LEGAL DOCUMENT

Data Processing Agreement

UK GDPR Article 28 compliant agreement governing the processing of personal data on the CrisisConnect platform

CrisisConnect Limited · Company No: 17210373 · May 2026

Status	This DPA forms part of the Customer Subscription Agreement and is incorporated by reference. It applies to all personal data processed by CrisisConnect Limited on behalf of subscribing organisations.

1. Definitions

Term	Definition
"Controller"	The Customer — the subscribing organisation that determines the purposes and means of processing personal data.
"Processor"	CrisisConnect Limited — which processes personal data on behalf of the Controller.
"Personal Data"	Any information relating to an identified or identifiable natural person entered into the Platform by the Controller.
"Processing"	Any operation performed on Personal Data, including collection, storage, retrieval, use, disclosure, erasure, or destruction.
"Sub-processor"	Any third party engaged by CrisisConnect Limited to process Personal Data on behalf of the Controller.
"UK GDPR"	The UK General Data Protection Regulation as retained in UK law under the European Union (Withdrawal) Act 2018.

2. Subject Matter and Duration

2.1 CrisisConnect Limited processes Personal Data on behalf of the Controller solely to provide the Platform services as described in the Customer Subscription Agreement.

2.2 Processing continues for the duration of the Customer Subscription Agreement and for 30 days thereafter, after which all Personal Data is permanently deleted.

3. Nature and Purpose of Processing

Element	Detail

Nature	Storage, retrieval, display, export, and deletion of Personal Data entered by the Controller into the Platform.
Purpose	To provide the operational management platform services to the Controller.
Categories	Member/client records (name, contact details, household composition, service usage), volunteer records, staff accounts. Potentially special category data including disability status, benefits status, employment status.
Data subjects	The Controller's members, clients, volunteers, and staff.
Retention	For the duration of the subscription plus 30 days.

4. Obligations of the Processor

4.1 CrisisConnect Limited shall:

- Process Personal Data only on documented instructions from the Controller
- Ensure all persons authorised to process Personal Data are bound by confidentiality obligations
- Implement and maintain appropriate technical and organisational security measures
- Not engage any Sub-processor without prior authorisation, except those listed in Schedule 1
- Assist the Controller in responding to data subject rights requests
- Assist the Controller in meeting obligations under Articles 32-36 of UK GDPR
- On termination, delete or return all Personal Data as instructed
- Provide information necessary to demonstrate compliance and allow for audits on reasonable notice

5. Security Measures

Measure	Description
Encryption at rest	Database and backup encryption using industry-standard algorithms
Encryption in transit	TLS 1.2+ for all data in transit
Access controls	Role-based access control; principle of least privilege; tenant data isolation
Authentication	Microsoft and Google SSO for staff accounts; password hashing for local accounts
Audit logging	All data access and modifications logged with timestamp and user identity
Backups	Regular automated backups with encrypted storage
Breach response	Documented procedure; notification to Controller within 72 hours of becoming aware

6. Sub-processors

Sub-processor	Purpose
Microsoft Azure	Cloud hosting and infrastructure. UK data centres.
SendGrid / Twilio	Transactional email delivery.
Stripe	Payment processing.
Clickatell	SMS delivery where SMS modules are active.

6.1 CrisisConnect Limited will notify the Controller of any intended changes to Sub-processors with 30 days' notice.

7. Data Subject Rights

7.1 The Controller is responsible for responding to data subject rights requests. CrisisConnect Limited provides tools within the Platform to locate, export, rectify, and delete Personal Data.

7.2 Where a data subject contacts CrisisConnect Limited directly, we will forward it to the Controller within 5 working days.

8. Personal Data Breaches

8.1 CrisisConnect Limited will notify the Controller within 72 hours of becoming aware of a Personal Data breach.

8.2 Notification will include: nature of the breach, categories and approximate number of data subjects, likely consequences, and measures taken.

9. International Transfers

9.1 Personal Data is stored in the United Kingdom. Where Sub-processors process data outside the UK, appropriate safeguards are in place under UK GDPR Chapter V.

10. Governing Law

10.1 This Agreement is governed by the laws of England and Wales.