Service Description

NTT AI Communications Gateway

01 February 2026| Document Version 1.0

Contents

List of abbreviations

Abbreviation	Meaning
CLI	Calling Line Identifier: The phone number used by a calling party using the PSTN
Contract	Means the agreement concluded between NTT and Client pursuant to which NTT provides Client with the Services described in this Service Description
Client	Means the Party contracting with NTT for purchasing the Service(s) described in this Service Description
Contact-Center	Means a communications platform managing the distribution of communications flows towards human-agents
Datacenter	A Datacenter is a facility used to house computer systems and associated components, such as telecommunications and storage systems
DDI	Stands for “Direct Dial In” and means the PSTN E.164 numbers as supplied by NTT as part of its Calling Plans Service
IAM	Stands for “Identity and Access Management” and it meant to ensure that the right people, machines, and software components access the right resources at the right time.
IDP	Stands for Identity Provider and is an entity that creates, maintains, and manages identity information
Key Performance Indicators (KPI)	Means a quantifiable measure used to evaluate the success of the Services
PSTN	Public Switched Telephone Network
Scheduled Maintenance Window	Maintenance operations scheduled in advance by NTT to implement a specific change on the NTT infrastructure.
Service-Desk	Service-Desk means a single point of contact (SPOC) for communication between NTT and its clients and business partners.
Service Number	Means a phone number from a national PSTN numbering plan meant to be assigned to a CX/Contact-Center application
SIP	Means “Session Initiation Protocol” and is a signaling protocol used for initiating, maintaining, and terminating real-time sessions
SKU	Stands for Stock Keeping Unit and is a distinct type of item for sale
Tenant	A Tenant is a group of Users who share a common access with specific privileges.
User	Means a Client’s customer, partner or another person making calls into the AI Communications Gateway. This is sometimes referred to as “end-User”.
WAN	Wide Area Network is a telecommunications network that extends over a large geographic area for the primary purpose of computer networking.

Document history

Issue	Date	Comments
1.0	February 1st, 2026	Initial document

1. Introduction to NTT DATA AI Communications Gateway

The purpose of this document is to provide a clear description of the NTT DATA AI Communications Gateway service offering for Clients having subscribed to our services.

NTT DATA's AI Communications Gateway service is designed to seamlessly integrate advanced Agentic Artificial Intelligence constructs with communication channels used by human beings, such as Voice.

This service is powered by NTT DATA long-standing Cloud Voice expertise and is hosted in NTT DATA's Cloud environment. and fronted by sub-agents deployed within customer ecosystems.

2. AI Communications Gateway components

The AI Communications Gateway is made of several components so as to properly orchestrate communications between human-beings and Agentic AI ecosystems.

2.1. AI Communications Agents

NTT DATA AI Communications Gateway is leveraging a central entity called AI Communications Agents.

AI Communications Agents can be created and managed live on NTT DATA portal. All agents created are solely made available to Client and several different functions are offered to customize, specialize and integrate these agents with Client's agentic ecosystem.

NTT AI Communications Agents primarily leverage language-models to interact with human-beings. NTT AI Communications Gateway offers a set of predefined options for this, depending on what type of interactions is expected for end-users.

2.1.1 NTT-provided language-models

The language-model deployment uses the global infrastructure of NTT to dynamically route customer traffic to NTT provided latest and evergreen models.

This delivers the best availability for the customer's inference requests. This option comes with additional features to further customize the language-model so as to better handle human interactions.

2.2. Client AI Tools

2.2.1 Description

Client AI Tools are designating the network of AI agents and other Information Systems implemented and operating within the Client's ecosystem. These AI Tools are seamlessly and securely connected to Client's AI Communications Agents, ensuring synchronized operations and unified data flow. The sub-agents can be tailored to meet specific business needs and integrate with existing systems, providing a robust and versatile AI solution.

2.2.2 Agentic protocols available

Client AI Tools must be compatible with the below protocols for integration with AI Communications agents:

- Copilot Studio Direct Line
- Agent-to-Agent (A2A)
- Model Context Protocol (MCP)

Integration between AI Tools and AI Communications Agents is secured via authentication methods such as oAuth2 and agentic conversations are fully encrypted.

2.3. Communication Channels

NTT DATA AI Communications Agents can be configured with several types of Communications Channels for human being to communicate.

2.3.1 NTT Cloud Voice Phone Numbers

Accessing NTT DATA AI Communications Agents is simplified through NTT DATA Cloud Voice DDIs, covering most countries with different number types.

These Direct Dial-In numbers allow end-users to easily call in, or be called into, and communicate via natural voice language.

2.3.2 NTT Cloud Voice BYON

Alternatively, Client can elect to bring some of its existing phone numbers to the AI Communications Gateway via leveraging NTT Cloud Voice's Bring Your Own Numbers solution.

2.4. Agent-Assist functions

2.4.1 Contextual Handoff to Human Agents

NTT DATA's AI Communications Gateway is designed to permit the transfer of a conversation to a human agent, in case the end-to-end automation of delivering the expected output from the Agentic AI construct was not possible.

The solution ensures that the human agent receives a comprehensive summary of the conversation, a sentiment analysis score, and suggested next step.

The Agent Assist feature in AI Communications Gateway integrates seamlessly with leading Contact-Center platforms to enhance agent-assisted conversations with AI-driven conversation insights.

During the call flow between AI Communications Gateway and the caller, the system securely connects to the NTT DATA AI platform to retrieve real-time insights, including a call summary and customer sentiment.

A unique interaction ID is automatically generated, captured, and used to track the call.

Before the call is delivered to a human agent, these insights are attached to the interaction and displayed directly on the agent's desktop as a screen pop. This ensures the agent has immediate context about the customer and the conversation.

The call is then routed to the appropriate available agent, enabling faster understanding, Detailed conversation insights, and improved customer experience.

The summary encapsulates key points discussed, providing the human agent with the necessary context to continue the interaction effectively.

The sentiment analysis score offers insights into the customer's emotional state, enabling the human agent to tailor their approach accordingly.

The next step outlines the immediate action required, ensuring a smooth and efficient resolution to the customer's query.

The solution relies on a webservice and requires a conversation ID. It is supported by the below Contact-Center solutions:

- Genesys Cloud
- Nice CX one
- Microsoft Dynamics Contact-Center

2.5. End-user authentication

As AI agents can respond to several queries or manage process automation that requires user authentication, our NTT DATA AI Communications Gateway can leverage authentication tools.

NTT DATA AI Communications Gateway provides a flexible and secure framework for agent-assisted authentication, offering multiple login paths, including device-based URL and code entry, app or web-generated numeric codes, and streamlined push-based approval. End-user authentication can also leverage SMS delivery when supported by the customer’s Identity Provider (IDP).

The solution is designed to adapt to each customer’s existing IDP platform and its authentication capabilities, ensuring seamless integration with both standards-based flows and vendor-specific mechanisms.

Connectivity is established through MCP or A2A protocols, which are expected to already exist within the customer’s environment. Depending on how these protocols are currently implemented, some targeted development or customization may be required to support particular use cases or IDP-specific behaviors.

Because IDP setups can vary significantly - including differences in code delivery methods, security controls, and authentication journeys - the solution remains intentionally flexible while maintaining strong security and a practical, user-friendly experience that aligns with each customer’s identity ecosystem.

2.6. NTT DATA AI Communications App

NTT DATA AI Communications App permits to configure and manage the AI Communications Gateway components and offers the following features:

- AI Communications Agents instantiation and management
- Client’s AI Tools connection and performance observation
- Communication channels ordering and management
- Settings for orchestrating the interactions between Agentic AI constructs and human beings

3. Service Operations

3.1. Service Management

Support for Customer's own AI Agents is not included when the Customer only subscribes to the AI Communications Gateway product. The scope of the support provided as part of Agentic AI Communications is limited to the elements under NTT DATA' control.

3.2. Global Integrated Operations Centre (GIOC) service-desk

The NTT DATA Global Integrated Operations offers English language support on a 24hours/365 days basis.

The NTT DATA Global Integrated Operations Centre is responsible for:

- Being the first point of contact for Customer Authorized Administrator
- Tracking, managing and completing Services and Incident Requests
- Responding to phone calls and service portal requests
- Manage requests with other vendors and internal escalation teams.

N.B. Service requests and incidents must be raised by a Customer Authorized Administrator.
Customer Authorized Administrators are one or more named individuals or a named Service Desk that are authorized to log cases to NTT DATA.

3.3. High Availability

NTT DATA has designed the AI Communications Gateway to be highly available, with the ability to use one of multiple regions within the underlying cloud to provide services. The hosting application for the AI communications agents is able to connect to instances of large-language model resources within a region, and across multiple regions, and if the targeted resource becomes unavailable it will connect to an alternate resource. If this happens during an interaction with an end-user or customer, it can resume the interaction without losing context.
Similarly, the underlying data stores are replicated in multiple regions so that if an entire region becomes unavailable, the application re-connects to an alternate replica of the data source in an adjacent region.

3.4. Service Monitoring

NTT DATA AI Communications Gateway is monitored 24x7 by our NOC team who have visibility of dashboards and real-time alerts and telemetry covering the components and micro-services which make up the service. This enables NTT DATA to efficiently diagnose, respond and escalate issues to internet teams or external providers as needed, and invoke the Incident Management process if required.

3.5. Incident Management

Incidents are defined as "unplanned interruption to service or reduction in the quality of service provided".
When it comes to the AI Communications Gateway Product, the below specifics apply.

3.5.1 Incident priority definition

Incidents are prioritized according to the matrix table below:

	Large scale	Medium scale	Small scale
High impact	P1	P1	P3
Medium impact	P2	P2	P3

Low impact	P2	P3	P3

Request for Information (RFI) are classified as P4

Large scale: Entire Site impacted / Several groups of end-users. A site is a company business office.
Medium scale: Group of several end-users. Can be a business department, a site floor, several users in different sites.
Small scale: A couple of users or Remote Workers.

High impact: Service not available (i.e. no calling / one-way audio / Communications Agent not responding)
Medium impact: Service partially available (i.e. Unable to reach some tools, some calls are failing, contextual hand-off not working, etc.)
Low impact: Poor service quality (i.e. Voice quality is not good, Observability statistics are not ideal, etc.)

3.5.2 Incident handling matrix

Incident handling is defined according to the matrix table below:

Incident Priority	Response Target (Auto)	Ticket Status Update	Time to Restore
P1	15 mins	2 Hours	4 Hours
P2	30 Mins	4 Hours	12 Hours
P3	4 Hours	24 Hours	72 Hours
P4	N/A	N/A	N/A

3.6. Monthly Service Availability Service Level Agreement (SLA)

3.6.1 Description

NTT DATA AI Communications Gateway Monthly Service Availability SLA applies from within AI Communications service boundaries (notably the NTT DATA AI Gateway clusters).

Monthly Service Availability is computed using the following formula:

MSA = (Total Monthly Minutes – Valid Downtime)/Total Monthly Minutes

Valid downtime includes, and is limited to the below events:

- End-users are unable to communicate with the AI Communications Gateway
- Calls cannot be handed over to human agents

Valid Downtime excludes downtime linked to Standard, Emergency and Scheduled Maintenance Windows. Downtime linked to these events shall be excluded from the calculation of the Monthly Service Objectives.

Downtime starts from the point at which a relevant priority incident is logged to the Service-Desk and ends when Client is notified that the incident has been resolved.

3.6.2 Scope

The Monthly Service Availability is calculated on a per tenant basis.

For example, should the service become unavailable for 100 minutes, then 100 minutes would be counted as Valid Downtime and withdrawn from the Total Monthly Minutes of 43 920 x 10 = 439 200 minutes.

Resulting MSA would be 99.98%.

3.7. Patch Management

The NTT DATA AI Communications Gateway uses several different technologies for patch management, utilizing the tools which are best suited for the different components of the infrastructure. In all cases, NTT DATA uses industry standard best patching processes with centralized control, automation, monitoring and management over the patching process to ensure that critical patches are completed in a timely fashion and in a process that is not service impacting. This management includes the normal vendor specific patching cadence, as well as the ability to quickly respond to security or zero-day patches in a time sensitive and critical manner.

3.8. Vulnerability Management

NTT DATA maintains a robust vulnerability management program designed to proactively identify and address security risks through ongoing monitoring with a mix of industry-standard and proprietary tools, combined with automated and manual penetration testing, secure software assessments, and third-party evaluations. Servers are equipped with mandatory vulnerability management tooling, with vulnerabilities reported centrally, and tracked for remediation, prioritized according to the assessed criticality. Platforms are regularly penetration tested, with findings assessed and prioritized and tracked for remediation.

3.9. Malware Prevention

Successful malware incursions can result in unauthorized access, sensitive data exfiltration, and broader network infiltration. NTT DATA deploys mandatory endpoint detection and response (EDR) tooling on server and workstation platforms, capable of detecting malware or ransomware, credential attacks, suspicious script or command executions and other behaviors. Detections are followed up in real time by NTT DATA's centralized security incident management team, who can remotely isolate devices, disconnecting them from the wider network, while also analyzing and stopping suspected malicious processes, collecting forensic artifacts, and applying wider blocks on suspected compromised remote addresses, executables, or behaviors. This tooling is supported by comprehensive mandatory staff training in addressing phishing, social engineering and other human attacks.

4. Security and data protection

NTT DATA’s AI Communications Gateway is fully featured with state-of-the-art Security and Fraud Management systems to protect our clients against cyberattacks, data security, privacy and access security risks. NTT DATA is committed to be proactively aligning with best practices in the field of security and data protection.

4.1. Multi-Cloud integrations principles

NTT AI Communications Gateway is a cloud-based interface connecting clients' cloud and on-premises platforms with security, data protection, and strict regulatory compliance as top priorities.
By leveraging advanced hyperscalers’ technologies, it provides highly scalable, standardized solutions with ongoing security updates and robust adherence to compliance frameworks.
The NTT DATA SaaS model ensures enterprise-level security, resilience, comprehensive compliance certifications, lower costs, greater scalability, and continuous innovation for clients - demonstrating NTT's ongoing commitment to meeting and exceeding industry regulations and standards.

4.2. Certifications and audits

NTT DATA is committed to be proactively aligning with best practices in the field of security and data protection.

4.2.1 Certifications

NTT DATA has been granted the certifications below:

- ISO27001
- ISO27701

4.2.2 Regulatory compliance

The NTT AI Communications Gateway is developed and operated in full compliance with the EU Artificial Intelligence Act and the General Data Protection Regulation (GDPR). It embodies a strong governance framework grounded in transparency, accountability, and ethical AI principles. All data processing adheres to privacy-by-design and privacy-by-default standards, ensuring secure, lawful, and responsible handling of information. Data storage and, where applicable, cross-border transfers are performed exclusively under GDPR-approved safeguards and EU adequacy mechanisms.

4.2.3 Security frameworks

The security posture aligns with the NIST, Cybersecurity Framework (CSF) and the Center for Internet Security (CIS).

4.2.4 Third-party assessments

NTT DATA has implemented processes designed to assess vendors, subcontractors and business partners involved in the provision of NTT AI Communications Gateway. These processes include risk-based reviews relating to data protection and privacy, information security, sanctions and restricted-party screening, and relevant regulatory considerations, including using recognized compliance and privacy management tools such as OneTrust. Third parties are selected and engaged based on their ability to meet applicable legal and regulatory requirements and NTT DATA’s internal standards, and, where applicable, are subject to a Data Processing Agreement governing the processing of personal data. Appropriate contractual provisions are used to support ongoing compliance. NTT DATA periodically reviews its third-party assessment practices in light of evolving legal, regulatory and risk considerations.

A Data Processing Agreement is always set up between NTT DATA and its third parties.

4.3. Identity, Authentication and Access management

NTT DATA implements a comprehensive Identity and Access Management (IAM) framework to ensure that all access to systems and services is secure, auditable, and appropriate to user roles and responsibilities. Access controls are granular and extend beyond standard Multi-Factor Authentication (MFA), aligning with enterprise security and compliance requirements.

4.3.1 Identity Management

NTT Internal (Employee) Access

- Employee identities are managed within the Global IDP environment, which governs authentication for all NTT DATA internal users.
- Internal users authenticate via Single Sign-On (SSO) and Multi-Factor Authentication (MFA) to access corporate portals and operational tools such as the Operator Portal.
- Access is provisioned following the principle of least privilege, ensuring users receive only the permissions required for their specific roles, such as system administrators, developers, or operations engineers.
- All internal access activities are governed by NTT DATA's enterprise wide IAM policies, supported by continuous monitoring, periodic access reviews, and audit logging to maintain compliance and traceability.

Customer and Partner Access

- External identities, including customers, guests, and partners, are managed within the Global IDP environment.
- The environment supports federated accounts through IDP federation, enabling customers to authenticate using their own enterprise identity providers.
- Non-federated accounts, created directly in IDP Portal, for users without an existing federated identity.

4.3.2 Access Controls

NTT DATA employs a comprehensive access control framework to ensure that all interactions with the Agentic Communications Management Solution are secure, auditable, and aligned with the principle of least privilege. The access model leverages IDP for centralized identity and access management, integrating both employee and external customer identities under a unified, federated architecture.

Role-Based Access Control (RBAC)

Customers can define and manage Role Based profiles within NTT DATA Services Portal, tailoring permissions to align with their specific organizational roles and operational needs. This ensures that access rights correspond precisely to job responsibilities, minimizing unnecessary privilege exposure.

The AI Communications Gateway solution offers the following roles:

- IT Admin

Federated and Non-Federated Identity Support

The environment supports both federated identities (via IDP Federation) and non-federated IDP -managed accounts. This dual model allows clients, partners, and guests to authenticate seamlessly through their existing enterprise identity providers, while still supporting direct Okta user account creation where required.

Continuous Authorization and Zero Trust Enforcement

Access validation is not limited to initial authentication events. Every request, whether user initiated or system-generated is authenticated and authorized in real time, reinforcing NTT DATA's Zero Trust Security Model. This continuous verification enhances operational resilience, ensuring that trust is never assumed but always verified.

Auditability and Compliance

All identity and access events are fully auditable within the Okta environment. Logs are retained and monitored to support compliance with internal governance frameworks and external regulatory requirements.

N.B. For some existing NTT DATA customers, an upgrade path to MFA is available if not already in place.

4.3.3 Enterprise Integration

NTT DATA delivers a comprehensive Identity and Access Management framework designed to provide secure, scalable, and automated user access across the AI Communications platform. Leveraging IAM architecture, this framework supports both internal enterprise users and external customer ecosystems, including partners, clients, and guest users, under a unified governance model.

Federated Authentication

NTT DATA implements federated identity through open standards such as SAML 2.0, OAuth 2.0, and OpenID Connect. This enables seamless Single Sign-On (SSO) for users authenticating into various portals. Federated identity allows both internal (employee) and external (customer or partner) accounts to authenticate securely via trusted identity providers.

Enterprise Directory Integration

The platform integrates natively with enterprise-grade identity providers, including Okta, Microsoft Azure Entra ID, Ping Identity, and Google Workspace. This facilitates centralized authentication, directory synchronization, and role-based access control across NTT DATA's internal organization and external customer tenants.

Automated User Lifecycle Management

Through System for Cross domain Identity Management based integrations, NTT DATA automates the end-to-end lifecycle of user accounts. Provisioning, role assignments, and deprovisioning are triggered automatically ensuring users gain the right access at the right time without manual intervention.

Real-Time Access Revocation

The IAM framework enforces real-time account deactivation across all integrated applications. When a user's role changes or their affiliation ends (e.g., termination of employment or customer Contract), access is immediately revoked through identity orchestration, minimizing exposure to unauthorized access.

4.3.4 Customer Transparency & Control

The platform provides extensive audit logging, recording all access events to resources with granular details on identity, time, and origin, thus enabling operational oversight and regulatory alignment. Data protection and privacy policies

NTT DATA is committed to ensuring that Client's data security and privacy is in Client's hands, not just NTT.

4.3.5 Encryption by default

NTT DATA enforces encryption across all layers of the AI Agent architecture to protect data both in transit and at rest.

At Rest: The data processed and stored by the AI model is encrypted using the AES-256 standard (256-bit key, 128-bit block size), ensuring robust protection of stored information. Data is encrypted either at the application layer, storage device layer, or in some cases, at both levels.

In Transit: Communications are secured using Transport Layer Security (TLS), supporting TLS 1.2+. All sessions include SSL certificate exchange to verify authenticity and maintain secure channel establishment during login, providing robust protection for data in transit.

Authentication mode: Encrypted credentials (login/password) and SSL Certificate are used to validate user identity and further strengthen session security.

4.3.6 Data Minimization & Classification

Data is securely stored within NTT-managed environments and remains visible to the customer through authorized interfaces. Retention and deletion of data are managed in accordance with the policies and practices defined in the Data Privacy Factsheet, ensuring alignment with compliance and contractual obligations.

4.3.7 Privacy by Design & Default

Data retention is configured by NTT in alignment with each customer's contractual and compliance requirements, ensuring that information is stored only for as long as necessary.

Default data storage is provisioned on NTT's Cloud within the customer's designated regional environment to meet data residency, sovereignty, and GDPR obligations.

Privacy Impact Assessments (PIAs) are conducted by NTT as part of the feature design and release process to proactively identify, evaluate, and mitigate potential privacy risks before deployment.

4.4. Personnel Security

NTT DATA implements a security policy framework influenced by ISO/IEC 27001. The security policies are communicated and made available for all NTT DATA' employees. The policies are reviewed by the Security Officer on a yearly basis

4.5. Client Obligations

Although NTT DATA makes every effort to detect and block fraudulent calls on its network, Client must always:

- Ensure that only authorized people use the Cloud Voice connected phone system to make and receive calls

- Take sensible precautions regarding security and access to systems, such as enforcing the use of strong passwords and PINs where applicable, to prevent unauthorized usage.

5. Reporting and QoS

By default, Client gets access to a set of online reporting elements on NTT DATA's selfcare portal via the "Cloud Voice and Agentic Comms" app.
Here-below are the main reporting elements provided with current release:

- Usage, Consumption and Quality of Service dashboards
- Custom reports (with ability to generate and download these reports)

These online reporting capabilities are evolving over time to ensure Clients get as much value as possible from their NTT Data AI Communications Gateway.

6. Billing

6.1. Standard Charge types

The AI Communications Gateway service is structured with the following SKUs:

SKU name	Description	Charge type
AI Voice Agent Premium - Multi-language	Advanced user experience with multi-lingual feature	Per-Minute Consumption Charges
AI Voice Agent Premium - Localized language	Advanced user experience with localized language feature– i.e. Cantonese, English (US, UK, Singapore, etc.)	Per-Minute Consumption Charges
AI Voice Agent Standard	Standard user experience covering key features	Per-Minute Consumption Charges

6.2. Billing Cycles

NTT DATA billing cycles start on the first calendar day of the month and ends on the last calendar day of the month.

Monthly Recurring Charges (i.e. TBD) and overage per-minute pay-as-you-go communication charges are computed on the last calendar day of the Month for invoicing (i.e. Communications of December 2025 are rated on December 31st and invoiced by mid-January 2026).

NTT DATA does not provide pro-rated charges but rather full month rating and invoicing.

6.3. One-Time Charges

Additional One-Time Charges are to be charged only once and following conditions described in the SoW if Professional Services (PS) activities are also included.

In case of the latter, the detailed description of what is covered by such charges shall be described in the PS Statement of Work.

6.4. Pay-as-you-go consumption charges

Client shall pay to NTT DATA charges calculated using a rate per minute as described in the Contract.

Calls are billed in 1 second increments and are rounded to the nearest upper two (2) decimal places (for currencies not featuring decimals rounding is done to the nearest upper integer place).

Minimum call duration is 1 second and all calls will be rated accordingly.

6.5. Minimum Monthly Commitment

Client understands and agrees that NTT DATA is entitled to charge a Minimum Monthly Commitment (MMC) as defined in the Contract.

Said MMC shall only be charged should the total amount of consumption due over a monthly period be inferior to this MMC amount. In such case the MMC only will be charged to Client superseding the sum of the other charges (excluding One-Time charges).

The MMC is computed at the Billing Account level.

6.6. Other charges

For all charges not listed in the Contract, Client must refer to its NTT DATA Account Manager. Should the provisioning of services not listed in the Contract be effective, NTT DATA shall charge for such services using its standard pricelist, available on-demand from Client's Account Manager.

6.7. Billing and Invoicing capabilities

By default, NTT DATA will invoice Client centrally in-country as initially agreed between the two parties.

Billing is not available in all countries, nor in all currencies. Feasibility must be checked upfront.