Clarion by TraCarta

Data Processing Agreement

Version 1.0, 13 Nov 2026

TraCarta India Private Limited, Gurugram, Haryana

1. Parties and purpose

- This Data Processing Agreement ("DPA") is between the client named below ("Client") and TraCarta India Private Limited ("TraCarta"). It forms part of the agreement under which TraCarta provides Clarion and related GST reconciliation services ("Services").

2. Roles

- For personal data in the Services, the Client is the Data Fiduciary and TraCarta is the Data Processor, as those terms are used in India's Digital Personal Data Protection Act, 2023 and its Rules ("DPDP law").

3. Instructions

- TraCarta processes personal data only to provide the Services and on the Client's documented instructions, including this DPA and the Client's use of Clarion. TraCarta tells the Client if it believes an instruction breaks the law.

4. Confidentiality

- TraCarta ensures everyone who can access the personal data is bound by confidentiality and accesses only what they need.

5. Security

- TraCarta keeps appropriate technical and organisational security measures, including those in Annexure B, and does not reduce their overall level during the term.

6. Outside services (sub-processors)

- The Client approves the sub-processors in Annexure C. TraCarta gives at least 30 days' notice of any new sub-processor; the Client may object on reasonable grounds. TraCarta holds each sub-processor to data protection terms at least as protective as this DPA and remains responsible for them.

7. Data location

- Personal data is stored and processed in India. TraCarta will not move it outside India without the Client's written approval, except where Annexure C says so.

8. Personal data breaches

- TraCarta notifies the Client without undue delay, and within 72 hours of becoming aware, of any breach affecting the Client's personal data, with the information the Client needs to meet its own obligations and helps the Client respond.

9. Help with rights and requests

- TraCarta helps the Client respond to requests from individuals (access, correction, erasure, grievances) and to the Data Protection Board and passes on any request it receives directly.

10. Return and deletion

- When the Services end, the Client can export all its data. TraCarta then deletes the Client's personal data within 30 days, except where the law requires it to keep some, and gives the Client a written deletion certificate.

11. Audits

- TraCarta makes available its Trust Centre, trust pack and policies, and answers reasonable security questions. Once a year, on 30 days' notice, the Client may audit TraCarta's compliance with this DPA at its own cost, in a way that protects other clients' confidentiality.

12. General

- Liability under this DPA follows the main agreement. If this DPA conflicts with the main agreement on personal data, this DPA applies. Indian law governs this DPA and the courts at Gurugram, Haryana have jurisdiction.

Annexure A. Data processed

- Purpose: GST input tax credit reconciliation of airline invoices, and access to invoices, data and reports through Clarion.
- People concerned: the Client's employees who travel (passengers).
- Personal data: passenger names on airline invoices.
- No sensitive categories of personal data are needed for the Services.
- Duration: the term of the Services, then deletion as in clause 10.

Annexure B. Security measures

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.

Annexure C. Approved 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

Signatures

For TraCarta India Private Limited

Ashish Kumar

Signature (signed electronically)

Ashish Kumar
Name

Founder and Director
Designation

13 Nov 2026
Date

For the Client

Signature (or digital signature)

Name

Designation

Company (legal name)

Date and place

To sign: fill in the boxes above (or print), sign, and upload the signed copy in Clarion under Settings -> Data and privacy, or email it to TraCarta. A digital signature (DSC) is welcome.