Clarion by TraCarta

# Security and trust pack

How Clarion keeps your GST data safe. Prepared 16 Nov 2026.

TraCarta India Private Limited, Gurugram, Haryana

## At a glance

### Your data stays in India

Clarion runs on Microsoft Azure in Pune, with backups in a second Indian region. Files live in TraCarta's Microsoft 365.

### Locked down at every step

Encrypted in transit and at rest. Every sign-in needs a password and a one-time code.

### Only the right people

Each client sees only its own data. TraCarta staff see only the clients they work on. Everything is logged.

### Yours to take or delete

Download everything at any time. Ask us to delete it and you get a signed certificate.

## ISO 27001

Clarion's security programme is built on the ISO/IEC 27001:2022 framework, and our policies and controls are mapped to its requirements. Clarion runs and stores files on Microsoft Azure and Microsoft 365, which are independently certified to ISO 27001, ISO 27018 and SOC 2.

## Security controls

### Where your data lives

- Clarion runs on Microsoft Azure in the Central India region (Pune). The database and app never leave India.
- Automatic daily backups, with point-in-time restore, are copied to a second Indian region.
- Airline invoices, credit notes and reports are stored in TraCarta's Microsoft 365 (SharePoint), not on personal devices or shared drives.

### Encryption

- All traffic uses HTTPS (TLS 1.2 or newer). Plain HTTP is turned away.

- The database, backups and stored files are encrypted at rest (AES-256) by Microsoft.
- Passwords are never stored. We keep only a one-way scrambled form (scrypt) that can't be turned back into the password.
- Passwords, keys and connection details sit in Azure Key Vault, never in the code.

### Signing in

- Two-step sign-in for everyone: password plus a 6-digit code sent by email. It can't be switched off.
- TraCarta staff sign in with their Microsoft work accounts and Microsoft's own two-step check. When someone leaves TraCarta, switching off their account locks them out at once.
- Sessions end after a period of no activity, and you can see and end every signed-in browser.
- We email you when your account is used from a browser we haven't seen before.
- Your Client Admin can limit sign-in to your office or VPN addresses, shorten the sign-out time, and restrict invites to your company's email domains.

### Who can see what

- Each client's data is kept apart. Every screen, download and API call checks who is asking before showing anything.
- Client Admins decide which companies each team member sees.
- TraCarta staff only see the clients they're assigned to. Only a few named TraCarta Admins see everything.
- API keys can only read data, never change it. Each key can be limited to certain data, certain addresses and an end date.

### Files and uploads

- Uploads are checked for file type and size before they're accepted.
- Microsoft 365 scans stored files for viruses, and downloading a file found to be infected is blocked.
- Download links work only for signed-in people who are allowed to see the file.

### Watching and testing

- Every sign-in, upload, download and change is written to an audit log that can't be edited. Client Admins can see and download their company's log.
- Cloudflare sits in front of Clarion and blocks common attacks and floods of traffic.
- We're alerted automatically if Clarion slows down, shows errors or goes offline.
- Every release passes automatic security and access checks first, and we run security scans before major releases. An independent penetration test can be arranged for clients who need one.

### People and process

- Everyone at TraCarta signs a confidentiality agreement and gets access only to what their job needs.
- Access is reviewed every quarter and removed the day someone leaves.
- Changes to Clarion are reviewed, tested on a separate copy, and can be rolled back in minutes.

## Policies

### Incident response and breach notice

What we do if something goes wrong, and how fast you hear about it.

- Anyone at TraCarta who suspects a security problem reports it straight away to the incident lead.
- We contain it first (for example, block access or turn off keys), then find the cause and fix it.
- If your data may be affected, we tell your named contacts without delay, and in any case within 72 hours, with what happened, what data is involved and what we're doing.
- We report to CERT-In within 6 hours where Indian rules require it, and to the Data Protection Board as the DPDP Rules require.
- After every incident we write down what we learned and what we changed.

### Business continuity and backups

How Clarion keeps running, and how quickly we recover.

- The database is backed up automatically every day and can be restored to any moment in the last 7 days or more.
- Backups are kept in a second Indian region in case a whole Azure region has a problem.
- Recovery point: at most 1 hour of changes could be lost in a serious failure; usually it's minutes.
- Recovery time: Clarion is back within 4 hours for most failures, and within 24 hours if a whole region fails.
- We test a full restore from backup every quarter.

### Access control

Who at TraCarta can reach your data, and how that's kept tight.

- People get access only to the clients and tools their job needs.
- Admin access to Azure and Microsoft 365 needs Microsoft two-step sign-in and is limited to named people.
- Access is reviewed every quarter and removed on someone's last day.
- No shared accounts. Every action is tied to a named person in the audit log.

### Data retention and deletion

How long we keep data, and how it's deleted.

- We keep your data for as long as you use Clarion, and for the records period you agree with us.
- When you leave, you can download everything first. We then delete your data within 30 days and send a signed deletion certificate.
- Backups containing your data expire on their normal cycle (within 35 days) and aren't restored for any other purpose.
- We keep only what the law makes us keep, such as our own invoices to you.

### Change management

How we change Clarion without putting your data at risk.

- Every change is recorded in version control and checked by a second person or automatic review.

- Automatic tests, including security and access checks, run before anything goes live.
- Changes go to a separate test copy first, then to the live Clarion.
- If a release causes a problem, we switch back to the previous version in minutes.

## Outside services (sub-processors)

| Service | What it does | Where | Data |
|---|---|---|---|
| Microsoft Azure | Runs the Clarion app, database and backups | India (Pune; backups in a second Indian region) | All Clarion data |
| Microsoft 365 | Stores invoices, reports and uploads (SharePoint); sends Clarion emails | India | Files; names and email addresses of people who get emails |
| Cloudflare | Protects Clarion from attacks and speeds up page loading | Global network; doesn't store Clarion data | Web traffic passing through, encrypted |
| GitHub | Keeps Clarion's program code and runs automatic tests | United States | Program code only. No client data |

## Privacy (India's DPDP Act)

### Who we are

- Clarion is run by TraCarta India Private Limited ("TraCarta"). For invoice data in Clarion, your company decides what is processed and TraCarta processes it on your company's behalf (TraCarta is the "data processor"). For your own Clarion account (name, email, phone, sign-in records), TraCarta is responsible for it.

### What we collect

- Your account: name, work email, phone number (optional) and role.
- Sign-in records: when you signed in, IP address and browser, to keep your account safe.
- Invoice data your company or its travel agent shares: airline invoices, GST details and, where present, passenger names.

### Why we use it

- To provide Clarion: show your data and documents, send sign-in codes and alerts, and keep the service secure.
- We never sell personal data or use it for advertising.

### How long we keep it

- For as long as your company uses Clarion and for the records period agreed with your company, then it's deleted. Sign-in records are kept for up to 2 years.

### Your rights

- Ask what personal data we hold about you, and get it corrected or deleted.
- Withdraw consent where we rely on it, and nominate someone to act for you.
- Raise a complaint with our Grievance Officer. If you're not satisfied, you can complain to the Data

Protection Board of India.

### Grievance Officer

- Shefali Kapoor, Grievance Officer, TraCarta India Private Limited. Email: shefali.kapoor@tracarta.in. We reply within 7 working days and resolve complaints within 30 days.
- For anything else: support@tracarta.com.

## Common questions

### Where is our data stored?

In India. Clarion runs on Microsoft Azure in Pune, with backups in a second Indian region. Files are kept in TraCarta's Microsoft 365.

### Is our data encrypted?

Yes. Everything travels over HTTPS, and the database, backups and files are encrypted at rest by Microsoft.

### Who at TraCarta can see our data?

Only the TraCarta team members assigned to your account, plus a small number of named admins. Every view and download is in the audit log, which your Client Admin can see.

### Can other Clarion clients see our data?

No. Every page, download and API call checks which client is asking before showing anything.

### Is personal data involved?

A little: passenger names on airline invoices. We use it only to provide Clarion, never for marketing, and never sell it. Your Clarion users' account details are covered by our privacy notice.

### Do you comply with India's DPDP Act?

Yes. We act as your data processor for invoice data, follow your instructions, keep data in India, help with rights requests and report breaches promptly. Our Grievance Officer is named in the privacy notice.

### How does Clarion approach ISO 27001?

Our security programme is built on the ISO 27001 framework, and our policies are mapped to its controls. Clarion runs on Microsoft Azure and Microsoft 365, which are independently certified to ISO 27001. We're happy to share our policies and answer your security questionnaire.

### Do you have a penetration test report?

We run automatic security checks on every release and security scans before major releases. If your policy needs an independent penetration test, we can arrange one and share the summary.

### Can we restrict access to our office network?

Yes. Your Client Admin can list your office or VPN addresses in Settings -> Security rules. Sign-in from anywhere else is blocked.

### Do you support single sign-on (Microsoft or Google)?

On request. Tell us, and we'll connect Clarion to your Microsoft Entra ID or Google Workspace.

### What happens to our data if we leave?

Download everything in one go, then ask for deletion. We delete it within 30 days and send a signed certificate.

### Will you sign our DPA or security questionnaire?

Yes. Accept our DPA online, or download it pre-signed. If you have your own DPA, send it and we'll review it. For questionnaires, most answers are in this Trust Centre and the trust pack. We're happy to fill in the rest.

## Documents and contacts

- Data Processing Agreement version 1.0 (13 Nov 2026): accept online in Clarion (Settings -> Data and privacy) or download it pre-signed from the Trust Centre.
- Security questions: support@tracarta.com, +91 98106 81799 (Monday to Friday, 9:30 am to 6:30 pm).
- Grievance Officer: Shefali Kapoor, shefali.kapoor@tracarta.in.