

1. Purpose

This procedure aims to inform individuals of their right to lodge a complaint regarding the processing of their personal data directly with UTAC.

This procedure establishes how the UTAC Group, acting as a data holder, receives, investigates, and resolves complaints relating to the processing, sharing, or access to employees and business contacts (clients, partners, leads, etc.) personal data.

It is designed to ensure compliance with:

- The Data (Use and Access) Act 2025
- The Data Protection Act 2018
- The UK GDPR

2. Scope and definition

This procedure applies to complaints concerning the processing, sharing, and access of UTAC employees and business contacts personal data.

A data protection complaint is any expression of dissatisfaction regarding the failure to comply with data regulations concerning the handling, access, disclosure, or use of personal data.

Hereinafter, some examples :

Scenario	Description
Individual cannot access their data	Subject access request was ignored or incomplete
Alleged unlawful data use	Data was used for marketing without consent
Inaccurate data used in decision-making	An employee is denied a promotion based on inaccurate information in their personnel file (e.g. alleged unjustified absences or performance issues that are incorrect or misattributed)
Confidentiality breach allegation	Email sent with visible recipients (no BCC), or incorrect recipient.
Lack of information	No privacy notice available to inform the data subject on its personal data processing
Excessive data collection	Collection of unnecessary personal data, for instance name for the subscription to a newsletter
No response or refusal to delete data without justification	Failure to respond to an erasure request within the prescribed time limits, or refusal to delete data where deletion is legally justified
Data sharing with a third-party	transmission of video recordings made on public roads during automotive tests to a client without information nor contractual framework
Use of the image without consent where required	Use of the image of a data subject for external communications without its consent

3. Submission Channels

Complaints may be submitted through any channel, including informal means (e.g. employees, social media). However, individuals are encouraged to use the preferred contact channel by reaching the Data Protection Manager directly via :

Email : dpo@utac.com

Online form : <https://www.utac.com/contact>

All employees must escalate complaints immediately to the Data Protection Manager.

4. Complaint Handling Process

Step 1 : Receipt and Logging

Complaints are recorded immediately in a dedicated Complaints Register. Information recorded is date of reception, identity of complainant, description of the issue, channel used, and relevant data processing activity concerned by the complaint.

Step 2 : Acknowledgement

The complaint is acknowledged within thirty (30) days. The acknowledgement includes confirmation of receipt, a description of next steps, the contact details. The date of the acknowledgement is recorded in the Complaints Register.

The identity of the complainant is verified where necessary.

Step 3 : Qualification

The Data Protection Manager determines where the issue constitutes a data protection complaint, a request under data subject rights or a general service complaint. Where unclear, clarification may be requested. In other words, whether this complaint is admissible.

Step 4 : Investigation

The Data Protection Manager takes appropriate steps to investigate, including :

- Reviewing relevant data processing activities
- Identifying applicable legal obligations
- Collecting evidence from internal systems
- Consulting relevant teams

The complainant is kept informed of significant progress, where appropriate.

Step 5 : Outcome and Response

The Data Protection Manager provides a reasoned response to the complainant within fifteen (15) days unless complexity justifies delay including :

- Findings of the investigation
- Whether a breach or failure occurred
- Corrective actions taken (if applicable)
- Preventive measures

Step 6 : Remediation

Where necessary, corrective actions may include :

- Rectification or deletion of data
- Restriction of processing
- Process improvements
- Staff training

5. Dispute Resolution and Escalation

If the complainant is not satisfied:

- They may request an internal review;
- The matter may be escalated under any applicable dispute resolution mechanism provided by regulation ;
- They retain the right to escalate to the relevant supervisory authority (e.g. Information Commissioner's Office (ICO), the CNIL, etc.).

6. Record-Keeping

The Data Protection Manager maintains the Complaints Register complete and accurate and the documentation of the investigation, decisions and actions taken.

7. Review and Continuous Improvement

This procedure is updated based on regulatory changes, complaint trends or audit findings.