AmbuNet

STREAMLINING AMBULANCE OPERATIONS

DATA PROCESSING AGREEMENT

Version 1.2

1st May 2026

Data Processing Agreement

This Data Processing Agreement ("**DPA**") forms part of the Terms of Use between:

- Care Nav Ltd (trading as **AmbuNet**) ("**Processor**"); and
- Any individual or organisation using the AmbuNet platform ("**Controller**")

(together, the "**Parties**").

Application of this DPA

This DPA applies automatically to all customers who access or use the AmbuNet platform and process personal data through it.

By accepting the Terms of Use, the Controller agrees to be bound by this DPA.

1. Definitions

1.1 In this Agreement:

- "**Applicable Data Protection Law**" means the General Data Protection Regulation, the UK GDPR, the Data Protection Act 2018, and any applicable implementing or supplementary legislation.
- "**Controller**" means the entity determining the purposes and means of processing Personal Data
- "**Processor**" means the entity processing Personal Data on behalf of the Controller
- "**Personal Data**" means any information relating to an identified or identifiable natural person
- "**Special Category Data**" includes data concerning health, racial or ethnic origin, or other sensitive data
- "**Data Subject**" means an identified or identifiable individual
- "**Sub-Processor**" means any third party engaged by the Processor to process Personal Data
- "**Personal Data Breach**" means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data

2. Subject Matter and Scope

2.1 This agreement governs the Processing of Personal Data by the Processor on behalf of the Controller in connection with the AmbuNet platform.

2.2 The Processor shall process Personal Data only for the purposes of:

- Delivering the AmbuNet SaaS platform
- Providing support, maintenance, and system improvements
- Enabling features such as employee management, event planning, patient records, and governance.

2.3 The Processor shall not process Personal Data for its own purposes.

3. Duration

3.1 This Agreement shall remain in force for the duration of the service agreement.

3.2 Obligations relating to confidentiality and data protection shall survive termination.

4. Nature and Purpose of Processing

4.1 Processing may include:

- Collection and input of data
- Storage and hosting
- Organisation and structuring
- Retrieval and consultation
- Transmission and sharing (where configured by the Controller)
- Deletion and destruction

5. Categories of Data Subjects

5.1 Data Subjects may include:

- Employees and contractors
- Applicants and prospective staff
- Patients and service users
- Clients and organisational contacts

6. Types of Personal Data

6.1 Personal Data may include:

- Names, addresses, contact details
- Dates of birth
- Employment records and qualifications
- Identification documents
- Medical and clinical data (Special Category Data)
- Incident and safeguarding records
- Communication records

7. Controller Obligations

7.1 The Controller shall:

- Ensure that it has a lawful basis for processing Personal Data
- Ensure that all Personal Data provided to the Processor is accurate and lawful
- Provide appropriate privacy notices to Data Subjects
- Be responsible for determining retention periods
- Ensure appropriate technical and organisational measures on its own systems

8. Processor Obligations

8.1 The Processor shall:

- Process Personal Data only on documented instructions
- Immediately inform the Controller if an instruction infringes Applicable Data Protection Law
- Ensure personnel are subject to confidentiality obligations
- Implement appropriate technical and organisational measures
- Maintain records of processing activities where required
- The Processor shall cooperate, where necessary, with the Controller's relevant supervisory authority, including those within the European Economic Area.

9. Security Measures

9.1 The Processor shall implement appropriate security measures including:

- Encryption in transit (HTTPS/TLS)

- Secure password hashing (bcrypt)
- Role-based access control
- Multi-factor authentication for sensitive access
- Logging and monitoring of system access
- Segregation of tenant data
- Secure hosting infrastructure
- Regular system updates and patching

9.2 The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

- pseudonymisation and encryption
- ability to ensure ongoing confidentiality, integrity, availability and resilience
- ability to restore availability in a timely manner
- regular testing and evaluation of measures

9.3 The Processor shall regularly review and update security measures.

10. Sub-Processors

10.1 The Controller authorises the use of Sub-Processors by the Processor.

10.2 Current Sub-Processors include:

- Hosting providers (UK-based infrastructure)
- Amazon Web Services (file storage and related services)
- Email and SMS communication providers

10.3 The Processor shall:

- Ensure Sub-Processors are bound by equivalent obligations
- Remain fully liable for their actions

10.4 The Processor shall notify the Controller of any material changes to Sub-Processors. The Processor shall inform the Controller of any intended changes and give the Controller the opportunity to object on reasonable grounds.

11. International Data Transfers

11.1 Personal Data may be processed in:

- The United Kingdom
- The European Economic Area (EEA)

11.2 The UK benefits from an adequacy decision by the European Commission.

11.3 No transfers outside these regions shall occur without appropriate safeguards.

11.4 Processing of Personal Data is carried out in accordance with GDPR requirements applicable within the European Union and European Economic Area.

12. Data Subject Rights

12.1 The Processor shall assist the Controller in responding to:

- Access requests
- Rectification requests
- Erasure requests
- Restriction requests
- Portability requests

12.2 The Processor shall not respond directly unless instructed.

13. Personal Data Breaches

13.1 The Processor shall notify the Controller without undue delay after becoming aware of a Personal Data Breach.

13.2 Notification shall include:

- Nature of the breach
- Categories and approximate number of Data Subjects
- Likely consequences
- Measures taken or proposed

14. Audit and Compliance

14.1 The Processor shall make available information necessary to demonstrate compliance.

14.2 The Controller may, upon reasonable notice, audit the Processor’s compliance, including by requesting documentation or conducting inspections, provided such audits are:

- limited to once per year unless required by law
- subject to confidentiality obligations
- not disruptive to the Processor’s operations

15. Data Retention and Deletion

15.1 Upon termination, the Processor shall:

- Provide access for data export
- Delete Personal Data within 90 days (unless otherwise agreed)
- Delete Personal Data immediately when explicitly requested to do so by the Controller

15.2 Data may be retained where required by law.

16. Confidentiality

16.1 The Processor shall ensure all personnel:

- Are bound by confidentiality
- Receive appropriate training