STRAVICA

Data Protection & GDPR Policy

1.0 Purpose

1.1 Objective

Stravica Ltd ("the Company") is committed to ensuring that all personal data handled within the organisation is processed lawfully, fairly, and transparently in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and related privacy legislation.

1.2 Policy Aim

This policy establishes the framework for how Stravica Ltd protects personal data belonging to employees, clients, suppliers, contractors, and any other identifiable individual ("data subjects") in all business operations including:

- Facilities management and cleaning services;
- Refurbishment, maintenance, and property-compliance projects;
- Government-contracting and DPS/CCS framework activities; and
- Digital operations via stravica.uk.

1.3 Corporate Commitment

Stravica Ltd recognises the confidentiality, integrity, and availability of personal data as critical business assets. The Company adopts a risk-based approach to processing, ensures accountability through robust documentation, and seeks continual improvement through audits, reviews, and staff awareness.

2.0 Scope and Application

2.1 Scope of Processing

This policy applies to all forms of personal data—electronic, paper, visual, or verbal—collected or processed by Stravica Ltd, including data held by approved processors and subcontractors.

2.2 Persons Covered

This policy applies to:

- Employees (permanent, temporary, agency, and secondees);

- Applicants and former staff;
- Contractors, suppliers, and consultants;
- Client representatives, site visitors, and service users;
- Members of the public interacting with stravica.uk or Company communications.

2.3 Systems and Locations

It covers all corporate systems, cloud platforms, mobile devices, on-site paper records, and any environment where personal data is stored or transmitted.

2.4 Non-Compliance

Failure to follow this policy may result in disciplinary action, termination of contract, and/or regulatory sanctions under the DPA 2018 and UK GDPR.

3.0 Legal and Regulatory Framework

3.1 Primary Legislation

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Privacy and Electronic Communications Regulations (PECR) 2003 (as amended 2019)
- Freedom of Information Act 2000 (reference for public-body requests)
- Investigatory Powers Act 2016 (security oversight)

3.2 Regulatory Guidance

The Company aligns with guidance issued by:

- The Information Commissioner's Office (ICO);
- The Crown Commercial Service (CCS) Supplier Standards; and
- Relevant ISO standards (ISO 27001 Information Security and ISO 27701 Privacy Extension).

3.3 Related Policies and Documents

- Information Security Policy
- Data Retention and Destruction Schedule
- Data Breach Management Procedure
- Subject Access Request (SAR) Procedure
- Recruitment and HR Privacy Notices
- Cookies and Website Privacy Policy

4.0 Definitions

4.1 Personal Data

Any information relating to an identified or identifiable living individual, whether directly or indirectly (e.g. name, ID number, email, CCTV image, IP address).

4.2 Special Category Data

Information revealing racial or ethnic origin, political opinions, religious beliefs, trade-union membership, genetic or biometric data, health data, sex life or sexual orientation.

4.3 Processing

Any operation performed on personal data – collection, recording, organisation, storage, alteration, retrieval, consultation, use, disclosure, erasure or destruction.

4.4 Controller

Stravica Ltd – determines the purposes and means of processing.

4.5 Processor

Any third party processing personal data on behalf of Stravica Ltd under contract (e.g., IT host, HR provider, security firm).

4.6 Data Subject

A living individual whose personal data is processed by the Company.

4.7 DPO (Data Protection Officer)

The designated internal role responsible for monitoring compliance and advising the Board. The DPO can be contacted via info@stravica.uk

4.8 Breach

Any security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Full glossary provided in Appendix A.

5.0 Roles and Responsibilities

5.1 Board of Directors

a) Provide strategic oversight and approve this policy.
b) Ensure resources and training are adequate to support compliance.
c) Receive annual DPO and audit reports on data-protection performance.

5.2 Managing Director / Senior Information Risk Owner (SIRO)

a) Acts as executive owner for information-risk management.
b) Ensures risk registers and controls reflect data privacy obligations.
c) Chairs quarterly information-governance review meetings.

5.3 Data Protection Officer (DPO)

a) Monitors compliance with UK GDPR and DPA 2018.
b) Advises on DPIAs, legitimate-interest tests and consent issues.
c) Coordinates responses to SARs and breach notifications.
d) Serves as primary contact for the ICO and data subjects.
e) Reports independently to the Board.

5.4 Information Asset Owners (IAOs)

a) Department heads who maintain asset registers and data maps.
b) Complete DPIA screening for new systems and projects.
c) Ensure access controls and retention rules are applied.

5.5 Managers and Supervisors

a) Implement policy locally on sites and projects.
b) Ensure staff training completion and secure record-keeping.
c) Report any suspected breaches immediately to the DPO.

5.6 All Employees and Contractors

a) Handle personal data lawfully and confidentially.
b) Use data only for authorised business purposes.

c) Follow secure working practices (e.g. lock screens, encrypt emails).
d) Complete mandatory privacy training annually.
e) Report suspected breaches without delay.

6.0 Data Protection Principles (Article 5 UK GDPR)

6.1 Lawfulness, Fairness and Transparency

Processing must be carried out lawfully, fairly and in a transparent manner to data subjects. Stravica Ltd maintains clear Privacy Notices and lawful-basis records for each processing activity.

6.2 Purpose Limitation

Data is collected for specified, explicit, and legitimate purposes and not further processed incompatible with those purposes without new consent or lawful basis.

6.3 Data Minimisation

Only adequate and relevant data necessary for the intended purpose is collected. Forms and systems are periodically reviewed to remove superfluous fields.

6.4 Accuracy

Data must be accurate and kept up to date. Individuals may update their records via self-service or written request.

6.5 Storage Limitation

Data is retained only for as long as necessary and then securely deleted or anonymised (see Appendix D).

6.6 Integrity and Confidentiality

Appropriate technical and organisational measures protect data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

6.7 Accountability

The Company must be able to demonstrate compliance with these principles through documentation, training records, and auditable controls.

7.0 Lawful Bases for Processing (Article 6 UK GDPR)

7.1 Overview

All processing undertaken by Stravica Ltd must be supported by a lawful basis. Each department must document the basis used in the Record of Processing Activities (RoPA).

7.2 Lawful Bases

a) Contract: Processing necessary for the performance of a contract or to take steps before entering a contract (e.g. client service delivery, employment contracts).
b) Legal Obligation: Processing to comply with a legal requirement (e.g. HSE, taxation, audits).
c) Legitimate Interests: Processing necessary for legitimate business interests balanced against data-subject rights (e.g. CCTV security, fleet monitoring).
d) Consent: Freely given, specific, informed and unambiguous consent for defined purposes (e.g. marketing or optional data use).
e) Vital Interests: Processing necessary to protect life or serious health (e.g. emergency incident reporting on sites).
f) Public Task: Processing necessary for a task carried out in the public interest under contract with a public authority (where applicable).

7.3 Special Category Data (Article 9 UK GDPR)

Processing of sensitive data will occur only where a lawful basis and a specific Article 9 condition apply (e.g. employment, health and safety, or substantial public interest).

7.4 Criminal Convictions Data

Only processed when authorised by law and where necessary (e.g. Disclosure and Barring Service checks for security-cleared personnel). Additional safeguards apply under Schedule 1 DPA 2018.

8.0 Consent

8.1 Principles

Stravica Ltd recognises consent as one of six lawful bases under Article 6 UK GDPR and applies it only where no other lawful basis is more appropriate. Consent must be:

- Freely given – without coercion or detriment for refusal;
- Specific – clearly describing the purpose(s) of processing;
- Informed – supported by a concise privacy statement;
- Unambiguous – signified by a positive action; and
- Verifiable – recorded and stored as evidence.

8.2 Obtaining Consent

a) Consent will be captured using written or electronic statements separate from other terms and conditions.
b) Pre-ticked boxes, silence or inactivity shall never constitute consent.
c) Consent requests will specify data-controller identity, processing purposes, and the right to withdraw at any time.
d) All consent records will be logged in the Consent Register, maintained by the DPO.

8.3 Withdrawal of Consent

a) Data Subjects may withdraw consent at any time by contacting info@stravica.uk

b) Withdrawal will be acted upon within 5 working days.
c) Where withdrawal affects service delivery, this will be explained clearly to the individual.

8.4 Explicit Consent

Explicit consent is required for Special Category Data or automated decision-making. It must include a clear statement ("I consent to …"), dated and signed or digitally confirmed.

9.0 Transparency & Privacy Notices

9.1 Purpose

Transparency ensures individuals understand how and why their personal data is used. Stravica Ltd issues layered, plain-English Privacy Notices at the point of collection.

9.2 Requirements

Privacy Notices must identify:

a) Stravica Ltd as controller and contact details of the DPO;
b) Purposes and lawful bases for processing;
c) Categories of personal data processed;
d) Recipients or categories of recipients;
e) Retention period or criteria for determination;
f) Data-subject rights and how to exercise them;
g) Right to lodge a complaint with the ICO;
h) Transfer details outside the UK; and
i) Whether provision is statutory or contractual.

9.3 Communication Formats

- Employees – via intranet and HR system.
- Clients / Residents / Visitors – through contract packs or on-site signage.
- Website Users – through the online notice at stravica.uk (see Appendix E).

10.0 Data Minimisation, Accuracy & Retention

10.1 Data Minimisation

Each department must ensure data collected is:

a) Adequate – sufficient to achieve the purpose;
b) Relevant – directly related to the task;
c) Limited – not excessive.

10.2 Accuracy

a) Data will be checked at collection and periodically reviewed.
b) Out-of-date or inaccurate records will be rectified or erased without delay.
c) Staff must update their own details via HR systems and report changes.

10.3 Retention Principles

a) Personal Data must not be kept longer than necessary for its purpose.
b) All departments must follow the Retention Schedule (Appendix D).
c) Where no legal period exists, the default retention shall be 6 years post-activity.
d) Deletion must use secure methods (e.g. cross-cut shredding, certified IT wipe).

10.4 Review and Destruction Audits

IAOs will review their records annually and complete a Destruction Certificate for DPO retention.

11.0 Security (Integrity and Confidentiality)

11.1 General Obligation

Stravica Ltd must protect Personal Data using appropriate technical and organisational measures to ensure confidentiality, integrity and availability.

11.2 Technical Measures

a) Encryption – full-disk and email TLS encryption mandatory for sensitive data.
b) Access Control – unique user IDs, MFA for remote access, least-privilege principle.
c) Network Security – firewalling, segmentation, endpoint protection, vulnerability patching.
d) Back-up & Recovery – daily back-ups, encrypted storage, periodic restore tests.
e) Data Loss Prevention (DLP) – monitoring of large exports and external sharing.

11.3 Organisational Measures

a) Confidentiality agreements for employees and suppliers.
b) Secure disposal of paper and IT media.
c) Physical controls – ID badges, CCTV, locked cabinets, clean-desk policy.
d) Visitor supervision on site.
e) Third-party processors audited annually for ISO 27001 or equivalent standards.

11.4 Testing and Review

The IT Manager will perform bi-annual security assessments and report results to the SIRO and DPO.

12.0 Personal Data Breach Management

12.1 Definition

A Personal Data Breach is any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

12.2 Immediate Action

a) Anyone discovering a breach must report it immediately to their manager and the DPO (via info@stravica.uk) subject "BREACH – URGENT").
b) Do not delete evidence or attempt independent investigation.
c) Contain further exposure (e.g. disconnect device from network).

12.3 Assessment & Notification

a) The DPO will risk-assess each incident within 24 hours.
b) If risk to rights and freedoms is likely, the DPO will notify the ICO within 72 hours of awareness.
c) If risk is high, affected data subjects will be notified without undue delay.

12.4 Record-Keeping & Lessons Learned

All breaches will be recorded in the Breach Register (Appendix C). Post-incident reviews will identify root causes and corrective actions.

13.0 Data Subject Rights (Articles 12–23 UK GDPR)

13.1 Summary of Rights
a) Right to be informed;
b) Right of access (SAR);
c) Right to rectification;
d) Right to erasure ("right to be forgotten");
e) Right to restrict processing;
f) Right to data portability;
g) Right to object (including direct marketing);
h) Rights related to automated decision-making and profiling.

13.2 Handling Requests

a) Requests must be sent to info@stravica.uklabelled “SAR – [Name]”.

b) Identity verification is mandatory before processing.

c) Responses within one month of receipt; extension of two months permitted for complex cases with prior notification.

d) No fee unless manifestly unfounded or excessive.

e) DPO to maintain SAR Log and template (Appendix B).

13.3 Automated Decisions

Stravica Ltd does not use fully automated decision-making that produces legal effects without human involvement. Any future use requires explicit consent and DPO approval.

14.0 Data Sharing & Processors

14.1 Internal Sharing

Data may only be shared internally on a need-to-know basis and for legitimate business purposes. Email sharing must use secure channels and minimal fields.

14.2 Third-Party Processors

a) Must sign contracts containing Article 28 UK GDPR clauses.

b) May not appoint sub-processors without written authorisation.

c) Must report breaches to Stravica Ltd without undue delay.

d) Must delete or return data after contract completion.

14.3 Joint Controllers

Where Stravica Ltd acts with another organisation as joint controller, a documented arrangement shall define responsibilities and identify the contact for data subjects.

14.4 Law-Enforcement or Regulatory Disclosures

Personal Data may be disclosed only when legally required and authorised (e.g. court order, police investigation). All such requests must be verified and logged by the DPO.

15.0 International Transfers

15.1 Principle

Personal Data shall not be transferred outside the UK unless appropriate safeguards exist to maintain protection equivalent to UK standards.

15.2 Approved Mechanisms

a) Adequacy Regulations (approved countries).
b) UK International Data Transfer Agreement (IDTA).
c) UK Addendum to EU Standard Contractual Clauses.
d) Binding Corporate Rules (where applicable).

15.3 Procedure

a) DPO approval required before any international transfer.
b) Conduct Transfer Risk Assessment (TRA) to document lawfulness and risk controls.
c) Maintain records of transfer mechanisms and destination locations within RoPA.
d) Transfers to third-party cloud providers outside the UK are permitted only if they have adequacy status or standard contractual protections.

16.0 Direct Marketing, Cookies and PECR

16.1 Overview

The Privacy and Electronic Communications Regulations (PECR 2003, as amended) apply to electronic marketing, cookies and similar technologies. Stravica Ltd follows PECR and ICO guidance to ensure marketing activities are lawful and respect individual rights.

16.2 Direct Marketing Rules

a) Marketing emails, texts or calls will only be sent with valid consent or a “soft opt-in” where lawful.
b) Every message will include a clear unsubscribe mechanism and our contact details.
c) Opt-out requests must be actioned within five working days and recorded in the suppression list.
d) Postal marketing will honour Mail Preference Service (MPS) lists.

e) Marketing to corporate subscribers will follow PECR and UK GDPR principles of fairness and transparency.

16.3 Cookies and Tracking

a) Non-essential cookies (e.g. analytics or marketing) require opt-in consent.
b) Our cookie banner at stravica.uk clearly states purposes and links to the Cookie Policy.
c) Consent records are stored and renewed every 12 months.
d) Users can change preferences or delete cookies via browser settings.

17.0 Privacy by Design and Data Protection Impact Assessments (DPIA)

17.1 Principle

Stravica Ltd incorporates data protection from the earliest stages of any project, system or process design. This is mandatory for all new technologies or large-scale processing activities.

17.2 When to Conduct a DPIA

A DPIA is required where processing:
a) Involves systematic monitoring (e.g. CCTV, vehicle telematics);
b) Processes special category or criminal-convictions data on a large scale;
c) Uses new technology or profiling; or
d) May impact vulnerable individuals or result in high risk to rights and freedoms.

17.3 Process

1. Identify need and complete screening form (Appendix G).
2. Describe processing, scope, purpose and data flows.
3. Assess necessity, proportionality and risk.
4. Identify mitigations and residual risk.
5. Obtain DPO review and sign-off before implementation.
6. Record outcome in the RoPA.

17.4 Consultation

If a DPIA identifies unmitigated high risk, the DPO will consult the ICO before processing begins.

18.0 Training, Awareness and Audit

18.1 Training Requirements

a) All personnel must complete data-protection induction training within one month of start.

b) Annual refresher training is mandatory.

c) Specialist training is provided for managers, IAOs, HR, IT and procurement roles.

d) Completion records are retained for six years.

18.2 Awareness

The DPO circulates quarterly briefings highlighting legislative updates, breach trends and lessons learned. Awareness posters and intranet alerts reinforce good practice on sites and in offices.

18.3 Audit Programme

a) The DPO and SIRO conduct annual compliance audits of key processes (e.g. recruitment, CCTV, supplier management).

b) Findings and recommendations are reported to the Board.

c) Corrective actions are tracked to closure within 90 days.

19.0 Records of Processing and Accountability

19.1 Record of Processing Activities (RoPA)

Each business area maintains a RoPA listing: purpose, lawful basis, data types, recipients, retention and security controls. The DPO maintains the master register.

19.2 Evidence of Compliance

Evidence includes DPIAs, LIAs, training records, breach logs, audit reports, processor contracts and policy approvals. All evidence is retained for audit purposes and to demonstrate accountability.

20.0 Policy Governance, Review and Version Control

20.1 Ownership

The Board owns this policy. The DPO maintains it on behalf of the SIRO and reports annually to the Board on effectiveness.

20.2 Review Cycle

This policy will be reviewed every 24 months or earlier following legislative change, ICO guidance updates or material business change.

20.3 Approval Record

Version	Date	Change Summary	Approved By
1.0	23 Oct 2025	Initial release aligned to UK GDPR and PECR; includes website notice and retention schedule.	Managing Director

Appendices

Appendix A – Glossary of Key Terms

(Full definitions: UK GDPR Art. 4)
Personal Data, Special Category Data, Processing, Controller, Processor, DPO, Data Subject, RoPA, DPIA, PECR, IDTA, Pseudonymisation, Anonymisation, SAR.

Appendix B – Subject Access Request (SAR) Form and Workflow

Process:

1. Email info@stravica.uk DPO logs request and verifies ID.
2. Locate data across systems.
3. Redact third-party and legally exempt content.
4. Respond within 30 days (extend by 60 for complex cases).
5. Log closure in SAR register.
6. Form Fields: Full name, relationship to Stravica, data requested, date range, preferred format, representative (if any).

Appendix C – Personal Data Breach Report Form

Field	Description
Reporter/Date	Name and time incident identified
Incident Type	Loss, unauthorised access, disclosure etc.
Data Categories	Personal, Special Category, Criminal
Risk Assessment	Likelihood and severity
Containment	Immediate actions taken
ICO Notification	Yes/No + timestamp
Data Subject Notified	Yes/No + method
Corrective Actions	Follow-up and lessons learned

Appendix D – Baseline Retention Schedule (Extract)

Record Type	Retention Period	Notes
Employee Records	6 years after termination	Statutory Limitation Act
Recruitment Data	6 months after decision	Legitimate Interest
Payroll / Tax	6 years	HMRC requirement
	3 years (40 yrs for exposure)	RIDDOR/ COSHH
CCTV Footage	30 days (default)	Review if incident
Client Contracts / Tenders	6 years post completion	CCS audit trail
Visitor Logs	12 months	Security purposes
Marketing Consent Logs	Active + 2 years	Audit requirement

Appendix E – Website Privacy Notice (stravica.uk)

Last Updated: 23 October 2025
Controller: Stravica Ltd, info@stravica.uk

We collect contact, usage and recruitment data to respond to enquiries, manage contracts and improve services. Processing bases: contract, legitimate interest, consent, legal obligation.
We do not sell data. Transfers outside the UK use IDTA or adequacy decisions. Retention periods per Appendix D. Rights of access, rectification, erasure, restriction, objection, and portability apply. Contact the DPO via info@stravica.uk

Appendix F – Supplier / Processor Clauses (Excerpt)

1. Processor acts only on documented instructions.
2. Ensures confidentiality and security measures.
3. Assists with SARs and DPIAs.
4. Notifies breaches without delay.
5. Deletes/returns data on contract end.
6. Permits audits and sub-processor control.

Appendix G – DPIA Screening Checklist

- Purpose of processing and lawful basis.
- Categories of data and subjects.
- Scale and sensitivity.
- Potential impact on rights.
- Proposed safeguards and security.
- DPO review and approval sign-off.

Appendix H – Secure Configuration and Access Control Baseline

- Role-based access control (RBAC) and MFA for remote systems.
- Encryption of portable devices and back-ups.
- Quarterly user access recertification.
- Automatic account revocation within 24 hours of exit.
- Patch management SLA ≤ 14 days critical.
- Secure disposal (CESG or equivalent standard).