Data Protection and Privacy 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 handles personal information in the course of providing technical hardware services, manufacturer maintenance, printer and EPOS support, AV services, storage, field support and normal business administration. This policy establishes the standards that apply whenever personal information is collected, accessed, used, shared, stored, retained or disposed of.

2. Scope

This policy applies to directors, employees, temporary and agency workers, contractors, consultants, suppliers and other people who process personal information for or on behalf of Roca Systems. It applies to information in electronic, paper, image, audio and any other format.

3. Legal framework

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Privacy and Electronic Communications Regulations 2003, where applicable;
- contractual, confidentiality and sector-specific requirements applicable to customer work.

4. Data protection principles

Personal information must be:

1. processed lawfully, fairly and transparently;
2. collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes;
3. adequate, relevant and limited to what is necessary;
4. accurate and kept up to date where necessary;
5. kept in identifiable form no longer than necessary;
6. protected by appropriate technical and organisational measures; and
7. handled in a way that allows Roca Systems to demonstrate accountability.

5. Roles and responsibilities

- **Directors:** are accountable for governance, resources, major risk decisions, regulator contact and approval of this policy.
- **Data Protection Lead:** coordinates privacy requests, complaints, breach records, policy reviews and advice. This role may be assigned to a director or another authorised person.
- **Managers and system owners:** ensure that processing within their area has a valid purpose, suitable access controls, retention arrangements and approved suppliers.
- **All workers and contractors:** must follow this policy, protect credentials and equipment, use personal information only for authorised work and immediately report incidents or concerns.
- **Processors and suppliers:** must act under appropriate written terms, maintain confidentiality and security, and assist Roca Systems with rights requests and incidents where relevant.

6. Information we may process

- customer, supplier and business contact details;
- service requests, job records, site details, equipment identifiers, warranty information and correspondence;
- invoices, payments and other accounting information;
- employee, applicant, contractor and training records;
- access, security, system and communications records;
- complaints, investigations, insurance and legal records;
- special category or criminal-offence information only where necessary, lawful and subject to additional safeguards.

7. Lawful processing

Before processing personal information, Roca Systems must identify and document an appropriate lawful basis. Depending on the activity, this may be contract, steps before a contract, legal obligation, legitimate interests, consent, vital interests or another lawful basis available under data protection law. Where legitimate interests are used, the purpose, necessity and impact on individuals must be considered. Privacy information must explain the relevant interests. Consent must be specific, informed, freely given and capable of being withdrawn.

8. Special category and criminal-offence information

Special category and criminal-offence information receives additional protection. It must not be collected merely because it may be useful. Processing requires both a lawful basis and an additional legal condition, together with safeguards such as restricted access, minimisation and appropriate documentation.

9. Transparency and privacy information

People must receive clear privacy information at the appropriate time. Notices should explain the controller, purposes, lawful bases, categories of information, recipients, international transfers, retention criteria, rights and complaint routes. Privacy information must be reviewed when processing changes.

10. Individual rights requests

Requests may be made verbally or in writing and must be sent promptly to the Data Protection Lead. Roca Systems will identify the right involved, verify identity where proportionate, search relevant systems, apply any lawful exemptions, and respond within the statutory period. No fee will normally be charged unless the law permits one for a manifestly unfounded, excessive or repeated request.

11. Data quality and minimisation

Only information necessary for an authorised purpose should be requested, copied or retained. Reasonable steps must be taken to keep information accurate. Unnecessary duplicates, informal exports and local copies should be avoided and securely removed.

12. Access and confidentiality

Access is granted on a need-to-know and least-privilege basis. Passwords and authentication information must not be shared. Personal information must not be discussed, displayed, emailed, photographed, copied to removable media or taken off site unless authorised and appropriately protected.

13. Security and acceptable handling

- use approved systems, devices, accounts and storage locations;
- apply secure passwords, updates, malware protection, backups and encryption where proportionate;
- verify recipients before sending information and use secure transfer methods for sensitive information;
- lock screens, secure paper records and protect portable devices;
- dispose of paper and electronic information securely;
- report lost devices, misdirected communications, unauthorised access, malware and other incidents immediately.

14. Sharing and processors

Personal information may be shared only where there is a lawful and necessary reason. Before appointing a processor, Roca Systems must consider the provider's security and privacy arrangements and put appropriate contractual terms in place. Sharing with manufacturers, customers, warranty providers, field partners, advisers or authorities must be limited to what is required for the purpose.

15. International transfers

Transfers outside the United Kingdom must use an available lawful transfer mechanism, such as an adequacy regulation or appropriate safeguards, and must include a documented assessment and controls appropriate to the risk.

16. Retention and secure disposal

Information must be retained in line with an approved business, legal, accounting, warranty, contractual or regulatory need. Retention should be based on category and purpose, not convenience. When information is no longer required, it must be securely deleted, anonymised or destroyed, including copies and exported files where practicable.

17. Data protection by design and default

Privacy and security must be considered when introducing or changing systems, suppliers, forms, monitoring, data sharing or business processes. High-risk processing must be escalated and assessed before it begins, including a data protection impact assessment where required.

18. Personal data breaches

All confirmed or suspected personal data breaches must be reported immediately and handled under the Roca Systems Personal Data Breach Policy. Every breach must be logged. If a breach is likely to result in a risk to people's rights and freedoms, Roca Systems will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. Where a high risk is likely, affected people will also be informed without undue delay, unless a legal exception applies.

19. Data protection complaints

Roca Systems provides a clear route for data protection complaints through service@roca.co.uk, 028 90 461 461 or the postal address in this policy. Complaints will be acknowledged within 30 days, investigated appropriately, progressed without undue delay, and concluded with an outcome communicated to the complainant.

20. Training, monitoring and non-compliance

People with access to personal information must receive instructions or training appropriate to their role. Compliance may be monitored through reviews, access checks, incident analysis and supplier assurance. Deliberate or negligent non-compliance may result in disciplinary, contractual or legal action.

21. Contact and complaints to the ICO

Roca Systems data protection contact

service@roca.co.uk
028 90 461 461
224 Newtownards Road, Belfast, BT4 1HB

Individuals may also complain to the ICO. See ico.org.uk/make-a-complaint.