# Forces Compare Limited

# Data Protection

# Complaints Policy & Procedure

## July 26

# Contents


| | | |
|---|---|---|
| 1 | Complaints Policy & Procedure | 3 |
| 2 | Our Logging and Investigation Process | 7 |
| 3 | Responding to the Complaint | 8 |
| 4 | Escalation to the ICO | 9 |
| 5 | Record Keeping | 10 |

# 1 COMPLAINTS POLICY & PROCEDURE

This document sets out the firms process for receiving, acknowledging, investigating, and responding to data protection complaints, in accordance with the Data (Use and Access) Act 2024, UK GDPR, and the Information Commissioners Office's guidance "How to deal with data protection complaints" as updated 8 May 2026.

This complaints policy and procedure relates specifically Data Protection complaints and no other type of complaints. The firm has a separate complaints policy and procedure that covers complaints from clients in relation to our provision of financial services.

In order to ensure that complaints are fairly, consistently and promptly dealt with and any proposed course of action or correspondence must be signed off by the Director. The Director is responsible for ensuring that any complaint is properly investigated and is done so competently, diligently and impartially and that the required timetable set by the Information Commissioners Office (ICO) rules is adhered to.

In the event that a complaint identifies a systemic, recurring or specific problem, the Director will seek to resolve it via discussion and the implementation of any conclusions arrived at.

We treat all complaints very seriously. We will use data about complaints and how they are handled as a key measure of how successful we are at achieving our overarching goals of conducting our business with integrity, due skill, care and diligence.

## 1.1 WHAT ARE DATA PROTECTION COMPLAINTS

A data protection complaint is any expression of dissatisfaction relating to:

- How the organisation processes personal data
- How the organisation has responded to a data protection request
- How the organisation has handled a data breach
- Perceived non compliance with UK GDPR or the Data Protection Act 2018
- Concerns about fairness, transparency, accuracy, security, or retention of personal data

A complaint does not need to be formally labelled as a complaint to qualify.

If someone considers that we have infringed data protection legislation because of the way we have handled their personal information (or the personal information of someone they're acting on behalf of), they can complain to us.

For example, people may submit complaints about:

- the way we have responded to their subject access request (SAR), or other rights request;
- the security measures we have used to store their information (eg someone who has been impacted by a data breach); or
- how we have collected or used their personal information (eg where we have stored it, how long we have kept it for, or its accuracy).

Sometimes people may complain about our service or other matters, whilst also exercising their data protection rights. This doesn't count as a data protection complaint. For example:

- an employee may raise a grievance issue, and also request copies of their personal information; or
- a person may complain about a customer service issue, and also request that we delete their information.

If we are not sure whether someone is making a data protection complaint, we must ask them to clarify.

## 1.2 INVESTIGATING, ASSESSING AND RESOLVING COMPLAINTS

Our obligations under the Data (Use and Access) Act 2025 are firstly that we must facilitate the making of complaints. Firstly, we must inform Individuals that they can complain to us or the ICO and we initially do this at the point of collecting personal data through disclosure of the right in our Privacy Notice as well as under the following scenarios:

- when restricting the information we provide to an individual in connection with their right to be informed;
- when responding to a subject access request (SAR);
- when refusing a rectification, erasure or restriction request; and

- when withholding information in response to a SAR, or the right to be informed, that is protected by legal professional privilege.

Individuals may submit complaints to us through any channel, including such as:

- Email
- Telephone
- Website contact form
- Social media messages
- In person communication
- Written letters

Staff must treat all such communications as potential complaints and route them into this process.

Upon receipt of a complaint, we must:

- acknowledge receipt of the complaint within the period of 30 days beginning on the day the complaint is received;
- explain to the individual the investigation process that we will undertake and the expected investigation and response timeline;
- without delay, investigate the complaint competently, diligently and impartially, obtaining additional information as necessary;
- assess fairly, consistently and promptly taking into account all relevant factors:
    - the subject matter of the complaint;
    - whether the complaint should be upheld;
    - what remedial action or redress (or both) may be appropriate;
    - if appropriate, whether we have reasonable grounds to be satisfied that another respondent may be solely or jointly responsible for the matter alleged in the complaint;
- offer redress or remedial action when we decide this is appropriate;

- explain to the complainant promptly and, in a way that is fair, clear and not misleading, our assessment of the complaint, our decision on it, and any offer of remedial action or redress; and
- comply promptly with any offer of remedial action or redress accepted by the complainant.

# 2 OUR LOGGING AND INVESTIGATION PROCESS

Upon receipt, the complaint must be logged within our system:

- Date received
- Complainant's details
- Summary of the issue
- Channel of receipt
- Any immediate risks identified
- Assigned handler

The Director will then determine whether:

- Immediate action is required (e.g., potential data breach)
- Additional information is needed
- Specialist teams (IT security, HR, legal, DPO, external compliance) must be involved

## 2.1 INDIVIDUAL IDENTIFICATION AND INVESTIGATION PROCESS

Firstly, we must satisfy ourselves that we have adequately identified the complainant – critical that we only respond to persons or their representatives where identity and authority has been established

Having verified identity, our investigations must then begin without undue delay and include:

- Reviewing relevant systems, records, and communications
- Speaking with staff involved in the processing activity
- Assessing compliance with UK GDPR principles
- Determining whether the organisation has met its legal obligations
- Documenting all steps taken

Investigations must be proportionate, fair, and evidence based.

The complainant must be kept informed of progress where appropriate.

# 3 RESPONDING TO THE COMPLAINT

Once the investigation is complete, we must:

- Provide the complainant with a clear, written outcome without undue delay
- Explain findings in plain language
- Describe any corrective or remedial actions taken
- Provide information on how the complainant can escalate the matter to the ICO
- Provide contact details for further queries

Outcomes must be respectful, transparent, and focused on resolving the individual's concerns.

# 4 ESCALATION TO THE ICO

If the complainant is dissatisfied with the organisation's response, they may escalate the matter to the Information Commissioner's Office (ICO).

We must provide:

- A link to the ICO's complaints page
- A statement confirming the individual's right to escalate
- Confirmation that escalation will not prejudice their rights or relationship with the firm

# 5 RECORD KEEPING

We must maintain records of:

- The detail of all complaints received including details of the date received and our acknowledgement
- As applicable, verification of complainant identity and/or authority to act of an agent
- Investigation notes
- Communications with complainants
- Outcomes and remedial actions
- Lessons learned and improvements made

Records must be retained for a period of 6 years from the date of complaint.