CLEAR LOOP SECURITY

PREPARE/PROTECT/RECOVER

A Guide to Implementing a Complaints Handling Procedure

Under the Data (Use and Access) Act 2025, organisations must put in place a procedure for handling data protection complaints by 19th June 2026. This doesn't need to be difficult, the ICO's advice is very clear and easy to follow:

https://ico.org.uk/for-organisations/how-to-deal-with-data-protection-complaints/

However, for an even easier approach, we've defined a procedure that can be dropped into your existing data protection policy with little adjustment. There may be additional considerations if you're a joint controller or processing personal data for law enforcement purposes but for most situations the guidance in this document will be sufficient to meet your legal obligations.

Right, no fluff or long-winded explanations, here we go…

- Take the procedure starting on the next page and insert into your existing data protection policy
- Edit the highlighted section in yellow to state the person responsible for handling data protection complaints
- Make sure your whole organisation knows about this so complaints get forwarded to the responsible party
- Implement the procedure - set up a log to record complaints and ensure any additional personal data created as result of the complaint is treated in accordance with your existing data protection practices, including adhering to retention periods and deletion procedures
- Let your data subjects know how to complain - update your privacy policies so the means of raising a complaint is clearly stated; pointing everyone to an email address is sufficient but you could use a form or other standard method that is used for contacting you
- Make sure you let data subjects know they can complain when responding to a data subject access request

Want to know more? Get in touch:

https://clearloopsecurity.com/

info@clearloopsecurity.com

https://www.linkedin.com/company/clearloopsecurity/

Complaints Handling Procedure

1. Overview

This section states the process for handling data protection complaints to ensure that data protection concerns are mitigated effectively, and to prevent further escalation of complaints to the Information Commissioner's Office (ICO). The [DPO/other role] will be responsible for handling these complaints.

2. Procedure

Step 1 - Acknowledge Receipt of the Complaint

Firstly, verify that this complaint has come from an appropriate person; ensure that the complaint concerns personal data that belongs to the person making the complaint or if the complaint is coming from a third party, ensure that this third party is entitled to receive information about how this personal data was handled. Examples may include legal representation or a data subject's Member of Parliament.

If the complaint comes from a child, we must assess the competence of the child to understand and exercise their rights.

After verifying this information, respond without undue delay to inform the complainant that we have received their data protection complaint and that it is being investigated. Under the Data (Use and Access) Act 2025, we must acknowledge receipt of the complaint within 30 days of its arrival. Note that the timer starts the day after the complaint is received and if the end date is a weekend or public holiday, the end date is delayed until the next working day.

The response must include the following information:

- What we will be doing at each stage of the investigation
- When the complainant can expect further communication
- Details for a point of contact for the complainant throughout the investigation
- An overview of this complaints procedure

Step 2 - Gather Information

Establish the facts of the complaint as thoroughly, fairly, and accurately as possible; this may require asking the complainant for additional information. At this stage it is also important to verify the gathered information against the details of the complaint.

The investigation process will differ from complaint to complaint, therefore it is important to ensure that all of the necessary information has been gathered so that a fair investigation can be conducted. The investigation should commence as soon as possible after receiving the complaint.

Step 3 - Provide Regular Updates

If the investigation is likely to take some time, update the complainant on the status of their complaint on a regular basis. Where possible, provide information on when the complainant can expect to receive further updates.

This ensures the complainant is aware that the issue is still open and reduces the likelihood of the investigation being escalated to the ICO.

Step 4 - Record All Actions

Record all relevant information concerning the investigation. Record the date that the complaint was initiated and the date that a response is due. Ensure that the details of any related conversations or

relevant documents are kept on file in a way that can be easily traced back to the complaint. Any decisions that have been made or actions that have or have not been taken with regards to the complaint should be logged along with the reasons.

In the event that the complaint is escalated to the ICO, they will expect to see all of the stated information documented thoroughly.

Step 5 - Respond to the Complainant

Following the investigation, respond to the complainant and inform them that the investigation has been concluded along with the outcome of the investigation. Explain in simple language what has been done to resolve the complaint, any actions that have been taken as a result, and information on how we have reached the conclusion. Where possible, provide evidence to support our decision.

We must also inform the complainant of their right to complain to the ICO if they are dissatisfied with the outcome of their complaint.

Step 6 - Review and Log Lessons Learned

Following the response to the complainant, review the outcome of the complaint and determine any lessons learned that may inform our current data protection practices, addressing changes as required.

It is possible that the complainant may escalate the complaint to the ICO if they didn't get the outcome they desired so all records relating to the complaint must be held in accordance with our data retention periods and a log of complaints retained.

About Clear Loop Security

CLEAR LOOP SECURITY

PREPARE/PROTECT/RECOVER

Clear Loop Security is a forward-looking cyber and information security consultancy focused on the real challenges of protecting your business and your customers' data. We believe that security is an ongoing effort, where your people, processes and technology form a continuous feedback loop, improving your defences as both your business and the world evolve. Your business isn't static, and neither is securing it.

We provide services based on three key pillars:

Prepare

"An ounce of preparation is worth a pound of cure." Preparing for cyber security problems before they arise is a more cost-effective investment of resources, is more likely to have a positive impact on your ability to defend against breaches and leaks, and allows you to make considered choices without the pressure of being under active attack.

- Security Management Programmes
- Training
- Cloud Architecture Design & Assessments

Protect

Keeping a constant eye on your organisation is essential to defending against attacks; Clear Loop Security has the expertise and insight to keep watch over your business, providing constant support while you focus on making your company excel.

- Monitoring and Alerting
- Virtual Security Manager/Outsourced CISO and DPO
- Testing and Vulnerability Management

Recover

Like death and taxes, breaches are inevitable, but it's how you respond that matters - swift, decisive action that closes the holes and provides a clear message to customers, investors, and the press can keep you in business.

- Incident Response Training
- Breach Exercises
- Incident Response Services