

28 Oct, 2025

Architecting Data Privacy Solutions with Cloud Data Masking and IDMC Services

- Robert Doan, Principal Consultant – Services Experience, IPS
- Diego Ferrandiz, Principal Solution Architect – Services Experience, IPS

Where data & AI come to 

Meet Our Webinar Experts

Presenters and Panelists Driving the Discussion



Diego Ferrandiz

Principal Solution
Architect



Robert Doan

Principal Consultant



Jim Beecher

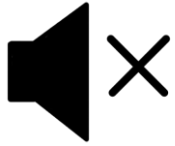
Consulting Manager



Harikrishna Tirunagaru,

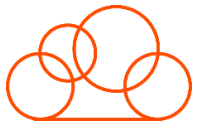
Sr. Principal Solution
Architect

Housekeeping Tips



- Today's Webinar is scheduled for **1 hour**
- The session will include a webcast and then your questions will be answered live at the end of the presentation
- All dial-in participants will be muted to enable the speakers to present without interruption
- Questions can be submitted to "All Panelists" via the **Q&A option** and we will respond at the end of the presentation
- The webinar is **being recorded** and will be available on our [Success Portal](#) - where you can download the **slide deck** for the presentation. The link to the recording will be emailed as well.
- Please take time to complete the **post-webinar survey** and provide your feedback and suggestions for upcoming topics.

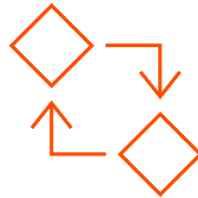
Feature Rich Success Portal



Bootstrap trial and
POC Customers



Enriched Customer
Onboarding
experience



Product Learning
Paths and Weekly
Expert Sessions



Informatica
Concierge



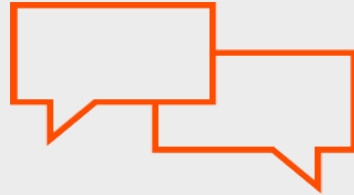
Tailored training and
content
recommendations

More Information



Success Portal

<https://success.informatica.com>



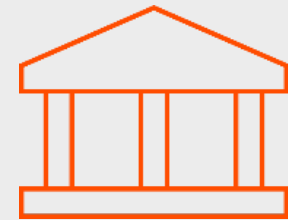
Communities & Support

<https://network.informatica.com>



Documentation

<https://docs.informatica.com>



University

<https://www.informatica.com/in/services-and-training/informatica-university.html>

Safe Harbor

The information being provided today is for informational purposes only. The development, release, and timing of any Informatica product or functionality described today remain at the sole discretion of Informatica and should not be relied upon in making a purchasing decision.

Statements made today are based on currently available information, which is subject to change. Such statements should not be relied upon as a representation, warranty or commitment to deliver specific products or functionality in the future.

Intended Participants

Data Stewards, Architects, and Privacy Experts Focused on Data Protection

This webinar is designed for professionals who are directly involved in managing and enforcing data privacy and security policies within their organizations, including:

- Data Stewards
- Solution Architects
- Technical Professionals responsible for data governance and privacy compliance
- Individuals overseeing sensitive data governance and compliance
- Professionals involved in architecting secure data environments
- Those who manage data masking implementations and are responsible for protecting Personally Identifiable Information (PII), financial data, and other sensitive attributes

If you are tasked with ensuring data privacy while enabling realistic development, testing, or operational use of data, this session will provide valuable insights to enhance your data protection capabilities using Cloud Data Masking and IDMC Services.

Agenda

- Why Data Masking?
- Data Masking methods
- Data Masking techniques
- Understanding Data Masking requirements
- Data Masking best practices
- Demo

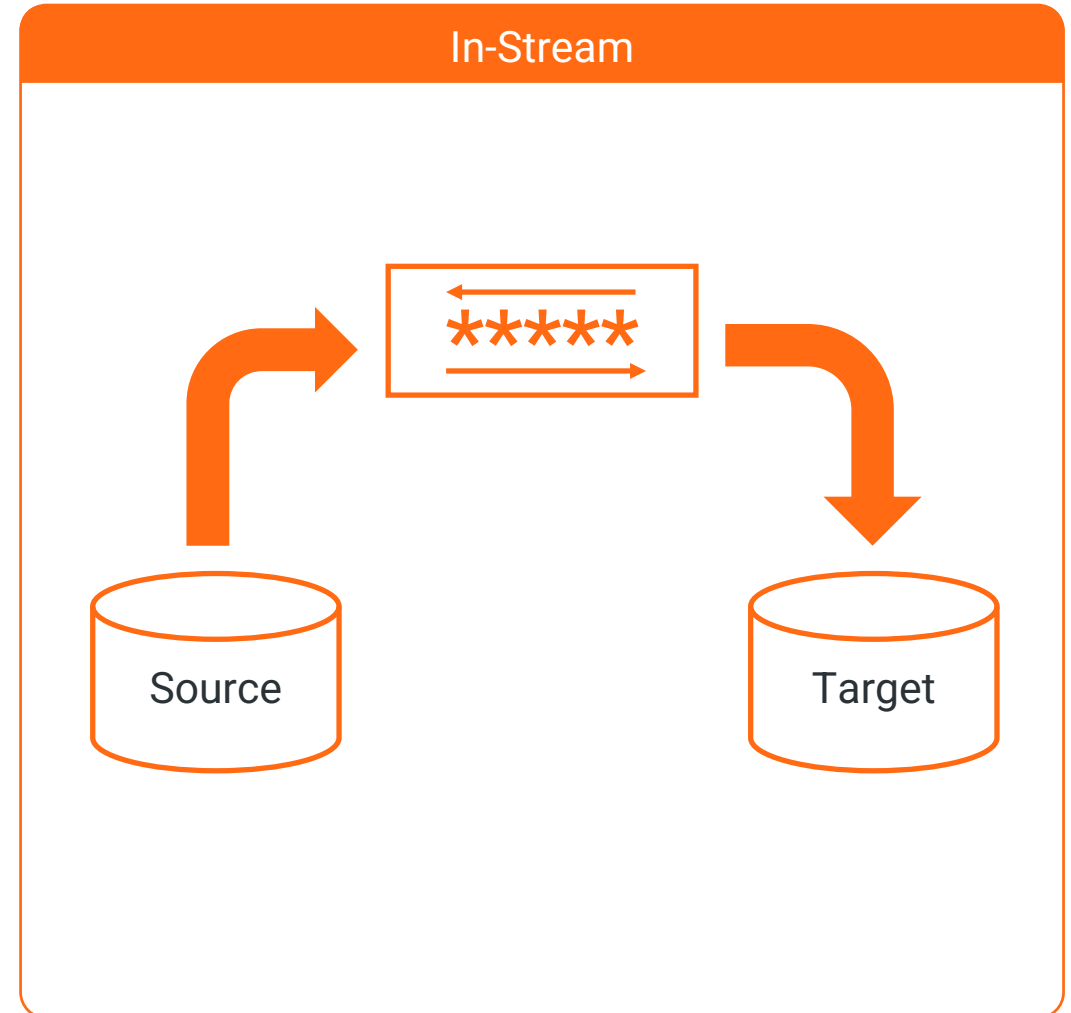
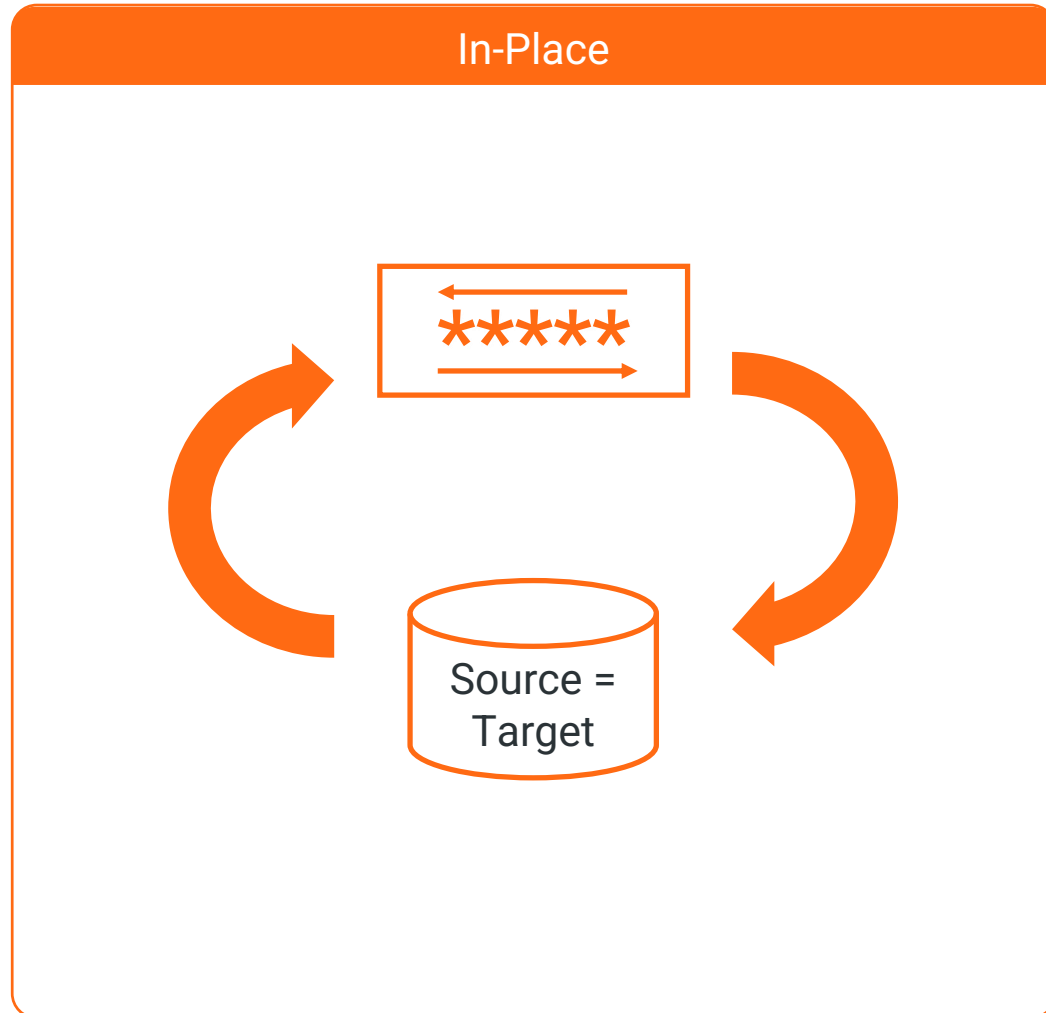
Why Data Masking Matters

Safeguarding Privacy Without Compromising Data Utility

- Data Masking is a critical technique to protect sensitive information such as Personally Identifiable Information (PII), financial data, and other confidential attributes.
- It helps prevent unauthorized access and data exfiltration, especially when sensitive data is used outside of production environments—such as in testing, development, or training.
- Data Masking preserves data format and realism, ensuring that masked data remains meaningful for application logic and usability while preventing exposure of original sensitive data.
- It plays a vital role in ensuring compliance with data privacy regulations like GDPR, HIPAA, and CCPA, which impose strict requirements and penalties for mishandling sensitive data.
- Typical challenges include maintaining data consistency, preventing reversibility, and balancing data usability with privacy.
- Properly implemented masking reduces business risks by mitigating potential privacy breaches and regulatory fines.

Data Masking Methods

In-Place and In-Stream Approaches to Secure Sensitive Data



Data Masking Methods

Comparing In-Place vs. In-Stream Techniques

In-Place

- Masks data directly in the same system and object (source = target)
- Performs an update that overwrites the original data
- Best when no copy of data is available (e.g., Salesforce instance)
- More performant due to direct data modification
- Irreversible—original data cannot be recovered
- Requires careful configuration to avoid unintended changes in production

In-Stream

- Masks data while transferring from source to a different target system
- Source data remains unchanged; masking applies only to the target
- Flexible, supports pre- and post-processing during transfer
- Typically, less performant due to extra data movement and processing
- Useful for delivering masked data to separate environments
- Suitable for complex integration and replication scenarios

Data Masking Techniques

Nullifying, Masking Out, Substitution, and Encryption Explained

Nullifying

Replacing real values with nulls, effectively removing data from view. It can be applied via masking rules or expression transformations, but care must be taken as it can affect referential integrity if used on key fields.

Masking Out

Scrambling part of a data value, such as masking portions of credit card numbers, Social Security numbers, or bank accounts by replacing part of the data with a character (e.g., "X") while leaving some information visible.

Substitution

Replacing original data with credible but unrelated values selected from data masking dictionaries. This technique maintains data format and consistency, utilizing pre-defined lookup dictionaries for fields like names, addresses, etc.

Encryption

Converting readable data into ciphertext using strong algorithms (e.g., AES-256), making data unreadable without appropriate decryption keys. In CDI, encryption and decryption functions can be used within expression transformations.

Setting the Foundation for Data Masking

Assessing Data Needs to Define Effective Masking Boundaries

- **Identify Sensitive Data Elements**

Conduct data profiling to discover and classify sensitive fields such as personally identifiable information (PII), financial data, addresses, emails, and other confidential attributes that require masking.

- **Evaluate Data Volume**

Understand the number of records and attributes in the source data that need to be masked. This assessment helps determine the best approach between In-Place and In-Stream data masking methods and informs whether data staging or replication is needed prior to masking, optimizing the overall solution strategy.

- **Define Masking Scope and Approach**

Decide on masking scope (full dataset vs. partial) and the best method (in-place or in-stream) based on data usage, system architecture, and privacy goals.

Understanding Data Masking Requirements

Maintaining Structural Integrity and Usability of Masked Data

- **Assess Data Composition and Format**

Understand the nature, format, and relationships of sensitive data to ensure masking preserves structural integrity—e.g., maintain the numeric pattern of Social Security Numbers or the geographic consistency of addresses.

- **Consider Data Usability and Integrity**

Ensure that masked data remains meaningful and usable for business applications such as development, testing, or training without compromising privacy.

- **Plan for Consistency Across Systems**

Use masking dictionaries and uniform rules to maintain consistent anonymization of data fields used across multiple systems or environments.

Understanding Data Masking Requirements

Implementing Security Controls and Verifying Masking Effectiveness

- **Address Compliance and Security Standards**

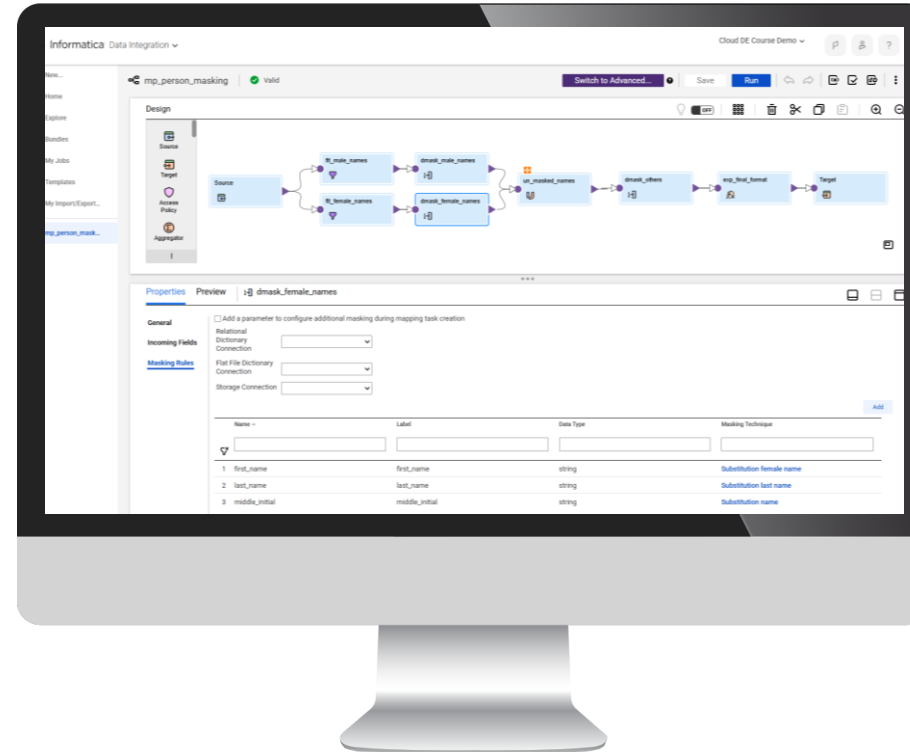
Align masking requirements with regulatory standards (e.g., GDPR, HIPAA, CCPA), enforcing access controls, auditing, and encryption where necessary.

- **Test, Validate, and Monitor**

Implement thorough testing of masked data to confirm masking effectiveness and system functionality; establish ongoing monitoring and auditing to safeguard privacy compliance.

DEMO

Masking Personal Identifiable Information (PII)



Best Practices

Ensuring Consistency, Security, and Compliance

- Identify and classify sensitive data accurately
- Use built-in Data Masking transformations within mappings
- Leverage masking dictionaries for consistent results
- Choose masking techniques suited to data types and privacy needs
- Ensure masked data remains realistic and usable
- Regularly test and validate masked data quality and security
- Monitor, audit, and document masking processes and policies
- Complement masking with encryption for enhanced security

Where data & AI come to

