Privacy Policy

Version History

Date	Version	Reason for Change	Author
24/02/2026	1.6.0	Section(s) updated: 1,2,3	Michael Flood
29/01/2026	1.5.0	Section(s) updated: 1,2,3	Michael Flood
04/01/2026	1.4.0	Section(s) updated: 1,2,3	Michael Flood
02/01/2026	1.3.0	Section(s) updated: 1,2	Michael Flood
01/08/2025	1.2.0	Section(s) updated: 1	Anthony Cox
01/08/2025	1.1.0	Section(s) updated: 1,3	Anthony Cox
31/07/2025	1.0.0	Initial generation	Anthony Cox

Privacy policy

Introduction

Codara Ltd respects the privacy of its customers, suppliers and partners. We have therefore formulated and implemented a policy on complete transparency regarding the processing of personal data, its purpose(s) and the possibilities to exercise your legal rights in the best possible way. For employees, we have formulated a separate privacy policy, available upon employment and upon request.

This privacy policy pertains to processing by Codara Ltd by means other than through the use of cookies. Codara Ltd has formulated a separate cookie policy, which can be found on our Codara Ltd 's websites: http://codara.co.uk/

Definitions

- Party responsible for processing personal data: Codara Ltd ; with registered address at Spencer House Morston Court, Aisecome Way, in United Kingdom; company registration number 16207251 and Data Protection Officer Michael Flood who can be reached at mstuartflood@gmail.com (the “Controller”).
- Data Protection Authority: The Data Protection Authority of United Kingdom.
- Data Protection laws:
    - For European citizens or residents, the EU GDPR 2018; the EU e-privacy directive 2002 (soon to be replaced by the EU e-privacy regulation);
    - For UK citizens or residents, the UK GDPR 2020 and the UK Data Protection Act 2018
    - and the national laws of the countries where we operate.

Collection of data

- Your personal data will be collected by Codara Ltd and its data processors.
- Personal data means any information relating to an identified or identifiable natural person (‘data subject’).
- An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The types of personal data we may process through third party applications:

Business process	Data	Legal basis
Compliance	Employees - Email Address, Last Name, First Name, Job Title	Legal Obligation Compliance
Marketing	Company - Non-PII data	Legitimate Interests
Task Management	Company - Intellectual Property	Legitimate Interests
Technical Tool	Company - Intellectual Property, Source Code Employees - Browser Information, First Name, Live Location, Online Activity, Last Name, Email Address, IP Address	Legitimate Interests
Testing	Company - Source Code, Email Address, Home Address, User Name, Intellectual Property	Legitimate Interests
Document Storage	Company - Intellectual Property, Contracts Employees - Contracts, Intellectual Property	Legitimate Interests
Security	Employees - Browser Information, First Name, Live Location, Online Activity, Last Name, Email Address, IP Address	Legitimate Interests
AI-Powered Tool	Company - Source Code	Legitimate Interests
Product Development	Company - Intellectual Property, Source Code, Email Address, Home Address, User Name	Legitimate Interests
Password Manager	Employees - Last Name, Email Address, First Name	Legitimate Interests
User Management/Authentication	Employees - Last Name, Email Address, First Name	Contract Performance
Email	Company - Non-PII data, Contracts, Intellectual Property Employees - Contracts, Intellectual Property	Legitimate Interests
Communication	Company - Contracts, Intellectual Property Employees - Contracts, Intellectual Property, Browser Information, First Name, Live Location, Online Activity, Last Name, Email Address, IP Address Users - First Name, Email Address, Last Name	Legitimate Interests
Website Hosting	Company - Non-PII data	Legitimate Interests

Application Hosting	Company - Non-PII data, Email Address, Home Address, User Name, Intellectual Property, Source Code Users - Last Name, Job Title, User Name, Email Address, First Name Patients - First Name, Medical Condition, Medical History, Non-medical tracking (e.g. sleep; food intake), Medicines, Medical tracking (e.g. blood pressure; blood values), Last Name, Date of Birth, Age or Age Group, General Health Data	Legitimate Interests
Work Planning	Company - Intellectual Property	Legitimate Interests

The types of personal data we may process through suppliers:

Business process	Data	Legal basis
Legal	Company - Email Address, Home Address, Telephone Number Employees - Email Address, Home Address, Telephone Number	Legal Obligation Compliance
Accountancy	Company - Telephone Number, Home Address, Email Address, Bank account or creditcard number Employees - Telephone Number, Home Address, Email Address, Bank account or creditcard number	Legal Obligation Compliance

Purposes

Codara Ltd processes personal data for one or more of the following purposes:

- Customer, employee, contractor, partner or supplier management
- Business and financial administration
- Direct marketing
- Delivery of goods or services
- Work planning

How we collect, store or otherwise process your data:

The following business processes describe how we may collect, store or otherwise process the types of personal information:

- Collection of cookies, subscription to newsletter or filling out the contact form on the website(s);

- Analyse trends and profiles, for our legitimate interest to aim to enhance, modify, personalise and improve our services and communications for the benefit of our customers;
- Process and respond to support requests, enquiries and complaints received from you through use of business email;
- Provide services and products requested and/or purchased by you and to communicate with you about such services and/or products. We do this as necessary in order to carry out a contract with you and in accordance with our legitimate interest to operate a business;
- Carry out administrative activities such as invoicing and collecting payments either locally on devices or using cloud-services;
- Store and exchange personal information contained in documents through email and cloud-services;
- Marketing and customer acquisition through email or using cloud-services.

Sharing data with third parties

We may have to share your data with third parties, including third-party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your Personal Data outside United Kingdom. If we do, you can expect a similar degree of protection in respect of your Personal Data.

We will only share your Personal Data with third parties in accordance with the GDPR and as outlined in the legal justification table above.

We share your personal data with the following enterprise third parties. We also share your data with SME third parties, details of which are available upon request. You will be notified when we have engaged with a new third party recipient of your personal data.

Naq Cyber

Function	Compliance
Data categories	Email Address, First Name, Job Title, Last Name
Data subjects	Employees

Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Ionos

Function	Application Hosting, Email, Marketing, Website Hosting
Data categories	Non-PII data
Data subjects	Company
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Github

Function	Product Development, Technical Tool
Data categories	Intellectual Property, Source Code
Data subjects	Company

Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Jira (Atlassian)

Function	Product Development, Task Management, Technical Tool
Data categories	Intellectual Property
Data subjects	Company
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Confluence

Function	Document Storage, Product Development, Work Planning
Data categories	Intellectual Property
Data subjects	Company

Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Claude

Function	AI-Powered Tool, Product Development, Technical Tool, Testing
Data categories	Source Code
Data subjects	Company
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Google Workspace

Function	Communication, Document Storage, Email
Data categories	Contracts, Intellectual Property
Data subjects	Company, Employees

Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

NordVPN

Function	Communication, Security, Technical Tool
Data categories	Browser Information, Email Address, First Name, IP Address, Last Name, Live Location, Online Activity
Data subjects	Employees
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

NordPass

Function	Password Manager, Security, User Management/Authentication
Data categories	Email Address, First Name, Last Name
Data subjects	Employees

Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Google Cloud

Function	Application Hosting
Data categories	Age or Age Group, Date of Birth, Email Address, First Name, General Health Data, Job Title, Last Name, Medical Condition, Medical History, Medical tracking (e.g. blood pressure; blood values), Medicines, Non-medical tracking (e.g. sleep; food intake), User Name
Data subjects	Patients, Users
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

App Store

Function	Application Hosting, Product Development, Testing

Data categories	Email Address, Home Address, Intellectual Property, Source Code, User Name
Data subjects	Company
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Slack

Function	Communication
Data categories	Email Address, First Name, Last Name
Data subjects	Users
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

International data transfers

The third parties we have engaged for the abovementioned business process may transfer your personal information to outside of your jurisdiction. Codara Ltd 's third party processors take all necessary measures to ensure the confidentiality, availability and integrity of personal data and to comply with the GDPR with regards to international data transfers. The international nature of its compliance certifications, as well as far-reaching technical security measures (including but not limited

to encryption of the personal data, making the data illegible to an unauthorised recipient) are sufficient to ensure that the data subjects continue to benefit from the fundamental rights they are entitled to under the GDPR.

Where Codara Ltd transfers data to third countries, it relies on the following legal grounds for international data transfers:

- An Adequacy Decision in accordance with article 45 of the GDPR
- In the absence of an Adequacy Decision, appropriate safeguards in the form of Standard Contractual Clauses or Binding Corporate Rules.

In the event that Codara Ltd is reliant on Standard Contractual Clauses for the legality of its international data transfer, it ensures that the Processor or Subprocessor takes supplementary security measures to safeguard the international data transfer with one or more of the following measures:

- Encryption;
- Anonymisation;
- Pseudonymisation.

Storage and protection of data

Your data is protected by Codara Ltd and its processors in pursuance to all legal requirements set by the relevant data processing laws. Codara Ltd has taken technical and organizational security measures to protect your data and requires its data processors to meet the same requirements. Codara Ltd has signed processing agreements with its processors to ensure an adequate level of data protection.

The following security measures are taken by Codara Ltd to protect your personal data in the course of the listed business processes:

Organisational security measures

Staff

Codara Ltd staff members are required to conduct themselves in a manner consistent with Codara Ltd ’s guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. All staff members undergo appropriate background checks prior to hiring and sign a confidentiality agreement outlining their responsibility in protecting customer data.

We continuously train staff members on best security practices, including how to identify social hacks, phishing scams, and hackers.

Access controls

Codara Ltd maintains your data privacy by allowing only authorized individuals access to information when it is critical to complete tasks for you. Codara Ltd staff members will not process customer data without authorization.

Data hosting

As a rule, data is hosted within countries and areas that provide a substantially similar level of protection as data subjects have under the GDPR. To ensure this, we rely on Adequacy Decisions as a legal basis for our international data transfers. In exceptional circumstances, where data is transferred to a country or area not subject to an Adequacy Decision, we rely on Standard Contractual Clauses with the recipient and take supplementary security measures to secure this data transfer, such as anonymisation.

Physical security

The data centres on which personal data is hosted are secured and monitored 24/7 and physical access to facilities is strictly limited to select staff.

Technical security measures

All devices which are used to access personal data for which we are responsible are secured with antivirus software, firewalls, encryption and access management. We regularly update operating systems and software to ensure vulnerabilities cannot be exploited.

We carry out regular vulnerability scanning of our website and have engaged credentialed external auditors to verify the adequacy of our security and privacy measures.

Your rights regarding information

Each data subject has the right to information on and access to, and rectification, erasure and restriction of processing of their personal data, as well as the right to object to the processing and the right to data portability.You also have the right to request that you are not made subject to decision making based solely on automated processes, including profiling, if these decisions would have a significant effect on you.

You can exercise these rights by contacting us at the following email address: compliance@codara.co.uk. If we have any doubts as to your identity, we may request you to provide us with proof of identification, such as through sending us a copy of your valid ID. Ensure that you write “Data Request” in the subject line of your email.

Within one month of the submitted request, you will receive an answer from us. We will not charge you for submitting your request unless the request is manifestly unfounded or otherwise unreasonable in its nature. Depending on the complexity and the number of the requests this period may be extended to two months.

Marketing

- You may receive commercial offers from Codara Ltd . If you do not wish to receive them (anymore), please send us an email to the following address: compliance@codara.co.uk and ensure that you write “Data Opt-Out” in the subject line of your email.
- Your personal data will not be used by our partners for commercial purposes.
- If you encounter any personal data from other data subjects while visiting our website, you are to refrain from collection, any unauthorized use or any other act that constitutes an infringement of the privacy of the data subject(s) in question. The collector is not responsible in these circumstances.

Data retention

The collected data are used and retained for the duration determined by law. You may, at any time, request your data to be deleted from any Codara Ltd account, system or other data processing medium in accordance with the process described above.

Applicable law

These conditions are governed by the laws and regulations of the country where we are headquartered. The court in the district where we are headquartered has the sole jurisdiction if any dispute regarding these conditions may arise, save when a legal exception applies.

Children's Data

We do not knowingly process children's data, unless specifically stated in this Privacy Policy. If you have concerns about or knowledge of a child using our services, products, websites or apps without parental consent, please contact our DPO via mstuartflood@gmail.com to ensure we can take appropriate action as soon as possible.

Contact

For questions about this privacy policy, product information or information about the website itself, please contact: compliance@codara.co.uk.

International data transfers

Third Party Applications

Naq Cyber

Third party headquarter address	Vlamingstraat 4, 2712BZ, Zoetermeer, The Netherlands
The primary location of processing is the The Netherlands.	Personal data collected by Naq Cyber may be stored and processed in any country where Naq Cyber or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and The Netherlands
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Naq Cyber's Privacy Policy	https://www.naqcyber.com/policies/privacy-policy

Ionos

Third party headquarter address	2 Logan Square 100 N 18th St, Ste 400, Philadelphia, PA 19103, United States of America
The primary location of processing is the United States of America.	Personal data collected by Ionos may be stored and processed in any country where Ionos or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible

For more information, see Ionos's Privacy Policy	https://www.ionos.com/terms-gtc/privacy-policy/

Github

Third party headquarter address	88 Colin P. Kelly Jr. Street, San Francisco, CA 94107, United States of America
The primary location of processing is the United States of America.	Personal data collected by Github may be stored and processed in any country where Github or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Github's Privacy Policy	https://docs.github.com/en/github/site-policy/github-privacy-statement

Jira (Atlassian)

Third party headquarter address	Level 6, 341 George Street, Sydney, Australia
The primary location of processing is the Australia.	Personal data collected by Jira (Atlassian) may be stored and processed in any country where Jira (Atlassian) or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Jira (Atlassian)'s Privacy Policy	https://www.atlassian.com/legal/privacy-policy

Confluence

Third party headquarter address	Level 6, 341 George Street, Sydney, Australia
The primary location of processing is the Australia.	Personal data collected by Confluence may be stored and processed in any country where Confluence or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Confluence's Privacy Policy	https://www.atlassian.com/legal/privacy-policy

Claude

Third party headquarter address	1600 Amphitheatre Parkway in Mountain View, California, United States of America
The primary location of processing is the United States of America.	Personal data collected by Claude may be stored and processed in any country where Claude or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Claude's Privacy Policy	https://policies.google.com/privacy

Google Workspace

Third party headquarter address	1602 Amphitheatre Parkway, Mountain View, CA, 94043, United States of America

The primary location of processing is the United States of America.	Personal data collected by Google Workspace may be stored and processed in any country where Google Workspace or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Google Workspace's Privacy Policy	https://policies.google.com/privacy?hl=en-US

NordVPN

Third party headquarter address	PH F&F TOWER, 50th Street & 56th Street, Suite #32-D, Floor 32, Panama City, Panama
The primary location of processing is the Panama.	Personal data collected by NordVPN may be stored and processed in any country where NordVPN or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see NordVPN's Privacy Policy	https://my.nordaccount.com/legal/privacy-policy/

NordPass

Third party headquarter address	PH F&F TOWER, 50th Street & 56th Street, Suite #32-D, Floor 32, Panama City, Panama

The primary location of processing is the Panama.	Personal data collected by NordPass may be stored and processed in any country where NordPass or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see NordPass's Privacy Policy	https://my.nordaccount.com/legal/privacy-policy/nordpass/

Google Cloud

Third party headquarter address	1602 Amphitheatre Parkway, Mountain View, CA 94043, United States of America
The primary location of processing is the United States of America.	Personal data collected by Google Cloud may be stored and processed in any country where Google Cloud or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Google Cloud's Privacy Policy	https://cloud.google.com/privacy

App Store

Third party headquarter address	Apple Inc. One Apple Park Way, Cupertino, California, 95014, United States of America

The primary location of processing is the United States of America.	Personal data collected by App Store may be stored and processed in any country where App Store or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see App Store's Privacy Policy	https://www.apple.com/uk/legal/privacy/en-ww/

Slack

Third party headquarter address	Salesforce Tower, 60 R801, North Dock, Dublin, Ireland
The primary location of processing is the Ireland.	Personal data collected by Slack may be stored and processed in any country where Slack or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and Ireland
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Slack's Privacy Policy	https://slack.com/intl/en-nl/trust/privacy/privacy-policy

Suppliers