Whitehead Monckton
Legal excellence, tailored to you

Data Protection Complaints Policy

The organisation is committed to protecting personal data and ensuring that concerns regarding data protection are addressed fairly, promptly, and transparently.

Purpose

This Data Protection Complaints Policy sets out how complaints relating to the collection, use, storage, disclosure, or handling of personal data are received, investigated, and resolved.

Scope

This policy applies to:

- All employees, contractors, consultants, and temporary staff.
- All personal data processed by the organization.
- Complaints made by customers, employees, suppliers, business partners, or any individual whose personal data is processed by the organisation.

Policy Statement

The organisation takes all data protection complaints seriously and will:

- Handle complaints confidentially and impartially.
- Investigate complaints promptly and thoroughly.
- Take appropriate corrective action where necessary.
- Comply with applicable data protection laws and regulations.
- Inform complainants of the outcome of investigations where appropriate.

What Constitutes a Data Protection Complaint

A data protection complaint may relate to:

- Unauthorised access to personal data.
- Inaccurate personal data.
- Failure to respond to data subject requests.
- Excessive or inappropriate collection of personal data.
- Unlawful disclosure of personal data.
- Retention of personal data beyond required periods.
- Security breaches involving personal data.
- Concerns regarding consent, transparency, or lawful processing.

Submitting a Complaint

Complaints may be submitted through any of the following channels:

- **Email: antoniofletcher@wmlaw.uk**
- **Postal Address: 5 Eclipse Park Maidstone Kent ME14 3EN**
- **Telephone: 01622 698000**

The complaint should include:

- Name and contact details of the complainant.
- Description of the concern.
- Relevant dates and circumstances.
- Supporting documentation, where available.

Anonymous complaints may be considered where sufficient information is provided to investigate the matter.

Complaint Handling Process

Step 1: Acknowledgement

The organisation will acknowledge receipt of the complaint within **30 days**.

Step 2: Assessment

The complaint will be reviewed to determine:

- The nature and scope of the issue.
- Whether immediate action is required.
- Whether the complaint relates to a potential data breach or regulatory matter.

Step 3: Investigation

An appropriate investigator, such as the Data Protection Officer (DPO) or designated privacy representative, will:

- Gather relevant information and evidence.
- Interview relevant personnel where necessary.
- Assess compliance with applicable data protection requirements.
- Identify any corrective actions required.

Step 4: Outcome

The organisation aims to provide a response within **30 calendar days** of receiving the complaint. Where additional time is required, the complainant will be informed of the reason for the delay and the expected timeframe.

The response may include:

- Findings of the investigation.
- Corrective measures taken.
- Recommendations for preventing recurrence.
- Information regarding escalation rights.

Step 5: Clarification

If aspects of the response are unclear, they may revert to the Investigator seeking further clarification.

Where permitted by law, individuals may also lodge a complaint with the relevant data protection regulator or supervisory authority.

Confidentiality

All complaints will be handled confidentially and shared only with individuals who need access to investigate and resolve the matter. Records will be maintained securely and in accordance with the organization's records management requirements.

Protection Against Retaliation

Individuals who raise concerns or complaints in good faith will not be subject to retaliation, discrimination, or adverse treatment as a result of making a complaint.

Record Keeping

The organisation will maintain records of:

- Complaints received.
- Investigation activities.
- Outcomes and decisions.
- Corrective actions implemented.
-

Records will be retained in accordance with applicable legal and regulatory requirements.

Roles and Responsibilities

Data Protection Officer / Privacy Officer

- Oversees complaint handling.
- Ensures compliance with data protection laws.
- Reports significant issues to management.
-

Managers

- Support investigations.
- Implement corrective actions where required.

Employees

- Report complaints promptly.
- Cooperate with investigations.
- Follow applicable data protection policies and procedures.

Policy Review

This policy will be reviewed at least annually or whenever significant changes occur in applicable legislation, regulatory requirements, or organisational practices.