Retroserve Limited
Data Protection and Information Governance Policy (UK GDPR/DPA 2018)

Part I: Governance and Accountability Framework

1.0 Policy Statement and Scope

Retroserve Limited (The Controller) complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The policy applies to all personal data processing activities (digital, verbal, or physical) involving all personnel and associated persons.

The scope covers all company operations, including the administrative functions at Unit 11, Shaftesbury Street South, Derby, DE23 8YH, construction sites, and remote operations involved in the installation of energy efficiency measures (EEMs). The Company maintains certifications for PAS 2030:2019 and PAS 2030:2023, TrustMark registration, and CHAS Advanced certification.

2.0 Key Roles and Accountability Structure

2.1 The Data Controller

Retroserve Limited operates as the Data Controller, determining the purposes and means of processing personal data.

- **Official Contact Address:** Unit 11, Shaftesbury Street South, Derby, DE23 8YH
- **Dedicated Email Address:** info@retroserve.co.uk

2.2 Executive Accountability

- **Chief Executive Officer (CEO), Adam Shaid:** Holds ultimate responsibility for ensuring the Company's compliance with the UK GDPR, including necessary resourcing and implementation of this policy.
- **Compliance and Operations Manager (DPL):** Designated as the Data Protection Lead (DPL). Responsible for operational execution of this policy, internal monitoring, coordinating staff training, overseeing Data Subject Rights requests, and acting as the official contact point for the Information Commissioner's Office (ICO).

2.3 Responsibilities of Personnel and Subcontractors

Adherence to this policy is mandatory for every employee and associated person, including subcontractors. All staff must undergo a mandatory review and acknowledgement of this policy during their initial workforce induction.

The official company contact points are designated as the required "Single Front Door" for all data protection communications, including formal Subject Access Requests (SARs).

Part II: The Data Protection Principles and Lawful Basis

3.0 The Data Protection Principles

Retroserve's processing activities adhere to the following principles:

- **3.1 Lawfulness, Fairness, and Transparency:** Comprehensive Privacy Notices must be provided to all data subjects. For clients, the notice must disclose mandatory data sharing and lodgement into the TrustMark Data Warehouse.
- **3.2 Purpose Limitation:** Data collected must be strictly limited to the stated purposes (e.g., retrofit design and EEM installation).

- **3.3 Data Minimisation:** Only personal data strictly necessary for the purpose shall be processed.
- **3.4 Accuracy:** Records must be accurate, current, and subject to routine verification.
- **3.5 Storage Limitation (Retention):** Data shall be retained only for the duration defined in the mandatory Retention Schedule (Section 8.0).
- **3.6 Integrity and Confidentiality (Security):** Robust Technical and Organisational Measures (TOMs) must be employed (Section 7.0).

4.0 Lawful Basis for Processing (Article 6)

The primary lawful bases for core processing activities are Performance of a Contract, Legal Obligation, and Legitimate Interests. Mandatory submission of project data (including assessment and certification details) into the TrustMark Data Warehouse is based on **Legal Obligation** to comply with the regulatory framework governing energy efficiency schemes.

Lawful Basis Assessment for Core Retroserve Activities

Processing Activity	Data Subjects Involved	Primary Lawful Basis (Article 6)	Data Processed (Examples)
Installation of EEMs (Quotes, Works)	Clients/Homeowners, Subcontractors	Performance of a Contract	Contact details, financial data, signed agreements, property access keys.
Mandatory Lodgement to TrustMark Data Warehouse	Clients/Homeowners, Property Occupants	Legal Obligation	Property details, EEM certification, assessment details, occupancy data.
Health & Safety Monitoring (Accident/Risk Reporting)	Employees, Clients, Third Parties	Legal Obligation / Vital Interests	Incident reports, investigation files, medical treatment details, Occupational Health referrals.
Financial and HR Administration	Employees, Suppliers	Legal Obligation (Tax, Employment Law)	Payroll, tax codes, bank details, supplier invoices, contracts.
Policy Enforcement (Drugs/Alcohol Testing)	Employees (Safety-Critical Roles)	Legitimate Interests / Legal Obligation (H&S Act 1974)	Test scheduling, testing results, disciplinary records.

5.0 Processing Special Category Data (Article 9)

5.1 Lawful Condition for Health Data

Retroserve processes Special Category Data concerning health (e.g., fitness-for-duty assessments and mandatory drug and alcohol testing results). The legal basis for processing this information is Article 9(2)(b): processing is necessary for the purposes of carrying out the Controller's obligations and exercising rights in the field of employment and social protection law.

5.2 Safeguards for Health Data

1. **Limited Access:** Access to testing results, disciplinary records, and occupational health referrals is strictly limited to authorized personnel within HR and Occupational Health.

2. **Segregation and Encryption:** Digital health records must be encrypted and logically segregated. Physical documents must be stored under lock and key.
3. **Confidentiality of Support Services:** Confidential support mechanisms, such as the Employee Assistance Programme (EAP), must maintain strict separation from disciplinary data processing.

Part III: Data Subject Rights and Accountability Procedures

6.0 Managing Data Subject Rights

6.1 Submission and Verification

Requests for data subject rights (including SARs, rectification, erasure, and restriction) must be directed to the DPL via the designated contact points. Mandatory steps must be taken to verify the identity of the requester before any personal data is disclosed.

6.2 Subject Access Request (SAR) Procedure

The statutory deadline for response is one calendar month.

SAR Handling Procedure

Step	Action Required	Responsible Party	Compliance Reference / Timeline
1. Receipt and Acknowledgment	Log request; Verify requester identity (ID checks)	DPL / HR	Within 3 working days of receipt.
2. Scope Clarification	Contact requester if scope is unclear or excessive; Offer to narrow search scope	DPL	One month timeline begins upon receipt of clarified scope.
3. Data Retrieval, Review, and Redaction	Search all relevant systems (HR, project management, email); Apply redactions for third-party personal data or legal professional privilege	System Owners / DPL	Must be completed to allow timely response.
4. Final Response Delivery	Provide personal data copy and all supplementary information (purpose, categories, retention, recipients)	DPL	**Without undue delay, and in all cases, within one calendar month.** Extension of up to two months possible for complex requests (documented justification required).
5. Record Keeping	Update SAR Log, documenting all searches, redactions,	DPL	Retain records for 3 years (Appendix B).

	exemptions, and communications.		

7.0 Data Security, Integrity, and Confidentiality (Technical and Organisational Measures - TOMs)

7.1 Digital Measures

Mandatory full-disk encryption is required for all company-owned devices (laptops, tablets, mobile phones) used to collect or store personal data. Strict access controls must be applied across all IT systems based on the "need to know" principle. Regular system reviews must be conducted.

7.2 Physical Security (Office and Site)

- **Office Security:** Sensitive physical documents (HR files, financial data) must be stored in locked cabinets within restricted-access areas.
- **Construction Site Security:** All devices containing project data or property details must be encrypted. When not actively supervised, devices must be transported off-site daily or secured in locked, monitored storage. Paperwork containing client contact or property details must not be left unattended or unsecured on site.

7.3 Subcontractor and Third-Party Risk

All Subcontractors acting as Data Processors must execute a robust Data Processing Agreement (DPA) contractually obligating them to implement equivalent security standards and adhere strictly to the purposes and limits of processing defined by Retroserve.

8.0 Data Retention and Secure Disposal

8.1 Retention Periods

Data shall only be retained for the minimum period necessary. All mandatory PAS 2035 project files, designs, and TrustMark lodgement confirmations must be retained for a mandatory period of **10 years**.

8.2 Secure Disposal Methods

Upon the expiry of the relevant retention period: Physical documents must be destroyed via cross-cut shredding. Digital media requires certified, irreversible wiping or physical destruction.

Appendix B: Data Retention Schedule Summary

Record Type	Example Data Processed	Minimum Retention Period	Legal/Operational Justification
Client Contracts and Commercial Files	Signed quotes, installation documentation, final invoice.	6 Years after Contract End	Statutory limitation period for contract claims (UK Limitation Act).
PAS 2030/2035 Project Audit Files (Mandatory Lodgement Data)	Retrofit assessments, designs, installation certifications, lodgement confirmations.	**10 Years**	Compliance with TrustMark/Funding body requirements; long-term warranty/liability assurance for EEMs.

Employee HR Files (Post-Termination)	Contracts, recruitment records, general staff in post data.	3 Years after Termination	HMRC requirements / Standard HR practice.
Health and Safety Records (Accidents/H&S Reports)	Accident reports, investigation files, Occupational Health (Fitness to Work) records.	6 Years	Compliance with RIDDOR, HASAWA, and H&S legislation.
Drug and Alcohol Testing Results (Positive/Disciplinary)	Confirmed positive test results, disciplinary actions taken.	6 Years after Policy Incident Closure	Evidence for potential employment tribunals or internal appeal processes.
Data Protection Requests (SARs, Erasure)	Request logs, search records, response packs.	3 Years	Evidence of compliance with statutory obligations.

Part IV: Incident Management and Review

9.0 Data Breach Management and Reporting

9.1 Internal Reporting and Containment

Any individual who detects a potential or confirmed personal data breach must immediately notify the Data Protection Lead (DPL) to initiate the response protocol. The initial response must prioritize containment, securing affected systems, isolating the breach source, and gathering facts.

9.2 Risk Assessment and Threshold Test

The DPL must conduct a rapid risk assessment to determine if the breach is *likely* to result in a risk to individuals' rights and freedoms.

9.3 ICO Notification (72-Hour Rule)

If the risk threshold is met, the DPL must report the breach to the ICO within **72 hours of becoming aware**. The report must detail the nature of the breach, the approximate number of individuals and records affected, DPL contact information, likely consequences, and mitigation measures.

9.4 Notification to Data Subjects

If the breach is determined to result in a **high risk** to the rights and freedoms of individuals, the affected data subjects must be notified directly, without undue delay, advising them on potential consequences and protective steps.

9.5 Mandatory Documentation

A comprehensive, detailed log of *all* personal data breaches-irrespective of whether the breach was reported to the ICO-must be maintained.

10.0 Data Protection Impact Assessments (DPIAs)

DPIAs must be conducted and reviewed prior to initiating any new processing activity that is likely to result in a high risk to data subjects (Article 35).

10.1 Mandatory DPIA Threshold Triggers

DPIAs are formally mandated for, but not limited to, the following high-risk activities:

- Processing Special Category Data systematically, such as employee health data related to the mandatory Drug and Alcohol Testing regime.
- Any new system involving systematic and extensive evaluation of personal aspects of individuals.
- New or significantly altered processing that involves mandatory and systemic data sharing with external third parties based on regulatory obligation, such as new systems for TrustMark Data Lodgement.

11.0 Policy Review and EnforcemenT

11.1 Training and Awareness

Mandatory annual refresher training on this policy is required for all personnel.

11.2 Enforcement

Any violation of this Data Protection Policy will lead to formal disciplinary procedures, up to and including immediate termination of employment or contract.

11.3 Review Cycle

This policy will be formally reviewed by the CEO and DPL annually, or immediately following any major change in UK legislation, regulatory body standards (PAS/TrustMark), or significant organizational or IT changes.

Signature: 
Full Name: Adam Shaid
Position: CEO
Date: 02/02/2025