SCOTTISHPOWER
CORPORATE SECURITY

Nov / 2017

ScottishPower Data Protection Policy

ScottishPower Data Protection Policy

In accordance with the Scottish Data Protection Policy ("the policy") and the Global Personal Data Protection Framework of the Iberdrola Group *[https://www.iberdrola.com/wcorp/gc/prod/en_US/corporativos/docs/personal_data_protection_policy.pdf]* (the "**Group Policies**"), the purpose of this ScottishPower Data Protection Policy and the Policies (as defined below) 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 UK data protection laws which apply to the conduct of business by the ScottishPower Group ("**ScottishPower**").

Policy Objective

Everyone has rights with regard to the way in which their personal information is handled. During the course of its activities, ScottishPower collects, stores and processes personal information about its customers, suppliers, employees and other third parties. ScottishPower recognises that the correct and lawful treatment of this information will maintain confidence in the organisation and will provide for successful business operations.

In accordance with the Group Policies, ScottishPower has designed a range of local policies, procedures and guidance documents to protect the security and ensure the integrity of information held by ScottishPower which are listed below (the "**Policies**").

ScottishPower's Board of Directors and senior management team expect all employees, contractors, suppliers and third parties to fully comply with the Policies, and failure to do so may result in disciplinary action.

Personal Data

The Policies relate to the protection of personal information. This is any information or data from which a living individual can be recognised. Common examples of personal data held by ScottishPower includes: customer contact details, customer financial information, credit check information for both customers and employees, prospective employee application information, employee personnel records and details for individuals at suppliers and other third parties that ScottishPower may work with.

In certain circumstances, ScottishPower may also hold more sensitive personal data, which includes information 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.

ScottishPower Data Protection Policy

UK Data Protection Laws

Current data protection laws for the UK are contained in the Data Protection Act 1998, however this is due to be replaced on 25 May 2018 by the General Data Protection Regulation ("**GDPR**").

The GDPR brings into force a number of changes in the law regarding the protection of personal data, in light of the changing role of personal data in our society driven by the use of new technologies.

While the protection of personal information has long been a priority for ScottishPower, the GDPR will place data protection at the heart of ScottishPower's culture going forward. As a result of a requirement under the GDPR, ScottishPower must be able to demonstrate its compliance with data protection laws. In particular, ScottishPower will need to be accountable for demonstrating compliance with key data protection principles enshrined in the legislation. Failure to do so will have severe consequences for the business including regulatory penalties and also reputational harm.

Data Protection Principles & Rights

As referred to above, ScottishPower needs to be able to account for its compliance with the following fundamental data protection principles:

1. Personal data should be processed lawfully, fairly and in a transparent manner.
2. Personal data should be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.
3. Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Personal data should be accurate and, where necessary, kept up to date.
5. Personal data should be kept for no longer than is necessary for the purposes for which they are processed.
6. Personal data should be processed in a manner that ensures appropriate security of the personal data.

ScottishPower is also required to ensure that personal data is processed in accordance with the following rights that all individuals have in respect of their personal data:

- The right to access a copy of their personal data.
- The right to have any inaccuracies in their personal data rectified.
- 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 purposes for which they were collected).

ScottishPower Data Protection Policy

- 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).
- The right to receive personal data provided by them to ScottishPower in an easily-portable format, and to have that information transmitted to another party in certain circumstances e.g. when asked by a customer to transfer the data to another energy provider we would provide the data in a format that is machine readable
- The right to object to certain types of processing (such as profiling).
- The right not to be subject to a decision based solely on automated processing of personal data.

There are also rules which require ScottishPower to only allow personal data to be processed outside the European Economic Area if certain conditions are in place, to help ensure the security of processing in areas not subject to the GDPR.

Implementation & Monitoring

ScottishPower's Data Protection Officer is Philomena Wilkes, who 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's Board of Directors. The Data Protection Officer is also responsible for liaising with the UK Information Commissioner's Office ("**ICO**") regarding ScottishPower's data protection compliance and accountability.

Different departments within ScottishPower will have different data protection responsibilities, however, our Customer Service, HR, Marketing and Legal departments are likely to be most impacted. If you are uncertain of your data protection responsibilities, you should speak to your line manager in the first instance, or if they are unavailable please contact the Data Protection Officer.

Report a Concern & Security Incidents

ScottishPower faces significant repercussions if it fails to comply with its data protection obligations. Under the GDPR, these repercussions will be more severe, as the ICO will have greater statutory powers and authority to issue significant fines for data protection breaches.

If you have breached the Policies or have any concerns regarding compliance with the Policies, if you become aware of a data security incident, or if you receive correspondence from an individual about exercising their data protection rights, you

should **immediately** contact the Data Protection Officer at the details noted above. Failure to comply with the terms of the Policies may result in appropriate disciplinary action being taken.

The Policies

All employees, contractors, suppliers and third parties must fully comply with the:

- Information Management Rule
- The Cyber Security Rules

More information about the UK's data protection laws can also be found at the ICO's website: https://ico.org.uk/.