



Service Definition Document Connect +

Contents

1. Service Overview	3
2. Service Components	3
3. Hosting, Architecture & Technical Requirements	4
4. Security & Compliance	5
5. Business Continuity, Backup & Disaster Recovery	6
6. Service Levels	6
7. Onboarding & Offboarding	7
8. Access to Data Upon Exit	7
9. Service Constraints	8
10. Outage & Maintenance Management	8

1. Service Overview

The Customer Communications Management as a Service (CCMaaS) platform is a cloud-based environment that enables the creation, management, orchestration, and delivery of personalised, omni-channel customer communications at scale. The service supports end-to-end communication lifecycle management, including data ingestion, content authoring, workflow automation, multi-channel output, and reporting—all delivered within a secure, compliant, and highly scalable Azure-based architecture.

The platform is designed for organisations seeking to unify fragmented communication systems, improve efficiency, enhance regulatory compliance, and provide customers with consistent, contextual and responsive interactions across all channels.

2. Service Components

Integration

The platform integrates with core back-office and line-of-business systems through secure interfaces, enabling seamless exchange of data and communication triggers. Supported standard protocols include secure FTP and REST API, with optional support for VPN, SOAP, and custom integrations where required. All integrations comply with industry-standard security models in cryptography and identity management.

Content & Template Management

A browser-based content and template management system allows organisations to control corporate identity, manage text fragments, images, and layout components, and maintain consistent messaging across channels. Intuitive business-user interfaces support content creation, approval and governance, reducing reliance on technical teams. API-driven content access ensures both centralisation and flexibility.

Production Engine

The production engine transforms large volumes of structured data into multiple output formats at high speed, supporting PDF, HTML5, DOCX, AFP, TXT, CSV and a wide range of print-stream formats. The engine ensures reliable processing for high-volume and peak-load scenarios.

Scenario & Workflow Management

Communication workflows can be fully automated using scenario management tools. Users can build omni-channel workflows that trigger communications based on defined rules, events or behaviours. A drag-and-drop interface allows the configuration of if/then logic, channel selections, and automated triggers. Organisations may self-manage workflows or delegate full scenario management as a managed service.

Omni-Channel Distribution

The service supports delivery across print and digital channels, including:

- Email
- SMS
- WhatsApp for Business
- Print and mail output
- Customer portals and user environments
- Voice messaging

Closed-loop reporting ensures visibility of message delivery, read-confirmations, and customer interactions.

Reporting & Analytics

Dashboard-based reporting provides real-time visibility into communication processes, KPIs, costs, and cross-departmental activity. All system activities and metadata are logged for a minimum of six months (extendable). Drill-down views allow detailed tracking of communication histories throughout the customer journey.

3. Hosting, Architecture & Technical Requirements

Cloud Hosting

The CCMAaaS platform is hosted on **Microsoft Azure West Europe (Amsterdam)**, with all data processing and storage remaining within this region. This supports organisations with strict data residency requirements.

Platform Architecture

The service is built on **Azure Kubernetes Service (AKS)** using Docker containers, providing:

- Elastic scalability
- High availability
- Automated workload distribution
- CI/CD deployment pipelines via Azure DevOps
- Controlled and secure update cycles

This architecture ensures reliability, rapid innovation, and resilience under peak loads.

Multi-Tenancy

A multi-tenant architecture allows cost efficiency, shared infrastructure, centralised upgrades, and reduced energy usage. Data isolation controls ensure that each tenant's data remains completely segregated. Single-tenant options are also available for organisations requiring dedicated environments.

4. Security & Compliance

Security by Design

The service adopts a privacy-by-design and security-by-design approach, encompassing:

- Secure infrastructure
- Protection of personal data in storage and transit
- Secure outbound communications
- Comprehensive compliance with regulatory requirements

Access Control

- Enterprise access via Azure Active Directory and SSO
- Portal access via username/password with optional MFA
- Role-based permissions and configurable identity management per tenant

Data Encryption

- Encryption at rest
- Application-level encryption of privacy-sensitive data
- SSL/TLS 1.2+ encryption for data in transit
- Web applications protected behind an Application Gateway with OWASP 3-aligned firewall rules

Data Isolation

Container-level isolation ensures secure resource separation between tenants, preventing cross-access to data or workloads.

Risk Management & ISO Certification

The service is **ISO 27001 certified**, following structured frameworks for identifying, assessing, and mitigating information security risks.

GDPR Compliance

As a processor of personal data, the service fully supports GDPR requirements, including:

- Configurable data retention
- Encrypted storage in a single central location
- Depersonalisation of personal data into unique reference IDs
- Full audit logging and traceability

5. Business Continuity, Backup & Disaster Recovery

Backup

- Automated backups of data and system components
- Secure storage within the Azure region
- Configurable retention periods

Disaster Recovery

Leveraging Azure's built-in continuity capabilities, the service provides:

- Rapid failover
- Infrastructure resilience through containerised architecture
- Geographic redundancy within the Azure regional zone

High Availability

The Kubernetes-based container architecture ensures continual availability, automatically scaling resources during peak load, and redistributing workloads during component failure.

6. Service Levels

Performance

The platform is designed for high-volume throughput and fast data processing across all supported output formats.

Scalability

Elastic scaling automatically increases or decreases capacity in line with workload volumes. Peak processing periods are fully supported without manual intervention.

Availability

The platform is designed for continuous availability through container redundancy, automated workload distribution, and Azure's resilient hosting environment.

Support Hours

Support models include 24/7 availability for platform uptime and critical incident management.

7. Onboarding & Offboarding

Onboarding Support

Typical onboarding activities include:

- Requirements definition and solution design
- Integration with source systems
- Content migration and template setup
- User training on content management and workflow tools
- Testing and acceptance processes

The service supports both standard and custom integrations depending on organisational needs.

Offboarding Support

Upon exit, customers retain full access to their data, which is provided in standard structured formats (e.g., JSON, XML, PDF, or export aligned with the Canonical Data Model).

Data extraction, environment decommissioning, and secure deletion protocols follow GDPR-aligned processes and ISO 27001 controls.

8. Access to Data Upon Exit

Data can be exported in:

- Native source format
- CDM-standardised JSON/XML
- Output formats generated during communication processing

The platform ensures all personal data is securely removed following contract termination and customer approval.

9. Service Constraints

Service constraints may include:

- Planned maintenance windows for upgrades (minimised via centralised multi-tenant updates)
- Dependency on customer system availability for data ingestion
- Channel-specific limitations set by third-party providers (e.g., SMS gateways, WhatsApp APIs)
- Customisation limits governed by the standardised nature of the multi-tenant platform

10. Outage & Maintenance Management

- System updates are delivered through Azure DevOps CI/CD pipelines, ensuring controlled, rapid, and secure deployment.
- Multi-tenant architecture enables simultaneous updates for all tenants, reducing downtime.
- Monitoring, alerting and automated recovery mechanisms minimise service disruption.
- All maintenance activities adhere to secure deployment practices aligned with OWASP and ISO 27001 controls.