ScottishPower

Data Protection Policy

Corporate Security, Data Protection

October 2023

Corporate Security

1. Purpose 2
2. Policy Objectives 2
3. Personal Data 2
4. Data Protection Principles 3
5. Data Subject Rights 3
6. Data Protection by Design and Default 4
7. Processing Activity Register & Impact Assessments 4
8. International Transfers 5
9. Third Party Engagement 5
10. Report Concerns & Data Breaches 5
11. Training 6
12. Implementation & Monitoring 6
Further Information 6

1. Purpose

ScottishPower is part of the Iberdrola Group. The purpose of the ScottishPower Data Protection Policy ("**the Policy**") and the Global Personal Data Protection Framework of the Iberdrola Group the (collectively "**the Group Policies**") is to:

i. implement the principles set out in the Group Policies at local level; and

ii. develop local internal procedures to meet the requirements of local data protection laws. In the UK, this includes the UK GDPR and the Data Protection Act 2018 (the "**UK Data Protection Legislation**"). These requirements apply to the processing of personal data by the ScottishPower Group ("**ScottishPower**") in the ordinary course of its business.

The Policy explains the key principles of ScottishPower's approach to data protection and meeting the requirements of UK Data Protection Legislation. It is supplemented by the internal rules and procedures that are set out in the Group Policies (including the Global Personal Data Protection Framework).

2. Policy Objectives

Everyone has rights with regards to the way in which their personal data is handled. During the course of its activities, ScottishPower collects, stores and processes personal data about its customers, suppliers, employees and other third parties. ScottishPower recognises that the correct and lawful treatment of this personal data is necessary for compliance with the UK Data Protection Legislation but will also maintain confidence in the organisation and provide opportunities for successful business operations.

In accordance with the Group Policies, ScottishPower has designed a range of local policies, rules, procedures and guidance documents to protect the security and integrity of personal data held by ScottishPower (the "**Policies**"). The Group Policies are implemented and supplemented by the local Policies.The Scottish Power Limited Board of Directors and senior management team require all employees, contractors, suppliers and third parties to fully comply with all Group Polices, local Policies, rules and procedures and failure to do so may result in action e.g., in the case of an employee, it may result in disciplinary action.

3. Personal Data

The Group Policies and local Policies relate to the protection of personal data. This is any data from which a living individual can be recognised (with each identifiable individual being a "**Data Subject**"). Common examples of personal data held by ScottishPower includes: customer contact details, customer financial data, credit check data for both customers and employees, prospective employee application data, employee personnel records and personal details of individuals from suppliers and other third parties that ScottishPower may work with.

In certain circumstances, ScottishPower may also process Special Category data, which includes data about an individual's physical or mental health or condition, their racial or ethnic origin, their religious views / beliefs, sexual orientation, trade union membership and criminal background.

4. Data Protection Principles

As referred to above, ScottishPower is accountable for its compliance with the following fundamental data protection principles:

I. Personal data should be processed lawfully, fairly and in a transparent manner.

II. Personal data should be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.

III. Personal data should be adequate, relevant, and limited to what is necessary in relation to the purpose(s) for which it is processed.

IV. Personal data should be accurate and, where necessary, kept up to date.

V. Personal data should be kept for no longer than is necessary for the purpose(s) for which it is processed.

VI. Personal data should be processed in a manner that ensures appropriate security of the personal data.

5. Data Subject Rights

ScottishPower is also required to enable Data Subjects to exercise the following rights in respect of their personal data:

I. The right to be informed about the processing of their personal data – ScottishPower must ensure that all Data Subjects are informed about the ways in which their Personal Data is being processed and the other rights they have in relation to this processing. ScottishPower therefore publishes privacy notices on its websites and provides Data Subjects with additional notices where required.

II. The right to access a copy of their personal data.

III. The right to have any inaccuracies in their personal data rectified.

IV. The right to have their personal data erased in certain circumstances (such as where the personal data no longer needs to be processed in relation to the purpose(s) for which it was collected).

V. The right to have the processing of their personal data restricted in certain circumstances (such as where the personal data does not need to continue to be processed but the individual does not want their data to be permanently erased).

VI. The right to receive their personal data, which they have provided to ScottishPower, in an easily-portable format and to have that data transmitted to another party in certain circumstances, e.g., when asked by a customer to transfer the data to another energy provider, ScottishPower would provide the data in a format that is machine readable.

VII. The right to object to certain types of processing (such as profiling).

VIII. The right not to be subject to a decision based solely on automated processing of personal data.

ScottishPower has procedures in place to enable Data Subjects to exercise their rights appropriately across its different business units. These include a Procedure for Privacy Notices and Consent and a Procedure for the Exercise of Rights.

It is imperative that any correspondence received from an individual about exercising their data protection rights is immediately referred to the relevant Data Protection Manager or the Data Protection Officer using the details noted at Section 12.

6. Data Protection by Design & Default

ScottishPower has a procedure that must be considered when going through the process of developing or procuring new products or services that will process personal data, e.g., a new processing activity or the development of a new software application, including situations in which these are contracted by third parties.

7. Processing Activity Register & Impact Assessments

ScottishPower captures all processes which involve the processing of personal data in its Processing Activity Register ("**PAR**"). The PAR is held and updated by ScottishPower to ensure compliance with its obligations under the UK Data Protection Legislation. The PAR captures details such as the categories of personal data, the purpose of the processing, any processing carried out by third parties, the systems involved in the processing, the lawful basis etc. If it is identified that the processing of certain personal data is deemed 'high risk' to the rights and freedoms of Data Subjects, ScottishPower will complete a Data Protection Impact Assessment ("**DPIA**") to identify and minimise any data protection risks associated with that particular high risk processing.

8. International Data Transfers

ScottishPower will only transfer personal data outside of the UK and EEA when it is legally permitted to do so and in compliance with the UK Data Protection Legislation. When ScottishPower shares personal data with third parties in countries outside of the UK and EEA, it will assess the transfer (including the data protection laws, customs and practices in the country of destination) and will put in place any required contractual arrangements, including any necessary safeguards including the UK's International Data Transfer Agreement, or the EU's Standard Contractual Clauses and the UK Addendum.

Iberdrola has implemented Binding Corporate Rules ("**BCRs**") which permit international transfers of personal data between Iberdrola Group companies for the type of international transfers specified in the BCRs, e.g. employee personal data.

These BCRs have been approved by the Spanish Data Protection Agency and are binding on all Group companies (including the ScottishPower Group). The BCRs and the list of Iberdrola entities who have signed up to them are available on our and Iberdrola's websites.

9. Third Party Engagement

Where ScottishPower engages a third party to process personal data, it will conduct all necessary due diligence and ensure agreements and contracts provide appropriate protection to the personal data. ScottishPower will do this both when appointing a third party to process personal data on its behalf or when sharing personal data with a third party who is processing personal data for its own purposes.

ScottishPower has a Procedure for Data Protection in Procurement which must be followed to ensure that any data sharing complies with the UK Data Protection Legislation and any applicable regulatory guidance.

10. Report Concerns & Data Breaches

ScottishPower could face significant repercussions if it fails to comply with its obligations under the UK Data Protection Legislation. The UK Information Commissioner's Office ("**ICO**") has statutory powers and authority to issue significant fines for breaches of the UK Data Protection Legislation.

It is imperative that employees understand and comply with the Group Policies and local Policies, and work to ensure that contractors, suppliers and other third parties with whom ScottishPower deals do likewise. Any questions or concerns regarding the Group Policies or local Policies or our compliance with them should immediately be referred to the relevant Data Protection Manager or the Data Protection Officer using the details noted at Section 12.

ScottishPower has an Incident Response Procedure in place which sets out the action to be taken in the event of any accidental or illegal destruction, loss or alteration of personal data, or any unauthorised processing of personal data for which ScottishPower is responsible (a "**Personal Data Breach**"). Accordingly if an employee (whether directly or indirectly through a contractor, supplier or other third party) becomes aware or suspects that a Personal Data Breach has occurred (or is occurring), the issue must be immediately reported to the responsible business area's Data Protection Manager or the Company's Data Protection Officer, using the details noted at Section 12.

Failure to comply with the terms of our Group Policies and local Policies may result in action being taken, e.g., in the case of an employee, this may result in disciplinary action.

11. Training

ScottishPower requires all staff to undertake mandatory training on Data Protection and Binding Corporate Rules. In addition, all staff are required to undertake regular refresher training.

12. Implementation & Monitoring

ScottishPower's Data Protection Officer can be contacted at dataprotection_corporate@scottishpower.com. The Data Protection Officer is responsible for the day-to-day oversight of the Policies and is responsible for monitoring and reporting compliance with the Policies to ScottishPower Limited's Board of Directors. The Data Protection Officer is also responsible for liaising with the ICO regarding ScottishPower's data protection compliance and accountability.

All departments within ScottishPower must implement and observe the Group Policies and local Policies. Any questions or concerns about the Group Policies and local Policies or their implementation in a specific area or department, or relating to any specific data protection responsibilities or considerations which may apply, should be referred to the Data Protection Manager for that area or department in the first instance, if the Data Protection Manager is unavailable, the questions or concerns should be referred to the Data Protection Officer.

Business Data Protection Managers can be contacted at the following:

Retail:- DataProtection@scottishpower.com
SP Energy Networks:- dp@energynetworks.co.uk
Onshore Renewables: - dataprotection_onshorerenewables@scottishpower.com
Offshore Renewables:- ukus_offshorerenewables@scottishpower.com
Corporate:- dataprotection_corporate@scottishpower.com

Further Information

More information about the UK Data Protection Legislation can also be found at the ICO's website: https://ico.org.uk/.