GDPR Policy – SRL Traffic Systems

Author:	Richard Doyle – IT Director
Version:	2.0.0
Created:	January 2026
Reviewed:	January 2027

Contents

About Us

We hire, sell, install, and maintain **temporary traffic systems**, including portable signals, CCTV, monitoring equipment, and associated traffic management technology.
We take privacy seriously and handle personal data in line with the **UK GDPR and EU GDPR** requirements.

What Personal Data We Collect

From Customers and Suppliers

- Name and contact details (email, phone, job title)
- Company and site address
- Purchase orders, delivery/collection information
- Payment and invoicing details

From Site Operations

Depending on the equipment hired, we may also collect:

- Site contact information
- Images/videos captured by mobile CCTV or monitoring equipment
- Equipment usage logs and telemetry (battery, connectivity, system uptime)

Important: We only collect operational data where necessary to support safety, security, or agreed monitoring functions.

Roles and responsibilities for Data Handling

To ensure personal and sensitive data is handled appropriately throughout the organisation, SRL assigns the following responsibilities:

All Employees

- Handle personal and sensitive data only when required for their role.
- Follow documented procedures for accessing, storing, transmitting, and deleting data.
- Report any suspected data breach immediately to their line manager and the Data Protection Lead.
- Ensure all physical materials (paper records, printed site sheets, USB drives) are kept secure when not in use.

Managers & Supervisors

- Ensure team members follow GDPR, company policies, and data-handling procedures.
- Authorise access to systems based on job role and need-to-know.
- Escalate data incidents in line with our incident-response process.

Data Protection Lead (DPL)

- Oversee compliance with UK GDPR and internal policies.
- Maintain the Record of Processing Activities (ROPA).
- Coordinate Data Protection Impact Assessments where required.
- Act as liaison point for customers, suppliers, and the ICO.

IT Department

- Implement and maintain technical security controls, including firewalls, endpoint protection, access management, and secure backup.
- Ensure secure configuration of company devices and systems.
- Monitor systems for potential threats and vulnerabilities.

Why We Use Your Data

We process personal data for the following purposes:

- **To deliver our services**
  (Equipment hire, installation, removal, maintenance, support)
- **To manage orders and contracts**
  (Quotes, invoices, delivery notes, asset tracking)
- **To ensure site safety and security**
  (Monitoring solutions such as CCTV)
- **To comply with legal requirements**
  (Finance records, insurance, health & safety, incident logs)
- **To improve system reliability and performance**
  (Remote diagnostics and equipment telemetry)
- **To communicate with you**
  (Service updates, scheduled visits, fault notifications)

Our Legal Bases

We process data because:

- **It is necessary to deliver our contract with you**
- **We have a legal obligation** to keep certain records
- **We have a legitimate interest** in ensuring system safety, security, and business operations
- **You have given consent**, where required (e.g., marketing emails)

CCTV and Monitoring Equipment

If you hire mobile CCTV, REMOS, or similar systems from us:

- You are the **Data Controller** for footage collected at your site
- We act as your **Data Processor** where we provide storage, remote monitoring, or maintenance
- We follow your instructions and provide a Data Processing Agreement (DPA) if required

We do **not** use surveillance data for any purpose other than agreed operational monitoring and safety.

Sharing Your Data

We only share personal data with:

- Trusted service providers (IT, hosting, remote monitoring, telematics)
- Payment processors and finance systems
- Delivery partners or subcontractors involved in site work
- Authorities or insurers if legally required (e.g., incident investigations)

We do **not** sell your data.

International Transfers

If any of our technology suppliers store data outside the UK/EU, we ensure they use approved safeguards such as:

- UK/EU Standard Contractual Clauses
- Adequacy decisions

Data Retention

We keep data only for as long as necessary:

- Customer & contract records: typically, **6–7 years** (legal/finance requirement)
- Equipment logs/telemetry: usually **3–12 months**
- CCTV footage: normally **7–30 days**, unless required for an investigation

Exact retention can vary depending on safety, insurance, or legal requirements.

Security

To protect personal and operational data, we use a layered security approach that includes:

Network & Infrastructure Protection

- Enterprise-grade **firewalls** with active intrusion prevention.
- Enforced **VPN** for remote administrative access.
- Network segmentation to restrict access to critical systems.

Device Security

- **All laptops and mobile devices are encrypted** using industry-standard encryption.
- All devices are **password-protected** with minimum-strength requirements and automatic lockouts.
- **Multi-factor authentication (MFA)** is used for key systems and cloud applications.
- **Antivirus/anti-malware** protection is deployed across all endpoints with automatic updates.

System & Data Access Controls

- Role-based access (RBAC) ensures staff can only access data needed for their job.
- Access rights are reviewed **quarterly** and revoked immediately when staff leave.
- Audit logs are maintained for system and data-access activities.

Data Storage & Transfer

- Data is encrypted in transit (TLS) and at rest.
- Secure file-transfer methods are used (SFTP, encrypted email, or approved portals).
- Customer data is stored only in approved systems hosted in the UK/EU unless otherwise agreed.

Business Continuity

- Regular backups of critical systems with secure off-site retention.
- Disaster recovery procedures tested annually.

Your Rights

You can request to:

- Access your data
- Correct inaccurate information
- Delete data (in certain circumstances)
- Restrict or object to processing

  To do this, contact: **gdpr@srl.co.uk**

You also have the right to contact the **Information Commissioner's Office (ICO)** if you're not satisfied with our response.

Cookies & Website Use

Our website may use basic cookies for functionality and analytics. You can manage your cookie preferences in your browser settings.

Staff Training and Awareness

All staff receive ongoing data-protection training to ensure compliance with UK GDPR and organisational requirements:

- **Mandatory induction training** for all new employees covering data protection, confidentiality, and secure working practices.
- **Annual refresher training** for all staff, including updates on new regulations or internal policy changes.
- **Role-specific training** for employees handling sensitive or high-risk data (e.g., CCTV operators, IT administrators, remote monitoring staff).
- Periodic **phishing awareness and cybersecurity training** to reinforce secure behaviour.
- Training records are maintained by HR and reviewed during internal audits.

Changes to this Policy

We may update this policy from time to time. Significant changes will be shared on our website or communicated directly where appropriate.

Revision History

Date	Revision No	Summary
January 2026	1.0	Original draft
March 2026	2.0	Sections added (Roles and responsibilities, IT Security measures, Staff Training and awareness)