

---

# Complivolve Ltd: Platform Privacy Notice

---

Last updated: 23 September 2026

## 1. Who We Are

For the purposes of the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("DPA 2018"):

### **Complivolve Ltd**

Company Number: 16865216

Registered Office: 86–90 Paul Street, London, EC2A 4NE

Email: [info@complivolve.com](mailto:info@complivolve.com)

Complivolve Ltd is registered with the Information Commissioner's Office ("ICO") under registration number **ZC048141**.

Complivolve provides a cloud-based software-as-a-service platform for CQC-regulated adult social care providers (the "**Complivolve Platform**").

Depending on the personal data involved, Complivolve acts either as:

- a **controller**, where Complivolve determines why and how personal data is used, for example in relation to account administration, billing, security and support; or
- a **processor**, where Complivolve processes Customer Personal Data on behalf of a Customer using the Platform.

This Platform Privacy Notice explains those different roles.

It applies to the Complivolve Platform and related account, billing and support activities. It does **not** apply to the public Complivolve marketing website, which is covered by our separate Website Privacy Policy.

## 2. How to Contact Us

For privacy or data-protection enquiries:

**Email:** [info@complivolve.com](mailto:info@complivolve.com)

### **Postal address:**

Complivolve Ltd  
86–90 Paul Street  
London  
EC2A 4NE

---

---

## 3. Our Role and the Customer's Role

A Customer using the Complivolve Platform will normally be the CQC-registered provider associated with the relevant Complivolve account.

### Where Complivolve acts as controller

Complivolve acts as controller for personal data that it needs for its own business purposes, including:

- creating and administering Platform accounts;
- managing subscriptions and billing;
- recording acceptance of contractual terms;
- authenticating users and maintaining Platform security;
- preventing fraud, abuse and unauthorised access;
- providing customer support;
- maintaining appropriate business, contractual, security and compliance records; and
- communicating with Customers and Authorised Users about the Platform and their accounts.

### Where the Customer acts as controller

The Customer is the controller of personal data which it enters into, uploads to, creates within or otherwise processes through the Platform for its own operational purposes.

This is referred to in our Subscription Terms as **Customer Personal Data**.

Complivolve processes Customer Personal Data on the Customer's documented instructions and in accordance with the Data Processing Schedule forming part of the Complivolve Subscription Terms.

The Customer is responsible for determining:

- what Customer Personal Data is entered into the Platform;
- why it is processed;
- the lawful basis for that processing;
- how long the Customer needs the information; and
- who should have access to it.

Complivolve does not determine the Customer's lawful basis for processing operational care, workforce or regulatory information.

## 4. Personal Data We Process

The personal data processed through the Platform depends on how the Customer uses it.

### 4.1 Account and Authorised User Data

This may include:

---

- 
- name;
  - email address;
  - Platform role;
  - Customer and Location association;
  - account status;
  - invitations and membership information;
  - authentication and multi-factor authentication information;
  - password-reset and security information;
  - contractual acceptance records; and
  - Platform activity associated with the user account.

Complivolve does not need access to users' raw passwords. Authentication is provided through our authentication infrastructure.

Where an Authorised User's name, role or other identifier also appears within an operational Customer record — for example as the person assigned to a task, the author of a record or a member of staff referred to within an incident — that information may form part of Customer Personal Data for which the Customer acts as controller.

## **4.2 Customer and Location Information**

This may include:

- Customer/provider name;
- CQC Provider ID;
- Location name;
- CQC Location ID;
- subscription status;
- Owner and Manager account associations; and
- other information required to administer the Customer's account and Locations.

Some provider and Location information is obtained from publicly available CQC information.

## **4.3 Billing and Transaction Data**

This may include:

- billing contact information;
- Stripe customer and subscription identifiers;
- subscription status;
- invoices and payment status;
- billing periods;
- discounts or promotional arrangements; and
- records necessary to administer subscriptions and payments.

Payment-card details are processed by Stripe and are not stored by Complivolve.

## **4.4 Technical, Security and Usage Data**

This may include information generated when a user accesses or uses the Platform, such as:

---

- 
- IP address;
  - authentication and login information;
  - timestamps;
  - device, browser or connection information where generated by our infrastructure;
  - security and rate-limiting information;
  - audit and activity records; and
  - technical information required for troubleshooting, security and Platform operation.

The Platform does **not** currently use advertising trackers, behavioural advertising technology, session-replay tools or website analytics technology.

## 4.5 Customer Personal Data

Customers may use the Platform to record and manage operational information including:

- CQC findings and action plans;
- assigned tasks and responsibilities;
- evidence and supporting files;
- incidents and incident narratives;
- witness information and witness statements;
- risk records;
- safeguarding records;
- complaints, feedback and related correspondence;
- duty of candour information;
- audit responses and evidence;
- notes, amendments and audit trails;
- management review and sign-off information; and
- sustainability or follow-up records relating to completed actions.

Customer Personal Data may relate to:

- employees and other workers;
- managers and other Authorised Users;
- witnesses;
- complainants and other third parties; and
- people receiving care or support from the Customer.

The current Platform is **not an employee HR-record system**. It does not currently provide functionality for storing employee training records, qualifications, DBS or right-to-work documentation, occupational-health records, immunisation records, next-of-kin records, supervision records, appraisal records or exit-interview records.

Where staff reference information is recorded, the Platform currently records limited information such as **name, email address and job role**.

Customers are encouraged to minimise directly identifying information about people receiving care.

Service Users are generally recorded using a **room number or other reference rather than their full name**. A first name may be recorded where appropriate in a duty-of-candour record.

---

---

However, information recorded using a room number, first name or other reference may still constitute personal data where the Customer can identify the individual concerned.

Operational records may therefore include **special category personal data**, particularly information concerning a person's health, where that information is relevant to an incident, risk, safeguarding concern, complaint or other operational record.

The Customer remains responsible for deciding whether information should be entered into the Platform and for establishing an appropriate lawful basis and, where applicable, condition for processing it.

## 5. How Personal Data Is Collected

We may obtain personal data through:

### Information provided directly by users

Users provide information when they:

- create or activate an account;
- accept contractual terms;
- configure their account;
- use the Platform;
- submit records or upload files;
- contact Complivolve for support; or
- otherwise communicate with us about their account or the Platform.

### Information provided by the Customer or other Authorised Users

Customers may invite users, assign Platform roles and enter information concerning employees, Service Users, witnesses or other individuals as part of their use of the Platform.

### Automated technical information

Technical and security information may be generated automatically when users access the Platform through authentication systems, server infrastructure, security controls, logs and rate-limiting services.

### Stripe

We receive limited subscription, transaction and payment-status information from Stripe so that we can administer subscriptions.

### Care Quality Commission

The Platform uses publicly available CQC information, including Provider and Location information and published inspection reports.

---

---

## 6. How We Use Personal Data Where Complivolve Is Controller

Where Complivolve acts as controller, we may use personal data for the following purposes.

### **Account administration and provision of the Platform**

To:

- create and administer accounts;
- identify Customers, Locations and Authorised Users;
- manage user roles and access;
- communicate with Customers and users about their accounts; and
- provide and administer subscriptions.

Depending on the circumstances, we rely on performance of a contract, our legitimate interests in providing and administering the Platform, or both.

### **Billing and financial administration**

To:

- administer subscriptions;
- process and record payments;
- maintain invoices and transaction records;
- manage failed payments and cancellation; and
- comply with accounting, tax and other legal obligations.

We rely on performance of a contract where applicable, legitimate interests in administering our business and recovering sums properly due, and compliance with legal obligations.

### **Security, authentication and fraud prevention**

To:

- authenticate users;
- operate multi-factor authentication;
- prevent unauthorised access;
- detect abuse or suspicious activity;
- rate-limit requests;
- investigate security incidents; and
- maintain appropriate security records.

We rely on our legitimate interests in protecting Complivolve, our Customers and Platform users, together with any applicable legal obligations.

### **Customer support and administration**

To respond to requests for assistance, investigate issues and communicate with Customers and users about the Platform.

---

---

We rely on our legitimate interests in operating and supporting the Platform and, where applicable, performance of our contractual obligations.

## Legal, compliance and contractual records

To maintain evidence concerning:

- contractual acceptance;
- account authority;
- subscriptions;
- billing;
- security;
- complaints;
- legal claims; and
- regulatory or compliance obligations.

We rely on our legitimate interests and applicable legal obligations.

## 7. Customer Personal Data Where Complivolve Acts as Processor

Complivolve does not determine the purpose for which the Customer processes Customer Personal Data through the Platform.

We process Customer Personal Data on behalf of the Customer to:

- host and make the Platform available;
- store and retrieve Customer Data;
- apply permissions and access controls;
- perform Platform workflows requested by the Customer;
- generate reports and exports;
- send relevant transactional notifications;
- provide technical support;
- maintain security and audit controls;
- maintain backups and resilience arrangements;
- investigate technical issues; and
- delete or return information in accordance with the Subscription Terms and Data Processing Schedule.

Our obligations as processor are set out in the **Data Processing Schedule contained within the Complivolve Subscription Terms**.

## 8. Artificial Intelligence and CQC Information

Complivolve includes functionality which can analyse **publicly published CQC inspection reports** and generate draft findings and suggested actions for management review.

The AI functionality currently receives publicly available CQC report information required for that purpose.

---

---

Complivolve does **not** currently send Customer operational records such as incidents, risks, safeguarding records, audits, action plans or Service User records to the AI model used for this functionality.

AI-generated findings and suggested actions are drafts. They require human review and may be accepted, amended or rejected by the Customer.

Complivolve does not use Customer Data or Customer Personal Data to train artificial-intelligence models.

Complivolve does not make decisions about individuals based solely on automated processing which produce legal or similarly significant effects.

## 9. Cookies and Local Storage Within the Platform

The Platform uses limited cookies and similar local-storage technology necessary to provide and secure the service, including for:

- authentication and session management;
- password-reset and account-security processes; and
- limited user-interface preferences.

The Platform does not currently use advertising cookies or behavioural advertising trackers.

The separate Cookie Policy published on the Complivolve website relates primarily to the public website.

## 10. Who We Share Personal Data With

Complivolve does not sell personal data.

We use a limited number of third-party providers to operate, secure and support the Platform.

Their roles differ depending on the information and service involved.

### Subprocessors of Customer Personal Data

Where Complivolve acts as processor for a Customer, the following providers may act as subprocessors of Customer Personal Data:

- **Supabase** — primary Platform database, authentication and file storage. Complivolve's production project is configured in the London region.
- **Vercel** — application hosting and server-side processing. Information may be processed transiently through Vercel infrastructure when users interact with the Platform.
- **Resend** — transactional email delivery.
- **Google Workspace** — business email and support correspondence where such correspondence contains Customer Personal Data.

Complivolve's use of subprocessors is governed by the Data Processing Schedule contained within the Subscription Terms.

---

---

## Other service providers

Complivolve also uses providers for processing carried out in other capacities:

- **Stripe** — subscription billing and payment processing. Stripe may act in different data-protection capacities, including as an independent controller for certain payment-processing activities.
- **Cloudflare** — DNS services and Turnstile security functionality. Cloudflare processes limited technical information used for bot detection and service security and may act as controller for certain processing undertaken to improve its Turnstile service.
- **Upstash** — limited rate-limiting and abuse-prevention functionality using technical identifiers such as IP addresses or user/account identifiers.
- **Anthropic** — AI processing of publicly available CQC report information as described in section 8. Anthropic does not currently receive Customer operational data through this functionality.

Further information about these providers, including their roles and our authorised subprocessors, is maintained in our separate **Subprocessors & Service Providers** document available through the Legal section of [www.complivolve.com](https://www.complivolve.com).

## 11. International Transfers

Some of our service providers, or their own authorised service providers, may process personal data outside the United Kingdom.

Where personal data is transferred outside the United Kingdom, Complivolve relies on transfer mechanisms recognised under UK data-protection law.

Depending on the destination and recipient, these may include:

- UK adequacy regulations;
- an applicable adequacy arrangement for an eligible recipient; or
- appropriate contractual safeguards, including the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses.

The mechanism applicable to a particular provider may differ according to that provider's contractual and processing arrangements.

## 12. How We Protect Personal Data

Complivolve applies technical and organisational measures designed to protect personal data against accidental or unlawful loss, alteration, disclosure, destruction or unauthorised access.

Measures include, as appropriate:

- encrypted transmission using HTTPS/TLS;
  - authentication controls;
  - multi-factor authentication;
  - role-based access controls;
  - tenant and Location access controls;
-

- 
- logical segregation of Customer information;
  - database row-level security controls;
  - audit and activity records;
  - security and rate-limiting controls;
  - controlled access to production systems; and
  - backup and recovery arrangements provided through relevant infrastructure services.

No method of electronic storage or transmission can be guaranteed to be completely secure, but Complivolve reviews and develops its safeguards as the Platform evolves.

## 13. Data Retention and Deletion

Complivolve retains personal data only for as long as reasonably necessary for the purposes for which it is processed, taking into account contractual, legal, regulatory, accounting, security and dispute-resolution requirements.

### Customer Data

Customers are responsible for exporting information they require **before their access to the relevant Location ends**.

When a Location Subscription ends:

- normal Customer access to that Location ends;
- operational Customer Data may remain within Complivolve's systems for up to **30 days** solely for recovery, support, administration and deletion purposes;
- the Customer has no contractual right to normal Platform access to that data during the 30-day period;
- following that period, operational Customer Data is deleted from Complivolve's **live systems**, unless applicable law requires otherwise or Complivolve and the Customer have lawfully agreed otherwise; and
- Complivolve provides a deletion certificate in accordance with its offboarding process.

Residual copies contained in backups may remain until they expire through the applicable backup lifecycle.

Backups containing Customer Data are not restored into ordinary operational use after termination except where reasonably necessary for legitimate backup recovery, disaster recovery, security or similar technical purposes.

If a Customer subsequently returns after its operational Customer Data has been deleted, Complivolve is not obliged to restore the previous data.

### Complivolve-controlled records

Complivolve may separately retain records which it controls for its own legitimate business or legal purposes, including:

- contractual acceptance and Terms-version records;
  - subscription and billing information;
  - financial and accounting records;
-

- 
- security and audit logs;
  - support correspondence;
  - records concerning complaints or disputes;
  - deletion and offboarding records; and
  - information required to establish, exercise or defend legal claims or demonstrate contractual, regulatory or legal compliance.

Account-deletion records may be retained for **12 months** in accordance with Complivolve's account-deletion process.

Different categories of information may therefore have different retention periods.

Where personal data is no longer required, it will be deleted, anonymised or otherwise disposed of appropriately.

## 14. Anonymised and Aggregated Information

Complivolve may create aggregated information from Customer Data where permitted by the Subscription Terms.

Where information has been genuinely anonymised so that no individual, Customer or Location is identified or reasonably capable of being identified, it is no longer personal data.

Complivolve will not treat pseudonymised information as anonymous merely because direct identifiers have been removed.

## 15. Your Data-Protection Rights

Data-protection law provides individuals with rights in relation to their personal data. Depending on the circumstances, these may include rights to:

- access personal data;
- have inaccurate information corrected;
- request deletion;
- request restriction of processing;
- object to particular processing;
- receive certain personal data in a portable format; and
- withdraw consent where processing is based on consent.

These rights are subject to the conditions and exemptions contained in data-protection law.

### Where Complivolve is controller

If your request concerns personal data for which Complivolve acts as controller — for example your Complivolve account, billing, security or support information — you can contact:

[info@complivolve.com](mailto:info@complivolve.com)

We may need to verify your identity before responding.

---

---

We normally respond to valid rights requests within the period required by data-protection law. In most circumstances this is one month, although the period may be extended where permitted by law.

### Where the Customer is controller

If your request concerns operational information entered into the Platform by a care provider — for example information contained in an incident, risk, safeguarding record, complaint or other Customer record — the relevant Customer is normally the controller responsible for responding to your request.

You should normally contact that care provider directly.

Where Complivolve receives a request concerning Customer Personal Data for which it acts only as processor, we will deal with it in accordance with the Customer's instructions and our Data Processing Schedule, including assisting the Customer where required.

## 16. Data-Protection Complaints

If you have concerns about how Complivolve has handled personal data for which we act as controller, please contact us at:

[info@complivolve.com](mailto:info@complivolve.com)

We will consider and respond to data-protection complaints in accordance with applicable law.

You also have the right to complain to the **Information Commissioner's Office (ICO)**, the UK supervisory authority for data protection.

Information about making a complaint is available at [www.ico.org.uk](http://www.ico.org.uk).

Where your concern relates to operational Customer Personal Data for which a care provider is the controller, you may also wish to raise the matter directly with that provider.

## 17. Changes to This Platform Privacy Notice

We may update this Platform Privacy Notice from time to time to reflect changes to:

- the Platform;
- our processing activities;
- service providers;
- legal or regulatory requirements; or
- our organisational arrangements.

The latest version will be made available through the Complivolve Platform and/or the Legal section of [www.complivolve.com](http://www.complivolve.com).

Where a change materially affects how Complivolve processes personal data as controller, we will provide appropriate notice, which may include notification by email or through the Platform.

---