LOSTOCK LEGAL SOLICITORS LTD

DATA BREACH RESPONSE PROCEDURE

UK GDPR Art. 33 & 34 | DPA 2018 | Reference: LL-DP-006 | June 2026

Document Ref	LL-DP-006
Version	1.0
Effective Date	June 2026
Responsible Person	Data Protection Lead / Compliance Partner

TIME CRITICAL: A reportable breach must be notified to the ICO within 72 hours of the Firm becoming aware of it. Do not delay.

1. What is a Personal Data Breach?

A personal data breach is a security incident that has affected the confidentiality, integrity, or availability of personal data. A breach may be accidental or deliberate. Examples include:

- Sending an email containing personal data to the wrong recipient
- Loss or theft of a laptop, phone, USB drive, or paper file containing personal data
- Unauthorised access to the Firm's systems or databases
- A cyber attack, ransomware, or malware infection affecting data
- Accidental deletion of personal data without backup
- Disclosure of a client file to an unauthorised third party
- A data subject's personal data included in correspondence sent to another client

Not every security incident constitutes a notifiable breach. The Firm must assess the likely risk to individuals before deciding whether notification is required.

2. Immediate Action — First Response

ANY member of staff who discovers or suspects a data breach must report it to the Data Protection Lead IMMEDIATELY. Do not investigate independently. Do not attempt to resolve it without reporting it first.

3. The Breach Response Process

1

Report — Immediately

Any staff member who discovers a suspected breach reports it to the Data Protection Lead immediately by telephone and follows up in writing. Record the date and time of discovery.

2

Contain — Within Hours

The Data Protection Lead takes immediate steps to contain the breach: recovering misdirected emails or documents; revoking unauthorised access; isolating affected systems; securing physical files. Document all containment steps taken and when.

3

Assess — Within 24 Hours

Assess the nature and scope of the breach: What data was affected? Whose data? How many individuals? What is the likely risk to those individuals? Is the data sensitive or special category data? Has the data been accessed by an unauthorised person?

4

Decide — ICO Notification Required?

A breach must be reported to the ICO if it is likely to result in a risk to individuals' rights and freedoms. A breach need NOT be reported to the ICO if it is unlikely to result in such a risk (e.g. a misdirected email immediately recalled, with no evidence of access). Document the decision and reasoning either way.

5

Notify the ICO — Within 72 Hours

If notification is required, report the breach to the ICO within 72 hours of the Firm becoming aware of it via report.ico.org.uk. If not all information is available within 72 hours, notify what is known and provide further details as soon as possible.

6

Notify Individuals — Without Undue Delay

If the breach is likely to result in a HIGH risk to individuals' rights and freedoms, notify the affected individuals without undue delay. The notification must describe the nature of the breach, likely consequences, measures taken, and contact details for the Data Protection Lead.

7

Document and Review

Record the breach in the Breach Log regardless of whether ICO notification was required. Review how the breach occurred and implement measures to prevent recurrence. Report to the Compliance Partner.

4. ICO Notification — What to Include

When notifying the ICO under Article 33 UK GDPR, the report must include:

- The nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned
- The name and contact details of the Data Protection Lead
- The likely consequences of the personal data breach
- The measures taken or proposed to be taken to address the breach, including, where appropriate, measures to mitigate its possible adverse effects

ICO Breach Report	report.ico.org.uk

ICO Helpline	0303 123 1113

5. Notifying Individuals

Notification to affected individuals is required under Article 34 UK GDPR when the breach is likely to result in a high risk to their rights and freedoms. Notification may not be required if:

- The Firm has implemented appropriate technical and organisational protection measures (e.g. encryption) that render the data unintelligible
- The Firm has taken subsequent measures that ensure the high risk to individuals' rights and freedoms is no longer likely to materialise
- It would involve disproportionate effort — in which case a public communication or similar measure must be used instead

Any decision not to notify individuals must be documented and the reasoning recorded. This decision must be approved by the Compliance Partner.

6. Notification Decision Matrix

No risk / negligible risk	No	No
Risk to individuals' rights and freedoms	Yes — within 72 hours	No (unless high risk)
High risk to individuals' rights and freedoms	Yes — within 72 hours	Yes — without undue delay

7. Breach Log

The Firm must maintain a record of all personal data breaches, regardless of whether they require notification to the ICO. The Breach Log must record:

- Date and time the breach was discovered
- Date and time the breach was reported internally
- Nature and description of the breach
- Categories and approximate number of individuals affected
- Categories and approximate number of data records affected

- Likely consequences of the breach
- Containment steps taken and when
- Decision on ICO notification (and date/time if reported)
- Decision on individual notification (and date if notified)
- Remedial measures implemented

The Breach Log is retained indefinitely as part of the Firm's accountability documentation. It must be made available to the ICO upon request.