SECURITY ADDENDUM TO THE
INFORMATICA LICENSE AND SERVICES AGREEMENT AND/OR DATA PROCESSING AGREEMENT

This Addendum to the Informatica License and Services Agreement or the applicable data processing agreement or other agreement under which Informatica provides cloud, support, or professional services to Customer (the "Agreement") identifies security policies and commitments of Informatica for its Cloud, Support, and Professional Services. Additional security features of each Cloud Service may be described in the Informatica Cloud and Product Description Schedule. Informatica's privacy policy (which applies to the information collected about Customer's employees and contractors) is separate from this Addendum and is available for reference at https://www.informatica.com/privacy-policy.html.

Informatica may update this Addendum from time to time to document changes in security policies for the Cloud Services and/or the Support Services, in accordance with Change Management below. Informatica will, upon request, certify to its compliance with this Addendum.

Data Security Program

Informatica has a risk-based data security program ("Program") designed to enable Support Services to be delivered in a secure manner and designed to protect Cloud Services and related Informatica systems from threats and data loss. This Addendum describes the controls of the Program as of the effective date of the Addendum. Informatica regularly assesses and makes improvements to the Program with reference to changing security threats, regulatory requirements, and industry standards.

Risk Assessment

Informatica conducts, or retains independent third parties to conduct, information security risk assessments at least annually and whenever there is a material change in Informatica's business or technology practices that may impact the privacy, confidentiality, security, integrity, or availability of data Customer submits to the Products or Services for processing ("Customer Data"). The risk assessment includes identifying reasonably foreseeable internal and external risks to privacy, confidentiality, security, integrity, or availability; assessing the likelihood of, and potential damage that can be caused by, identified risks; assessing the adequacy of personnel training concerning the Program; updating the Program to limit and mitigate identified risks as appropriate and to address material changes in relevant technology, business practices, and personal information practices and regulations; and assessing whether the Program is operating in a manner reasonably calculated to prevent and mitigate unauthorized access to or disclosures of Customer Data ("Security Incidents").

Standards

Informatica adopts best practices from a number of standards, including, but not restricted to the National Institute for Standards and Tehcnology (NIST) and ISO27001, AICPA and Cyber Essentials. For Type I, II, and III Cloud Services (as defined below) operated on Google Cloud Platform, Microsoft Azure and Amazon Web Services infrastructure, excluding Technical Preview services and functionality, Informatica annually receives third party audits for compliance with AICPA SOC 1 Type 2, SOC 2 Type 2, SOC 3, and the U.S. Health Insurance Portability and Accountability Act ("HIPAA"), including as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"). For Type IV Cloud Services operated on Microsoft Azure and Amazon Web Services infrastructure, Informatica annually receives third party audits for compliance with AICPA SOC 2 Type 2, SOC 3, and HIPAA/HITECH. The most recent certifications including an SSAE No. 18 report, are available upon Customer request under NDA. The most recent SOC 3 report is available upon request and is also available publicly on the Informatica Trust Center website at https://www.informatica.com/trust-center.html.

Data Processing and Storage

Processing and storage requirements for Customer Data on computer systems owned or licensed by Informatica or its suppliers for the Cloud Service or Support Service ("Informatica Systems") are determined by the type of Informatica Cloud Service or Support Service subscribed by Customer. Customer has sole responsibility for selecting a Cloud Service, and for designing a system of which the Cloud Service is a part, that complies with laws and regulations applicable to Customer's use.

Cloud Services may depend on a Customer-managed installation of a high function runtime version of Informatica's data processing execution component ("the Informatica Cloud Secure Agent") that moves data among sources, local systems, and targets.

There are three categories of metadata that may be stored by Cloud Services on Informatica Systems: Operational and Usage Metadata, Technical Metadata, and Customer Business Metadata (collectively, "Metadata"). Metadata are not Customer Data. Operational and Usage Metadata include information extracted from service and activity logs such as connection and schedule data and information about how the Cloud Services are used, such as transactions conducted by the Customer in its data marketplace. Technical Metadata include data schemas, rules and data profile statistics, and design metadata that define integration tasks and processes, such as data sync, data replication, mappings and templates, task flows, process definitions, and data lineage. Customer Business Metadata contain information related to Customer Data, including data classifications and glossaries designated by Customer. Users may optionally provide feedback to automated natural language features of the Services such as Informatica CLAIRE GPT. That feedback, including the prompts and the information, suggestions, and other outputs (excluding Customer Data) to which it relates, will be used anonymously with respect to Customer and user for product usage observability and improvement.

Type I Cloud Services do not process or store Customer Data on Informatica Systems, provided that Type I Cloud Services may include an optional data preview display feature that send Customer Data to Informatica Systems solely for display. Type II Cloud Services may transiently process Customer Data on Informatica Systems without persistent storage. Informatica will not use or disclose Customer Data without Customer's consent for any purpose other than that of performing its obligations in connection with the Agreement. Type III Cloud Services may persistently store Customer Data on Informatica Systems. Type IV Cloud Services, which include Informatica "Data-as-a-Service" products and their variants, may transiently store Customer Data that are phone numbers, addresses, emails, or other applicable communication data.

Collection of Metadata by Cloud Services, including the Informatica Cloud Secure Agent, is necessary to provide the Cloud Services and cannot be disabled. This information will be used to improve the customer experience including facilitation of Support Services, deployment and usage analysis, and usage suggestions. Operational and Usage Metadata may be analyzed and used to improve the Cloud Services, provided that the output of the analysis will not identify Customer or any individuals. Subject to Customer's opt-out rights, Technical and Customer Business Metadata may be analyzed and used to improve the Cloud Services, provided that the output of the analysis will not identify Customer or any individuals. Customer may have the option to opt-in to the analysis and use of Customer Data to improve the Cloud Services, provided that the output of the analysis will not identify Customer or individuals.

CLAIRE GPT and CLAIRE Copilots Use of Microsoft Azure OpenAI and Claude on Amazon Bedrock

Some features of Informatica CLAIRE GPT and the Informatica Cloud Services CLAIRE Copilots use Microsoft Azure OpenAI or Anthropic Claude ("CLAIRE External LLMs"). Use of CLAIRE External LLMs may transfer (i) Technical Metadata, Customer Business Metadata, and Customer Data to an enterprise instance of Microsoft Azure OpenAI provisioned under Informatica's Azure account located in the USA and in the European Economic Area ("EEA"); and (iii) Customer Data to an enterprise instance of Anthropic Claude provisioned via Amazon Bedrock located in the USA, the EEA, the UK, and the APJ region.

CLAIRE GPT and CLAIRE Copilots Data and Metadata Transfer

Informatica CLAIRE GPT and the Informatica Cloud Services CLAIRE Copilots process Technical Metadata, Customer Business Metadata, and Customer Data at a point of delivery in the geography selected by Customer, except that use of CLAIRE External LLMs at points of delivery outside of the USA and EEA may result in transfer of Technical Metadata and Customer Business Metadata to the USA or EEA for processing. CLAIRE External LLMs that process Customer Data on Microsoft Azure OpenAI are not available at points of delivery outside of the USA and the EEA. CLAIRE External LLMs that process Customer Data on Amazon Bedrock are not available at points of delivery outside of the USA, the EEA, the UK, and the APJ region.

Select Informatica Cloud Services by Type

Cloud Service	Type
IDMC – Advanced Data Integration	I

IDMC – Advanced Data Integration with Serverless	II
IDMC – Data Integration	I
Salesforce outbound messaging function of IDMC – Data Integration and Advanced Data Integration	II
IDMC – Application Integration	I
IDMC – Application Integration with Serverless	II
IDMC – API Center	II
IDMC – API Management	II
IDMC – B2B Gateway	I
IDMC – CLAIRE GPT	II
IDMC – Cloud Data Access Management	I
IDMC – Customer Managed Key	I
IDMC – Data Validation	I
IDMC – INFACore	I
IDMC – Industry Solutions	I
IDMC – Integration Hub	I
Informatica hosted repository function of IDMC – Integration Hub	III
IDMC – Mass Ingestion	I
IDMC – SQL ELT	I
IDMC – Advanced Data Quality	I
IDMC – Advanced Data Quality with Serverless	II
IDMC – Data Quality	I
Data profiling, data dictionary, and data quality exception functions of IDMC – Data Quality and Advanced Data Quality	III
IDMC – Data Governance and Catalog	I
Data profiling and lookup table functions of IDMC – Data Governance and Catalog	III
IDMC – Data Marketplace	I
IDMC – Data Masking	I
Informatica-hosted secure agent of IDMC	II
Verbose logging functions of IDMC with Serverless or of Informatica-hosted secure agent of IDMC	III
Verbose logging functions of other IDMC Cloud Services	II
INFAConnect	I
Operational Insights	I
PowerCenter Cloud Edition	I
Cloud Test Data Management	I
MDM Cloud Edition	III
MDM SaaS	III

Premium Address Cleansing	IV
Email Verification	IV
Global Phone Number Validation	IV

Professional Services

Professional Services may require Informatica to access Customer Data. Where Informatica needs to receive Customer Data, Customer will transmit such Customer Data via secure FTP site or physical media, and Informatica will store such Customer Data on Informatica systems solely for the duration of the applicable Professional Services implementation for the Customer and shall dispose of the Customer Data in accordance with the section titled Disposition of Data below.

Professional Services may require Informatica to receive either remote access to Customer's computer systems via Informatica or Customer issued workstations or onsite access to Customer's physical location. Customer will notify Informatica of any reasonable Customer policy or procedure required for access before Customer grants such access. Customer is responsible for implementing security measures to prevent unauthorized use and access of Customer's computer systems and physical location, and for revoking access after completion of the applicable Professional Services.

Customer may allow Professional Services to access Customer's computer systems via Informatica issued workstations. Informatica issued workstations will have relevant security measures to prevent unauthorized access and use. Customer is responsible for implementing security measures to prevent unauthorized use and access of Customer's computer systems and for revoking access after completion of the applicable Professional Services.

Professional Services interactions between Informatica personnel and Customer through virtual meetings may be recorded. By joining a virtual meeting session, Customer consents to recording and to Informatica's remote access to Customer's computer systems for provision of Professional Services. Customer is responsible for notifying Informatica personnel prior to exposure or possible exposure of personally identifiable information during virtual meeting sessions and for redirecting Informatica personnel and/or halting the session to avoid exposure.

Support Services

Support Services do not require Informatica to receive personal data and Informatica discourages uploading of any personal data. Customer must notify Informatica immediately in the event it mistakenly uploads personal data to ensure deletion from the system. Support Services may require Informatica to receive Customer Data such as a detailed description of Customer's environment, a copy of Customer's repository, or a sample of the Customer's data. Customer will transmit such Customer Data via secure FTP site or physical media, and Informatica will store such Customer Data at an Informatica Support Services facility at any location authorized in the Agreement solely for the duration of the applicable Support Services investigation in accordance with the section titled Disposition of Data below.

Support Services interactions between Informatica personnel and Customer through virtual meetings may be recorded. By joining a virtual meeting session, Customer consents to recording and to Informatica's remote access to Customer's computer systems for provision of Support Services. Customer is responsible for notifying Informatica personnel prior to exposure or possible exposure of personally identifiable information during virtual meeting sessions and for redirecting Informatica personnel and/or halting the session to avoid exposure.

Security – Overview

Informatica uses reasonable methods designed to safeguard Customer Data from unauthorized access, use, and loss including physical, technical, and administrative safeguards. Processed Customer Data from different customers are segregated logically and/or physically. Informatica may use additional measures to enhance security beyond those listed below.

Security – Physical Security

Physical access to Informatica locations holding Informatica Systems have limited access points, which are governed by card or biometric access devices and monitored by surveillance cameras. Access to servers, network ports, wireless access points, routers, firewalls, or any physical computing equipment involved with data hosting is physically restricted.

Security – Access

Informatica's Program limits access to Informatica Systems to authorized Informatica personnel.

Informatica's Program limits access to the Cloud Services environment in which Customer Data are processed to authorized Informatica Support Services personnel solely as needed to assist with a support case opened by Customer or otherwise as needed to resolve critical release or security issues. Such access is conducted solely upon notification to Customer and, for MDM SaaS, consent of the Customer.

Informatica's Program does not allow access to Customer Data except as specifically directed by Customer, provided that verbose logging enabled by Customer may include Customer Data and maybe be available in the environment accessible as specified above.

Upon Customer's written request, Informatica will promptly identify in writing all Informatica personnel who have been granted access to the Customer Data as of the date of the request. Access authorizations for Informatica personnel are reviewed at least semi-annually and rescinded promptly upon change of roles or separation from Informatica. Informatica maintains logs of access by Informatica personnel.

Security – Authentication

All Cloud Services are accessible to Customers through interfaces requiring authentication. Type I, II, and III Cloud Services include optional support for two factor authentication for user access.

Security – Encryption

Type I, II, and III Cloud Services use TLS certificates with at least 2048-bit RSA/DH groups, 256-bit ECC/symmetric keys, SSH, and IPsec protocols for data transmission and remote access over public networks, and AES encryption for transmission and for protecting the database containing Customer Data or Metadata. Type IV Cloud Services use encryption for all Web-enabled transactions that require user authentication or transfer of Customer Data. This is accomplished using one of the following methods: (a) TLS v1.2 or newer version, (b) Secure Shell (SSH), (c) Secure File transfer protocol (SFTP), or (d) Virtual Private Network (VPN).

Informatica implements an encryption key management process. Encryption/decryption keys are managed independently of the native operating system access control system; stored with reasonable protections; protected during transmission or distribution, changed at or before they reach the end of their crypto period; and retired if Informatica becomes aware that their integrity has been compromised. With the exception of one-time use password communication, all user passwords are encrypted with cryptography in transit and at rest on Informatica Systems. All user identifier and password combinations are encrypted via TLS while in transit.

Security – Architecture

Informatica Systems accessible to the Internet are protected with server hardening, patch management, and incident management. Informatica Systems accessible to the Internet are protected with application firewalls in a DMZ architecture, with back-end systems such as databases further protected by a second set of application firewalls. Firewall and router rules are default-deny and reviewed for unnecessary services and IP address exposures at least once per six months.

Security – Product Development

Informatica implements Security as a Design Principle. The lifecycle of cloud product development, from secure application development training, application and code reviews, source code scans, vulnerability scans, penetration tests, responsible disclosure program, and other controls are implemented continuously to reduce the probability and/or impact of application vulnerabilities.

Security – Harmful Code and Patches

Informatica determines remediation priority of vulnerabilities and schedules remediation and mitigation in accordance with the Informatica Security Vulnerability Patching Policy.

User Access Logs

Informatica maintains 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.

Customer Security Controls

Certain Cloud Services include configurable security controls as indicated in the corresponding Documentation, including unique user identifiers to help ensure that activities can be attributed to the responsible individual, controls to revoke access and/or lock out a user after multiple failed login attempts, password length controls, termination of a session after a period of inactivity, and geographical and/or chronological restrictions on access.

Employees and Contractors

Informatica personnel that operate or support Cloud Services receive annual education on the importance of security, confidentiality, and privacy of Customer Data, Informatica policies and associated data security practices, and the risks to Informatica and its customers associated with Security Incidents. Informatica implements measures designed to ensure that its personnel are sufficiently trained, qualified, and experienced to be able to fulfill their functions under the Program and any other functions that might reasonably be expected to be carried out by the personnel responsible for safeguarding Customer Data.

Incident Management

Informatica cloud operations personnel receive regular training on standard operational procedures and tactics to minimize the impact of production cloud incidents. Such incidents are classified according to severity of impact, with high-severity incidents triggering root cause analysis and reviews to identify areas for long-term improvement.

Change Management

Informatica plans to enhance and maintain the Cloud Services and Support Services during the Term, including but not limited to changes in response to relevant technology and systems, unauthorized access to Customer Data, and the discovery of material privacy or security vulnerabilities. Security controls, procedures, policies, and features may change or be added but will deliver a level of security protection that is not materially lower than that provided as of the effective date.

Informatica maintains a change management process with separation of duties and appropriate approvals required for modification to Informatica Systems, including patch management for the Cloud Services.

Business Continuity and Disaster Recovery

Any facility housing Informatica Systems is designed to withstand adverse weather and other reasonably predicable natural conditions and is also supported by on-site back-up generators in the event of a power failure. All networking components and web and application servers are configured in a redundant configuration.

Informatica 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 and Metadata 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.

Cyber Security

Informatica or an authorized third party performs periodic testing, including penetration testing, against Cloud Services available to the Internet. Informatica's security operations center, staffed by the office of Informatica's Chief Information Security Officer, is responsible for scanning and monitoring system activity and has pre-defined procedures for addressing or escalating vulnerabilities and events as needed. A security incident response team ("SIRT"), also staffed by the office of the Chief Information Security Officer and directed by Informatica's legal team, is responsible for investigating and responding to information-security related events escalated to their attention and determining if a Security Incident has taken place. Informatica Systems, including firewalls, routers, network switches and operating systems log information to enable the SIRT to detect, investigate, and resolve potential Security Incidents. Pre-defined

procedures are also available to guide those efforts, including when to involve other internal groups in a response process and associated notification activities. Customer and Informatica share responsibility for cybersecurity of Cloud Services environments. Customer is responsible for acts and omissions of Customer and Affiliates and their Users and agents that impact the cybersecurity of Customer environments, including but not limited to ingress, egress, network security, and high entropy credentials.

Insurance

Informatica maintains information security liability insurance and errors & omissions insurance covering liability for Security Incidents. Upon written request, Informatica will furnish to Customer a certificate of insurance evidencing required coverage and limits. In the event the policy is cancelled or modified before termination or expiration of the Agreement such that required coverage and limits are no longer met, Informatica will deliver notice of such cancellation or modification to Customer in accordance with Informatica's insurance policy provisions.

Transition of Services

Pursuant to mutually agreed upon transition fees where applicable, Informatica shall reasonably cooperate to support a transition of Customer Data and Customer-specific Technical and Customer Business Metadata ("Transition Data") from Production Cloud Services to the services of another provider or to Customer's internal operations. Customer may submit the transition request via its customer service manager or by emailing privacy@informatica.com.

Transition Data may be exported via the standard Cloud Services user interface as described in the Documentation. Specifically, users with export role privileges may export assets for which they have read permission. The export file may be in zip format with associated metadata and JSON file where applicable. Some Cloud Services also enable export via API, also as described in the Documentation. Assets generated by CLAIRE GPT are exportable after publication into the respective IDMC Cloud Service.

For Customers of Production Cloud Services domiciled in Europe: The request shall be submitted two months before the requested transition date, and Informatica will provide reasonable assistance without undue delay during a transition period not to exceed a maximum of thirty (30) days, which may be extended once upon customer written request. Transition Data will thereafter be retained and deleted as specified in the Disposition of Data section below. Informatica will inform Customer if the transition period is technically infeasible and provide an alternative transition period, which shall not exceed seven months. Customer will notify Informatica when the transition is completed, and Customer's subscription to the applicable Cloud Services will be deemed terminated and Customer will be notified of the termination. Informatica will pass on to Customer any third party egress costs. Informatica will comply during the transition period with the obligations of a provider of data processing services under the Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 (the "Data Act") to the extent applicable to the Cloud Services, including but not limited to the obligations of articles 25(2)(a)(i-iv) and 25(2)(b) of the Data Act. If the transition results in termination of the applicable Cloud Service subscription prior to the end of its committed Term under the Agreement, the fees for the remainder of the committed Term shall become due as an early termination fee. See Informatica's Processor Binding Corporate Rules at https://www.informatica.com/legal/binding-corporate-rules.html for information required by article 28 of the Data Act.

Disposition of Data

For Type I Cloud Services and multi-tenant Type II and III Cloud Services, Informatica's policy is to retain Customer Data and Customer-specific Technical and Customer Business Metadata 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 and de-identify or delete Customer-specific Technical and Customer Business Metadata 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. For Type III Cloud Services identified as "Cloud Edition", Informatica's policy is to delete Customer Data and de-identify or delete Customer-specific Technical and Customer Business Metadata 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 Metadata are included in backup and disaster recovery logs the integrity of which requires that they remain unmodified. Daily backups of all Metadata in Type I, II, and III Cloud Services, and of all Customer Data in Type II and III 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.

To the extent Type IV Cloud Services retain Customer Data, they do so as follows: Informatica Address Verification Data Quality Center, Partner branded Informatica Address Verification Data Quality Center, and Informatica Email Verification batch processing: sixty (60) days, at which time they are deleted; Informatica Address Verification batch processing: forty-five (45) days; Informatica Email Verification web services: one (1) day with up to an additional one (1) day if necessary to retry the address; system logs, which may include email addresses, for Informatica Email Verification batch processing and web services: one (1) year; Informatica Address Verification web services and Informatica Global Phone Number Validation web services: Not retained.

Informatica will promptly comply to the extent practicable with written requests to destroy Customer Data within shorter time periods than those indicated above and provide written certification of destruction of Customer Data upon Customer's written request.

Informatica policy is to delete Customer Data from Informatica Support Services systems upon termination of the Support Services investigation, including deletion of data from the secure FTP site, databases, hard drives, and virtual machines, and to delete the virtual meeting session, provided that correspondence between Informatica and Customer via the support portal or email relating to support cases are retained.

Destruction of data as referenced herein includes, at minimum, secure erasure of media and secure disposal of records so that the information cannot be read or reconstructed.