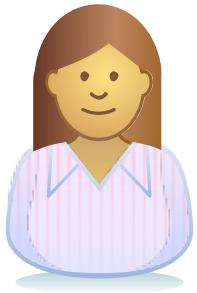
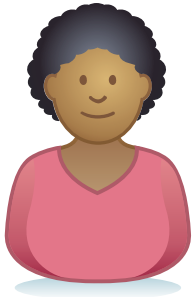
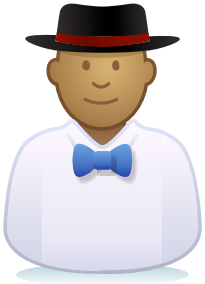
End User



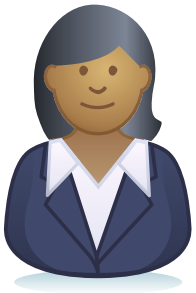
Cloud Operations



Data Officer



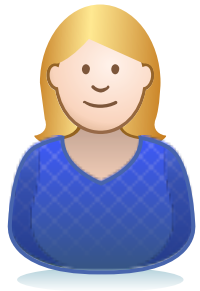
Data Processing Authority



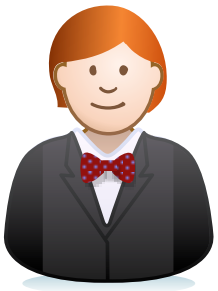
Client Representative

Offering Manager

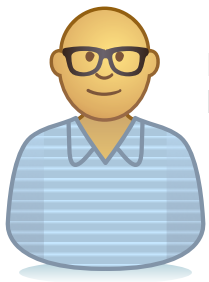
Security Officer



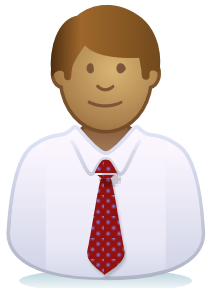
Incident Manager



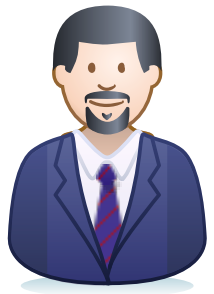
Sales



Development Lead



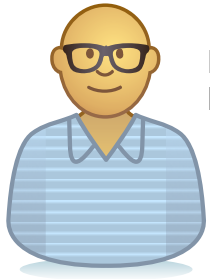
Privacy Officer



Executive Leadership

Offering Manager

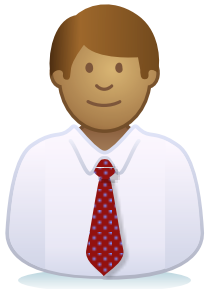
The offering manager is responsible for investment decision related to the offering. As such they make choices on the types of data that are collected by their offering, the processing that the offering performs on data, what data is stored and shared. These decisions set the stage for the compliance requirements that the offering must support and the offering manager is accountable for achieving the balance between data processing function verses data protection and the privacy of the individuals who are the data subjects.



Development Lead

The development lead (aka offering architect) is an experience developer in the offering team who is responsible for:

Ensuring the offering development team is practicing privacy by design and secure engineering in the coding of the offering.
Maintaining the data processing descriptions for the offering.
Overseeing the testing of the offering before deployment to ensure it passes the data processing certification and security certifications.

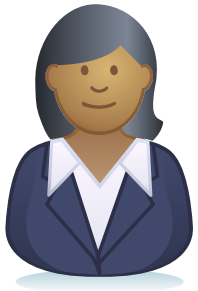


Privacy Officer

The privacy officer is a person assigned to the offering team to provide expertise on privacy legislation. He/she is aligned with the Corporate Chief Privacy Office and the related legal teams.

The privacy officer is responsible for:

Providing guidance on privacy matters relating to the offering's capabilities.
Deciding on whether a privacy impact assessment is required.
Completing and publishing the privacy impact assessment.
Seeking resolution of the privacy concerns raised in the privacy impact assessment.
Signing off the data processing certification
Supporting the offering team during a data breach incident.



Client Representative

A client representative is an employee, or legal representative of one of our clients that is able to sign a contract with use around the use of our offerings. This includes the permission to collect, store and process data, plus agreements on sharing and distribution of the data.

A client representative is also involved during any data breach incident where personal data from their tenant is compromised.

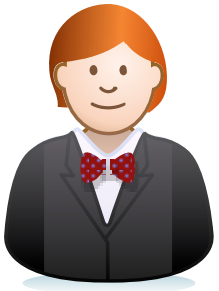
End User

The end user is a person that uses one of our offerings' user interfaces, or services via one of our client's UIs or services.

Typically, an end user may be an employee of one of our clients, or a customer of one of our clients, or an individual that has signed up to our services in a B2C style interaction.

Our offerings may gather information about the end users to improve the service we offer and this may require that our offering gets additional permission to collect and process this data.. End users may upload data about other people into our offerings and in this instance our offerings need to request confirmation that the end user has permission from the people described in the data to perform this processing.

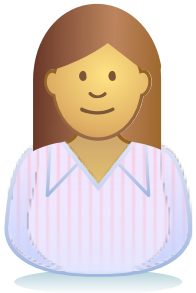
See the personal data processing patterns to understand the role of the end user in our privacy and security compliance.



Sales

The sales teams negotiate the sales of our offerings to clients. They need to be sure that our clients understand and agree to the processing that an offering performs.

They make use of the data processing and security descriptions made available to them through the cloud transparency tool and standard contracts that include these descriptions to ensure we have legal rights to process our client's data.



Cloud Operations

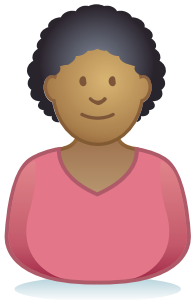
The cloud operations team run the offering in production. The practices they operate are critical to keeping the offering's data safe. They must also maintain the infrastructure definitions in the data catalog so there is traceability from the offering to the deployment environment.

Security Officer

The security officer is a person assigned to the offering team to provide expertise on security. He/she is aligned with the Corporate Chief Information Security Office.

The security officer is responsible for:

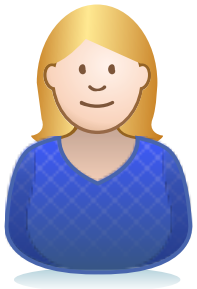
Supporting the use of secure engineering in the development team, providing guidance on security matters relating to the offering's capabilities.
Signing off the security certification when the offering is deployed.
Ensuring secure operations is being practiced in the cloud data centers.
Supporting the offering team during a data breach incident.



Data
Officer

The data officer is a person assigned to the offering team to provide expertise on the business value of data and how it can be used to improve the capabilities and margins that that the offering brings. He/she is aligned with the Corporate Chief Data Office.

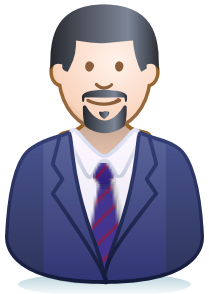
The data officer supports the offering manager as they plan the capabilities for the next release of the offering with expertise and research into the latest data capture and processing research. Our cognitive strategy encourages a greater collection and use of data in our offering and the data officer's input into the offering planning process is invaluable.



Incident Manager

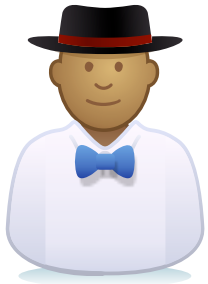
The incident manager is part of the CSIRT team and works with the offering team and cloud operations team to handle reported security incident such as the detection of suspicious activity in order to bring it to resolution. As such the incident manager is a key figure during a data breach incident.

The CSIRT team and Chief Privacy Office have agreed procedures to follow during a data breach incident.



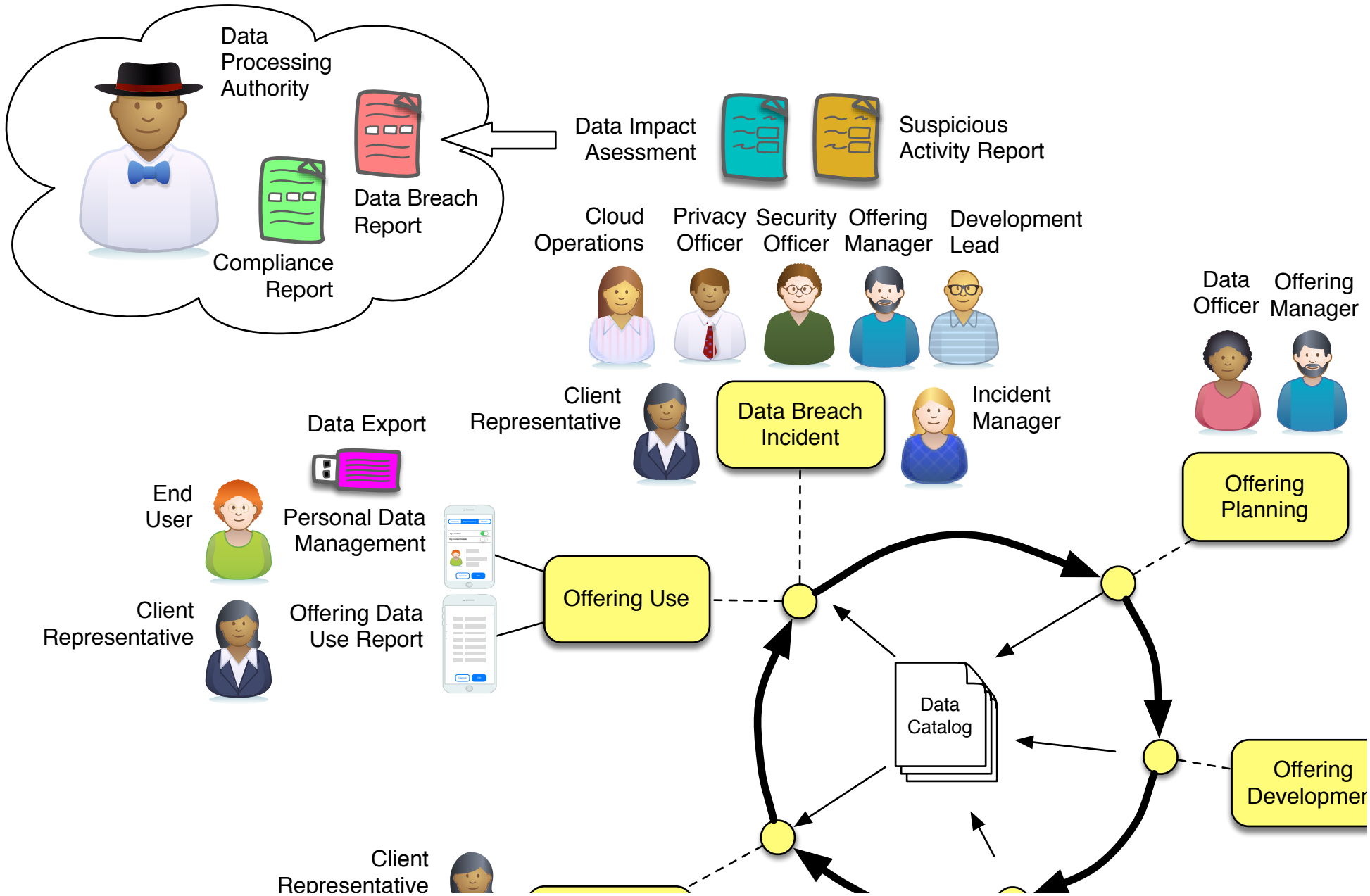
Executive Leadership

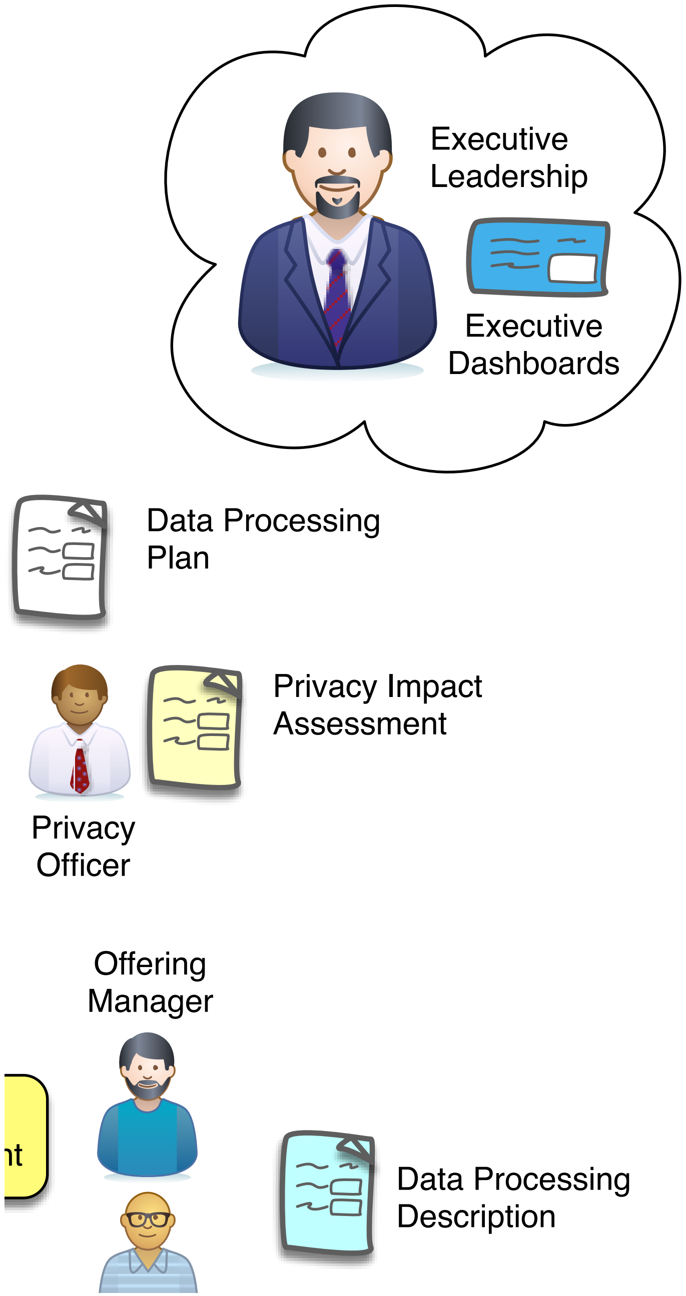
The executive leadership of a business unit (general manager, development leadership and offering management leadership) have overall accountability for the business success and compliance of their offerings. Today they have access to dashboards that show the business metrics for their offerings. This will be complemented with information about the compliance of their offerings and the choices being made by their teams.

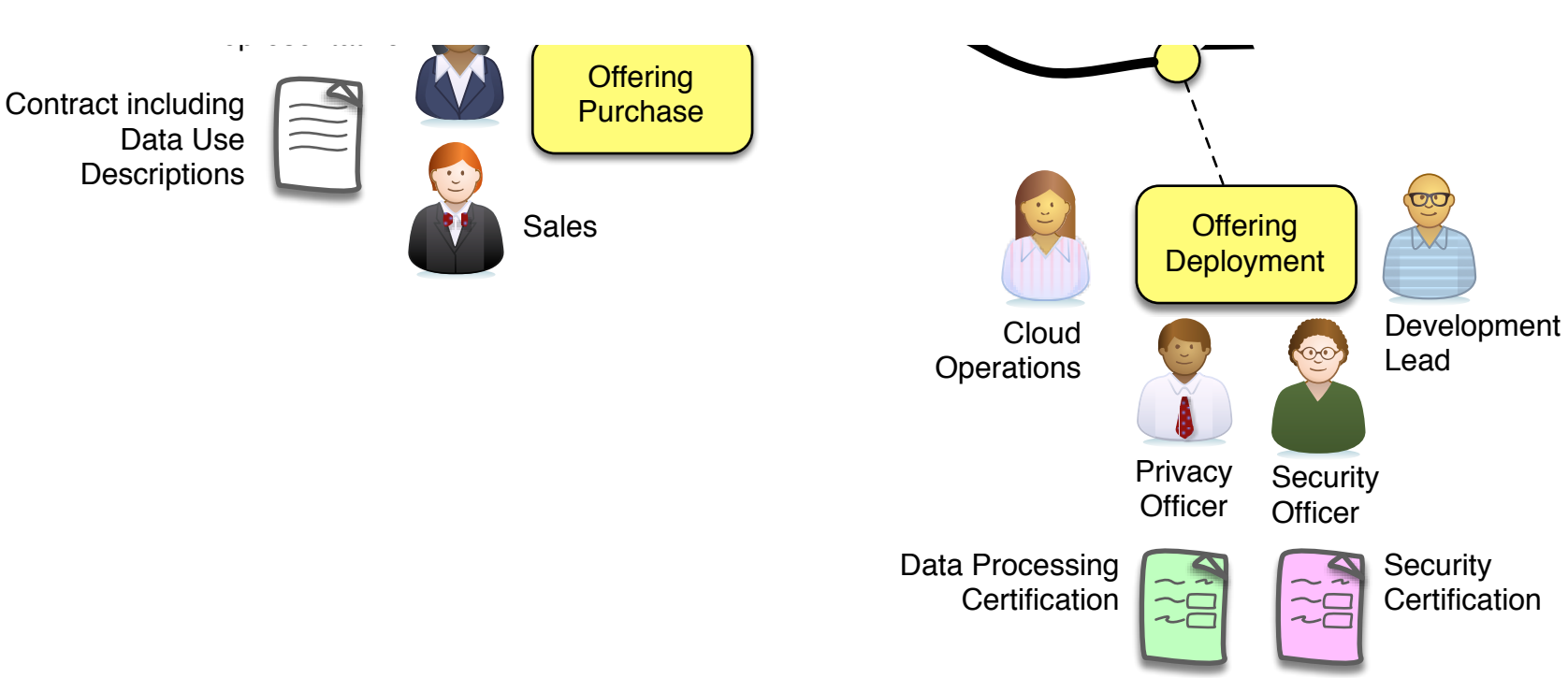


Data Processing Authority

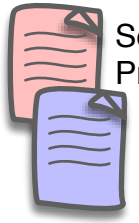
Every country has an organization that administers the local data protection law. These organizations are collectively referred to as the DPAs or data processing authorities. They set additional requirements for processing data both in their country and about their citizens and are involved in data protection disputes and data incidents. Some may request an audit of the data protection and privacy processes that are used for our offerings.


Data
Processing
Authority
Data Breach
Report
Compliance
Report
Data Impact
Asessment
Suspicious
Activity Report
Cloud
Operations
Privacy
Officer
Security
Officer
Offering
Manager
Development
Lead
Data
Officer
Offering
Manager
Client
Representative
Data Breach
Incident
Incident
Manager
Data Export
End
User
Personal Data
Management
Offering Use
Offering
Planning
Client
Representative
Offering Data
Use Report
Data
Catalog
Offering
Developmer
Client
Representative


Executive
Leadership
Executive
Dashboards
Data Processing
Plan
Privacy Impact
Assessment
Privacy
Officer
Offering
Manager
Data Processing
Description


Contract including
Data Use
Descriptions
Offering
Purchase
Sales
Offering
Deployment
Cloud
Operations
Development
Lead
Privacy
Officer
Security
Officer
Data Processing
Certification
Security
Certification

Development Lead



Secure Engineering Practice

Privacy by Design Practice

Data Processing Plan

Privacy Impact Assessment

Data Processing Description

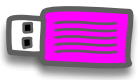
Data Processing Certification

Security Certification

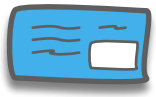
Contract including
Data Use
Descriptions

Offering Data
Use Report

Personal Data
Management



Data Export



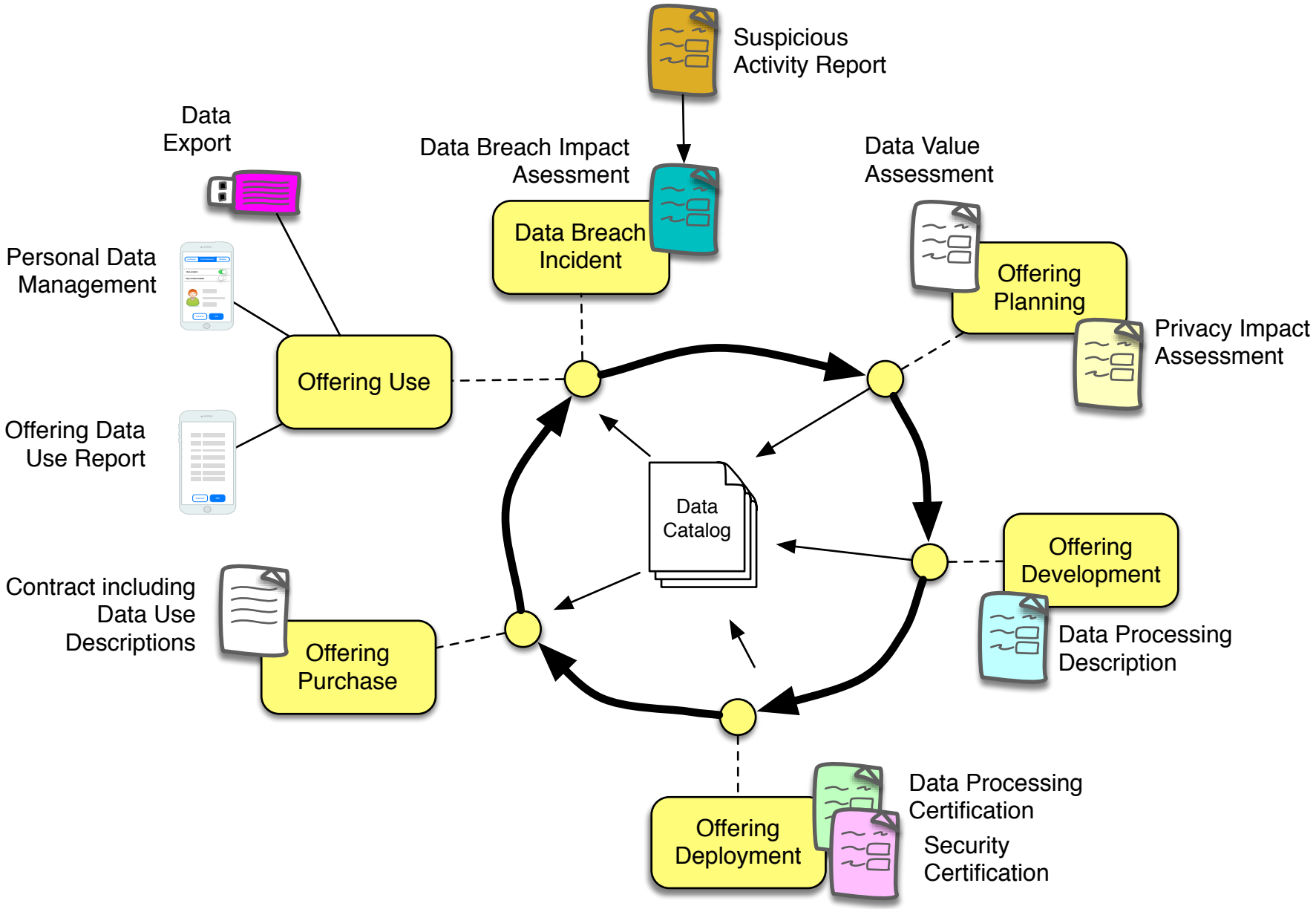
Executive
Dashboards

Compliance
Report

Suspicious
Activity Report

Data Impact
Asessment

Data Breach
Report


Suspicious
Activity Report
Data
Export
Data Breach Impact
Asessment
Data Value
Assessment
Personal Data
Management
Data Breach
Incident
Offering
Planning
Privacy Impact
Assessment
Offering Use
Offering Data
Use Report
Data
Catalog
Offering
Development
Contract including
Data Use
Descriptions
Offering
Purchase
Data Processing
Description
Offering
Deployment
Data Processing
Certification
Security
Certification

Secure Engineering Practice

Privacy by Design Practice

Secure Operations Practice