Security, Privacy and Architecture of Informatica from Salesforce Intelligent Data Management Cloud

Published: March 17, 2026

Salesforce's Corporate Trust Commitment

Salesforce is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including protection of Customer Data as defined in Salesforce's MSA.

Services and Features Covered

This documentation describes the architecture of, the security- and privacy-related audits and certifications received for, and the administrative, technical and physical controls applicable to the following services and features (collectively, for purposes of this document only, the 'Covered Services"):

(1) The services and features branded as:
- Intelligence Data Management Cloud (IDMC)
- Master Data Management SaaS (MDM SaaS)
- Master Data Management Cloud Edition (MDM Cloud Edition)
- Data-as-a-Service (DaaS)

Services or Features Not Covered

This documentation does not apply as described below:

(1) Reliability, Backup, and Business Continuity, Return of Customer Data, and Deletion of Customer Data sections of this documentation do not apply to non-Production Orgs such as Tech Sales PoC Orgs or PreRelease Orgs. These Orgs should not contain personal data or other sensitive data types.

(2) This documentation does not apply to other Salesforce services that may be associated with or integrate with the Covered Services

(3) To the extent a Covered Service is accessed through or interoperates with another Salesforce Service, certain Customer Data and/or Content may be transferred from such service to the Covered Services for processing, however such Customer Data remains subject to the Security, Privacy and Architecture Documentation applicable to such underlying product available here.

Architecture and Data Segregation

For IDMC, MDM SaaS, and DaaS, the Covered Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via unique ID. The specific infrastructure used to host Customer Data is described in the "Infrastructure and Sub-processors" documentation available here.

For MDM Cloud Edition, the Covered Services operate in a single tenant execution environment ("Single Tenant Cloud Services"). The specific infrastructure used to host Customer Data is described in the "Infrastructure and Sub-processors" documentation available here.

Control of Processing

Salesforce has implemented procedures designed to ensure that Customer Data is only processed as instructed by the customer, throughout the entire chain of processing activities by Salesforce and its sub-processors. In particular, Salesforce and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to the processing activities provided by them. Compliance with such obligations as well as the technical and organizational data security measures implemented by Salesforce and its sub-processors are subject to regular audits by Salesforce and/or independent third-party auditors designated by Salesforce. The "Infrastructure and Sub-processors" documentation available here describes the sub-processors and certain other entities material to Salesforce's provision of the Covered Services.

Third-Party Functionality

Certain features of the Covered Services use functionality provided by third parties. Customers may be able to disable such features. See product specific additional disclosures below for further information and Notice and License Information documentation available here.

Audits and Certifications

The Covered Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.

The following security and privacy-related audits and certifications are applicable to the Covered Services on select platforms. Except as specified below, Salesforce's most recent audit reports and certifications are available for download at Salesforce's compliance website. Please review the individual certifications to determine specific product scoping.

- **Esquema Nacionale de Seguridad (ENS):** Informatica from Salesforce has obtained (Esquema Nacional de Seguridad) ENS certification for the Covered Services on select platforms with the exclusion of MDM Cloud Edition and DaaS.
- **EU Binding Corporate Rules (BCR) for Processors:** Customer Data submitted to the Covered Services is within the scope of the Informatica EU BCR for Processors to the extent described therein.
- **Data Privacy Framework Certifications:** Customer Data submitted to the Covered Services is within the scope of annual certifications to the EU-US Data Privacy Framework and UK Extension to the EU-US Data Privacy Framework, as administered by the US Department of Commerce. The current certifications are available at https://www.dataprivacyframework.gov/s/ by searching under "Informatica."
- **ISO 27001/27017 certification**: Informatica from Salesforce operates an information security management system (ISMS) in accordance with the ISO 27001 and ISO 27017 international standard. Informatica from Salesforce has achieved ISO 27001/27017 certification for its ISMS from an independent third party. The ISO certifications name the Covered Services with the exclusion of MDM Cloud Edition.
- **System and Organization Controls (SOC) reports**: Salesforce's information security control environment applicable to the Covered Services undergoes an independent evaluation in the form of SOC 1 (SSAE 18 / ISAE 3402), SOC 2 or SOC 3 audits.

As further described in the "Infrastructure and Sub-processors" documentation available here, Salesforce uses Infrastructure Providers outlined in that document to host or process Customer Data submitted to certain Covered Services and features. Information about security and privacy-related audits and certifications received by the Infrastructure Providers, including information on the associated certification and report, is available from the Infrastructure Providers.

Security Controls

The Covered Services include a variety of configurable security controls that allow customers to tailor the security of the Covered Services for their own use. Please see additional information on such controls for IDMC and MDM SaaS in the Informatica Security Guide. For more information on MDM Cloud and DaaS, contact your Customer Account Team. Information on Multi-Factor Authentication and Single Sign-On for access to the Covered Services is set forth in the applicable Notices and License Information (NLI). As further described in the "Infrastructure and Sub-processors" documentation available here, Salesforce uses infrastructure provided by the Infrastructure Providers to host or process Customer Data submitted to certain Covered Services and features. Information about security provided by the Infrastructure Providers is available from the Infrastructure Providers.

Security Policies and Procedures

The Covered Services are operated in accordance with the following policies and procedures to enhance security:

- For native password-based authentication, user credentials are hashed and securely stored.
- The Covered Services maintain access logs to the Cloud Services including date, time, and User identifier. Informatica can provide Customer the access logs as required to comply with governing law to assist in forensic analysis if there is a suspicion of inappropriate access. Access logs for Production Cloud Services will be maintained in a secure area for a minimum of ninety (90) days during the Term and destroyed in accordance with Disposition of Data below. Passwords are not logged under any circumstances.
- Passwords are not logged.
- Salesforce personnel will not set a defined password for the user. This must be done through application functionality. Upon account setup or reset, users are required to set up their own password.

Further information about security provided by Infrastructure Providers is available from the Infrastructure Providers.

Intrusion Detection

Salesforce, or an authorized third party, will monitor the Covered Services for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. Salesforce may analyze data collected by users' web browsers for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Covered Services function properly.

Security Logs

Salesforce systems used in the provision of the Covered Services log information to their respective system log facilities or a centralized logging service (for network systems) in order to enable security reviews and analysis.

Incident Management

Salesforce maintains security incident management policies and procedures. Salesforce notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Salesforce or its agents of which Salesforce becomes aware to the extent permitted by law.

Salesforce publishes system status information for the Covered Services on https://pulse.informatica.com/.

User Authentication

Access to Covered Services requires authentication via one of the supported mechanisms as described for IDMC and MDM SaaS in the Informatica Security Documentation, password-based, single-sign-on (SSO) based, certificate-based, and token-based as determined and controlled by the customer.

Additionally, IDMC and MDM SaaS support web SSO-based security assertion markup language (SAML) 2.0 providers, which include support for any third-party identity provider (IDP) that supports SAML protocol for authentication and authorization. Additionally, IDMC also supports service-to-service authentication using short-lived token-based authentication (OAuth 2.0).

All Cloud Services are accessible to Customers through interfaces requiring authentication. IDMC, MDM SaaS, and MDM Cloud Edition include optional support for two factor authentication for user access.

Physical Security

Our public cloud providers are responsible for providing appropriate physical security measures. Further information about the physical security provided by Infrastructure Providers is available from the Infrastructure Providers.

Reliability, Backup, Business Continuity, and Disaster Recovery

The Covered Services maintains a business continuity and disaster recovery program. Policies and procedures are in place to provide Cloud Services and Global Customer Support Services with minimal interruptions, including disaster recovery planning and testing capabilities, recovery site management and standard backup and recovery procedures. Informatica's Program is designed to meet a recovery point objective of twenty-four (24) hours and a recovery time objective of eight (8) hours. Backups of Customer Data are deleted promptly upon exceeding seven days. Informatica maintains geographically separate failover data centers for Cloud Services with a strict backup schedule for data at those facilities.

Viruses

The Covered Services do not scan for viruses that could be included in attachments or other data uploaded into the Covered Services by customers. Uploaded attachments, however, are not executed in the Covered Services and therefore will not damage or compromise the Covered Services by virtue of containing a virus.

Data Encryption

The Covered Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Covered Services, including through Transport Layer Encryption (TLS). The Customer Data is also encrypted at rest.

Deletion and Return of Customer Data

IDMC and MDM SaaS
The Covered Services policy is to retain Customer Data if not deleted earlier by the Customer for at least thirty (30) days after termination or expiration of Customer's subscription to the Cloud Service, and to delete Customer Data if not deleted earlier by the Customer within sixty (60) days of termination or expiration of Customer's subscription to the Cloud Service, solely except as otherwise provided herein or to the extent such metadata are included in backup and disaster recovery logs the integrity of which requires that they remain unmodified.

Daily backups of all Customer Data in Cloud Services are retained for seven (7) days, at which time they are deleted, except that IDMC – Data Quality retains backups for thirty (30) days. Prompts and outputs (excluding Customer Data) of automated natural language features of the Services such as Informatica CLAIRE GPT will be retained for six months during the Term for retrieval by Customer.

MDM Cloud
For MDM Cloud, the Covered Service's policy is to delete Customer Data promptly upon termination or expiration of Customer's subscription to the Cloud Service but in any event within sixty (60) days, solely except as otherwise provided herein or to the extent such Customer Data is included in backup and disaster recovery logs the integrity of which requires that they remain unmodified.

DaaS
For DaaS functionality, the following deletion policies are followed: For Informatica Address Verification, Partner branded Informatica Address Verification, and Informatica Email Verification batch processing, the Covered Service's policy is to delete Customer Data after sixty (60) days. For Informatica Address Verification batch processing, the Covered Service's policy is to delete Customer Data after forty-five (45) days. For Informatica Email Verification web services, the Covered Services will Delete Customer Data within one (1) day, with up to an additional one (1) day if necessary to retry the address. For system logs, which may include email addresses, for Informatica Email Verification batch processing and web services, the Covered Services policy is to delete Customer Data within one (1) year. For Informatica Address Verification web services and Informatica Global Phone Number Validation web services Customer Data is not retained.

Sensitive Data
If the Customer submits sensitive or otherwise regulated data to the Covered Service's Cloud offering, the Customer is responsible for ensuring that its use of the Covered Service's Cloud Offering to process that information complies with all applicable laws and regulations associated with that data including review of the Audits and Certifications section to determine if the Cloud Offering has the necessary Audits and/or Certifications to process that sensitive data.

Analytics
Salesforce may track and analyze the usage of the Covered Services for the purposes of security and helping Salesforce improve both the Covered Services and the user experience (including customer support services) in using the Covered Services. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality.

Salesforce may share anonymous usage data with Salesforce's service providers for the purpose of helping Salesforce in such tracking, analysis, and improvements. Additionally, Salesforce may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show trends about the general use of our services.

Salesforce will not share Customer Data consisting of personally identifiable information, nor any data that will or could be used to identify customers, their users, their consumers, or any individual, company or organization. Salesforce may use Customer Data to create metrics showcasing the use of our services for marketing purposes. Any such metrics will be aggregated so as to not identify any individual or customer.

Interoperation with Other Services

The Covered Services may interoperate or integrate with other services provided by Salesforce or third parties. When third-party systems connect to the Covered Services, these external systems supply metadata to the Covered Services for the purpose of maintaining the intended functionality of the integration; for example an external system may supply a third-party record ID, file name, folder name, or similar label intended to identify a record that is being sent to the Covered Services. Salesforce may collect and store such metadata to ensure product functionality, and to assist in debugging, support and for security purposes. Salesforce provides appropriate protections for such metadata and treats it consistently with our Privacy Statement. Security, Privacy and Architecture documentation for services provided by Salesforce is available in the Trust and Compliance Documentation. Salesforce also provides a variety of platforms and features that allow Salesforce users to learn about Salesforce products, participate in communities, connect third-party applications, and participate in pilots, testing and assessments, which are outside the scope of this documentation. Salesforce may communicate with users that participate in such platforms and features in a manner consistent with our Privacy Statement. Additionally, Salesforce may contact users to provide transactional information about the Covered Services; for instance, through the Adoption Manager program or through system-generated messages, such as Chatter notifications.

Salesforce offers customers and users the ability to deactivate or opt out of receiving such messages.

Additional Disclosures

IDMC and MDM SaaS have certain functionality related to providing Customer Support and product improvement, including training AI models using customer metadata. If Customers do not want to participate in either of these functionality options, they are required to opt out through their Administration Module.