

1. System Name: WMATA Customer Service Contact Center
2. System Locations: Records are maintained in WMATA-owned or contractor-operated information systems, including authorized cloud-based environments (e.g., Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service). Data may be stored at WMATA facilities and at approved service provider locations.
3. Categories of Individuals Covered by System:
 - External Users
 - Individuals who contact WMATA via phone, chat, SMS, social media, or email channels.
 - Law-enforcement subjects or complainants where interactions relate to MTPD incidents.
 - Internal Personnel
 - WMATA employees and/or contractors who staff or operate contact center functions.
 - Contractor, subcontractor, and/or Vendor staff/personnel engaged in implementation, integration, or operations (when performing job duties).
4. Categories of Records in the System:
 - Contact Metadata (Routing & Reporting): date/time stamps; call, chat, social media, and SMS identifiers; customer service agent identifiers; contact duration and disposition codes; and channel type.
 - Personally Identifiable Information Supplied by Users (Identification & Communication): full name, contact phone number, email address, mailing address (if provided), Smart Trip card number and account reference numbers, and other contact details.
 - Interaction Content (Quality & Case Documentation): voice call recordings; chat and SMS transcripts, and attachments; social media posts, messages, and attachments; and email bodies and attachments.
 - Operational Data (Case Management & Feedback): Interactive Voice Response (IVR) menu selections and inputs, agent notes and disposition forms, ticket/case numbers, customer satisfaction survey/responses and post-interaction feedback.
 - Location Metadata (Service Optimization): user-provided location (e.g. Metrobus/Metrorail number, stop ID, station selection, IP address) or derived geolocation (latitude/longitude) when using WMATA Trip Planner.
 - Agent Performance & Employee Workforce Metrics (Performance Monitoring): occupancy rates, and handle time.
 - Security & Audit Logs (Accountability & Compliance): access logs and audit trails, and system configuration change records.
5. Principle Purpose: To provide WMATA with a centralized, cloud-based contact center platform for receiving, routing, recording, and reporting customer and internal service interactions; to enable omni-

channel service delivery and incident response (voice, chat, SMS, email, and social); to support workforce management and reporting; to enable self-service and IVR functions; to escalate and route sensitive incidents to appropriate WMATA and/or law enforcement teams; and to maintain records required for operational reporting, service quality, compliance, billing, and performance analytics.

6. Routine Uses of Records Maintained in the System:

- General Routine Use A (Disclosure for Law Enforcement Purposes);
- General Routine Use B (Disclosure Incident to Requesting Information);
- General Routine Use C (Disclosure to Requesting Agencies);
- General Routine Use D (Disclosure to Congressional Offices or Offices of Elected Officials in the Transit Zone);
- General Routine Use E (Disclosure to Courts or Administrative Bodies);
- General Routine Use F (Disclosure to Contractors, Grantors, Grantees, Federal Government Agencies, and Others);
- General Routine Use G (Disclosure for Administrative Claims, Complaints, and Appeals);
- General Routine Use H (Disclosure in Connection with Litigation);
- General Routine Use I (Disclosure to WMATA Unions);
- General Routine Use J (Disclosure to the Government Accountability Office (GAO), Federal Transit Administration (FTA), or Other Government Oversight Agencies); and
- Disclosure to third-party service providers under contractual obligations for the limited purpose of integration functions.

7. Policies and practices for storing, retrieving, accessing, retaining and disposing of records in the system:

Retrieved by: Records are searchable and retrievable by phone number, email address, ticket/case number, Smart Trip account number (if provided), WMATA-furnished personnel identification number, interaction ID, date/time ranges, or other identifiers provided or referenced related to an interaction.

Storage:

- Primary storage is in the Genesys Cloud tenant and provider data stores.
- WMATA-managed extracts, reports, and backups are stored on WMATA servers and secured cloud storage associated with WMATA accounts.
- Temporary copies may reside on contractor systems only as required for troubleshooting or implementation and only under contractual security provisions.

Safeguards:

- Encrypt data in transit (TLS) and at rest (provider-standard encryption).
- Enforce role-based access control (RBAC) and least-privilege for all WMATA and contractor users.
- Require WMATA approval and multi-factor authentication (MFA) for privileged accounts.
- Track agent log-in/access, configuration changes and administrative actions, and retain audit trails as applicable.

Retention and Disposal: Records are retained and disposed of in accordance with applicable WMATA Records Retention Policy.

8. Systems Manager/Administrator:

- System Owner / Manager: IT Program Portfolio Manager, Office of Digital Modernization (DM).
- Technical Administrator: WMATA IT Telecomm & Contact Center Operations (names and titles recorded in internal admin roster). Genesys tenant administrative roles are controlled by WMATA designated admins; contractors are granted access only per contract and RBAC.

9. Procedure for Notice, Access, and Contesting: Any individual who wants to know whether this system of records contains a record about him/her, who wants access to his/her record, or who wants to contest the contents of a record, should make a written request to the Privacy Administrator at (1) PARP@wmata.com; or (2) **Office of General Counsel 7E, PO Box 44390, Washington, D.C. 20026-4390**. Requesters will be required to provide adequate identification, such as a driver's license, WMATA personnel identification card, or government-issued identification document. Requests for correction or amendment must identify the information to be changed and the corrective action sought. Additional information is available in WMATA's Policy/Instruction 9.2 (Privacy Policy), which is posted on WMATA's website.

10. Records source categories:

- From customers, employees, and contractors related to interactions;
- WMATA internal systems (ServiceNow, CRM/Oracle systems, Workforce Management, Avaya logs, historical call/contact databases);
- External data providers: Next-Bus/Next-Train APIs, Open Trip Planner (OTP), GTFS feeds, Smart Trip system, third-party social/chat platforms, and other transit data services; and
- Contractors and vendors (Genesys, integrators) supplying configuration, integration logs or support records.