STRAVICA

COMPANY POLICY | WATER HYGIENE & LEGIONELLA CONTROL

Data Protection & GDPR Policy

Trusted Access. Protected Data. Accountable Delivery.

Stravica Ltd | Company No. 16756638
20-22 Wenlock Road, London N1 7GU
www.stravica.uk | info@stravica.uk

Version 1.0
Issued 24 October 2026
Next Review October 2027

Document Control

Item	Detail
Document Title	Data Protection & GDPR Policy - Water Hygiene & Legionella Control Services
Organisation	Stravica Ltd (Company No. 16756638)
Registered Address	20-22 Wenlock Road, London N1 7GU
ICO Registration	ZC189105
Document Reference	STR-POL-DP-001
Version	1.0 (supersedes the Data Protection & GDPR Policy issued 23 October 2025)
Issue Date	24 October 2026
Next Scheduled Review	October 2027, or earlier following a personal data breach, change in legislation or ICO guidance, or a material change to processing
Policy Owner	Adeola Olanrewaju, Director and Data Protection Lead
Approved By	Adeola Olanrewaju, Director, on behalf of the Board of Stravica Ltd
Data Protection Contact	info@stravica.uk (subject line "Data Protection") or by post to the registered address
Classification	Public

Revision History

Version	Date	Summary Of Change	Approved By
1.0	24 Oct 2026	Full rewrite for Stravica Ltd's specialist water hygiene and Legionella control services. Clarifies controller and processor roles on client contracts, governs delivery partners as sub-processors, and adds controls for resident, vulnerability, access, photographic, sampling, outbreak and sensor data. Updates the legal framework for the Data (Use and Access) Act 2025, adds a data protection complaints procedure, an Appropriate Policy Document and a water hygiene retention schedule, and replaces the DPO designation with a Data Protection Lead.	A. Olanrewaju, Director

Related Stravica Policies

This policy should be read alongside the Health & Safety Policy (STR-POL-HS-001), the Environmental Policy (STR-POL-ENV-001), the Modern Slavery & Human Trafficking Policy (STR-POL-MS-001), the Equality & Diversity Policy and the Anti-Bribery & Corruption Policy.

Contents

1. Introduction And Purpose 5
2. Scope 6
3. Legal And Regulatory Framework 6
4. Definitions 7
5. Statement Of Intent 7
6. Controller And Processor Roles 8
7. Governance And Responsibilities 8
8. Data Protection Principles 9
9. Lawful Bases And Special Category Data 10
10. Personal Data In Water Hygiene Delivery 11
11. Delivery Partners And Other Processors 12
12. Information Security 12
13. Personal Data Breach Management 13
14. Individuals' Rights And Complaints 14
15. Retention And Secure Disposal 14
16. Privacy By Design And DPIAs 15
17. International Transfers 16
18. Marketing, Website And Cookies 16
19. Freedom Of Information And Commercial Confidentiality 16
20. Training And Awareness 16
21. Monitoring, KPIs And Review 17
Appendix A - Summary Record Of Processing Activities 18
Appendix B - Breach Response Procedure 18
Appendix C - Rights Request Procedure 19
Appendix D - Appropriate Policy Document 19
Appendix E - Delivery Partner Data Protection Checklist 20

Appendix F - Field Data Rules For Operatives 20

Appendix G - Glossary 21

1. Introduction And Purpose

1.1 About Stravica Ltd

Stravica Ltd is a UK prime contractor specialising in water hygiene and Legionella control. We deliver Legionella risk assessments, water hygiene monitoring, Legionella and water sampling, water tank cleaning and disinfection, water system remedial works and planned water hygiene maintenance. Our clients include housing providers, healthcare and care settings, education establishments, local authorities, transport operators and commercial estates. Operational delivery is carried out by vetted specialist delivery partners working under Stravica's contract management and assurance.

1.2 Purpose

This policy sets out how Stravica Ltd complies with UK data protection law and protects the personal data entrusted to it by clients, residents, building users, delivery partners, staff and others. It defines responsibilities, controls and procedures for every stage of the data lifecycle, from collection through use, sharing and storage to secure deletion.

1.3 Why Water Hygiene Data Needs Particular Care

Water hygiene contracts give Stravica and its delivery partners access to information that is often sensitive and always confidential:

- Names, addresses and contact details of residents whose homes we visit.
- Vulnerability information, such as residents who are elderly, immunocompromised or disabled, which clients share so that we can plan visits and protect people at higher risk from Legionella. Much of this is special category health data.
- Access information, including key safe codes, key holding arrangements and plant room access, which could cause serious harm if misused.
- Photographs taken inside homes, healthcare buildings and schools.
- Sampling and monitoring results linked to specific flats, wards or rooms.
- In rare cases, information about cases of Legionnaires' disease connected with a site.
- Operative records, including right to work, DBS checks, training and health surveillance.

Clients rely on Stravica to handle this information with the same care they would apply themselves. This policy is built around that responsibility.

1.4 Objectives

- Process all personal data lawfully, fairly and transparently, and only for specified purposes.
- Act strictly on client instructions wherever Stravica processes data on a client's behalf.
- Hold delivery partners to the same standards through binding sub-processor terms.
- Protect personal data with security measures appropriate to the risk, especially vulnerability and access data.
- Detect, contain and report personal data breaches promptly.
- Respect and respond to individuals' rights within the legal timescales.
- Keep data only as long as necessary, and dispose of it securely.

2. Scope

- All personal data processed by or on behalf of Stravica Ltd, in any format: electronic, paper, photographic or verbal.
- All directors, staff, agency workers and consultants of Stravica Ltd.
- All delivery partners, laboratories, software providers and other suppliers that process personal data in connection with Stravica contracts.
- All systems used for Stravica business, including email, cloud storage, job management and digital logbook systems, mobile devices and the stravica.uk website.
- All Stravica contracts across England, Scotland and Wales.

Failure to comply with this policy may result in disciplinary action for Stravica personnel, termination of contract for delivery partners and suppliers, and regulatory action by the Information Commissioner.

3. Legal And Regulatory Framework

Legislation Or Guidance	Relevance
UK General Data Protection Regulation (UK GDPR)	Core principles, lawful bases, individuals' rights, controller and processor duties, security and breach notification.
Data Protection Act 2018	Supplements UK GDPR, including the conditions in Schedule 1 for special category and criminal offence data and the requirement for an Appropriate Policy Document.
Data (Use and Access) Act 2025	Amends UK GDPR, the Data Protection Act 2018 and PECR. Changes include clarifying that searches in response to subject access requests must be reasonable and proportionate, introducing a requirement for controllers to handle data protection complaints, recognising certain legitimate interests and raising PECR penalties. Stravica applies each provision as it comes into force.
Privacy and Electronic Communications Regulations 2003 (PECR)	Electronic marketing, cookies and similar technologies.
Computer Misuse Act 1990	Unauthorised access to computer systems and data.
Freedom of Information Act 2000 and Freedom of Information (Scotland) Act 2002	Public sector clients may receive requests for information about their contracts, including information supplied by Stravica.
Human Rights Act 1998	Article 8: the right to respect for private and family life, home and correspondence, which is directly engaged when entering people's homes.
ICO guidance and codes of practice	Including guidance on controllers and processors, security, breach reporting, subject access and employment practices.

3.1 Registration

Stravica Ltd is registered with the Information Commissioner's Office under registration number ZC189105 and pays the data protection fee annually.

4. Definitions

Term	Meaning
Personal data	Any information relating to an identified or identifiable living individual, such as a name, address, telephone number, photograph or a flat number linked to a sampling result.
Special category data	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data, or data concerning a person's sex life or sexual orientation. Vulnerability information about residents is often health data.
Criminal offence data	Data about criminal convictions and offences, including the results of DBS and PVG checks.
Controller	The organisation that decides the purposes and means of processing.
Processor	An organisation that processes personal data on behalf of, and on the instructions of, a controller.
Sub-processor	An organisation engaged by a processor to carry out processing for the controller. On client contracts, Stravica's delivery partners are normally sub-processors.
Processing	Any operation on personal data, including collecting, recording, storing, using, sharing and deleting it.
Personal data breach	A security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Data subject	The individual to whom personal data relates.
DPIA	Data Protection Impact Assessment, a process for identifying and minimising data protection risks in high-risk processing.

5. Statement Of Intent

Stravica Ltd is committed to protecting the privacy of every person whose data we handle. We recognise that entering homes, hospitals and schools to protect people from water-borne disease is a position of trust. We will respect that trust by handling personal data lawfully, securely and only for the purposes for which it was entrusted to us.

Stravica Ltd will:

- Comply with UK GDPR, the Data Protection Act 2018, PECR and all related legislation.
- Act only on documented client instructions when processing data on a client's behalf.
- Collect only the minimum personal data needed for each task.
- Protect vulnerability, access and health information with enhanced controls.
- Bind every delivery partner and supplier that handles personal data to written data protection terms.
- Notify clients and, where required, the ICO and affected individuals of personal data breaches within the legal and contractual timescales.
- Respond to individuals' rights requests promptly and fairly.
- Train everyone working on Stravica contracts in data protection.
- Keep records that demonstrate our compliance.

Policy Approval

- Signed on behalf of Stravica Ltd by Adeola Olanrewaju, Director.
- Date of approval: 24 October 2026.
- This statement is issued to every delivery partner and published at www.stravica.uk.

6. Controller And Processor Roles

Understanding who is the controller is essential, because it decides who sets the rules for each piece of data. Stravica's roles are as follows.

Data	Stravica's Role	What This Means
Resident, occupant, patient and building user data received from or collected for a client	Processor (delivery partners are sub-processors)	Processed only on the client's documented instructions and under the contract's data processing terms. The client decides purposes, retention and responses to rights requests.
Water hygiene records containing personal data, such as logbooks, risk assessments and sample results linked to flats	Processor	Records belong to the client and are returned or deleted at the end of the contract as the client instructs.
Stravica's own staff and applicants	Controller	Stravica decides purposes and lawful bases, and is responsible for privacy information and rights requests.
Delivery partner contacts and named operative information held for vetting, ID and competence checks	Controller	Held to manage the supply chain, safety, safeguarding and contract compliance.
Client and prospect contacts for contract management and bidding	Controller	Held for business relationship and contract management purposes.
Website visitors and enquirers	Controller	Governed by the stravica.uk privacy notice and PECR.

Where a contract does not clearly set out the parties' roles, Stravica will agree them in writing with the client before processing begins. If Stravica ever decides the purposes of processing client data for itself, it would become a controller of that data. Stravica will therefore never use client data for its own purposes, such as marketing.

7. Governance And Responsibilities

7.1 Data Protection Officer Status

Stravica Ltd is not a public authority, and its core activities do not consist of large-scale regular and systematic monitoring or large-scale processing of special category or criminal offence data. It is therefore not required to appoint a Data Protection Officer under Article 37 of UK GDPR. Stravica has instead designated the Director as Data Protection Lead, with the responsibilities set out below. This decision is reviewed annually as the business grows.

Role	Responsibilities
Director (Data Protection Lead)	Accountable for data protection compliance. Approves this policy. Maintains the record of processing activities. Approves DPIAs. Manages breaches and ICO notifications. Handles rights requests and complaints. Approves sub-processors and data processing terms. Acts as contact for the ICO, clients and individuals.
Compliance & Procurement Administration	Maintains processing records, the breach log, the rights request log and supplier data protection evidence. Applies retention rules. Supports training records.
Delivery Partner Contract Managers	Ensure their organisation and operatives comply with sub-processor terms and the field data rules in Appendix F. Report breaches to Stravica immediately.
Operatives and Risk Assessors	Collect and record only what is needed. Protect devices and paperwork. Never share access codes or resident information. Report incidents immediately.
All Persons	Handle personal data in line with this policy, complete training and report concerns.

8. Data Protection Principles

Stravica applies the seven principles in Article 5 of UK GDPR to all processing.

Principle	How Stravica Applies It In Water Hygiene Work
Lawfulness, fairness and transparency	A documented lawful basis for every activity; privacy information provided to staff and through clients to residents; resident notification letters explain who will visit and why.
Purpose limitation	Resident and site data are used only to deliver the contracted water hygiene services, and never for marketing or unrelated purposes.
Data minimisation	Operatives receive only the data needed for each visit. Vulnerability details are limited to what affects how the visit is carried out. Photographs show assets, not people or personal belongings.
Accuracy	Access failures and incorrect contact details are reported to the client so that records can be corrected. Monitoring records reflect actual readings.
Storage limitation	Data is kept only for the periods in Section 15, and client data is returned or deleted at contract end.
Integrity and confidentiality	Security measures in Section 12, with enhanced controls for vulnerability and access data.
Accountability	Records of processing, DPIAs, contracts, training records, breach and request logs, and annual review.

9. Lawful Bases And Special Category Data

9.1 Processing Where Stravica Is Controller

Processing Activity	Lawful Basis (Article 6)	Additional Condition
Employment and payroll of Stravica staff	Contract; legal obligation	Health data: Article 9(2)(b) and Schedule 1 paragraph 1 DPA 2018 (employment)
Right to work checks	Legal obligation	Not applicable
DBS and PVG checks for operatives working in sensitive premises	Legitimate interests; legal obligation where the client's regulated setting requires it	Criminal offence data: Schedule 1 DPA 2018 conditions, covered by the Appropriate Policy Document (Appendix D)
Operative competence, training and ID records	Legitimate interests (safe, competent delivery); legal obligation (health and safety)	Not applicable
Health surveillance and RPE face-fit records	Legal obligation (COSHH and health and safety)	Article 9(2)(b) and Schedule 1 paragraph 1 (employment, health and safety)
Client and supplier business contacts	Legitimate interests	Not applicable
Website enquiries	Legitimate interests; consent for non-essential cookies	Not applicable

9.2 Processing On Behalf Of Clients

When Stravica processes data as a processor, the client as controller determines and is responsible for the lawful basis and any Article 9 condition. This is typically public task or legal obligation for public bodies, or legitimate interests for other clients, combined with the condition for health and social care, public health or substantial public interest where vulnerability data is involved. Stravica processes this data only as instructed and will tell the client immediately if it believes an instruction would breach data protection law.

9.3 Consent

Stravica does not rely on consent for core service delivery, because people cannot freely refuse processing that is needed to keep their water safe. Consent is used only for optional activities, such as marketing communications, non-essential website cookies, or the use of a photograph or case study that identifies an individual. Consent is recorded and can be withdrawn at any time by emailing info@stravica.uk.

10. Personal Data In Water Hygiene Delivery

This section sets the standards for the specific types of personal data encountered in water hygiene work.

Data Type	Risk	Required Controls
Resident names, addresses and contact details	Misuse; unwanted contact; disclosure to others	Shared with operatives only for the visits allocated to them; held in secure systems, not on personal phones; not used after the visit except as the contract requires
Vulnerability information (for example immunocompromised, disabled, elderly, hearing impaired)	Special category data; distress or discrimination if disclosed	Shared only as a short operational flag, such as "requires alternative water supply during works" or "allow extra time to answer", not as a diagnosis; restricted access; never written on paper visit sheets left in vehicles
Key safe codes, key holding and access arrangements	Burglary or harm to vulnerable residents	Never written down, texted to personal numbers or stored in shared documents. Provided through secure systems for each visit only. Keys signed in and out. Any suspected compromise is reported immediately as a breach.
Photographs inside homes, wards and schools	Capturing people, children, patients, personal belongings or documents	Photograph assets only; check the frame before taking; never photograph people, children, patients, screens or personal papers; company devices only; delete any accidental capture immediately
Sampling and monitoring results linked to flats or rooms	Disclosure of property-level information	Reported to the client only; shared with laboratories using site and sample point references rather than residents' names
Legionnaires' disease case information	Highly sensitive health data	Received only where necessary to support an investigation; restricted to the Data Protection Lead and named investigators; never included in routine reports
Access failure evidence (calling cards, photographs of doors)	Recording a person's home or movements	Photograph the door number only, never people or the interior; retain only as long as needed to evidence the visit
Remote temperature sensor data	Usage patterns in homes may reveal occupancy	DPIA before deployment in residential properties; data limited to water system parameters; access restricted
Telephone and email contact with residents	Social engineering; disclosure	Verify identity before discussing appointments; never disclose information about other residents

Field Rule

If you would not want it read out in the street, it does not go on paper, in a text message or on a personal phone. Use the approved system, take only what you need, and report anything that goes missing straight away.

11. Delivery Partners And Other Processors

11.1 Sub-Processor Requirements

Where Stravica is a processor for a client, its delivery partners are sub-processors. Stravica will:

- Obtain the client's prior written authorisation, specific or general, before engaging a delivery partner as a sub-processor, and inform the client of any intended changes.
- Put in place a written contract with each delivery partner that imposes the same data protection obligations as the client contract, including the requirements of Article 28(3) of UK GDPR.
- Remain fully liable to the client for the delivery partner's compliance.

11.2 Minimum Contract Terms

1. Process personal data only on documented instructions.
2. Ensure that everyone who handles the data is bound by confidentiality.
3. Implement appropriate technical and organisational security measures.
4. Not engage further sub-processors without Stravica's prior written authorisation.
5. Assist Stravica and the client in responding to individuals' rights requests.
6. Notify Stravica of any personal data breach without undue delay, and in any case within 24 hours of becoming aware of it.
7. Assist with DPIAs and consultations with the ICO.
8. Delete or return all personal data at the end of the contract, as instructed.
9. Make available all information needed to demonstrate compliance, and allow audits and inspections.
10. Not transfer personal data outside the UK without authorisation and appropriate safeguards.

11.3 Other Processors

Laboratories, software and cloud providers, and any other supplier processing personal data for Stravica are assessed for security and compliance before use and bound by written Article 28 terms. Laboratories receive sample references rather than residents' personal data wherever possible.

12. Information Security

12.1 Technical Measures

- Stravica maintains Cyber Essentials certification, renewed annually, and requires delivery partners handling client data to hold Cyber Essentials or an equivalent standard.
- Business data is held in reputable cloud services with encryption in transit and at rest.
- Multi-factor authentication is enabled on email, cloud storage and job management systems.
- Access follows the principle of least privilege and is removed promptly when someone leaves or changes role.
- Devices used for Stravica work are password or biometric protected, encrypted, kept up to date and able to be wiped remotely.
- Personal data is sent by secure, access-controlled sharing links or encrypted email, not as open attachments to wider distribution lists.

- Data is backed up and restoration is tested.

12.2 Organisational Measures

- Confidentiality obligations are included in staff contracts and delivery partner agreements.
- Paper records are avoided. Any unavoidable paperwork is kept out of sight, never left in an unattended vehicle overnight, and returned or shredded promptly.
- Keys are signed in and out and stored securely, with key tags that carry no address.
- Screens are locked when unattended, and devices are not used in a way that lets others see personal data.
- Visitors and unknown callers are not given information about residents, sites or access arrangements.

12.3 Phishing And Social Engineering

Requests to change bank details, share access codes or send resident data are verified independently by telephone using a known number before any action is taken. Suspicious emails are reported, not opened.

13. Personal Data Breach Management

13.1 Reporting

Anyone who discovers or suspects a personal data breach must report it immediately to the Data Protection Lead by telephone and to info@stravica.uk with the subject line "Data Breach - Urgent". Examples include a lost phone or tablet, an email sent to the wrong person, a lost key or a compromised key safe code, a stolen visit sheet, or unauthorised access to a system.

13.2 Response

Step	Action	Timescale
Contain	Recover data, remotely wipe devices, revoke access, recall emails, change compromised codes in liaison with the client	Immediately
Assess	Establish what data, how many people, the sensitivity and the likely consequences	Within 24 hours
Notify client (where Stravica is processor)	Inform the controller with all available details, then provide updates	Without undue delay, and within any contractual deadline (normally within 24 hours)
Notify ICO (where Stravica is controller)	Report if the breach is likely to result in a risk to individuals' rights and freedoms	Within 72 hours of becoming aware
Inform individuals (where Stravica is controller)	Tell affected people directly if the risk to them is high, with advice on protecting themselves	Without undue delay
Record and learn	Log every breach, whether or not reported, with facts, effects and remedial action; review root causes	Within 14 days

Where access codes or keys may be compromised, the client is told immediately by telephone so that codes can be changed and vulnerable residents protected without delay.

14. Individuals' Rights And Complaints

14.1 Rights

Individuals have the right to be informed, the right of access, and the rights to rectification, erasure, restriction of processing, data portability and to object, together with rights relating to automated decision-making. Stravica does not make decisions based solely on automated processing that have legal or similarly significant effects on individuals.

14.2 Requests Where Stravica Is Controller

- Requests can be made in any form, but should preferably be sent to info@stravica.uk with the subject line "Data Request".
- Identity is verified proportionately before any information is disclosed.
- Responses are provided within one month of receipt. This may be extended by up to two further months for complex or numerous requests, in which case the individual is told within the first month.
- Where clarification is genuinely needed, the response time is paused until it is received, as permitted by law.
- Searches are reasonable and proportionate, and no fee is charged unless a request is manifestly unfounded or excessive.
- Third-party information is redacted where required.

14.3 Requests Where Stravica Is Processor

Requests relating to client data, such as a resident asking for records about their home, are forwarded to the client within two working days, and Stravica assists the client in responding. Stravica will not respond directly unless the client authorises it.

14.4 Data Protection Complaints

Anyone can complain to Stravica about how their personal data has been handled by emailing info@stravica.uk with the subject line "Data Protection Complaint". Stravica acknowledges complaints within 30 days, investigates them without undue delay, and informs the complainant of the outcome. Individuals also have the right to complain to the Information Commissioner's Office at ico.org.uk or on 0303 123 1113.

15. Retention And Secure Disposal

Personal data is kept only as long as necessary. Where a client contract specifies retention, the client's requirements take precedence for client data. Stravica's default schedule is set out below.

Record	Retention	Basis
Water hygiene records containing personal data (logbooks, risk assessments, sampling and completion records)	Five years, or as the client instructs, then returned or deleted	ACoP L8 record requirements; client instructions
Resident contact and visit scheduling data	Duration of the contract, then returned or deleted as instructed	Contract delivery

Record	Retention	Basis
Vulnerability flags	Only while relevant to current visits; refreshed from the client before each programme	Data minimisation
Access codes and key arrangements	Only for the visit; not stored in Stravica records	Security
Access failure photographs	Until the visit is evidenced and accepted by the client, and no longer than 12 months	Contract evidence
Staff personnel and payroll records	Six years after employment ends	Limitation periods; tax law
Right to work checks	Duration of employment plus two years	Home Office requirements
DBS and PVG check outcomes	Record of the check and outcome only; certificates not retained beyond six months	DBS Code of Practice
Health surveillance records	40 years	COSHH Regulations
Unsuccessful applicant data	Six months after the decision	Defence of claims
Delivery partner vetting and operative competence records	Duration of engagement plus six years	Contract and safety compliance
Breach log, request log and complaint records	Six years	Accountability
Website enquiries that do not lead to business	Two years	Legitimate interests

Electronic data is deleted securely, including from shared drives and email folders. Devices are wiped to a recognised standard before disposal or reuse. Paper is cross-cut shredded or destroyed by a certified confidential waste contractor.

16. Privacy By Design And DPIAs

Data protection is considered at the start of every new contract, system and process. A Data Protection Impact Assessment is carried out before any processing likely to result in a high risk to individuals, including:

- Deploying remote temperature or water usage sensors in residential properties.
- Introducing a new job management, logbook or resident communication system that will hold vulnerability or access data.
- Processing large volumes of special category data, such as vulnerability registers across a whole housing stock.
- Any use of new technologies, such as AI tools, with personal data.

Each DPIA describes the processing, assesses necessity and proportionality, identifies risks and mitigations, and is approved by the Data Protection Lead. Where Stravica is a processor, it assists the client with the client's own DPIA. If a high risk cannot be mitigated, the ICO is consulted before processing begins.

17. International Transfers

Stravica's policy is to keep personal data within the UK wherever possible. Personal data is only transferred outside the UK where the transfer is authorised (by the client, where Stravica is processor) and is protected by UK adequacy regulations, the International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or another lawful mechanism, supported by a transfer risk assessment where required. Cloud and software providers are checked for data location before they are used.

18. Marketing, Website And Cookies

- Client and resident data obtained through contracts is never used for marketing.
- Business-to-business marketing to corporate contacts follows PECR and UK GDPR, identifies Stravica clearly and includes a simple way to opt out. Opt-outs are actioned within five working days.
- Marketing to individuals (sole traders and partnerships) is sent only with consent or under the soft opt-in.
- The stravica.uk website uses only cookies that are strictly necessary or otherwise permitted by PECR without consent. Any other cookies require prior opt-in consent through the cookie banner.
- The website privacy notice explains how enquiry data is used and how to exercise rights.

19. Freedom Of Information And Commercial Confidentiality

Public sector clients are subject to the Freedom of Information Act 2000 or the Freedom of Information (Scotland) Act 2002 and may receive requests for information about their contracts with Stravica. Stravica will assist clients in responding, will identify any information it considers commercially sensitive or exempt, and will ensure that personal data in contract records is protected from inappropriate disclosure. Stravica itself is not a public authority under these Acts.

20. Training And Awareness

Audience	Content	Frequency
All Stravica personnel	This policy; principles; breach reporting; rights requests; secure handling; phishing awareness	Induction and annually
Delivery partner operatives on Stravica contracts	Field data rules (Appendix F); photography; access codes and keys; devices; breach reporting	Contract induction and annual toolbox talk
Delivery partner contract managers	Sub-processor obligations; breach notification timescales; requests; retention	Induction and annually
Data Protection Lead	Legal updates, including the Data (Use and Access) Act 2025; ICO guidance; DPIAs; breach assessment	Annually

21. Monitoring, KPIs And Review

KPI	Target
Delivery partners with signed sub-processor terms before handling client data	100%
Client authorisation in place for every sub-processor	100%
Breaches reported to clients within the contractual timescale	100%
Reportable breaches notified to the ICO within 72 hours	100%
Rights requests answered within the statutory timescale	100%
Complaints acknowledged within 30 days	100%
Staff and operatives completing data protection training	100%
Client data returned or deleted at contract end with written confirmation	100%

The Data Protection Lead reviews breaches, requests, complaints and KPIs at least quarterly. This policy and the record of processing activities are reviewed annually and whenever legislation, guidance or processing changes significantly. Delivery partner data protection compliance is checked during Stravica audits.

Appendix A - Summary Record Of Processing Activities

Activity	Categories Of Data Subject	Categories Of Data	Recipients	Role
Water hygiene service delivery	Residents, occupants, building users	Contact details, address, access arrangements, vulnerability flags, photographs of assets	Client; delivery partners; laboratories (references only)	Processor
Outbreak support	Cases and contacts	Health data	Client; UKHSA, Public Health Scotland, Environmental Health	Processor
Supply chain management	Delivery partner staff	Names, ID photos, training, DBS outcomes, right to work assurance	Clients (named operative lists)	Controller
Employment	Staff and applicants	Contact, bank, pay, health, right to work, DBS	HMRC; pension provider; payroll provider	Controller
Business relationships and bidding	Client and supplier contacts	Names, roles, contact details	Internal only	Controller
Website	Visitors and enquirers	Enquiry details; necessary cookie data	Website host	Controller

Appendix B - Breach Response Procedure

1. Report immediately to the Data Protection Lead by telephone and to info@stravica.uk with the subject line "Data Breach - Urgent".
2. Contain: recover, recall, wipe, revoke or change codes as appropriate.
3. Record: what happened, when, what data, how many people, and actions taken so far.
4. Assess the risk to individuals, considering sensitivity (especially vulnerability, health and access data), volume, likely consequences and mitigation.
5. Where Stravica is processor, notify the client without undue delay and within the contractual deadline.
6. Where Stravica is controller, notify the ICO within 72 hours if there is a risk to individuals, and inform affected individuals if the risk is high.
7. Investigate root cause and agree corrective actions.
8. Log the breach and its outcome, and share lessons learned with delivery partners.

Appendix C - Rights Request Procedure

1. Log the request on receipt, with the date, requester and nature of the request.
2. Determine whether Stravica is controller or processor for the data concerned. If processor, forward the request to the client within two working days.
3. Verify identity proportionately.
4. Clarify the request if genuinely necessary, noting that the response time pauses while clarification is awaited.
5. Carry out reasonable and proportionate searches across email, cloud storage and systems.
6. Review and redact third-party data and exempt information.
7. Respond within one month, or explain any extension within the first month.
8. Record the outcome in the request log.

Appendix D - Appropriate Policy Document

This Appropriate Policy Document is required by Schedule 1 Part 4 of the Data Protection Act 2018. It covers Stravica's processing, as controller, of special category and criminal offence data under the Schedule 1 conditions.

Item	Content
Data processed	Health data of staff for employment, health surveillance and RPE face-fit purposes. Criminal offence data from DBS and PVG checks of operatives deployed in sensitive premises.
Conditions relied upon	Schedule 1 paragraph 1 (employment, social security and social protection). For criminal offence data, paragraph 1 (employment) and, where applicable, paragraph 18 (safeguarding of children and individuals at risk).
Lawfulness, fairness and transparency	Processing is necessary for the stated purposes and is explained in staff and operative privacy information.
Purpose limitation	Data is used only for employment, health and safety and safeguarding purposes.
Data minimisation	Only the outcome of DBS and PVG checks is recorded; certificates are not copied or retained beyond six months. Health records are limited to what the law requires.
Accuracy	Records are updated when circumstances change and corrected on request.
Storage limitation	Retention follows the schedule in Section 15.
Security	Access is restricted to the Data Protection Lead and authorised administration, with the controls in Section 12.
Review	This document is reviewed with this policy and retained for six months after the processing ends.

Appendix E - Delivery Partner Data Protection Checklist

Requirement	Evidence Required
ICO registration	Registration number verified on the ICO register
Data protection policy	Current, signed policy
Cyber security	Cyber Essentials certificate or equivalent
Devices	Confirmation that devices are encrypted, protected and remotely wipeable
Systems	Details of job management or logbook systems used, and where data is stored
Sub-processors	List of any further sub-processors, such as software providers
Training	Data protection training records for operatives
Breach procedure	Written procedure including notification to Stravica within 24 hours
Contract	Signed sub-processor terms meeting Section 11.2

Appendix F - Field Data Rules For Operatives

Do	Do Not
Use only the approved system or device for job and resident information	Store resident details, codes or photographs on a personal phone
Take only the information you need for today's visits	Print or write down visit lists unless there is no alternative
Photograph tanks, outlets, plant and labels only	Photograph people, children, patients, screens, documents or personal belongings
Check identity before discussing an appointment by phone	Tell anyone about another resident or their home
Sign keys in and out and keep them secure	Leave keys, paperwork or devices in an unattended vehicle overnight
Use sample point references on laboratory forms	Write residents' names on sample labels
Lock your device whenever you put it down	Share login details or codes with anyone
Report anything lost, sent to the wrong person or seen by others immediately	Wait to see whether a lost item turns up before reporting it

Appendix G - Glossary

Term	Meaning
Article 28	The UK GDPR article setting out the contract terms required between controllers and processors
DBS	Disclosure and Barring Service (England and Wales); PVG is the Protecting Vulnerable Groups scheme in Scotland
ICO	Information Commissioner's Office, the UK data protection regulator
IDTA	International Data Transfer Agreement
PECR	Privacy and Electronic Communications Regulations 2003
Record of processing activities	The record required by Article 30 of UK GDPR describing processing activities
Vulnerability flag	A short operational note shared by a client so that a visit can be adapted for a resident's needs

Stravica Ltd

- 20-22 Wenlock Road, London N1 7GU
- info@stravica.uk | www.stravica.uk
- Company No. 16756638 | ICO Registration ZC189105