Personal Data Breach Policy

Roca Systems Ltd
Effective: 6 August 2026

Document owner	Directors / Data Protection Lead
Version	1.0
Review date	6 August 2027
Status	Approved company policy

1. Purpose

Roca Systems Ltd must respond quickly and consistently to events that may compromise personal information. This policy explains how to report, contain, assess, document and learn from personal data breaches and information security incidents.

2. Scope

This policy applies to all personal information handled by Roca Systems in any format and to all directors, employees, temporary workers, contractors, consultants, suppliers and processors acting for the company.

3. What is a personal data breach?

A personal data breach is a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. A suspected breach must be treated as an incident until assessed.

- loss or theft of a laptop, phone, storage device, paper record or equipment containing personal information;
- an email, attachment, invoice or document sent to the wrong recipient;
- unauthorised access, account compromise, malware, ransomware, hacking or website defacement;
- accidental deletion, corruption or unavailability of personal information;
- sharing credentials or inappropriate access to customer, employee or supplier records;
- loss of availability caused by equipment failure, fire, flood or denial of service;
- a supplier or processor incident affecting information handled for Roca Systems or its customers.

4. Responsibilities

- **Everyone:** must report a suspected incident immediately, preserve evidence and follow containment instructions. Do not wait until all facts are known.
- **Director / Data Protection Lead:** coordinates triage, records the incident, assigns an investigation lead and decides escalation and notifications.
- **Investigation Lead:** gathers facts, assesses risk, coordinates containment and recovery, and documents actions and recommendations.
- **System owners and managers:** support containment, evidence gathering, restoration and corrective action.
- **Processors and suppliers:** must notify Roca Systems without undue delay where an incident affects information processed on its behalf and provide necessary assistance.

5. Immediate reporting

Report immediately

Email: service@roca.co.uk - use subject: URGENT - DATA BREACH
Telephone: 028 90 461 461
If discovered outside normal hours, report as soon as practicable and do not delay urgent containment.

The initial report should include, where known:

- what happened and how it was discovered;
- date and time of the incident and discovery;
- systems, devices, documents and locations involved;
- categories and approximate volume of personal information;
- number and categories of people affected;
- whether information was encrypted or otherwise protected;
- actions already taken and whether the incident is ongoing;
- contact details for the person reporting it.

6. Containment and recovery

The priority is to stop further loss while preserving evidence. Appropriate actions may include recalling or requesting deletion of a misdirected email, disabling accounts, resetting credentials, isolating equipment, blocking access, recovering records from backup, contacting a recipient, or involving IT, hosting, email or security providers.

Containment actions must be proportionate. Do not delete logs, reimage equipment or communicate externally unless authorised, as this may destroy evidence or worsen the incident.

7. Investigation and risk assessment

An investigation should begin immediately and, where practicable, an initial risk assessment should be completed within 24 hours. The assessment must consider the nature, sensitivity and volume of the information; identifiability; likely consequences; affected people; protections; recipients; customer obligations; and whether Roca Systems is controller, joint controller or processor.

8. Notification decisions

All decisions and reasons must be documented, including a decision not to notify.

- **ICO:** If the breach is likely to result in a risk to people's rights and freedoms, the ICO must be notified without undue delay and, where feasible, within 72 hours after Roca Systems becomes aware of it. Information may be provided in phases if all details are not yet available.
- **Affected people:** If the breach is likely to result in a high risk, affected people must be informed without undue delay in clear language, unless a legal exception applies.
- **Customers or controllers:** Where Roca Systems processes information for a customer, the customer must be informed without undue delay in accordance with the contract so that the customer can meet its own obligations.
- **Others:** Police, insurers, banks, manufacturers, professional advisers or other parties may be contacted where necessary and authorised.

9. Breach record

Roca Systems will maintain a record of all personal data breaches, whether or not they are reported to the ICO. The record must include the facts, effects, risk assessment, decisions, notifications, containment and corrective actions.

10. Communications

External communications, including contact with affected people, customers, regulators, media or law enforcement, must be coordinated by an authorised director or delegate. Communications must be accurate, timely and should not speculate or conceal material facts.

11. Post-incident review

After containment, the Investigation Lead will document the root cause, chronology, impact, response effectiveness and lessons learned. Actions may include technical changes, access reviews, supplier remediation, updated procedures, staff training and testing. Action owners and deadlines must be recorded.

12. Non-compliance

Failure to report or cooperate with an incident may result in disciplinary or contractual action. Nothing in this section prevents Roca Systems from taking immediate steps necessary to protect people, information or services.

Appendix A - Personal Data Breach Report Form

Complete as much as possible. Missing details must not delay immediate reporting.

Field	Details
Incident reference	
Date and time discovered	
Date and time incident occurred (if known)	
Person reporting and contact details	
Location / system / device involved	
Description of what happened	
Is the incident ongoing?	Yes / No / Unknown
Immediate containment action taken	
Categories of personal information involved	
Approximate number and categories of people affected	
Was the information encrypted or otherwise protected?	Yes / No / Unknown - details:
Could the information have been accessed or misused?	
Customer / controller affected	

Appendix B - Assessment and notification record

Assessment	Decision / details
Investigation Lead	
Initial severity	Low / Medium / High / Critical
Likely consequences for affected people	
Risk to rights and freedoms likely?	Yes / No - reasons:
High risk likely?	Yes / No - reasons:
ICO notification required?	Yes / No
ICO notified date/time and reference	
Affected people notification required?	Yes / No
Affected people notified date/time and method	
Customer/controller notified date/time	
Other notifications	
Recovery actions	
Root cause	
Corrective actions, owner and deadline	
Closure approved by and date	

Appendix C - First 72 hours checklist

- Report immediately and start the incident log.
- Contain the incident and preserve evidence.
- Confirm whether Roca Systems is controller or processor.
- Identify the information, people, systems and recipients involved.
- Assess likely risk and high risk to people.
- Notify the customer/controller without undue delay where applicable.
- Decide whether ICO notification is required and track the 72-hour deadline.
- Decide whether affected people must be told without undue delay.
- Document every decision, action and reason.
- Plan recovery, corrective actions and a post-incident review.

Legal references

ICO breach guidance: ico.org.uk/for-organisations/report-a-breach/

UK data protection legislation: legislation.gov.uk