IBM Guardium Discover and Classify

Data Subject Access Request

Interdependence of the Indonesia PDP Law with IBM Security

Strengthen data privacy protection, build customer trust and grow your business

Secure the User

Right of Access by the Data Subject, Right to Rectification, Right to be Forgotten, Right to Object, Supervise data processing parties, Prevent illegal access to personal data

IBM Security Verify

IBM Security Trusteer

Secure the Data

Pseudonymization and Encryption of Personal Data, Ensure Confidentiality of Personal Data, Data Subject Access Request (DSAR)

IBM Security Guardium

IBM Security Discover and Classify

Secure the Device

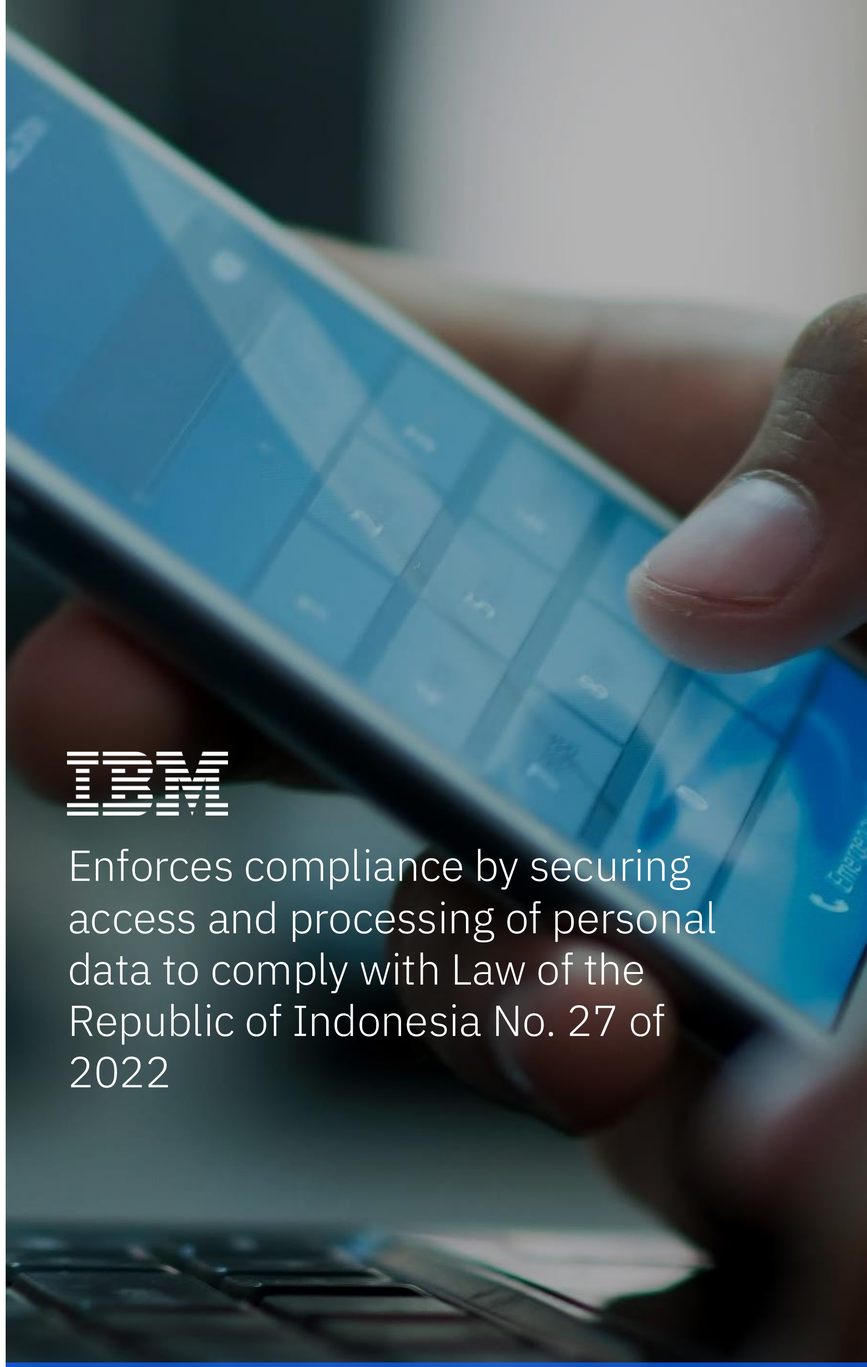
Technical measures to ensure a level of security appropriate to the risk of processing personal data

IBM Security MaaS360

Secure the Threat

Monitor and control the processing of personal data

IBM Security QRadar XDR



IBM Security / © 2023 IBM Corporation

You can’t secure what you don’t know exists

Discover your sensitive data

Database — MongoDB. ORACLE MySQL IBM Db2 elasticsearch

Cloud — aws Azure

SaaS — salesforce slack Jira workday. Office 365

DBaaS — snowflake databricks

Understand your data

Build an asset inventory

- Discover structured & unstructured data
- Classify how sensitive it is
- Map to regulations and policies
- Compile this to a central inventory

Explain data for compliance

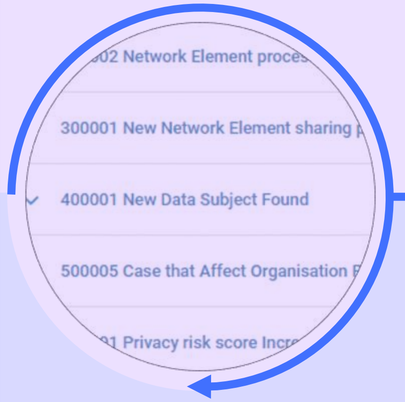
- Who and what is accessing your data?
- What have they done, and what *can* they do?
- Who has privileged entitlements to sensitive data?
- What controls are in place on this data store?
- When did this change take place and who performed it?

I can tell you

IBM Security Guardium

Discover

Automate discovery and classification of on premises and cloud data and uncover critical vulnerabilities



Guardium
Discover and Classify

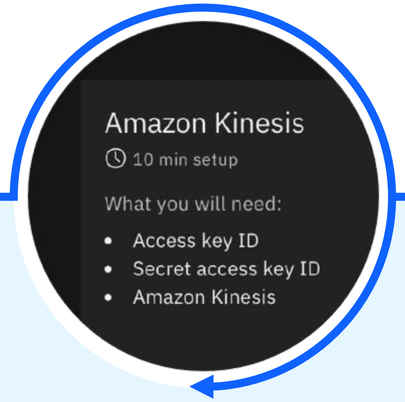
Encrypt

Safeguard privacy and confidentiality of data at rest, in motion, and in use with encryption and key management

Guardium
Data Encryption and Key Lifecycle Manager

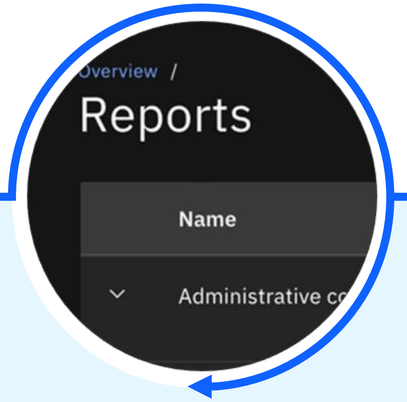
Monitor

Protect and harden on-prem and cloud data sources, including Azure Event Hubs, AWS Kinesis, Snowflake, SAP, etc.



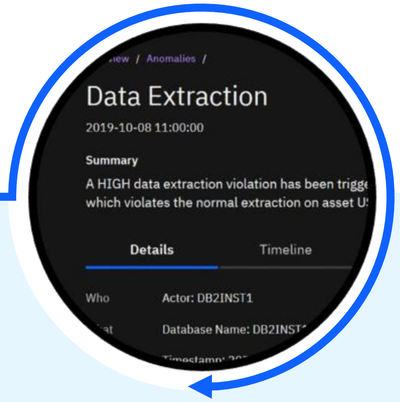
Analyze

Generate reports and automate notification on long-term data activity within seconds, across the audit lifecycle



Respond

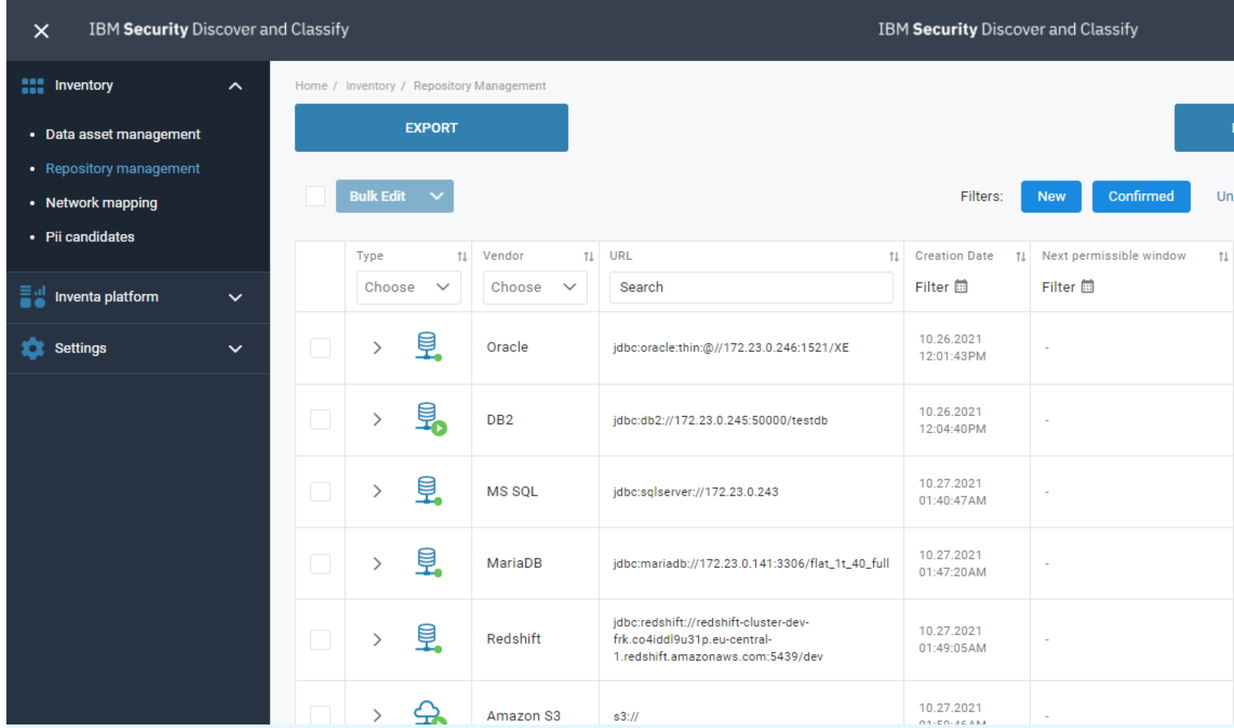
Identify and respond to compliance and data security risks, across environments and teams, from one place



Guardium
Data Protection and Insights and Vulnerability Assessment

IBM Guardium Discover and Classify

Uncover your sensitive data intelligence to speed up security, compliance, and privacy use cases



Identify unknown data at scale

A network-based approach to discover and map sensitive data, both at rest and in-motion

Classify sensitive data with AI

AI & ML classify both structured and unstructured data at the data element or repository level

Automate insights, playbooks

Understand data subjects, data lineage, stakeholders, processes… then assess risk, assist breach investigations, speed compliance, and remove unnecessary PII

Integrate with Guardium

Ready-to-use integration with Guardium Data Protection for stronger data classification, database monitoring, and vulnerability assessment

Data Aware Security

Enables clear protection by classifying data sources to prioritize data protection needs

Improve Efficiency

Significantly reduces false positives, which means analysts don’t need to spend hours on them

Reduce Risk

Improve risk posture by combining data classification, activity monitoring and vulnerability management

IBM Security Discover and Classify

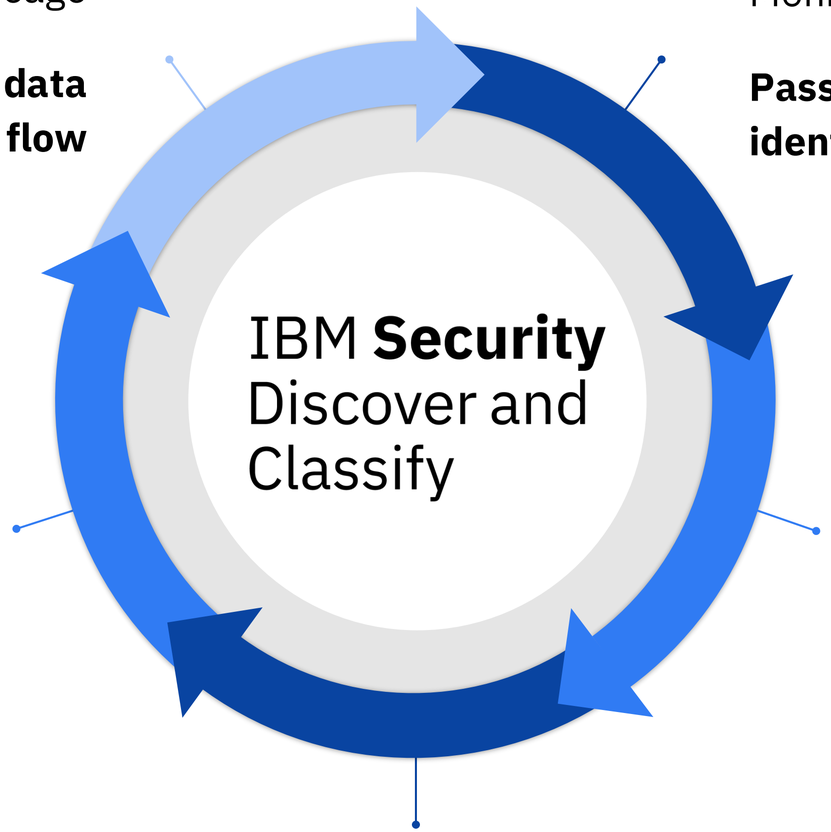
How does IBM Security Discover and Classify work?

Produce data lineage

Produce master catalog, data lineage and data flow

Monitor network traffic

Passively monitor network and identify network elements



Consolidate PII

Consolidate sensitive data and combine with root data asset

Identify sensitive data on the network

Identify sensitive data and data at rest repositories to be scanned

Scan repositories

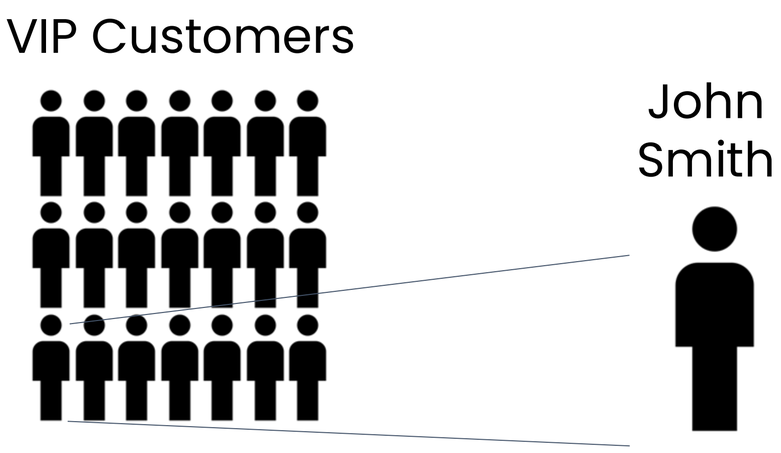
Scan data at rest structured and unstructured repositories

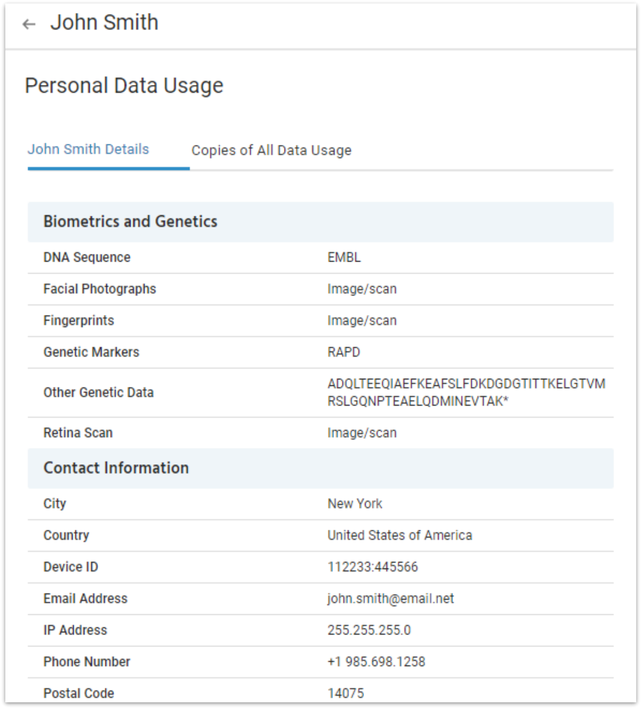
IBM Security Discover and Classify

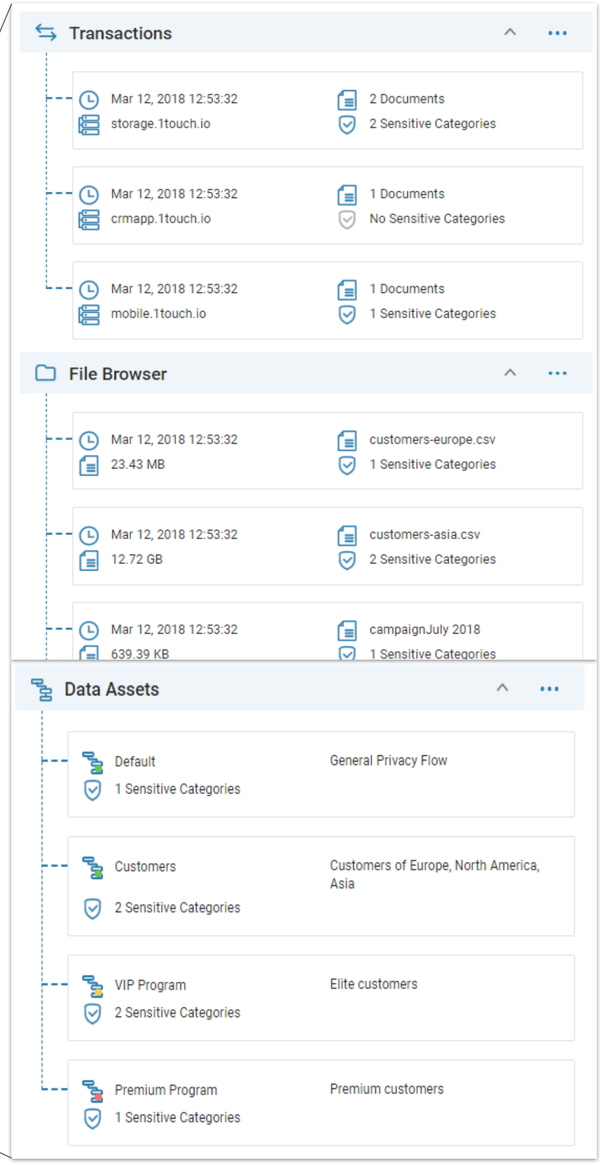
IBM ISDC for Privacy Producing Master Catalog

Update data subject record and references to found PII

- Files, transactions, database records, log files, etc.
- Data subject relationship(s) with company







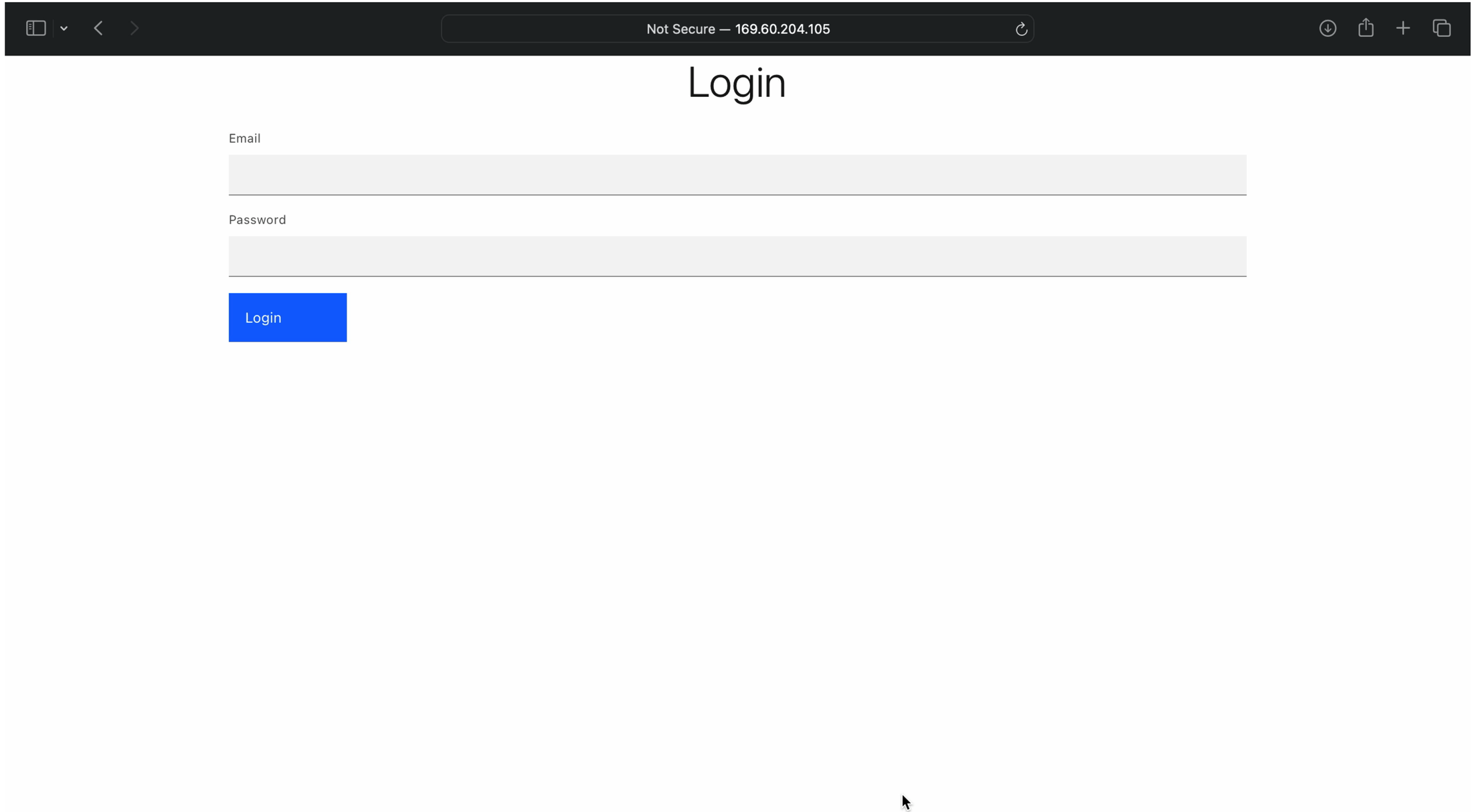
Customer

Request Access for data personal

Request Access for data personal

Customer:

- Go to user portal
- Asking for access data personal

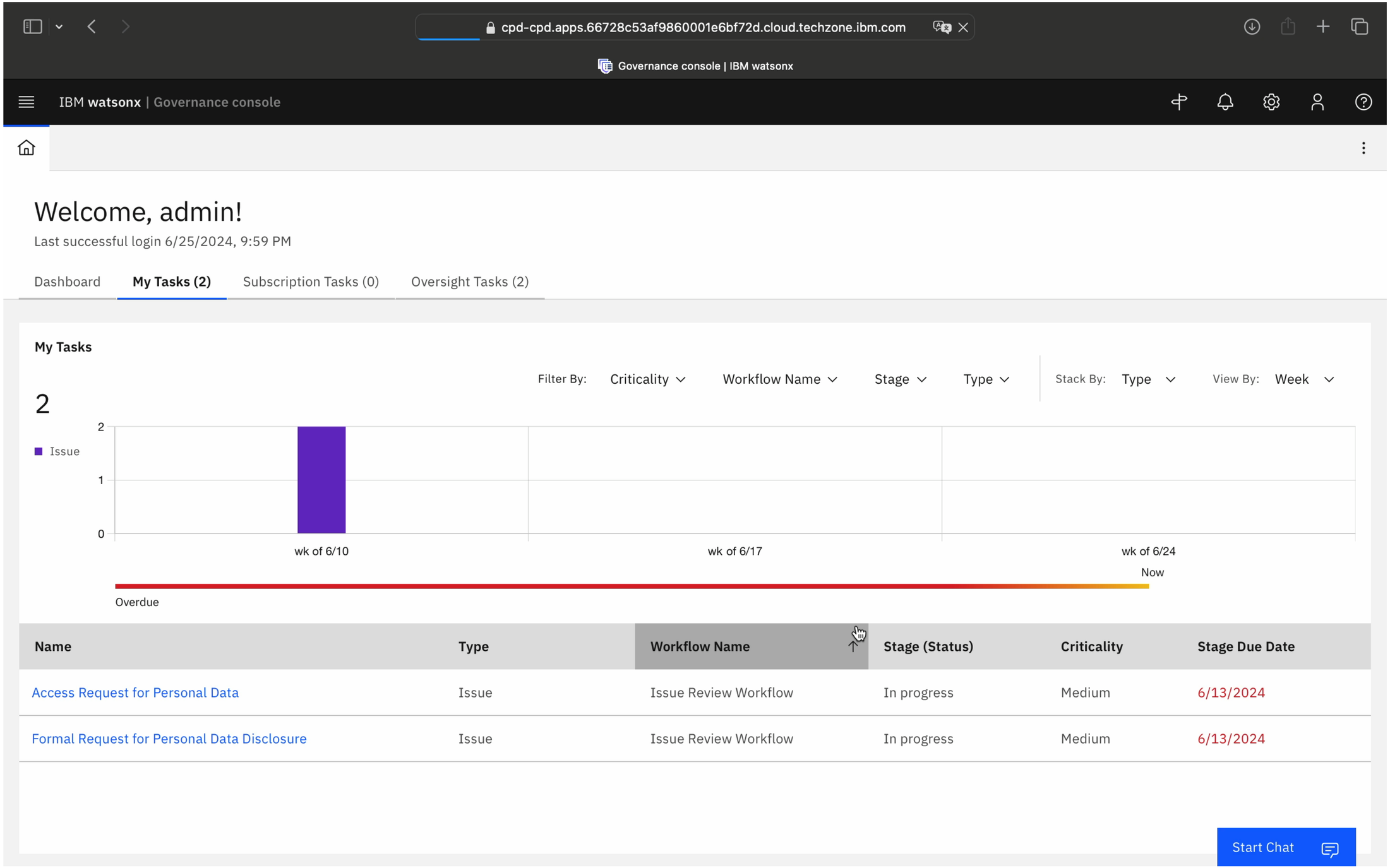


Data Protection Officer (DPO)

Issue data personal

Request Access for data personal

DPO:
- Check request
- Request issue to Data Owner for data personal

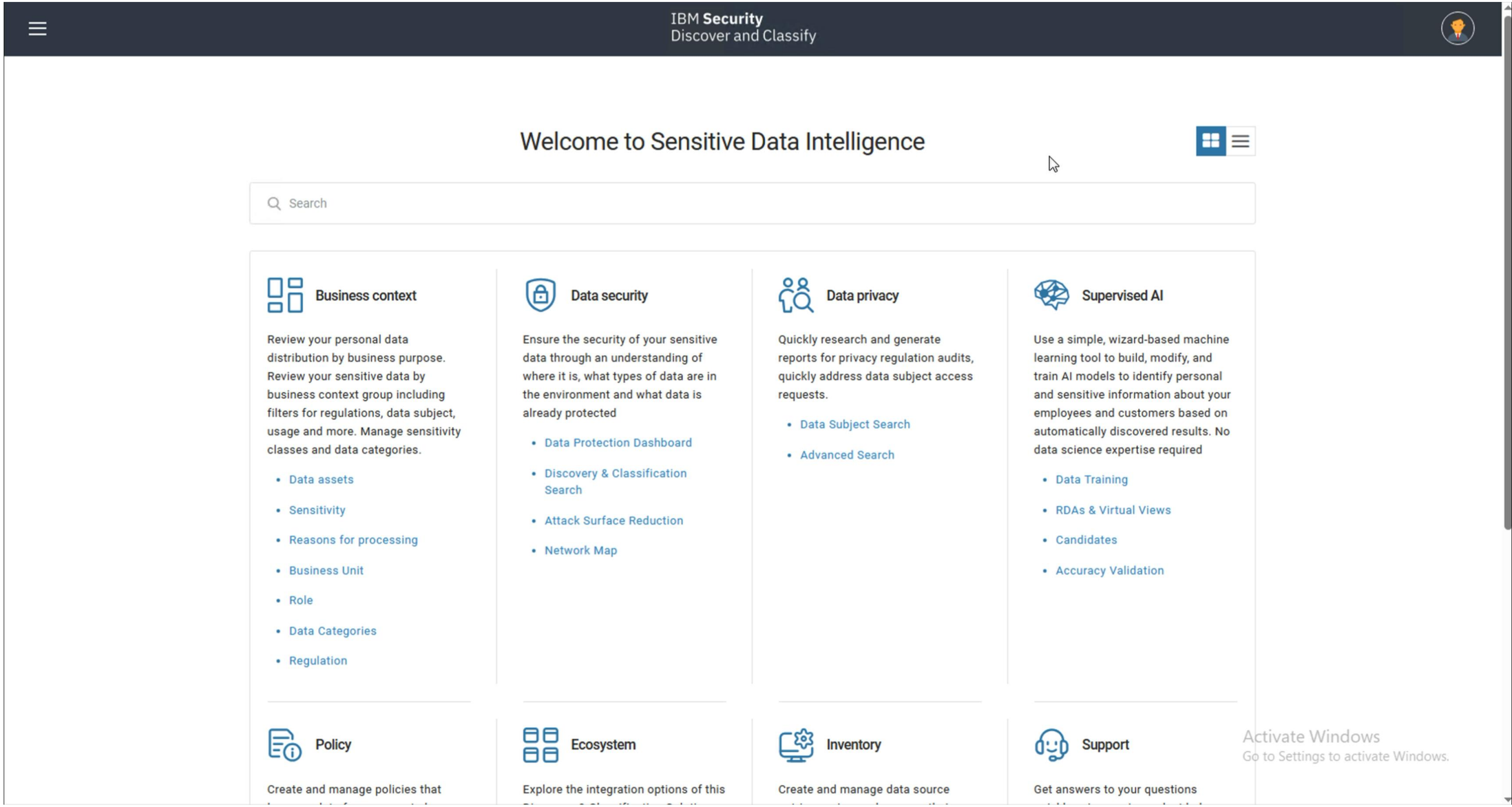


Data Owner

Discover an access of data personal

Data owner will check and generate the report

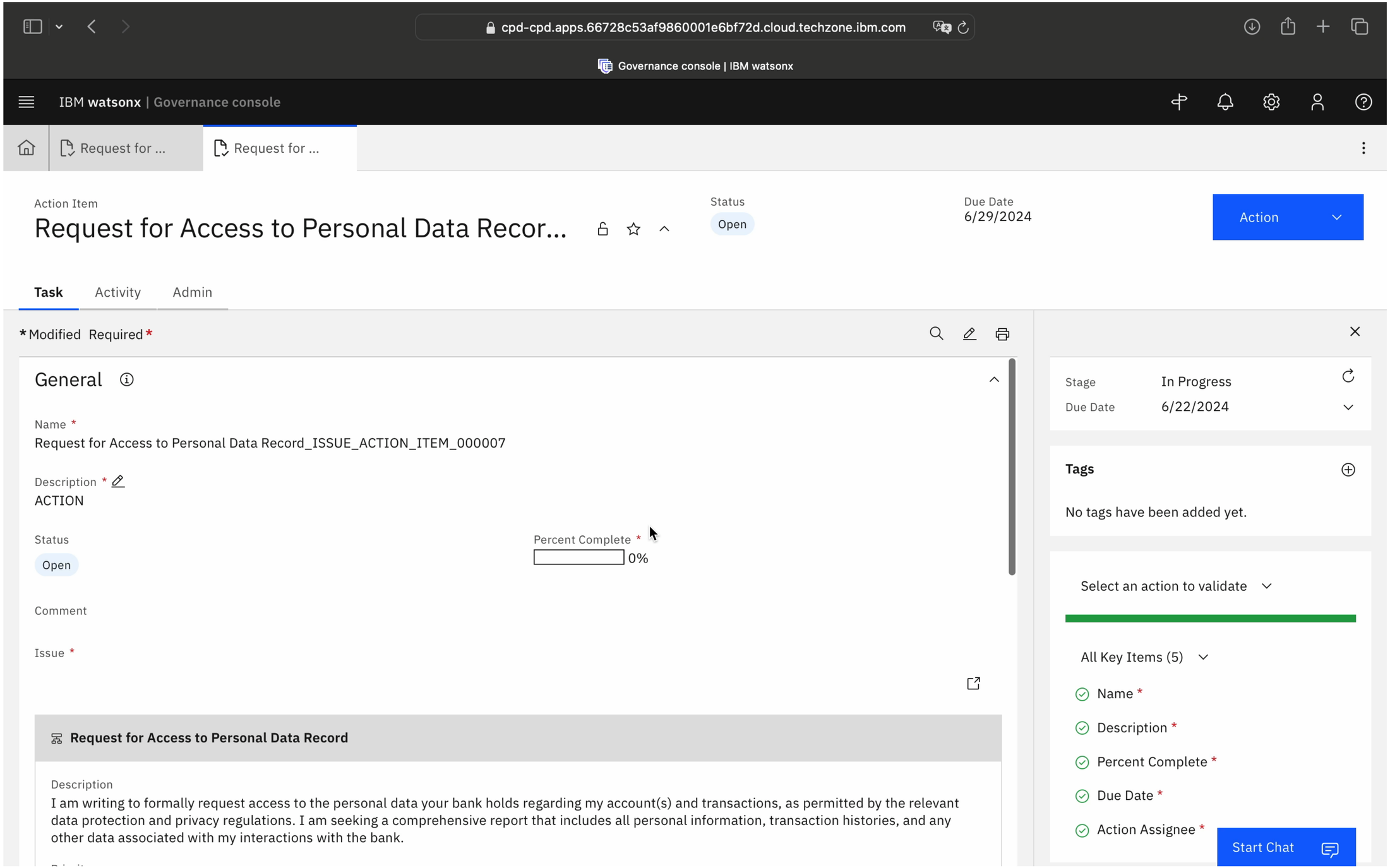
Data Owner:
- Check request
- Get the personal data access



GUID: bae347eb-f3d2-4356-a2fa-58e084f03348

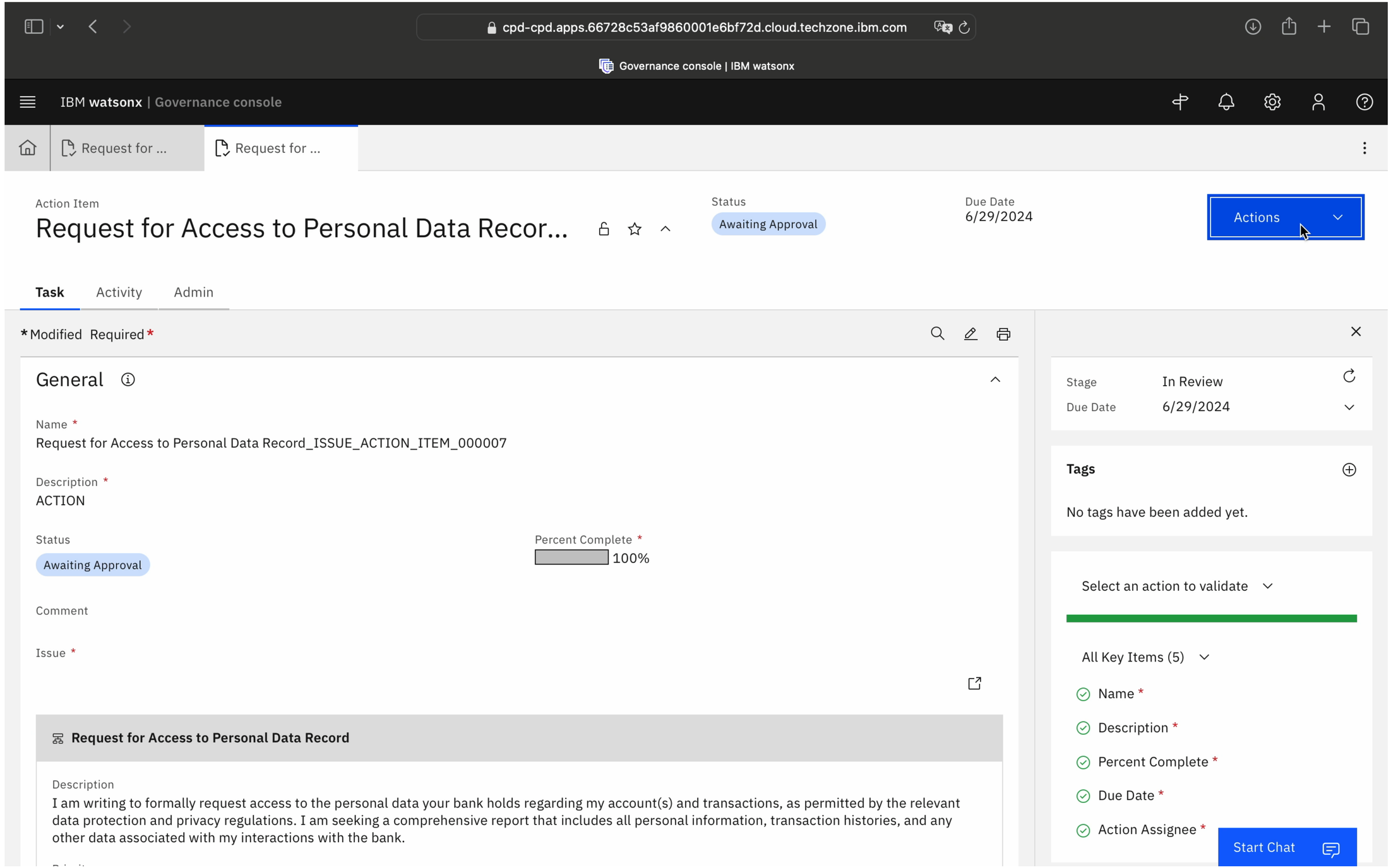
Data owner will check and generate the report

Data Owner:
- Submit and request for approval (as expected or not)
- Waiting and completed



Data Protection Officer (DPO)

Approve and closed the issue

Request Access for data personal

DPO:
- Check approval
- Completed the issue request