# Data Protection Complaints Procedure

Colin Sclare Ltd
Colin Sclare – Director – Data Protection Lead
Effective Date – 1/11/2026
Review Date – 1/11/2027

## 1. Purpose

This procedure explains how we handle complaints about the way we collect, use, store, disclose or otherwise process personal information.

The procedure is designed to comply with the data-protection complaints requirements introduced by the Data (Use and Access) Act 2025 and the current guidance issued by the Information Commissioner's Office (ICO).

All staff are responsible for identifying potential data-protection complaints and ensuring that they are referred promptly to the person responsible for data protection.

## 2. What is a data-protection complaint?

A data-protection complaint is a complaint from an individual who believes that we have not complied with data-protection law in the way it has handled their personal information.

A person does not have to use the words "GDPR", "data protection" or "personal data" for their communication to be treated as a potential data-protection complaint.

Examples include:

- a client believes that their personal information has been disclosed to another person without justification;
- a customer believes that their personal information has been incorrectly disclosed;
- a customer believes that inaccurate information is being held about them;
- a customer challenges why their personal information is being retained;
- a customer believes that their information has been used for a purpose they were not told about;
- a customer believes their personal information has not been kept secure;
- a customer complains about the way we have handled a request to access, correct or delete their personal information.

The ICO distinguishes a data-protection complaint from a request to exercise a data-protection right. For example, a request for a copy of personal information is normally a Subject Access Request, whereas a complaint that we have failed to handle that request properly is a data-protection complaint.

A communication may contain both a rights request and a data-protection complaint. Where this occurs, we will deal with each element appropriately.

### 3. Difference between a service complaint and a data-protection complaint

Not every complaint received is a data-protection complaint.

For example:

> "The negotiator hasn't returned my telephone call."

This will normally be dealt with through our ordinary complaints procedure.

However:

> "The negotiator has disclosed my telephone number to another tenant without justification."

This may constitute a data-protection complaint.

Where there is uncertainty, the complaint should be referred to the Colin Sclare rather than being dismissed as an ordinary service complaint.

### 4. How a data-protection complaint can be made

We provide reasonable and accessible ways for individuals to make a data-protection complaint.

Complaints may be made:

- by email;
- by post;
- verbally in person; or
- through another reasonable communication channel.

Where a complaint is received through social media, we will avoid requesting personal information through the social-media platform. The complainant will be directed to a secure contact method where appropriate.

Our Privacy Notice explains how individuals can raise data-protection concerns.

### 5. Responsibility for complaints

Colin Sclare is the Date Protection Lead and can be contacted via telephone on 020 8444 3351 or email: info@colinsclare.co.uk.

We will ensure that arrangements are in place to deal with complaints during periods of absence, including holidays and sickness.

## 6. When a complaint is received

Any employee receiving a potential data-protection complaint will:

1. Record the date and time the complaint was received.
2. Obtain the complainant's contact details where necessary.
3. Record the nature of the concern as accurately as possible.
4. Refer the matter to the Data Protection Lead without undue delay.
5. Avoid making admissions or promises about the outcome before the matter has been investigated.

Employees will not decide themselves that a complaint is not a data-protection matter.

## 7. Acknowledgement

We will acknowledge receipt of a data-protection complaint as soon as possible, but always within **30 days**.

The 30-day period begins on the day after the complaint is received.

The acknowledgement may be made by the same method used by the complainant unless another method has been requested or is more appropriate.

The acknowledgement will:

- confirm that the complaint has been received;
- provide a complaint reference where used;
- identify the person dealing with the matter;
- explain what will happen next; and
- provide contact details for further communication.

Where a complaint is received verbally, it may initially be acknowledged verbally. Where appropriate, this should be followed up in writing.

If the complaint has already been investigated and the outcome provided within the 30-day period, a separate acknowledgement may not be necessary.

## 8. Investigation

The investigation must begin without undue delay.

We will make appropriate enquiries having regard to the circumstances of the particular complaint.

The investigation may include:

- reviewing relevant emails;
- reviewing CRM records;

- reviewing property-management records;
- reviewing viewing records;
- reviewing referencing records;
- reviewing AML/CDD records;
- reviewing ID-verification records;
- speaking to relevant employees;
- checking disclosures or transfers of information;
- checking relevant policies and procedures;
- checking processor or supplier involvement;
- reviewing relevant access or audit logs;
- checking whether information was accurate;
- considering the applicable lawful basis for processing;
- considering whether information was retained for an appropriate period.

The level of investigation will be proportionate to the nature and seriousness of the complaint.

We are not required to undertake enquiries that would be unreasonable or disproportionate, and where this approach is taken we will justify it.

### 9. Keeping the complainant informed

We will keep the complainant appropriately informed of progress without undue delay.

Where an investigation is likely to take longer than expected, we will explain this and, where possible, provide an indication of when the investigation is expected to be completed.

We will avoid allowing a complaint to remain unanswered simply because an internal target or review period has not yet expired. We will investigate and respond without unjustifiable or excessive delay.

### 10. Related data-protection matters

During the investigation, the Data Protection Lead will consider whether the complaint also involves:

- a Subject Access Request;
- a rectification request;
- an erasure request;
- an objection;
- a restriction request;
- a personal-data breach;
- a complaint concerning direct marketing;
- a complaint concerning automated decision-making;
- a complaint concerning a processor or third-party supplier.

Where another statutory process applies, that process will be followed in addition to this complaints procedure where appropriate.

## 11. Outcome

We will provide the complainant with the outcome of the investigation without undue delay.

The outcome will explain, as appropriate:

- the issue investigated;
- the relevant facts established;
- whether the complaint is upheld, partially upheld or not upheld;
- the reasons for the decision;
- any corrective action taken;
- any further action proposed; and
- the complainant's ability to raise the matter with the ICO if they remain dissatisfied.

The response will not disclose personal information relating to other individuals.

## 12. Corrective action

Where a complaint identifies an error or weakness in our processes, appropriate corrective action will be considered.

This may include:

- correcting inaccurate information;
- changing a procedure;
- restricting access;
- deleting information where appropriate;
- providing additional staff training;
- changing a supplier process;
- reviewing a privacy notice;
- reviewing retention periods;
- reviewing security controls;
- carrying out a DPIA;
- reviewing a processor contract.

## 13. Data breaches

If the investigation identifies a possible personal-data breach, the matter will immediately be referred to our Data Breach Procedure.

The fact that the issue was raised as a complaint does not remove the need to assess whether the incident constitutes a reportable personal-data breach.

## 14. Records

We maintain a Data Protection Complaints Log.

The log records:

- complaint reference;
- date received;
- complainant;
- nature of complaint;
- date acknowledged;
- person responsible;
- relevant processing activity;
- investigation undertaken;
- relevant evidence;
- outcome;
- corrective action;
- date closed.

Records are retained in accordance with our Data Retention Schedule.

## 15. Confidentiality

Information relating to complaints is only accessed by people who need it for the purposes of investigating, managing or resolving the complaint.

Care is taken not to disclose personal information about another individual while investigating or responding to the complaint.

## 16. Management Review

The Data Protection Lead periodically reviews complaints to identify:

- recurring problems;
- weaknesses in procedures;
- training requirements;
- supplier problems;
- security issues;
- inaccurate or excessive data collection;
- inappropriate retention;
- trends in complaints.

Significant findings are reported to senior management.

## 17. ICO escalation

An individual who remains dissatisfied may raise their concerns with the Information Commissioner's Office.

We cooperate appropriately with any enquiry from the ICO.

## 18. Review of this procedure

This procedure is reviewed:

- at least annually;
- following a significant data-protection incident;
- following a material change in our processing activities; or
- following significant changes to data-protection legislation or ICO guidance.

**Approved by:** _____

**Position:** _____

**Date:** _____