independent Energy Limited etc) which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

"**Data Processor**" means the party that processes Personal Data on behalf of the Data Controller (for example, call center service provider, payments service provider, payroll service provider etc).

"Record of Processing Activity (ROPs)" is a formal record of all categories of processing of personal data undertaken by a Data Controller and Data Processor. Each record much include specific information such as the purpose of the processing, type of personal data processed, list of data subjects whose personal data is being processed, recipients of the data, jurisdictions where the personal data will be stored/processed/transferred.

"Data Protection Impact Assessment (DPIA)" is the mechanism used by ESB to identify and control the privacy risks associated with the processing of personal data of our customers and staff. It is an important tool that demonstrates compliance with the accountability principle under the GDPR.

"Data Subject Request" is a request made by a Data Subject to exercise any right(s) under Data Protection Laws (Appendix B) that is outside your normal business-as-usual queries. Requests can be submitted via any channel and to any person in the organisation and should be immediately notified to dpo@esb.ie