

Here's a clear summary of your recorded conversation, broken down by your requested points:

1. What is the main function of the application?

The application is a new API management platform built using Apigee. It includes:

A Management Plane – where developers configure APIs, apply security rules, and manage endpoints.

A Gateway – handles API traffic.

A Developer Portal – where external partners register to access APIs.

This platform provides full lifecycle API management and partner onboarding.

2. What is the intention of the project?

The project is a greenfield (built-from-scratch) initiative, not a migration from on-premises.

It's aimed at consolidating and modernizing API management.

It adds capabilities (especially the Developer Portal) that were not present in older stacks like Azure API Management (APM) and Envoy.

3. Is there a move to cloud?

Yes, the platform is cloud-native, hosted in Google Cloud (GCP).

Though there isn't an existing CPAP (Cloud Program Access Point), they are planning to get a cloud governance record (GCC/GDCC).

It's being tracked under the Horizon One program for cloud deployment alignment.

4. What is the impact to data?

No internal employee data is stored. SSO is used for internal access.

For external users (vendors or partners):

Their name, email, phone number, and country are collected.

Their business information is captured: legal name, business type, address, website, description, and Line of Business (LOB) they engage with.

Geolocation filters (e.g. blacklisted countries) are enforced.

Their email acts as user ID — they don't create it manually.

No sensitive personal data (like SIN, DOB, etc.) is collected.

5. What type of data is captured (categories)?

Two primary categories of data:

A. External user identity & business info:

First name, last name, email

Phone number

Country (for access control)

Legal business name

Address details (city, postal code, etc.)

Business website and description

B. API configuration data:

Hosted on the Management Plane

Includes:

API endpoint URLs (e.g. <https://amcb.td.tdapi.com>)

Deployment and environment config (e.g., gateway destination, F5 URLs)

No raw customer data or payload content is stored here

6. Data Retention & Disposition

Not extensively discussed in this recording.

However, a Data Impact Assessment (DIA) is being prepared, with reference to:

Multiple malcodes (internal system IDs)

Corresponding DBoR records (Data Book of Record) to identify what each component stores and for how long

A full retention and disposition plan will be defined in that DIA form submission

Would you like me to help you draft a clean 1-paragraph summary or executive bullet points for a report or DIA form?