Data Processing Agreement

This Data Processing Agreement ("Agreement") forms part of the contractual terms between Invisible Systems Ltd ("Processor", "we", "us", or "our") and our business customers ("Controller", "you" or "your") for the provision of our products and services.

This Agreement outlines how we process personal data on your behalf in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1. Definitions

- Personal Data: Any information relating to an identified or identifiable natural person.
- Processing: Any operation or set of operations performed on personal data (e.g. collection, use, storage).
- Sub processor: A third party engaged by the Processor to process personal data on behalf of the Controller.
- UK GDPR: The United Kingdom General Data Protection Regulation and applicable data protection laws.

2. Scope and Role of the Parties

- You act as the Controller, determining the purpose and legal basis of processing.
- We act as the Processor, processing personal data solely on your documented instructions.
- We will inform you if we believe any instruction infringes applicable data protection law.

3. Purpose and Nature of Processing

We process personal data solely to deliver our services, which include wireless monitoring, data analysis, alerts, reporting, and dashboard visualisation.

- Nature: Collection, storage, transmission, and reporting of sensor data and user access credentials.
- Purpose: To enable remote monitoring, reporting, and alerting services in line with your service agreement.

4. Categories of Data and Data Subjects

- Data subjects: May include your employees, contractors, or other individuals you authorise to use the services.
- Personal data: Name, job title, contact number, email address, login credentials, and IP address (as applicable).

We do not intentionally collect special category data unless explicitly agreed in writing.

5. Processor Obligations

We will:

- Process data lawfully, fairly, and transparently under your instructions.
- Ensure all staff handling data are subject to confidentiality obligations.
- Implement appropriate technical and organisational measures to ensure data security.
- Assist you with requests from data subjects.

- Notify you of any personal data breaches without undue delay.
- Maintain records of processing activities.
- Return or delete data at the end of the service term, unless retention is required by law.

6. Sub Processing

We may engage sub processors to support the delivery and operation of our services. All sub processors are subject to data protection obligations equivalent to those set out in this Agreement, including appropriate security, confidentiality, and data handling requirements.

Current sub processors may include (but are not limited to):

- Hosting Providers: Microsoft, Amazon Web Services (AWS)
- Ticketing Platforms: HubSpot, Formcrafts, JotForm
- Communications Providers: SendGrid, HubSpot, Microsoft, Essendex

A current list of sub processors is available on request. We will notify you in advance of any intended changes concerning the addition or replacement of sub processors. Objections must be raised in writing within 14 days of notice. We will work with you in good faith to address concerns or suggest alternative arrangements.

7. International Transfers

We do not transfer personal data outside the UK or EEA unless:

- It is to a jurisdiction with an adequacy decision, or
- We have appropriate safeguards in place (e.g. Standard Contractual Clauses or UK IDTA).

8. Data Subject Rights

Where applicable, we will assist you in responding to data subject requests, including:

- Access
- Rectification
- Erasure
- Restriction
- Objection
- Portability

You are responsible for handling requests unless explicitly delegated to us under a separate agreement.

9. Data Security

We implement and maintain:

- Encryption of data at rest and in transit
- Access controls and authentication
- Regular data protection training
- Physical and logical security measures

We continuously assess and improve these measures in line with industry standards.

10. Breach Notification

In the event of a data breach, we will:

- Notify you without undue delay
- Provide details of the breach and its likely impact
- Cooperate with you in any investigation or remediation

11. **Termination and Deletion**

Upon termination of our services:

- We will delete or return all personal data, unless legal obligations require retention.
- Deletion will be performed securely in accordance with industry standards.

We retain personal data only for as long as necessary to fulfil the purpose for which it was collected, or to comply with legal, contractual, or regulatory obligations. Retention periods are reviewed regularly.

12. Legal and Operational Safeguards

- We do not engage in automated decision-making or profiling as defined under UK GDPR Article 22.
- Nothing in this Agreement shall be construed as establishing joint controller status between the parties.
- Each party shall be liable for its own acts or omissions in relation to personal data processing and indemnify the other against losses resulting from breach of this Agreement.
- You may audit our compliance with this Agreement once per year with reasonable notice.
- Audits must not disrupt our operations and may be fulfilled through provision of security documentation or certifications where appropriate.

13. General Provisions

- This Agreement is governed by the laws of England and Wales.
- Any disputes shall be subject to the exclusive jurisdiction of the courts of England and Wales.
- This Agreement supplements your existing contract with Invisible Systems Ltd and takes precedence in the event of a conflict regarding data protection.

Contact

Data Protection Officer
Mikiel Hibbard
Email: mikiel@invisible-systems.com