Informatica

16 Sep, 2025

A Practical Introduction to Data Access Management

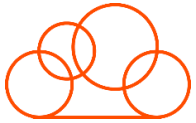
- Varun Sharma, Solution Architect, IPS
- Deep Mani, Principal Advisory Consultant, IPS

Where data & AI come to LIFE

Housekeeping Tips

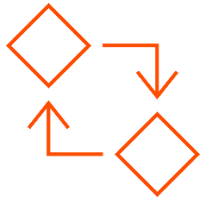
- Today's Webinar is scheduled for 1 hour
- The session will include a webcast and then your questions will be answered live at the end of the presentation
- All dial-in participants will be muted to enable the speakers to present without interruption
- Questions can be submitted to "All Panelists" via 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

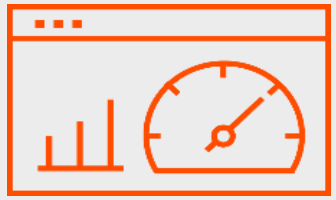


Product Learning Paths and Weekly Expert Sessions

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.

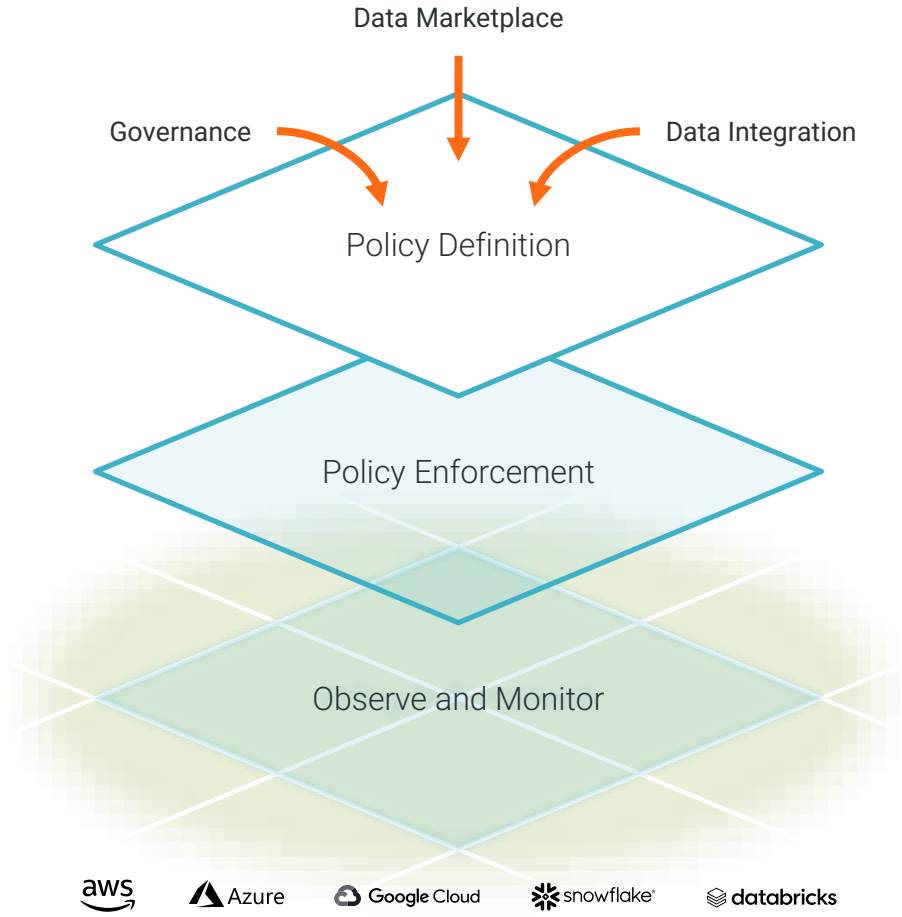
Agenda

1. Introduction – CDAM
2. Design Patterns – Policy Enforcement
3. Sizing
4. Change Management/User experience

Informatica's Data Access Management

Ensure the right people have access to the right data at the right time

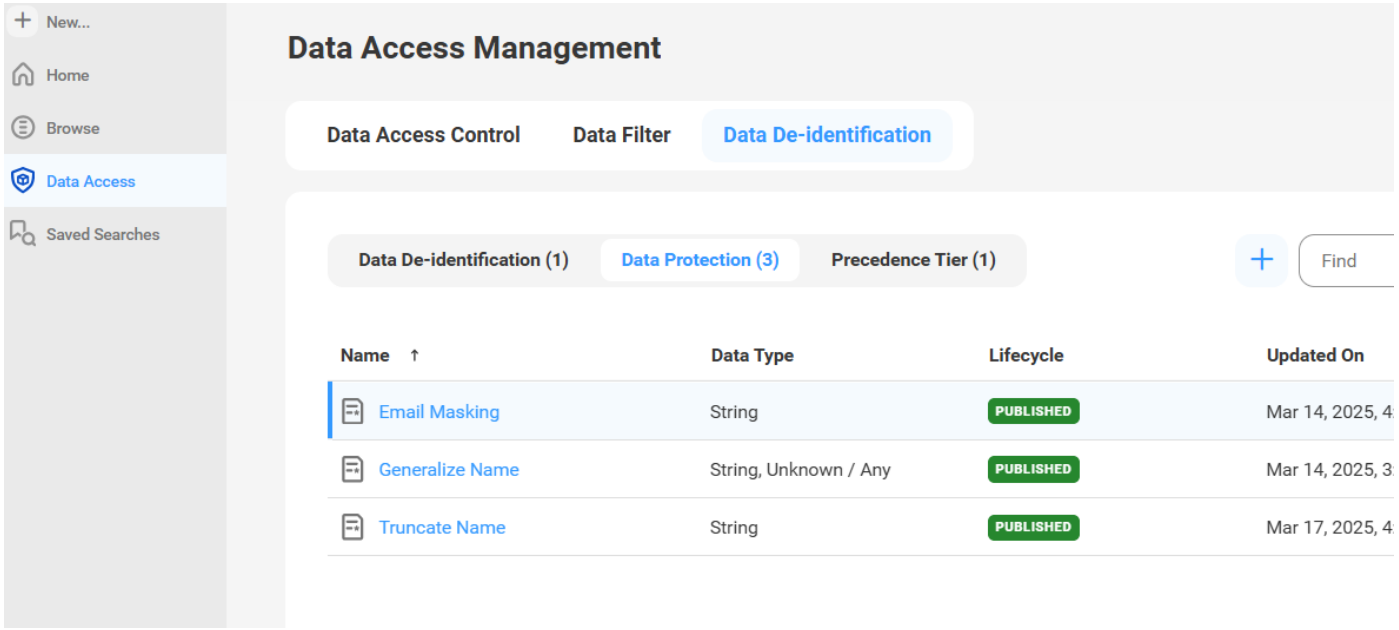
- Metadata-driven policies, universal enforcement
- Leverage discovery and classification
- Defined in one place, enforced everywhere
- Re-usable, scalable, logical policies
- Broad range of policy enforcement points
- Streamline access requests
- Observe, monitor, and audit data access



Defined in one place, enforce everywhere

Data Access Management is accessible via Data Governance and Catalog interface. Use Data Access Management page to develop policies that can be applied within Data Operation through Data Integration or self-service access through Data Marketplace.

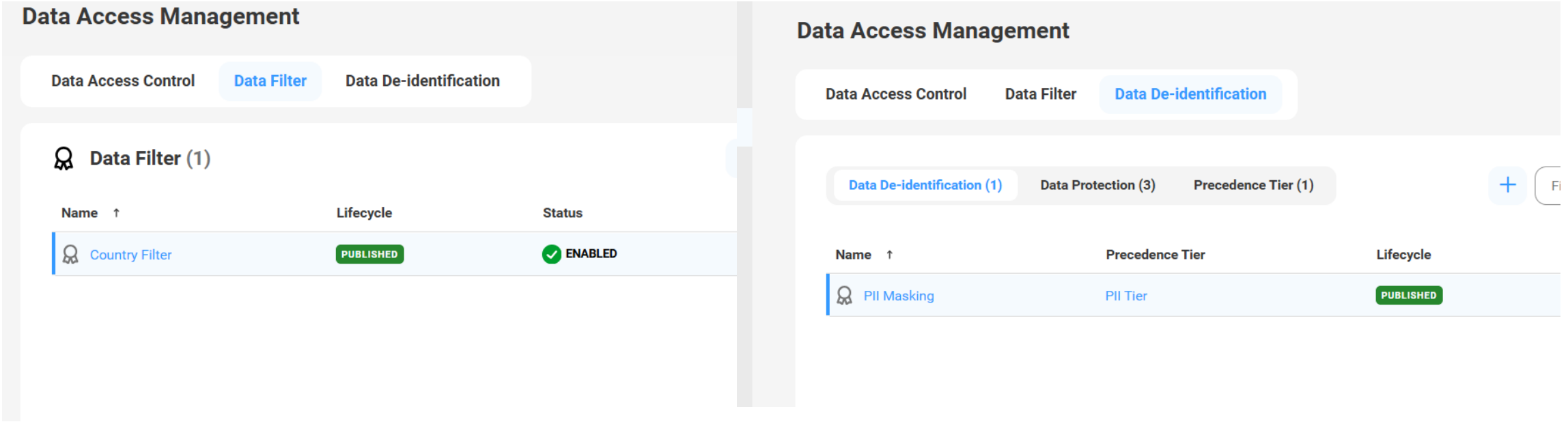
- Intuitive, no -code policy authoring to align data access management with approved business use
- A comprehensive range of controls to minimize risk and preserve utility
- Use conditional logic to compose rules mapping data classifications and contextual attributes to controls



Re-usable, Scalable, Logical Policies

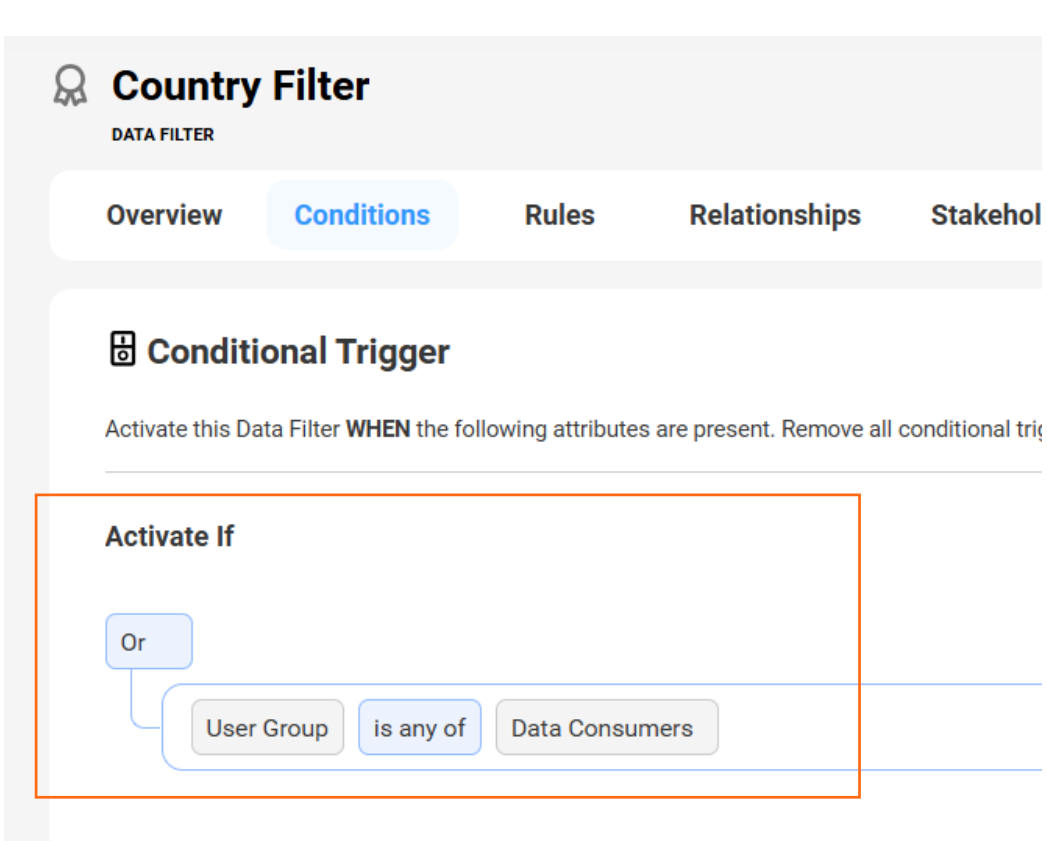
There are following types of policies to protect data and control access to your data:

- Data access control policies - grant groups of users read, write, or delete access to tables or views
- Data filter policies - restrict or limit which records Data Access Management delivers to users
- Data de-identification policies – de-identify sensitive data while retaining data utility

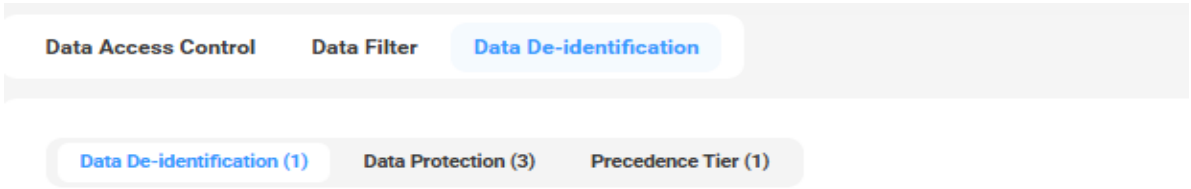


Data Filter - Conditions & Rules

The **condition** defines when the policy will be triggered, while the **rule** specifies the actions tat will be executed as part of policy.

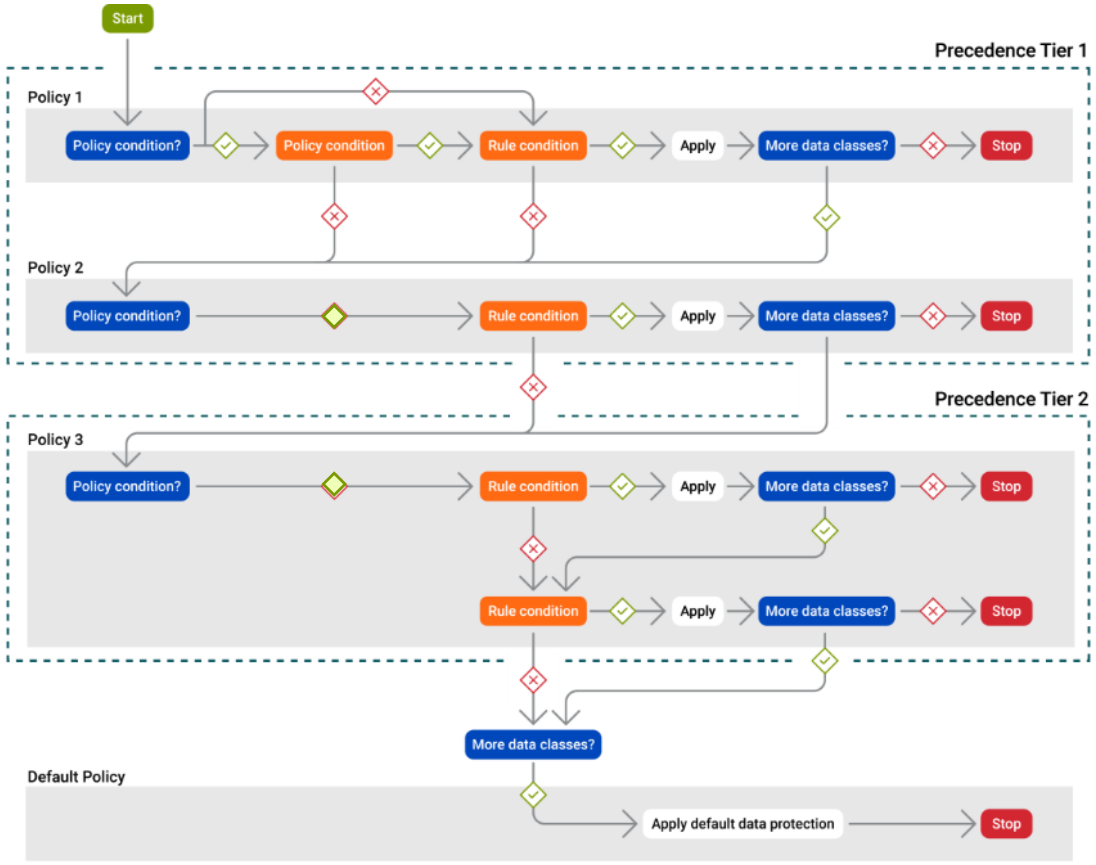


Data De-identification



Precedence tiers

- The priority and sequence of evaluating data de-identification policies and applying data protections.
- Data Access Management processes based on rank from lowest integer to highest.
- Within each precedence tier, Data Access Management processes data de-identification policies from top to bottom.

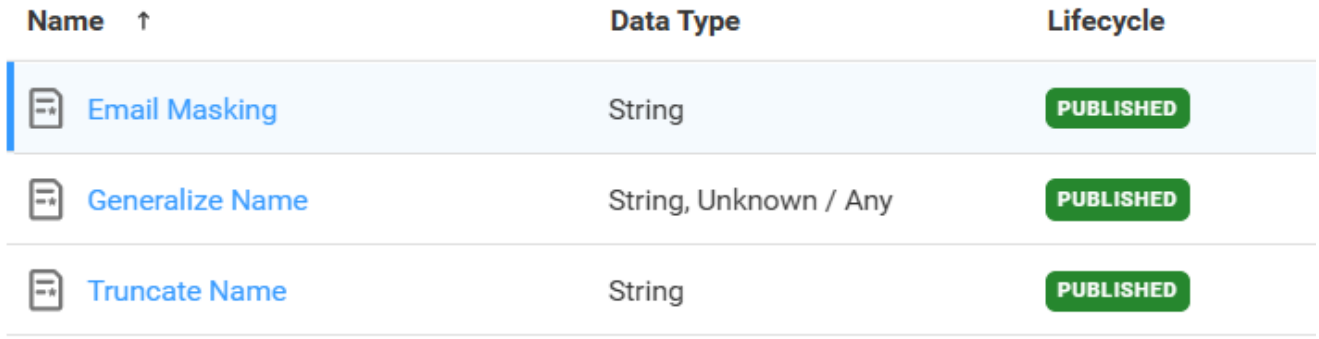


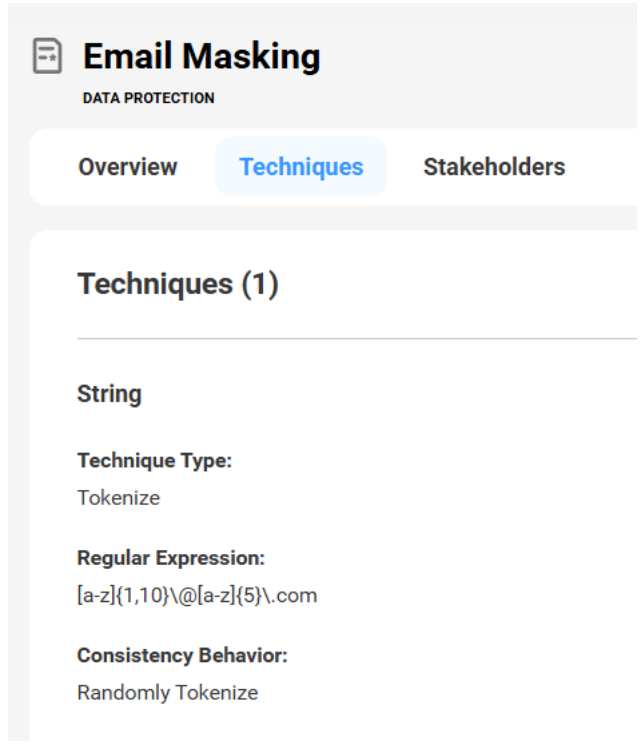
Data De-identification

Transform data to de-identify sensitive data using a range of data protection technique.

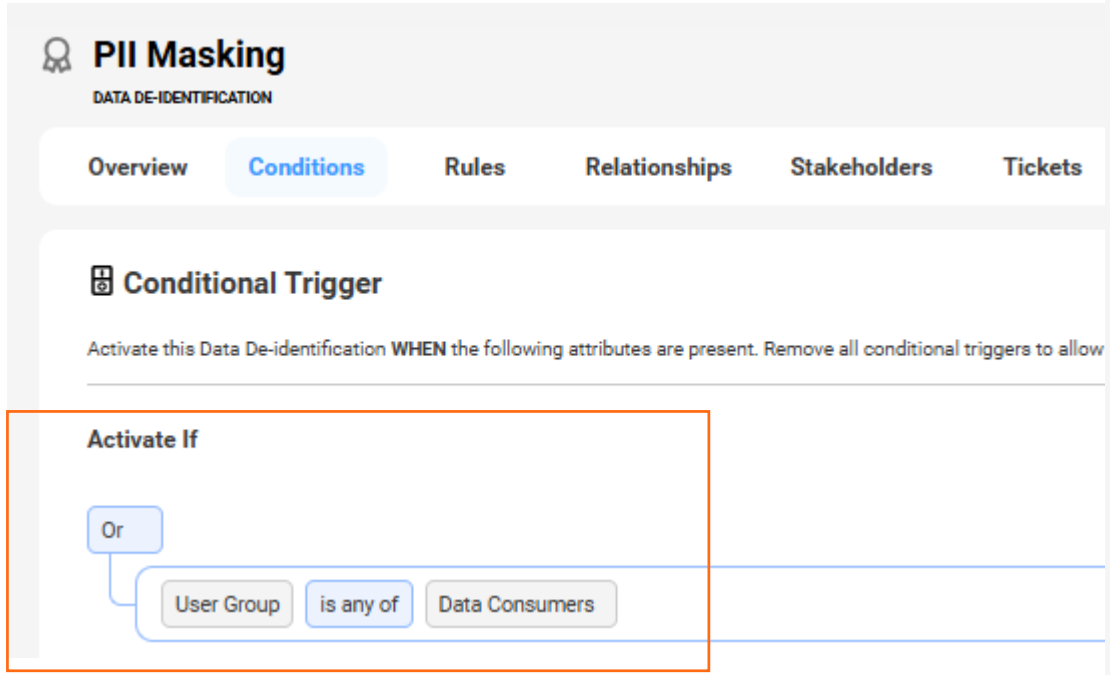
Data Protection technique includes:

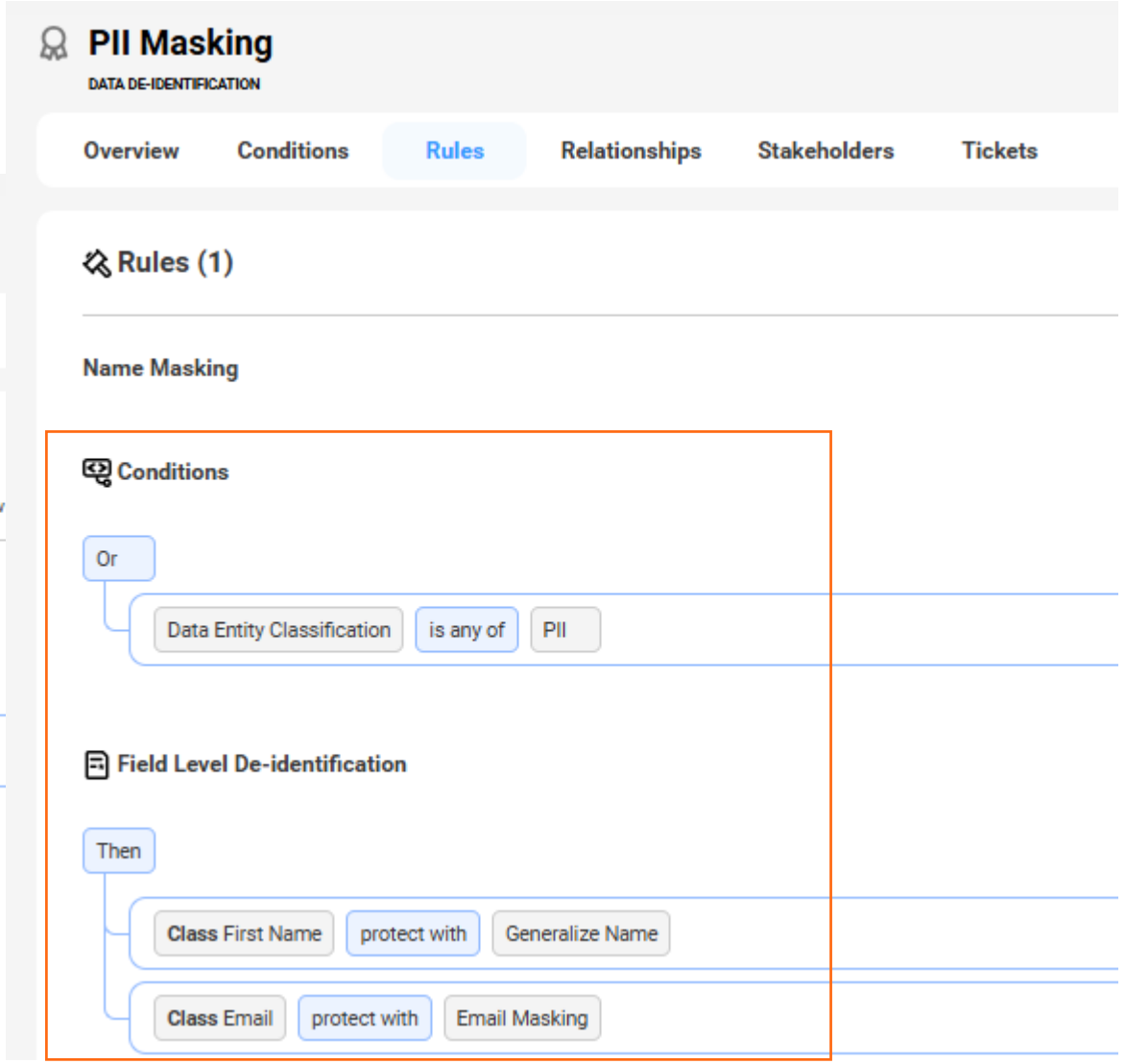
- **Tokenize** to maintain the original format and replace input with randomly generated equivalents
- **Generalize** to convert input to a common year or month
- **Truncate** to keep only minimal contents visible
- **Constant value** to mask string value with piece of text
- **Hashing** to replaced input value to hashed value
- **Substitute value** to replaces input values with readable substitutes





Data De-identification





CDAM Policy Enforcement

3 ways to achieve this

Integration into CDI.

This is your data copying mechanism. Data is read from source, policy applied, de-identified copy is written to target.

Dynamic de-identification (the proxy).

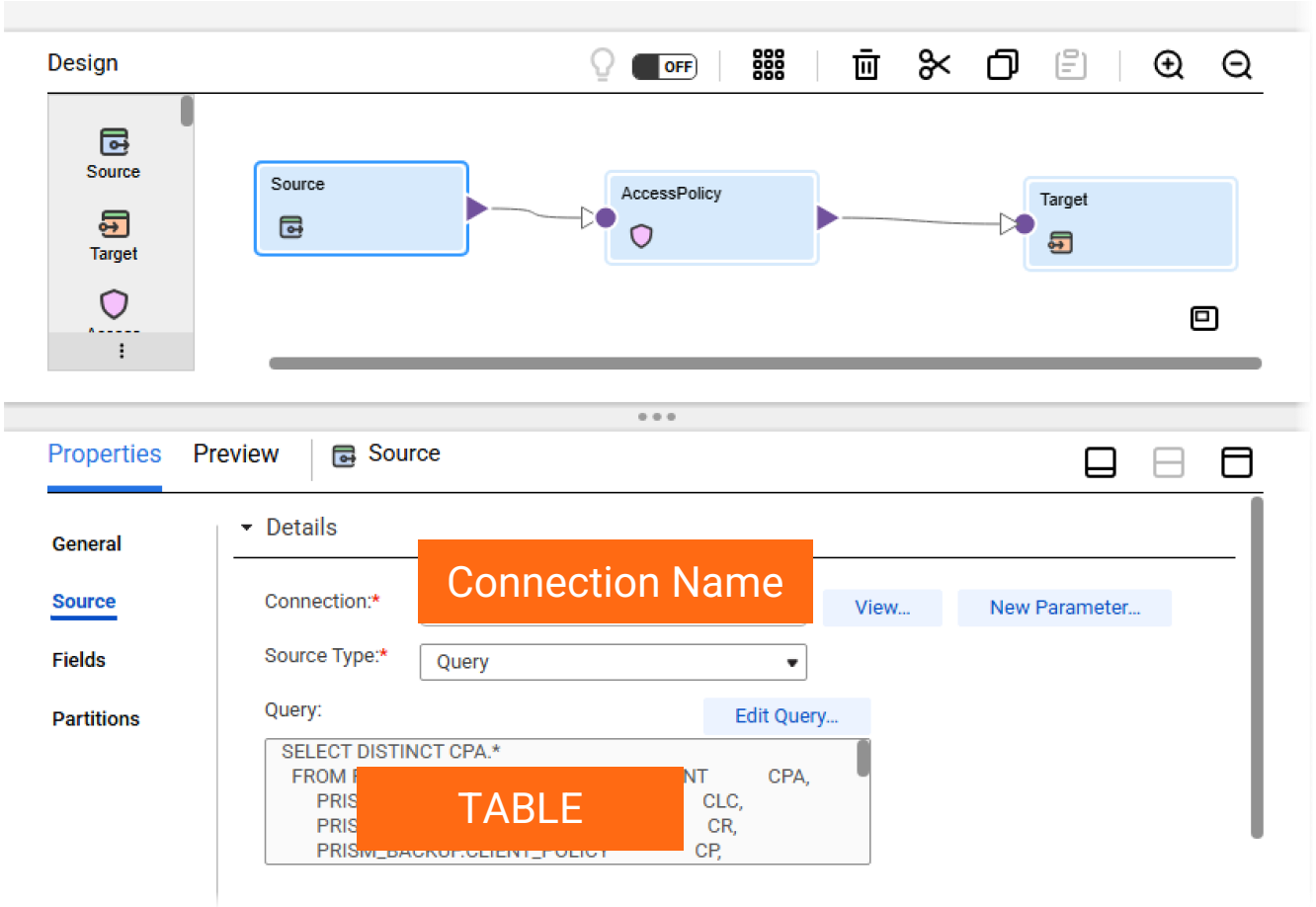
The underlying data is never changed. The proxy is a middleware layer between the data consumer (in DBeaver, e.g.) and the database. The data consumer connects to the proxy and issues queries. The proxy sends these queries to the underlying database, gets the result set, applies the policy to the result set, and sends the de-identified result set to the data consumer.

Pushdown, a.k.a. Native Access Controls.

For now, this is at an object-level only (tables/views). You create a Data Access Control policy that dictates a group has read, write, or delete permissions on some set of technical assets (tables/views). CDAM converts this to GRANT statements on the native platform, calls the native platform, and issues the appropriate GRANT statements. Effectively we sync the access controls in our policy with the access control mechanism of the native platform. We support Databricks and Snowflake.

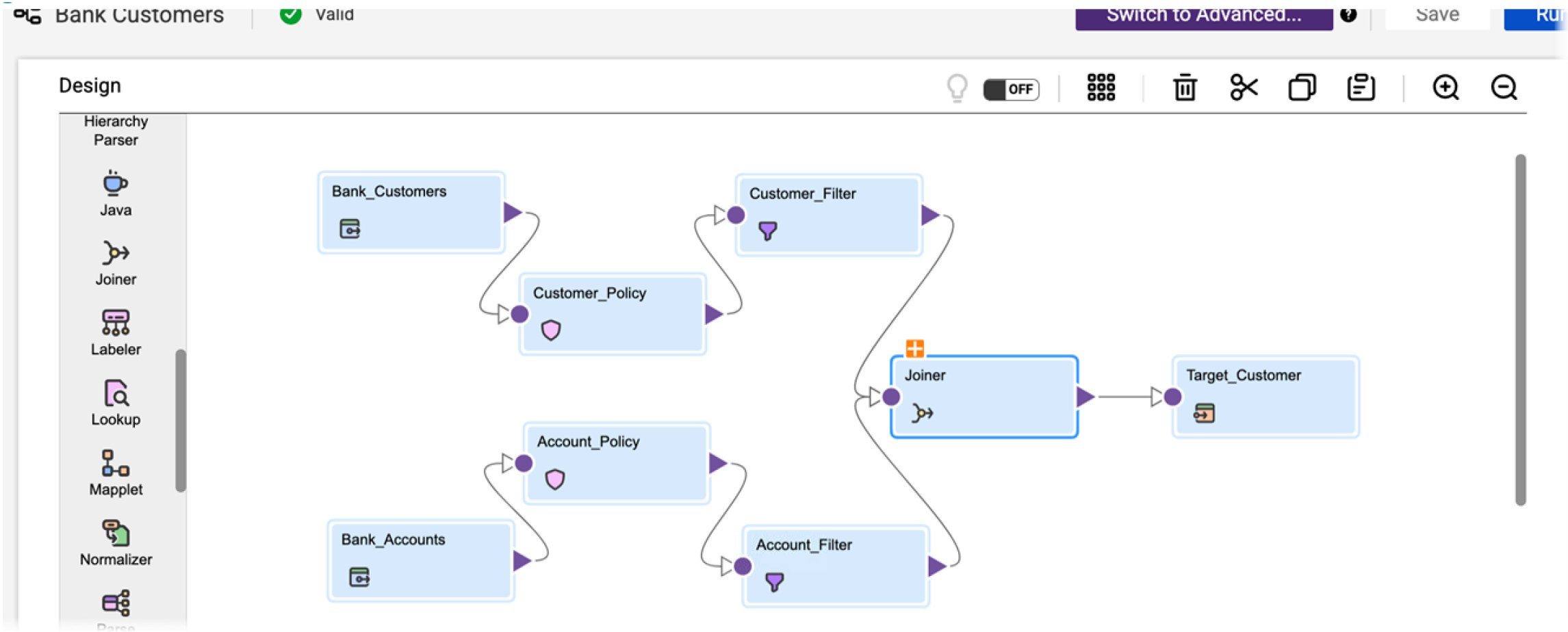
Design Patterns- CDI CDAM

Multiple tables in source – Option 1



Design Patterns- CDI CDAM

Multiple tables in source –Option 2



Design Patterns- CDI CDAM

Multiple tables in source –Option 3

Create views

Create views in applications for multiple tables

- Use views in the catalog and CDAM steps

Design Patterns- CDI CDAM

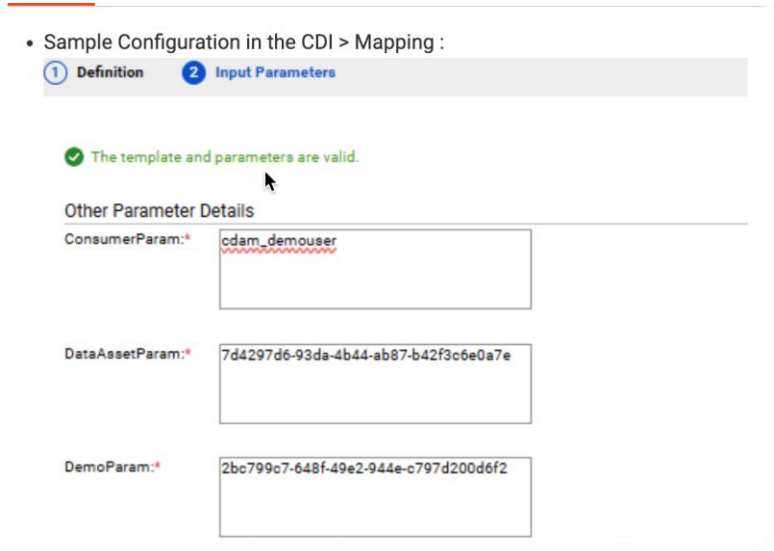
Pro's/Con's

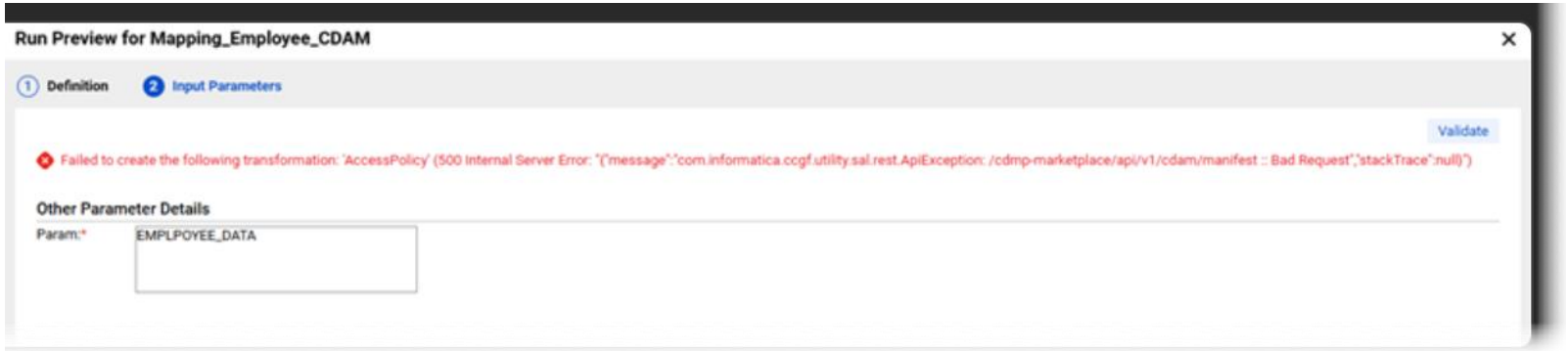
Considerations	Option1(SQ)	Option2(JOIN)	Option3(VIEWS)
Cost	Less than option 2	IPU can be more compared to option 1 and option 3	Less than option 2
Changes in Application/DB	SQL required for ETL	No changes joins are done at ETL	More Change Management on Application side

Design Patterns- CDI CDAM

Parameters : Use of reference id in Access Policy transformations

- Sample Configuration in the CDI > Mapping :





For the parameters to be used in the Access Policy Transformation , we need to make use of the Asset ID of the Usage Context / Consumer / Data Asset .

Design Patterns- CDI CDAM

Avoid Schema Mismatch

In CDI , when using snowflake as Source in 'Access Policy Transformation', all column values are redacted to NULL. The session logs indicate an error:

TRANSF_1_1_1> AccessPolicy_0 [2025-06-12 04:24:19.420] [ERROR] Result failed. Reason: Mismatch between input record schema and the Privitar Platform schema. Privitar schema has 6 field(s) with names: [ADDRESSID, CITY, PARTYID, STATE, STREET, ZIPCODE] while the input record has 8 field(s) with names: [ADDRESSID, CITY, COUNTRY, EMAILID, PARTYID, STATE, STREET, ZIPCODE]

Sizing

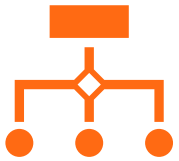
- Asset Volume & Concurrency: More data assets and simultaneous tasks demand greater processing capacity (CPU, memory, Secure Agents).
- Data Characteristics: Large, high-velocity data volumes increase resource consumption.
- Policy Complexity: Metadata-driven policies can simplify management, but complex policies (row, column, cell-level controls) demand more processing.
- Native Platform Leverage: Utilizing "policy pushdown" to native controls in platforms like Snowflake or Databricks can reduce Secure Agent workload.

CDAM-Marketplace Design Pattern

CDAM-Change Management

Workflow- User Experience

Controlled and Secure Policy Editing: Users don't edit live data access policies directly. Instead, they propose changes in a safe, version-controlled "draft" mode. This prevents accidental or unauthorized modifications to who can access sensitive data.



Automated Approval Workflows: Once a change is proposed, the system automatically routes it to the correct stakeholders (like Data Owners or a governance board) for review. This eliminates manual emails and ensures a formal, consistent approval process is always followed.

Clear, Transparent Review: Approvers are shown a simple side-by-side comparison highlighting exactly what has changed (e.g., a masking rule being removed). This allows for quick, informed decisions without having to decipher complex technical settings.

Automated Enforcement and Auditing: After final approval, the new policy is automatically deployed and enforced on the underlying data platform (like Snowflake or Databricks) with no manual steps required. The entire lifecycle—from request to enforcement—is logged in a complete audit trail for compliance.

Summary

- Permissions: https://knowledge.informatica.com/s/article/000242364?language=en_US
- CDAM: https://onlinehelp.informatica.com/IICS/prod/DGC/en/index.htm#page/ae-data-accessmanagement/The_Data_Access_Management_page.html
- Data filter: https://onlinehelp.informatica.com/IICS/prod/DGC/en/index.htm#page/ae-data-accessmanagement/Data_filter_policy_behavior.html
- Data De-identification: https://onlinehelp.informatica.com/IICS/prod/DGC/en/index.htm#page/ae-data-accessmanagement/Creating_data_de-identification_rules.html
- Data Protection: https://onlinehelp.informatica.com/IICS/prod/DGC/en/index.htm#page/ae-data-accessmanagement/Data_protections.html
- Precedence tiers: https://onlinehelp.informatica.com/IICS/prod/DGC/en/index.htm#page/ae-data-accessmanagement/Precedence_tiers.html


Informatica
Thank You
Where data
& AI come to LIFE