ScottishPower

DP Complaints Procedure

Corporate Security, Data Protection

June 2026

Corporate Security

Index

1. Document Version Control

Version	Date	Owner	Approved by
1.0	16/06/2026	Head of Data Privacy & Protection (Data Protection Officer)	Security Resilience Digital Technology Committee

2. Purpose and Scope

The **ScottishPower Group** is a group of companies controlled by Scottish Power Limited. This procedure applies to all customers, employees, suppliers, landowners, stakeholders, users, and any other individuals ("you") whose personal data is processed by a company in the ScottishPower Group ("we", "us").

This Procedure explains how you can raise a Data Protection Complaint with a ScottishPower Group company, how we handle and investigate your complaint, and how you can escalate concerns if you remain dissatisfied, in line with our obligations under the UK GDPR, Data Protection Act 2018 and Data Use and Access Act 2025 ("Data Protection Legislation").

A Data Protection Complaint can be made when you believe our handling of your personal data has infringed UK data protection law. For example, how we collected, used, stored, secured, retained, or responded to a rights request about your data. This is different from exercising your data protection rights—such as asking for access to your data, having it corrected, or requesting deletion—which are specific requests for us to take action with respect to your personal data rather than concerns about how it has been handled overall.

A "Data Protection Complaint" is an expression of dissatisfaction asserting that the organisation has not complied with applicable Data Protection Legislation in its collection, use, storage, disclosure, or other processing of personal data. Such complaints may concern matters including, but not limited to, unlawful or unfair processing activities, insufficient technical or organisational security measures, inappropriate sharing of personal data, or failures to uphold an individual's rights (such as rights of access, rectification, restriction, or erasure).

Concerns that are not about how we collect, use, share, or protect personal data are not considered Data Protection Complaints. These may include, for example, complaints about service delivery, decisions or outcomes, employment or HR matters, contractual or financial issues, or general dissatisfaction that does not relate to the handling of personal data. As these matters fall outside the scope of this Data Protection Complaints Procedure, they will not be investigated under this process.

3. How to make a Data Protection Complaint

You can make a Data Protection Complaint via our online webform which can be accessed through our website privacy notices. This form is part of our Data Protection Portal, OneTrust, which we will use to communicate with you about your complaint.

When completing the form, please describe what happened, and include relevant dates, any reference numbers, and any other additional information that will help us investigate. You can also attach supporting documents to provide evidence or additional information.

If you are unable to use the webform or need a reasonable adjustment, you can make a written complaint to: Data Protection, Corporate Security, ScottishPower HQ, 320 St Vincent Street, Glasgow, G2 5AD. Please include your full name, postal address, contact details, account or reference numbers; any other additional information that we may need to confirm your identity; and as much detail as possible about what has happened, including relevant dates.

4. How we will handle your Data Protection Complaint

4.1. Step 1 - Acknowledgement

We will endeavour to acknowledge your complaint within 7 calendar days of receipt and confirm which data protection team is handling it.

4.2. Step 2 – Investigation

We will investigate your complaint without undue delay by gathering relevant facts, making enquiries, and checking our records and policies. If we need more information, clarification, or proof of identity to progress your complaint, we will ask for this promptly.

To ensure we disclose and investigate personal data only in relation to the correct individual, we may need to verify the complainant's identity; where this is required, the investigation timescale will pause until satisfactory verification is received, which may extend the overall response timeframe.

Our investigation will be conducted using reasonable and proportionate steps, considering the nature, scope and potential impact of the issues raised.

4.3. Step 3 – Updates

We will keep you informed of any progress and aim to respond within 30 calendar days. This timescale is a target rather than a statutory deadline, and where a complaint is complex, we will provide regular updates on progress and revised estimated timescales.

4.4. Step 4 - Outcome

We will tell you about the outcome without undue delay. Our response will explain:

- the findings and outcome of our investigation,
- any steps we have taken or will take to resolve the matter (including remediation actions or process improvements, where appropriate), and
- our complaint escalation process should you remain dissatisfied.

5. Frequently Asked Questions

5.1. Can someone make a complaint on my behalf?

We will make reasonable adjustments to help vulnerable people and children raise complaints. Where appropriate, we may assess competence and/or seek appropriate written authority from a representative acting on someone's behalf, and will request:

- power of attorney; or
- signed letter of authority from the person they are acting on behalf of.

If this written authority is not provided, we may be unable to proceed with investigating the complaint on your behalf. In these circumstances, we will write to explain the position and outline any next steps available.

5.2. What if my complaint is about something else?

If your concern is not about how we collect, use, share, or protect personal data, it is not considered a Data Protection Complaint. This includes matters such as customer service issues, decisions or outcomes, contractual concerns, and HR or employment-related matters, including grievances, recruitment issues, or workplace disputes. These types of complaints fall outside the scope of this Data Protection Complaints Procedure and will be handled through the appropriate alternative process.

If your concern includes both a non-data protection issue and a data protection related matter (for example, a data protection concern, request to access, correct, or delete personal data), we will handle the data protection element, and the remaining aspects will be redirected through the relevant complaints or HR process. Where appropriate, we will advise you of the correct route or team to contact for support.

5.3. Can I complain via social media or other informal channels?

If you raise data protection concerns through social media or in conversation with our staff, we may record it as a potential Data Protection Complaint and capture it in this process. We will request to move the discussion to a private channel to protect your information and we may need to verify your identity.

6. Escalation Process

6.1. Escalation to Data Protection Officer ("DPO")

If you are dissatisfied with the outcome provided by the Data Protection Team, you may request a review by the DPO's Office.

We will provide a link in our outcome response to a new webform, which can be used should you require escalation. In the event that your original complaint was not processed using our webform, via OneTrust, we will provide another method for escalation.

In your complaint escalation you will be requested to provide your name, contact details, your original complaint reference number, and a summary of why you remain dissatisfied.

What happens next

The DPO's Office will:

- acknowledge your escalation request within 7 calendar days.
- review the original investigation and actions taken by the Data Protection Team that investigated your complaint, to determine whether any further steps can be taken to resolve the matter or provide further reassurance.
- aim to provide an outcome within 30 calendar days, however if more time is required, we will keep you updated on progress and estimated timescales.
- provide the outcome of the review and, where appropriate, confirm any further actions, remediation, or process improvements.

6.2. Escalation to the Information Commissioner's Office ("ICO")

Once you have received your outcome from the DPO's Office, if you remain dissatisfied with the outcome or the way in which your complaint was handled, you can raise your concerns with the Information Commissioner's Office ("ICO"). The ICO is the UK's independent regulator for data protection; however, they typically expect you to have raised your concerns with us first.

Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.
Telephone: 0303 123 1113
Website: https://ico.org.uk/ (see "Make a complaint")

7. Our Commitment to Improvement

We review complaint trends to identify root causes and to improve our privacy practices (e.g., training, policies, security, data retention, and transparency). This supports our accountability obligations and helps resolve issues early, without the need for regulatory escalation.