



Composure247

LEGAL

Data Processing Agreement

How CITSYS LIMITED processes personal data on your behalf when you use Composure247, under UK GDPR.

VERSION

1.1

DATE

28 October 2026

FOR

Composure247 customers

1. Parties and scope

1.1 Parties. This Data Processing Agreement ("DPA") is between **CITSYS LIMITED**, a company registered in England and Wales with company number **07254892**, whose registered office is at **248 Church Lane, Kingsbury, London, NW9 8SL**, which provides Composure247 ("**we**", "**us**", the "**Processor**"), and the business that has agreed to the Composure247 Terms of Service ("**you**", the "**Controller**").

1.2 How it fits. This DPA forms part of the agreement between us for Composure247 (the "**Agreement**"): the Terms of Service, the Free Trial Agreement while you are on a trial, and any order form. You accept it when you accept the Terms of Service, including by ticking the box at sign-up. We record the version you accepted and when.

1.3 What it covers. It applies whenever we process personal data on your behalf to provide the Service, including during a free trial. It does not cover data we process as a controller in our own right, such as your account and billing details (Terms of Service, section 8.5).

1.4 Which document wins. On data protection, this DPA prevails over the Terms of Service. A signed order form prevails over both only where it expressly says it changes this DPA.

2. Definitions

2.1 "Data Protection Law" means the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003, as amended or replaced from time to time.

2.2 "Controller", "processor", "data subject", "personal data", "personal data breach", "processing" and "supervisory authority" have the meanings given in Data Protection Law. The supervisory authority in the UK is the Information Commissioner's Office ("**ICO**").

2.3 "Customer Personal Data" means personal data in Customer Data (as defined in the Terms of Service) that we process on your behalf to provide the Service.

2.4 "Sub-processor" means a third party we engage to process Customer Personal Data.

2.5 Other capitalised words have the meanings in the Terms of Service.

3. Roles and instructions

3.1 Roles. For Customer Personal Data, you are the controller and we are your processor. Annex 1 sets out the subject matter, duration, nature and purpose of the processing, the types of personal data and the categories of data subjects.

3.2 Your instructions. We process Customer Personal Data only on your documented instructions. Your instructions are:

- the Agreement, including this DPA;
- your configuration and use of the Service, by you and your Users (for example, the contacts you add, the incidents you raise and the messages you send or approve);
- any further written instructions you give us that are consistent with the Agreement.

3.3 Unless the law requires otherwise. If the law requires us to process Customer Personal Data other than on your instructions, we will tell you before we do, unless the law forbids that on important grounds of public interest.

3.4 Unlawful instructions. We will tell you straight away if, in our opinion, an instruction breaks Data Protection Law. We may then decline to follow it until you confirm or change it.

3.5 Your responsibilities as controller. You are responsible for:

- having a lawful basis for the processing, and for contacting each person you send messages to;
- giving data subjects the information Data Protection Law requires, including that their details are held in Composure247;
- the accuracy of Customer Personal Data;
- not putting special category data, criminal offence data or payment card data into the Service unless we have agreed in writing.

4. Our people

4.1 Confidentiality. Everyone we authorise to process Customer Personal Data is bound by a duty of confidentiality, by contract or by law.

4.2 Need to know. Our staff access Customer Personal Data only as needed to provide, secure and support the Service.

4.3 Support access is recorded. When our support staff need to see the Service as one of your Users to investigate a problem, they use a time-limited session that is recorded. Your administrators can see the record (Terms of Service, section 3.5).

5. Security

5.1 Our measures. We implement and maintain appropriate technical and organisational measures to protect Customer Personal Data, as Article 32 of the UK GDPR requires. They are summarised in Annex 2.

5.2 We keep them up. We may update our measures as technology and threats change, but we will not materially reduce the overall protection they give during the Agreement.

5.3 Your part. Some security depends on you: who you make an administrator, whether you require a second sign-in step for all your Users, removing access promptly when someone leaves, and keeping credentials confidential.

6. Sub-processors

6.1 General authorisation. You give us general authorisation to engage sub-processors. The sub-processors we use today are listed in Annex 3, and the current list is kept at composure247.com/subprocessors.

6.2 Notice of changes. We will update that list at least **30 days** before a new sub-processor starts processing Customer Personal Data. We will also email your administrators.

6.3 Objecting. You may object to a new sub-processor on reasonable data protection grounds within that notice period. We will work with you in good faith to address the concern. If we can't, you may end the Agreement and receive a pro-rata refund of prepaid fees for the unused period.

6.4 Same protection. We impose data protection terms on each sub-processor that are at least as protective as this DPA, and we remain responsible to you for how they perform them.

6.5 Emergencies. If we must replace a sub-processor urgently, for example because it has failed or poses a security risk, we may do so straight away and will tell you as soon as we reasonably can. Your right to object still applies.

7. International transfers

7.1 Where data is held. We store Customer Personal Data in the UK (London region).

7.2 Where it is processed elsewhere. Some sub-processors process it outside the UK, as Annex 3 shows. In particular:

- email delivery runs in the EU (Ireland), which the UK recognises as adequate;
- AI drafting, and text and WhatsApp message delivery, run in the United States;
- Meta, which carries WhatsApp messages, may process them in its data centres worldwide, including the United States.

7.3 Safeguards. We transfer Customer Personal Data outside the UK only where Data Protection Law allows: to a country the UK has found adequate, to a US organisation certified under the UK Extension to the EU-US Data Privacy Framework, or under the ICO's International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, with a transfer risk assessment where one is needed.

7.4 On request. We will give you a copy of the relevant transfer terms, with commercial details removed, if you ask.

8. Helping you meet your obligations

8.1 Data subject requests. Most requests you can handle yourself: your administrators can find, correct, export and delete contacts and Users in the Service. If we receive a request directly from one of your data subjects, we will pass it to you within **5 business days** and won't answer it ourselves unless you ask us to. Where you can't meet a request using the Service, we will help you, taking into account the nature of the processing.

8.2 Impact assessments and the ICO. We will give you reasonable help with data protection impact assessments and any prior consultation with the ICO, so far as they concern the Service and the information is available to us.

8.3 Cost. This help is free where it is reasonable and occasional. For help beyond that, we may charge at our standard rates, agreed with you in advance.

9. Personal data breaches

9.1 We tell you quickly. If we become aware of a personal data breach affecting Customer Personal Data, we will tell you without undue delay, and in any event within **48 hours**. That leaves you time to meet your own 72-hour deadline to report to the ICO.

9.2 Who we tell. We notify your administrators by email, and by phone where the breach is serious. If you give us a separate privacy contact in writing, we notify them too.

9.3 What we tell you. As far as we know it at the time, and adding the rest as we learn it:

- what happened, and when;
- the categories and approximate number of data subjects and records affected;
- the likely consequences;
- what we have done and propose to do to contain it and reduce harm;
- a contact for more information.

9.4 We act, and you decide. We will take reasonable steps to contain the breach and stop it recurring. You decide whether to notify the ICO and data subjects. We won't notify them about your data without your agreement unless the law requires us to.

9.5 Not an admission. Telling you about a breach is not an admission of fault or liability.

10. Records, information and audits

10.1 Records. We keep the records of processing Article 30(2) of the UK GDPR requires of a processor.

10.2 Information. On request, we will give you the information reasonably needed to show we meet this DPA. That includes our security overview, our sub-processor list, answers to a reasonable security questionnaire, and the latest summary of our independent security testing.

10.3 Audits. If that information isn't enough, or a supervisory authority requires it, you (or an independent auditor you appoint, bound by confidentiality) may audit our compliance with this DPA:

- no more than once in any 12 months, unless there has been a personal data breach or the ICO requires it;
- with at least **30 days'** written notice and an agreed scope;
- during UK business hours, without unreasonably disrupting our business or putting other customers' data at risk.

Audits of our sub-processors take place through the reports and certifications they publish. You pay the costs of any audit you carry out, including your auditor's fees.

11. Return and deletion

11.1 Export first. For **30 days** after the Agreement ends, you can ask us for an export of your Customer Personal Data in a common format, and we will provide it.

11.2 Then deletion. After that, we delete Customer Personal Data within **90 days**, unless the law requires us to keep it.

11.3 Backups. We keep daily backups for 7 days. Copies of deleted Customer Personal Data in them are gone within 7 days, as the backups age out. Until then they are kept secure and not used.

11.4 Trials. If a free trial ends without a subscription, the Free Trial Agreement's timings apply instead.

11.5 Confirmation. On request, we will confirm in writing that deletion is complete.

12. Liability, term and general

12.1 Liability. Each party's liability under this DPA is subject to the limits and exclusions in the Terms of Service (section 13).

12.2 Term. This DPA lasts as long as we process Customer Personal Data on your behalf, including after the Agreement ends until deletion under section 11.

12.3 Changes. We may update this DPA where Data Protection Law changes or to reflect a change in how we provide the Service, on the same notice terms as the Terms of Service (section 14.1). Each version has a number and a date, and we record which version you accepted.

12.4 Law and courts. This DPA is governed by the law of England and Wales, and the courts of England and Wales have exclusive jurisdiction.

Annex 1: Details of the processing

Subject matter	Providing Composure247, the incident communication service for managed service providers, under the Agreement.
Duration	The term of the Agreement, then until deletion under section 11.
Nature of the processing	Collecting, storing, organising, retrieving, using, sending, publishing to the customer portal, and deleting. It includes AI drafting from the information you enter, and syncing from tools you connect. It also includes sending incident updates, service-restored and resolution notices on WhatsApp to contacts who have agreed to receive them, and receiving replies and delivery reports from the text and WhatsApp provider. All our customers share one Composure247 WhatsApp number, so when someone replies STOP to it, we switch WhatsApp off for that phone number for every customer who holds it, and we answer other replies automatically, at most once a day, to say the number can't read them.
Purpose	Raising and tracking incidents; drafting, approving and sending customer updates by email and text, and by WhatsApp to contacts who have agreed; recording a contact's agreement to receive updates on WhatsApp, and their opt-outs; confirming whether messages were delivered; the branded customer portal; reminders and escalation; post-incident reviews and Root Cause Analyses; planned maintenance notices; sign-in, access control and auditing.
Categories of data subjects	Your staff and other Users; your customers' contacts who receive updates or use the portal; people named in incident notes you enter; people who send a message to the Composure247 WhatsApp number that we link to you (the message quotes one of yours, you messaged that number last, or only you hold it as a contact). We delete such messages after 90 days.

Types of personal data	Names, business email addresses, phone numbers, job titles and roles; sign-in data (hashed passwords, second-step sign-in settings, single sign-on identifiers); content you enter about incidents, maintenance and reviews; message delivery records (recipient, time, status, and the delivery report from the text or WhatsApp provider, such as delivered, read or failed, with the reason); WhatsApp consent records (whether the contact agreed in the portal or you confirmed their agreement, who confirmed it, when, the wording shown and the phone number), and when and why WhatsApp was switched off; messages your contacts send to the Composure247 WhatsApp number; audit records and IP addresses of sign-ins and actions; data from tools you connect, such as HaloPSA ticket details or Microsoft Entra ID directory attributes.
Special category data	None intended. The Service is not designed for it, and you agree not to put it in (section 3.5).
Frequency	Continuous, for as long as you use the Service.

Annex 2: Security measures

The measures in place today. Our security overview at composure247.com/security describes them in more detail.

Keeping customers apart

- Each customer's data is separated in the database itself, by access rules on every table, so one customer can never read another's data even if the application has a fault.
- The settings that control what is sent to customers can only be changed by the Service's own server functions, not directly by any user.
- Customer portal users can see only their own organisation's data.

Signing in and access

- Administrators must use an authenticator app as a second sign-in step. Customers can require it for all their Users.
- Single sign-on and user provisioning through Microsoft Entra ID, for customers who connect it.
- Passwords of at least 12 characters, checked against known breached passwords.
- Set-up and reset links are single-use and expire quickly. We never set a password for anyone.
- Permissions by role, enforced in the database, on the server and in the interface.
- Our support staff's access to a customer's account is time-limited and recorded.

Protecting data

- Encryption in transit (TLS everywhere, with HSTS) and at rest.
- Automated daily backups, kept for 7 days.
- Hosting in the UK (London region).
- Secret keys are held in a managed secret store, never in source code or the browser.

Hardening and monitoring

- Strict browser security headers, including a content security policy.
- Rate limits on actions that could be abused, and a bot check on public sign-up.

- Untrusted text is passed to the AI as data, never as instructions. A person approves AI drafts before customers see them, except the two automatic emails described in the Terms of Service (section 7.3).
- An audit log of privileged actions.
- Regular self-assessment against the OWASP Application Security Verification Standard and API Security Top 10, with automated database security checks run every day.

People and process

- A documented incident response and breach notification process.
- Staff access only on a need-to-know basis, under a duty of confidentiality.

We are not yet certified to ISO 27001 or SOC 2.

Annex 3: Authorised sub-processors

As at 26 October 2026. The Terms of Service, section 9, lists the sub-processors at 24 October 2026; changes since then are made under section 6 of this DPA.

Sub-processor	What it does	Personal data it handles	Where
Supabase	Database, sign-in and server functions	All Customer Personal Data	UK (London)
Vercel	Hosts the web application	Web request details only (IP address, browser)	Global edge network
Resend	Sends emails	Recipient email addresses and message content	EU (Ireland)
Twilio	Sends texts and WhatsApp messages; receives replies and delivery reports	Recipient phone numbers, message content, replies and delivery status	United States
Meta (WhatsApp Business Platform, through Twilio)	Carries WhatsApp messages and replies	Recipient phone numbers, message content, replies and delivery status	Global (Meta data centres, including the United States)
Anthropic	AI drafting	The incident details used to draft a message; not used for training, and deleted within 30 days	United States
Cloudflare	The "not a robot" check on the sign-up page	Browser signals of the person signing up; no Customer Personal Data	Global
Microsoft	Single sign-on and user provisioning, only if you connect Microsoft Entra ID	Sign-in assertions and directory attributes	Your Microsoft tenant

Version 1.1, 28 October 2026. Composure247 is software provided by CITSYS LIMITED. Changes from version 1.0: WhatsApp (sections 7.2, Annex 1 and Annex 3): sending updates on WhatsApp, consent records, replies and delivery reports, and Meta as a sub-processor.



Composure247

Every customer kept informed.
Every incident closed properly.

TALK TO US

sales@composure247.com

SIGN IN

app.composure247.com

Data Processing Agreement · Version 1.1 · 28 October 2026

Composure247 is a product of CITSYS LIMITED. © 2026 CITSYS LIMITED. All rights reserved.