# GRACE HOPPER CELEBRATION

ANITA B.ORG

# Privacy Engineering for Everyone

The 2018 General Data Privacy Regulation (GDPR) brought personal data privacy to the forefront. Privacy engineering, as part of the overall product development lifecycle is paramount to ensuring compliance with the new (and more complex) regulations. This workshop will present the basics of privacy engineering and demonstrate, through privacy engineering exercises, that we all can have a privacy engineering mindset.

# About Us

**Lisa Bobbitt (**CISSP, CIPM, CIPP-E): Lisa is Cisco's Privacy Engineering architect missioned with embedding data privacy and security controls into Cisco's processes, applications, and offerings.. Lisa has a BS in Computer Science from NCSU and an MBA from Duke University.

lbobbitt@cisco.com

**Michele D. Guel:** Michele is a Distinguished Engineer and IoT Security and Privacy Strategist at Cisco, she has been an avid speaker, influencer and evangelist in the cybersecurity industry for 30 years.

mguel@cisco.com


**Saran Morgan (**CIPM, CIPP-E): Saran joined Cisco's Chief Privacy Office in 2018 as the 1st person to enter Cisco with the title of Privacy Engineer. She's committed to increasing privacy awareness, supporting privacy by design, and advocating for comprehensive data privacy legislation.

samorgan@cisco.com

# Take away

## Privacy Regulations

The landscape is expanding and changing rapidly due to volume of data generated.

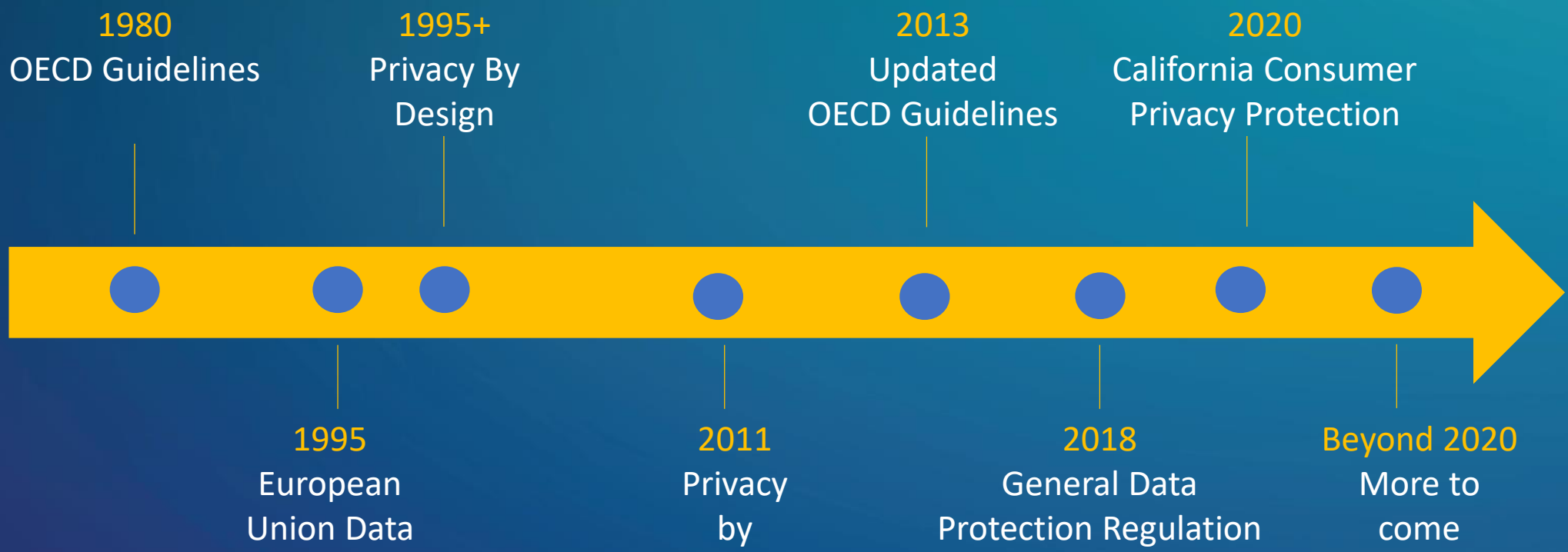
## Mindset of a Privacy Engineer

You see data and think about data context. You understand the high-level basics of privacy engineering.

## Emerging Technology Changes the Game

A stronger awareness of how emerging technology creates challenging for ensuring data privacy.

# The Changing Privacy Landscape



# Global Privacy Regulation are Increasing

Imagine it is 2025…

Each of us experience over 5000 digital interactions per day. Lifesize robotic assistants are commonplace and wearable screens are hip.

- There are 75 billion “things”.
- There are 175 zettabytes of data.
- AI will animate, infiltrate and accelerate every part of our lives.

# How Can I Manage and Protect Data?

- How do I know what data my application and/or I process?
- What is the definition of privacy in my environment?
- Why is privacy so important for my organization?
- How do I know what is required for privacy?
- How do I prioritize these requirements?
- How do I develop these in my processes and technology?

# Privacy Engineering is the Answer

Data-centricity

Innovation

Process

*"A methodology to design, build, and manage things that process PII in a manner that provides appropriate levels of privacy throughout the lifecycle of the data that is processed."*

## Data Centricity

Privacy engineering is about curating throughout the data lifecycle to maximize value and minimize risk.

Where other requirements are constrained by the application software or the platform hardware, data requirements must be managed across the scope of the organization, its sub-processors, and your customers and employees.

## Innovation

Privacy Engineering is also “innovation centric” and works to balance the data’s opportunity value with the risk given the sensitivity and personal potential harm of the data in the processing context.

Innovation is about maximizing the value of data while ensuring privacy, security, and compliance.

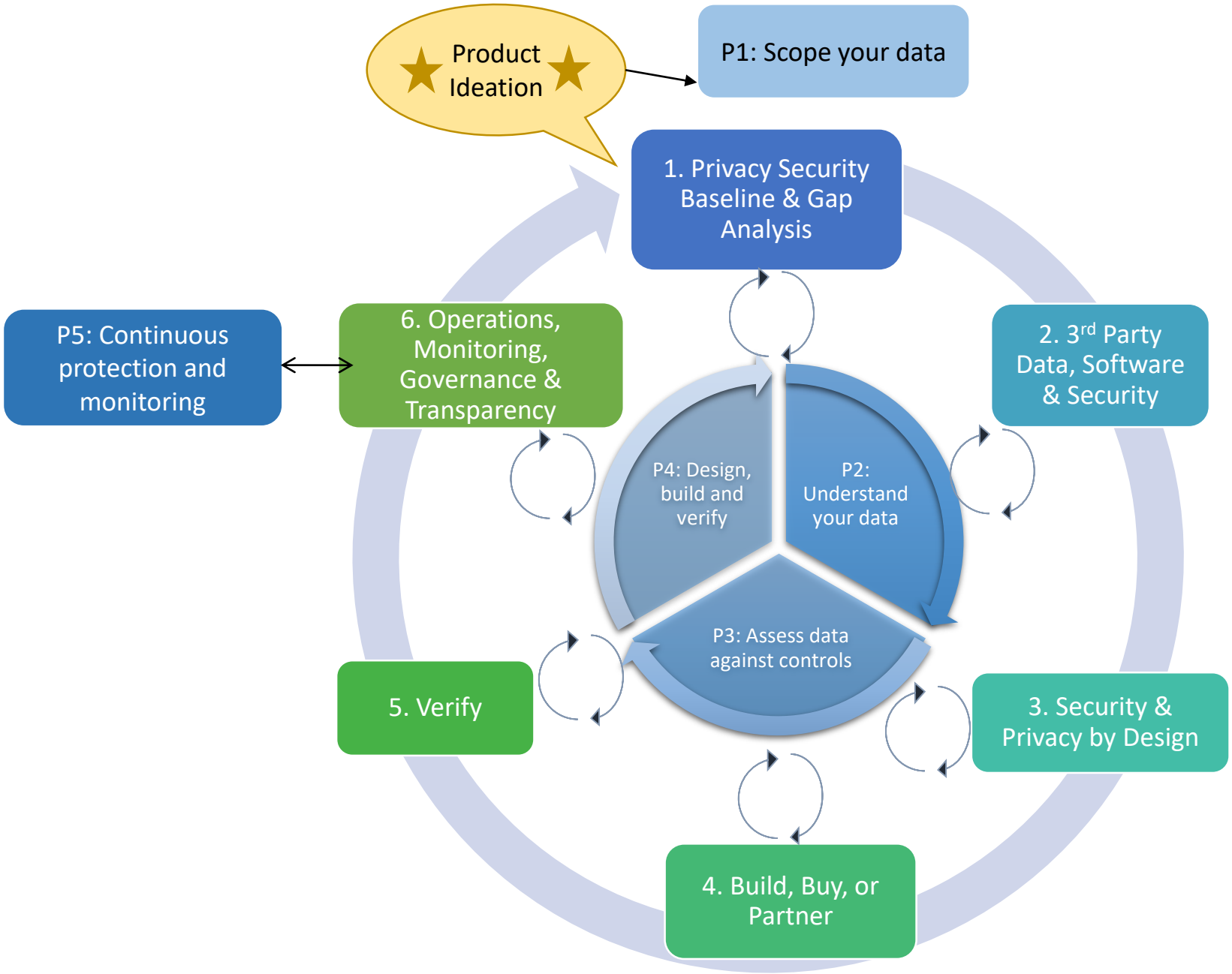
## Process

Privacy engineering is a journey of applying privacy requirements to data contexts involving personally identifiable information (PII) and ensuring needs of those requirements are met either by process or mechanism so that threats to PII and the individuals it represents is both reduced and manage.

# Privacy Engineering Process Steps

- Scope the data
- Understand the data
- Assess the data against controls
- Design, build and verify

# Privacy and Security Development Lifecycle



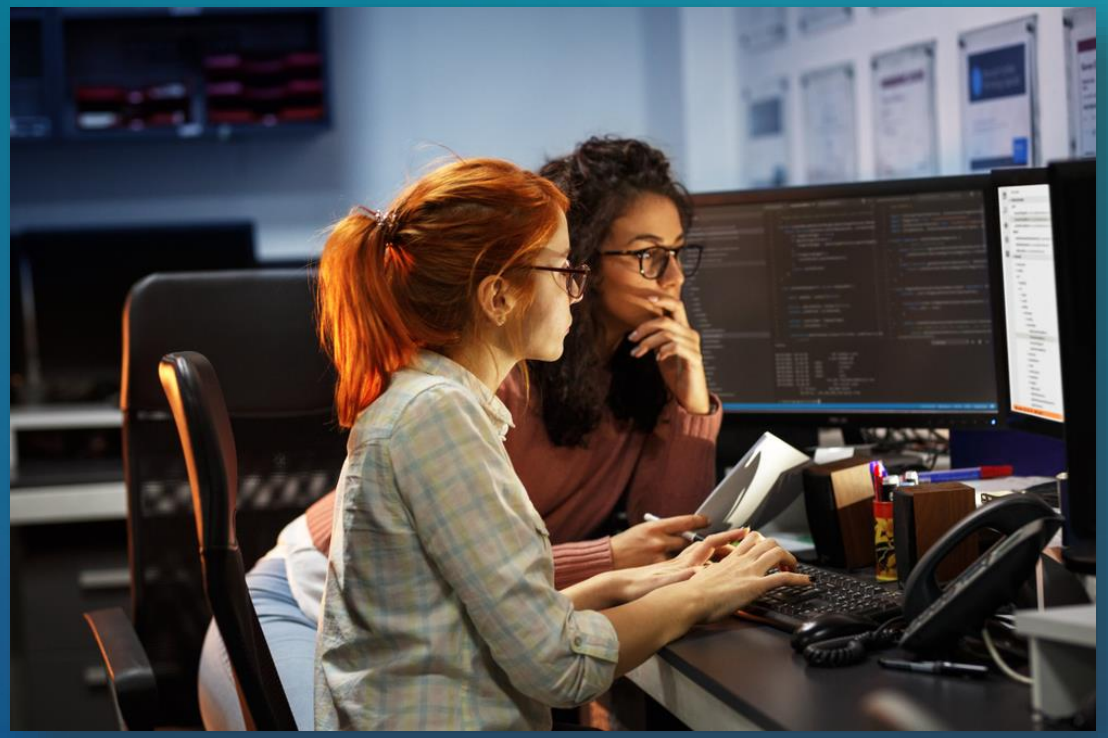

- Data Context
- Legal Basis
- Collection Limitations
- Transparency
- Proportionality
- Use Limitation
- Data Minimization
- Security
- Retention & Deletion
- Onward Transfer
- Individual Rights
- Accountability & Operations Requirements

# Step 1: Scope the Data

- What data are you collecting, transacting or storing?
- Does any of this data already exist within the organization? Who is the steward of it?
- In what context are you collecting the data?
- Which elements or collections of elements are PII?
- Will you be  combining any data sets?
- What market requirements, regulations and corporate policies apply?

# Step 2: Understand the Data

- What data is absolutely necessary for this application?
- Who will you share the data with?
- Where will the data be processed?
- Are there any third-parties involved?
- Who needs access to the data (RO, RW)?
- How long must you keep it?
- Where will the data be stored and how is it protected there?



# Step 3: Assess Data Against Controls

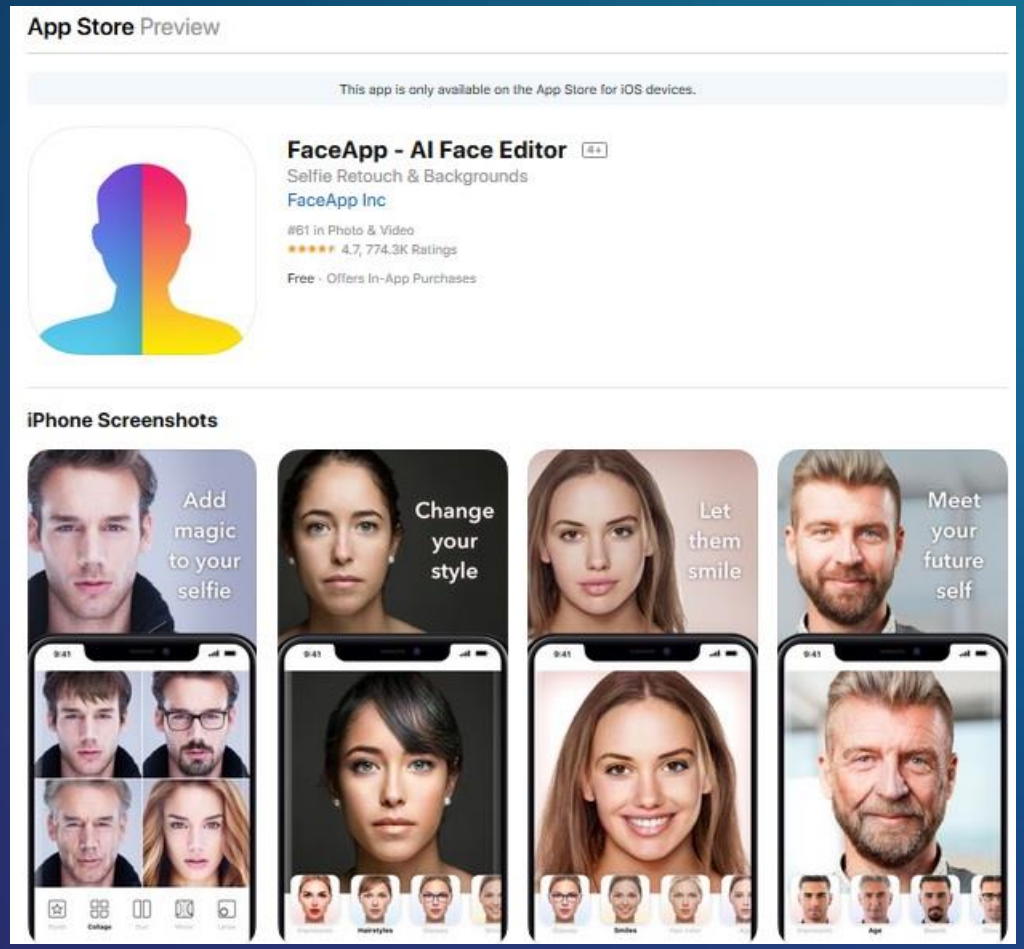
- Data Context
- Legal Basis
- Collection Limitations
- Transparency
- Proportionality
- Use Limitation

- Data Minimization
- Security
- Retention & Deletion
- Onward Transfer
- Individual Rights
- Accountability & Operations Requirements


# Exercises

Refer to workbook handouts for this portion of the workshop.

# Exercise One: Let's Look at FaceApp




Think about and share with your table:

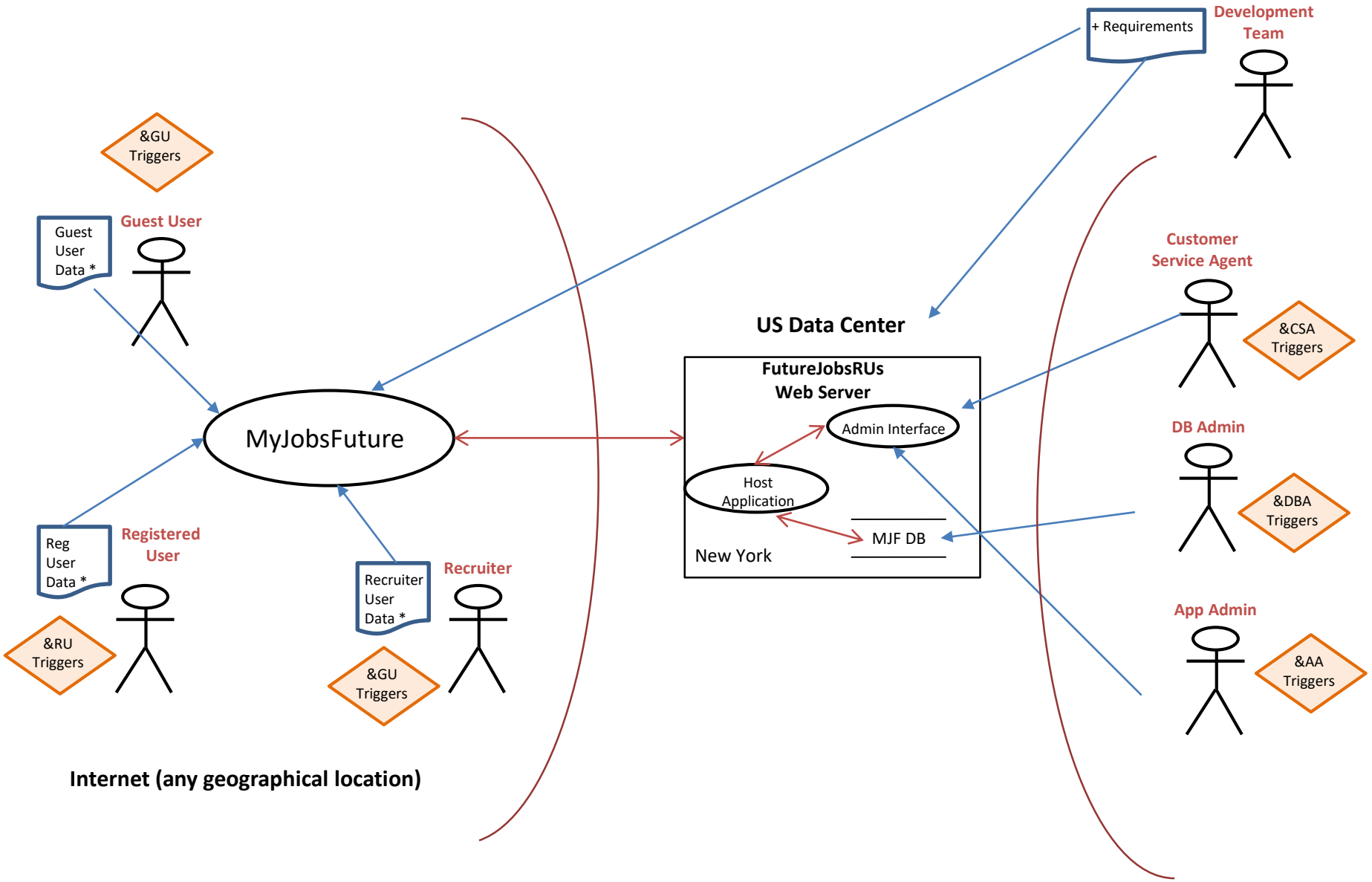
1. What data do you think it is collecting?
2. Where is it stored?
3. How is it shared?
4. How might it be mis-used?
5. How might it be monetized?

# Use Case Summary

**Summary:** MyCareerStages is a web based and mobile application framework than includes functions such as internships opportunities, resume posting, job searches, recruiting activities, mentor relationship career training and more. The primary end users of the application framework include college students, work re-entry participants, active professionals, HR recruiters and mentors.  This mobile application framework is intended to be a one stop career foundations and advancement experience.  The application framework has three levels of functionality that can be enabled. Each major release has been grouped into an epic.

Epic 1 (MyJobsFuture): is intended for college students and work re-entry professionals who are not ready to start full time work but are looking for internship or apprenticeship opportunities as they complete their education and training.  Applicants can create a profile describing their capabilities and types of jobs they are interested, at which point they are considered a "Registered User" They can also request their name be placed in the pool for consideration for internships and apprenticeships.  Registered Users must reside in the United States or Europe and they do not pay any fees for use of the service.

# Use Case Diagram: MyJobsFuture



# Exercise Two:  Perform a Data Inventory

Read short summary of MyJobsFuture and focus on Guest User and Registered User only.

- Make a list of all the date elements you think are being captured or processed.
- Identify which of them are direct identifiers of a person (for example, Name, SNN, Address).
- Mark which of them are PII because they combine to identify a specific person (for example, Street name, plus house number).
- Are there data elements that you feel are not necessary?
- Are there data elements that you feel would be a benefit?

# Exercise 3: Review Use Case Diagram and Identify Requirements

- What is the legal basis of your processing?
- Do we need to provide a notice to user?
- Do we need to obtain specific permission to collect information?
- Where would you expect the privacy notice to be displayed?
- Is the information being used only for the reason stated for collecting?
- Is the data collected the minimum necessary to achieve the intended purpose?
- What are some security controls that should be in place?
- How long should the data be retained?
- What rights should a guest user and registered user expect?
- Which users have access to the data?

# Exercise 4: Create User Stories

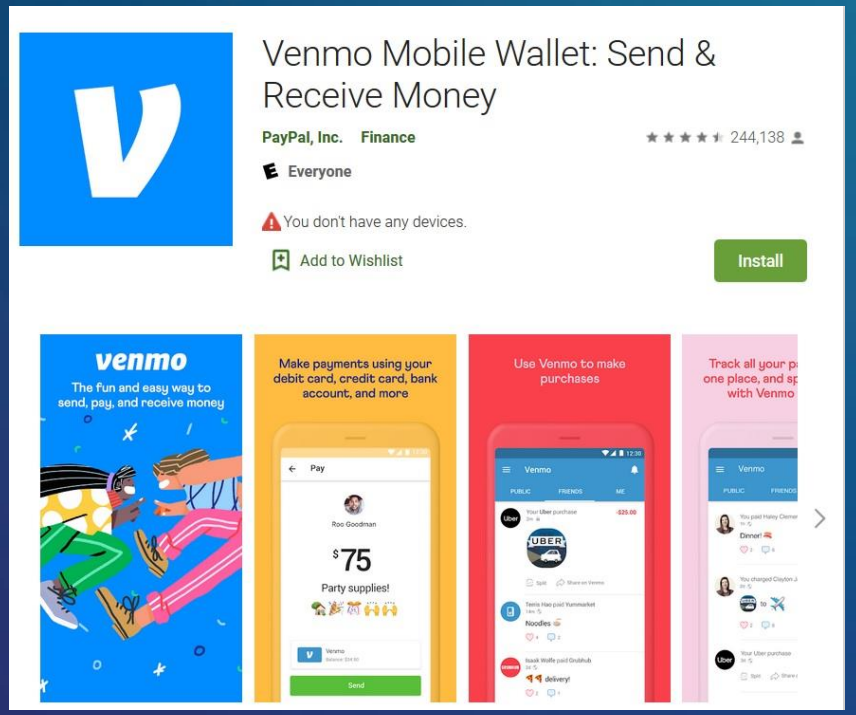
Identify 3 “Users” from the Use Case Diagram.  For each user write 2-3 short user stories.  Share a user store with your table.

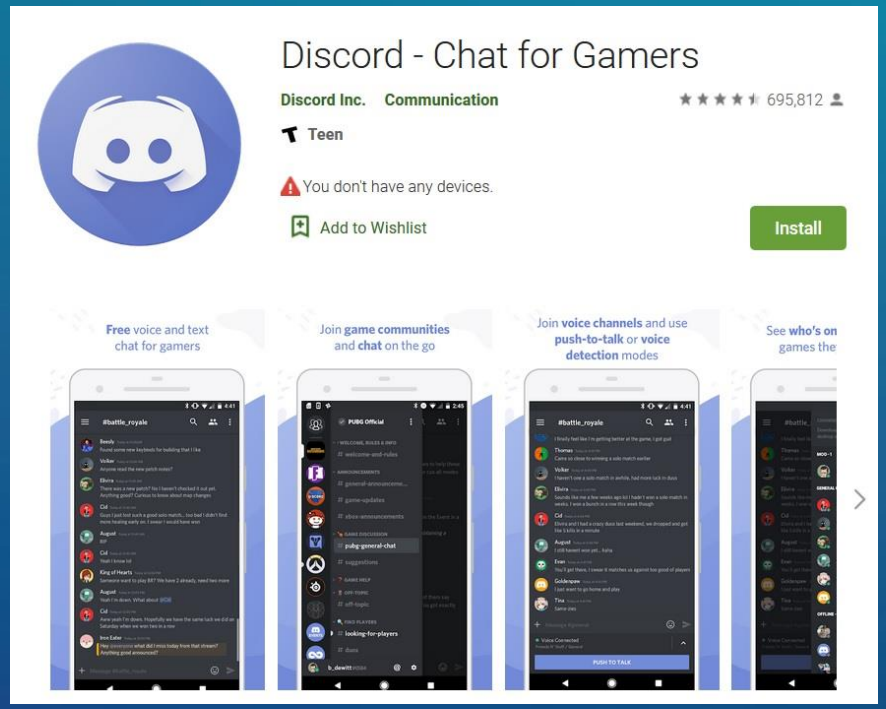
Examples:

> “As a Registered User, I need the ability to edit my profile information.”
>
> “As a Registered User, I want to provide consent for capture of cookie information.”
>
> “As a Developer, I need to know the single source of truth where the data will be stored.”

# Exercise 5:  Assumptions of Privacy by Default

For this exercise, pick one of the two apps below and review the “Terms of Agreement”. Write down 3 things that you found surprising or vague enough that you want more details.  Share 1 or 2 concerns with your table.



# We Are All Privacy Engineers

A privacy engineer…

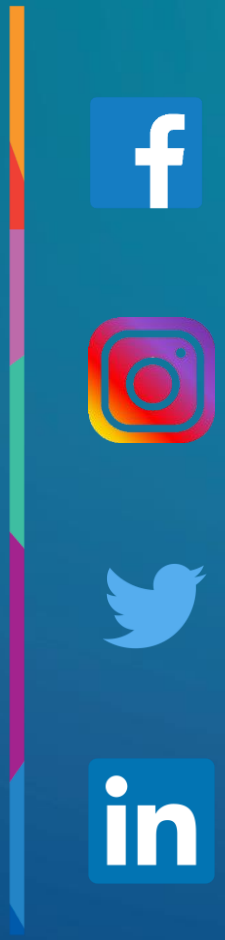
- Needs more than just technical skills to **protect** and **extend** the **value** of data.
- Draws from artistic **creativity** and expression to **innovate.**
- Learns from, **but disregards**, the failures of the past.
- Is passionate about the appropriate use of data.

Please remember to complete the session survey in the mobile app.

# THANK YOU

## You Can Follow Us

@lbobbitt
@MicheleDGuel
linkedin.com/in/saranmorgan



GRACE HOPPER CELEBRATION

ANITA B.ORG

#GHC19

# Additional Information

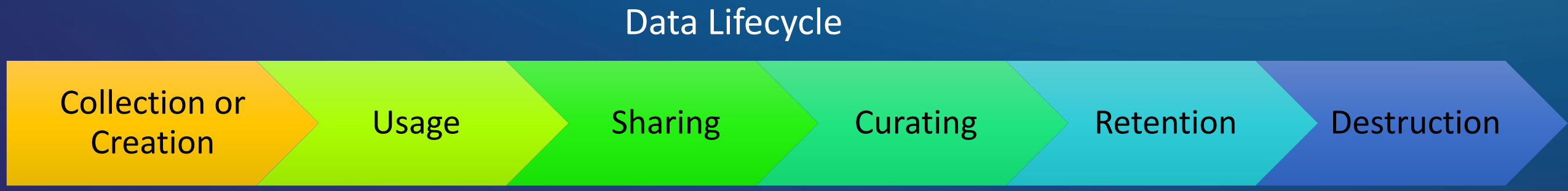
# GDPR – One Year Later


## Additional Guidance Expected in 2019/2020

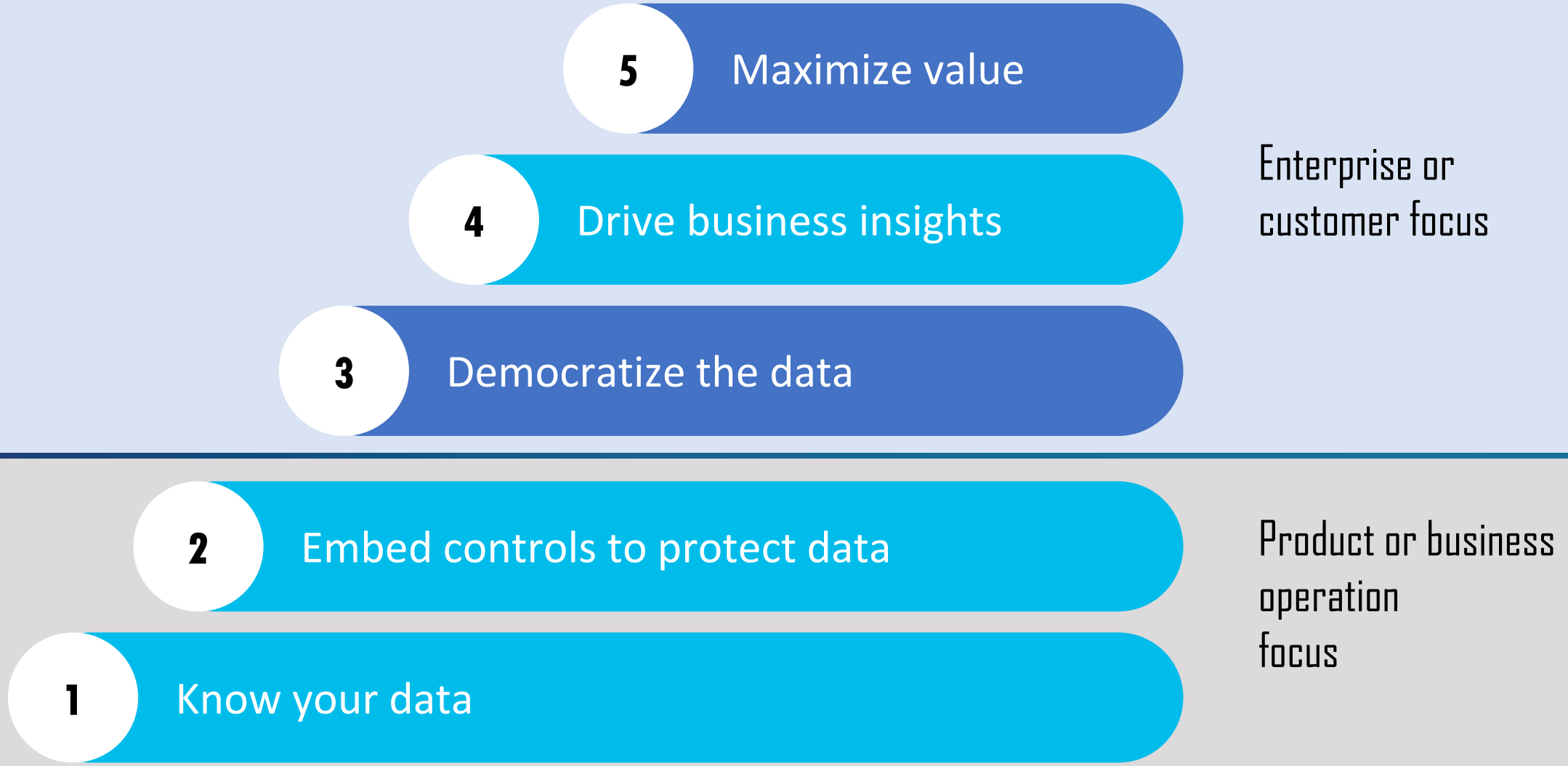
- Data protection by design/default
- Children's data
- Law enforcement access
- Connected vehicles
- Video surveillance and monitoring
- Targeting social media users
- And more…

# Data-Centric: Keep the Data Lifecycle in Mind

- Data Policy may change
- Data may need to be archived longer than product is operational per regulation or business need
- Data may be transferred to a newer functional offering
- Data may be shared with other applications with new functions
- Data may be shared/sold with 3rd party processors
- Data may need to be returned to the owner/controller

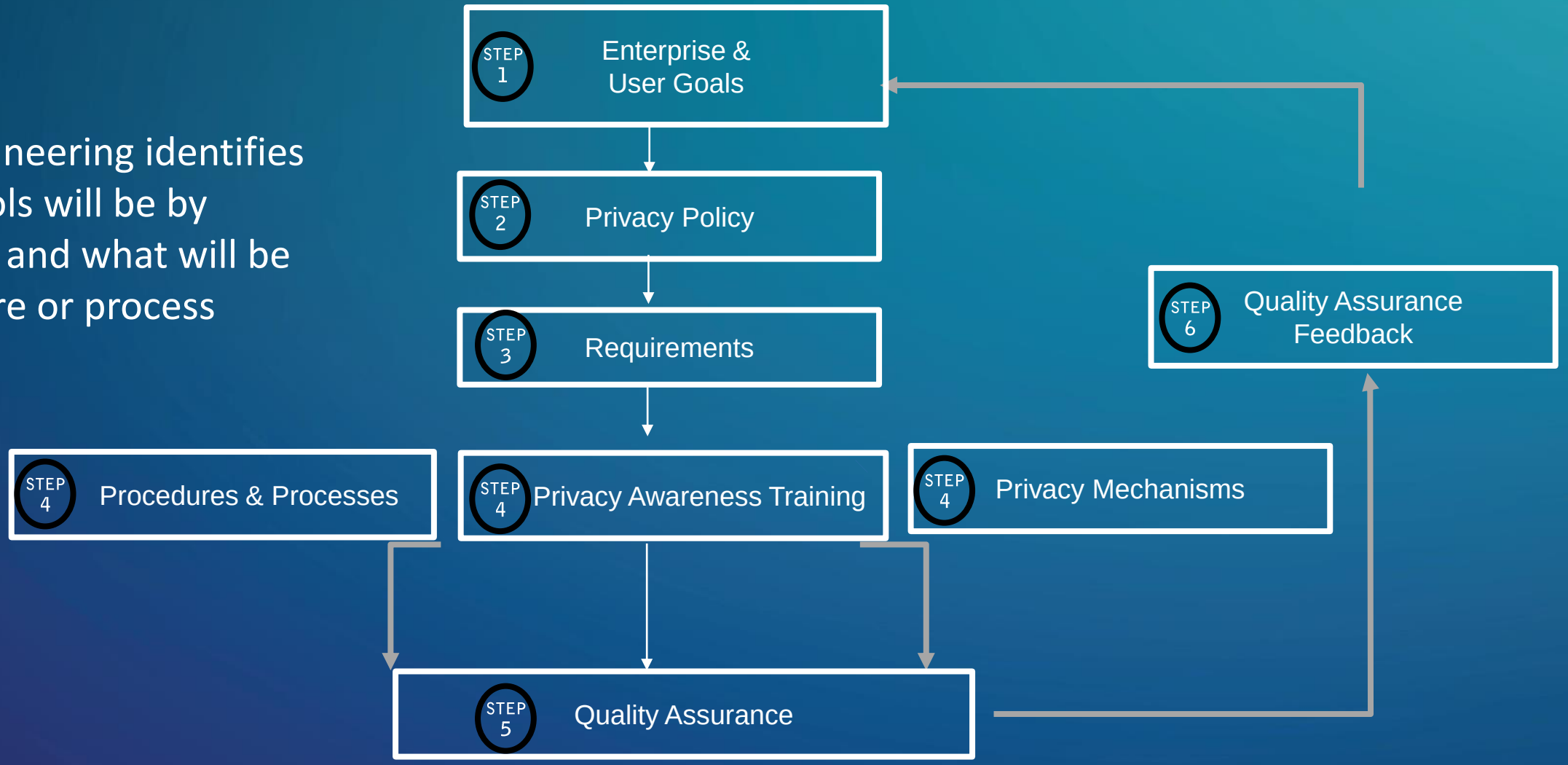


# Innovation Centric: Maximizing the value of data



# Process Centric

Privacy Engineering identifies what controls will be by mechanism and what will be by procedure or process



# Privacy = Fair and legitimate processing of personally identifiable information

## Fair information principles

Collection limitation
Data quality
Purpose specification
Use limitation
Security safeguards
Individual participation
Accountability

## Legitimate = legal basis

Contractual necessity, consent, legitimate interest, public interest, vital interests, compliance with legal obligation

## Processing

Collection, storage, use, organization, recording, alignment, combination, disclosure by transmission, consultation, erasure, destruction, alteration, etc.

## Personally identifiable information (PII)

Any Data that identifies an individual or from which you can derive identity or contact information of an individual

Includes otherwise non-personal information when you **associate** or **combine** with personal information

# Data Privacy Policies = Privacy Requirements = Meta Privacy Use Cases

Realistic technology capabilities and limitations

Ethical obligations

Enforceability and compliance

Economic pressure to create value through efficient sharing / relationship building

Usability, access and availability for end users of information systems

Industry standards

Brand identity

Permission marketing / customer relationship management / business intelligence


Local and international legal, jurisdictional and regulatory necessities

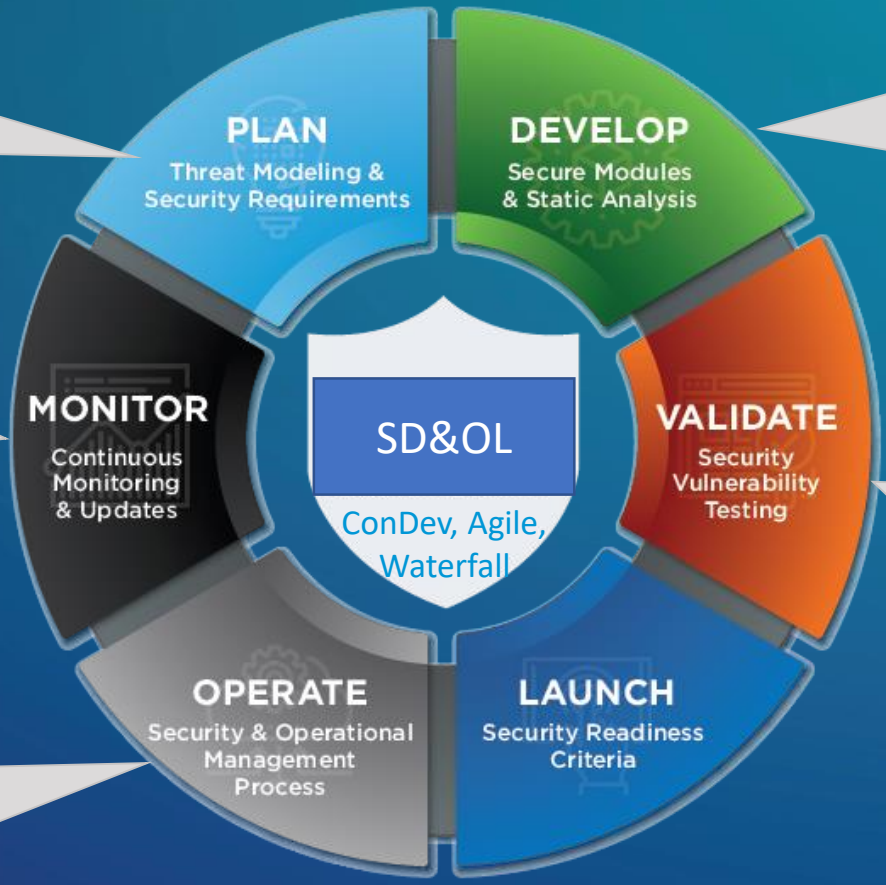
Organization / business requirements

# Embed privacy engineering into secure offering lifecycle

- Data scoping workshop
- Establish privacy policy & requirements

- Privacy policy/rqmts/control Review & update with required remediation

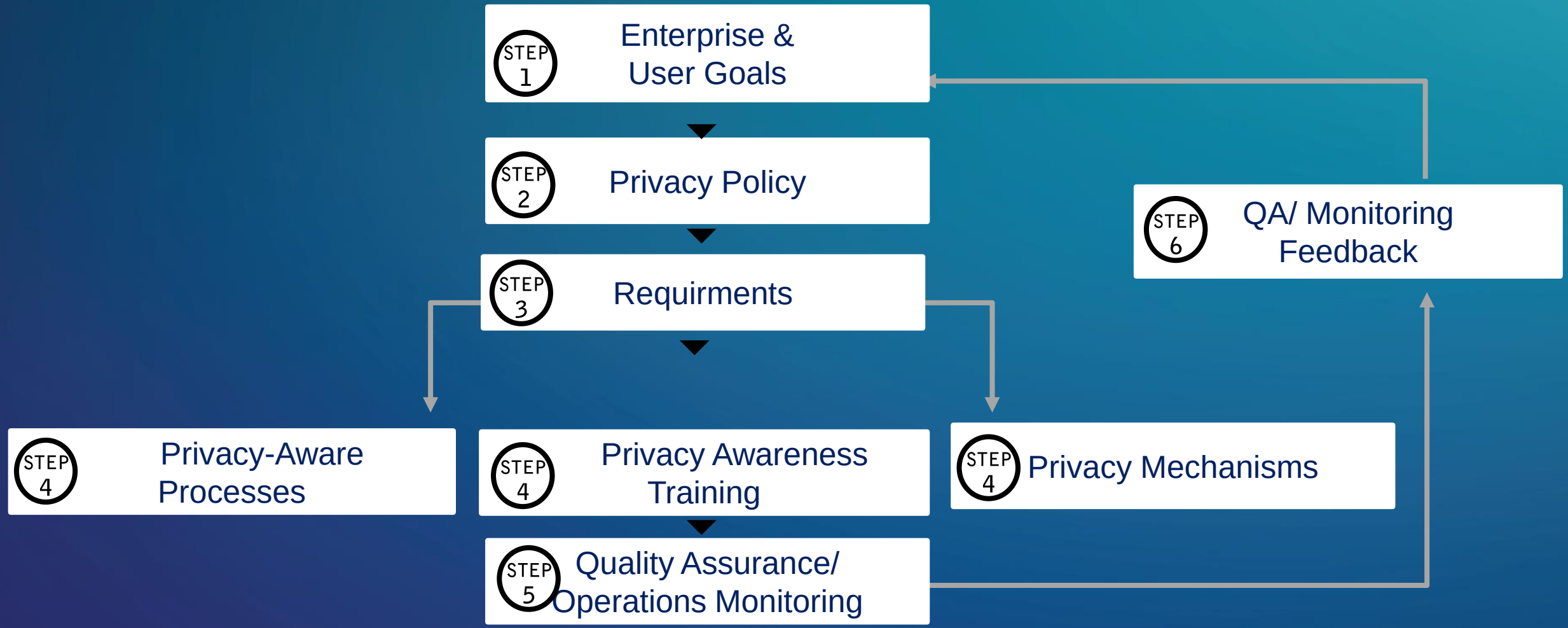
- Update privacy data sheet
- Update PIA & controls
- Operationalize
- Privacy controls




- Privacy Impact Assessment (PIA); third-party contracts
- Embed privacy controls
- Update PIA

- Validate privacy controls
- Update PIA & controls
- Privacy data sheet, map data flows

# Privacy engineering development process



# Step 1: Scope the Data

Gather all your data privacy & protection documentation established by company culture, statute or regulation

**Work with your …**

- Development
- IT
- Legal
- Industry compliance
- Records management
- Third-party providers

What market requirements, regulations, and corporate policies apply?

Whose data are you processing? Where did it come from? Do you have the legal basis to process it? Where is the data?

Where are your employees and customers?

What applications are you running? Where? What data do they process?

What data do you use in your processes?

Whose data are you using?

Where is data stored?

With whom do you share it?

Where do your cloud providers securely process data?

What is your security plan for infrastructure, application, and product development?

# Step 2: Understand the Data

Inventory & classify your data & document its lifecycle

- Determine what data is necessary for your application/product
- Establish your data identification and confidentiality criteria from your data policies (governance, protection, privacy)
- Identify and tag your data context
- Outline your data lifecycle as the data controller and/or processor

# Step 3: Assess Data Against Controls

- Establish your data controls criteria per your data policies (governance, protection, privacy)
  - Example: legal basis in contract vs. opt-in consent
  - Standards: NIST(800-53), ISO 27000, GDPR
- Prioritize control requirements for data and context including third-party sharing, location, and legal basis under which you are processing
  - Example: financial data is restricted before announcement but is public afterwards

# Step 3 (cont): Set controls

- Capture agile privacy-aware user stories
  - As a business owner, I need  to be able update end- and operation users' PII
  - As a business owner, I need to know if any automated decision threatens a fundamental right of the users
  - As an end-user, I need to be able to find the privacy notice within 1 click
  - As an operations user, I need a mechanism to delete end- and operation users' PII on behalf of other end- and operation user
- Embed consistent privacy-enhancing processes and technologies wherever possible

# Step 4: Be transparent

## Privacy data sheets & data maps

Cisco Public

Cisco Webex Messenger - Privacy Data Sheet

### Cisco Webex Messenger

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco Webex Messenger.

**1. Overview of Cisco Webex Messenger Capabilities**

Cisco Webex Messenger ("Webex Messenger" or the "Service") is a cloud-based messaging service made available by Cisco to companies or persons ("Customer," "you" or "your") who purchase it for use by their authorized users (each, a "user"). Webex Messenger enables collaboration via instant messaging, desktop sharing, and presence. For more details on the Service, please see Cisco Webex Messenger.

Because the Service enables collaboration among users, you will be asked to provide your personal data in order to use it. The following sections describe Cisco's processing of personal data in connection with the delivery of the Service, the location and transfers of that data, and how it is secured in accordance with privacy principles, laws, and regulations. Cisco will use your personal data consistent with this Privacy Data Sheet. Note that this Privacy Data Sheet is a supplement to the Cisco Privacy Statement.

**A Note on Cisco Jabber**

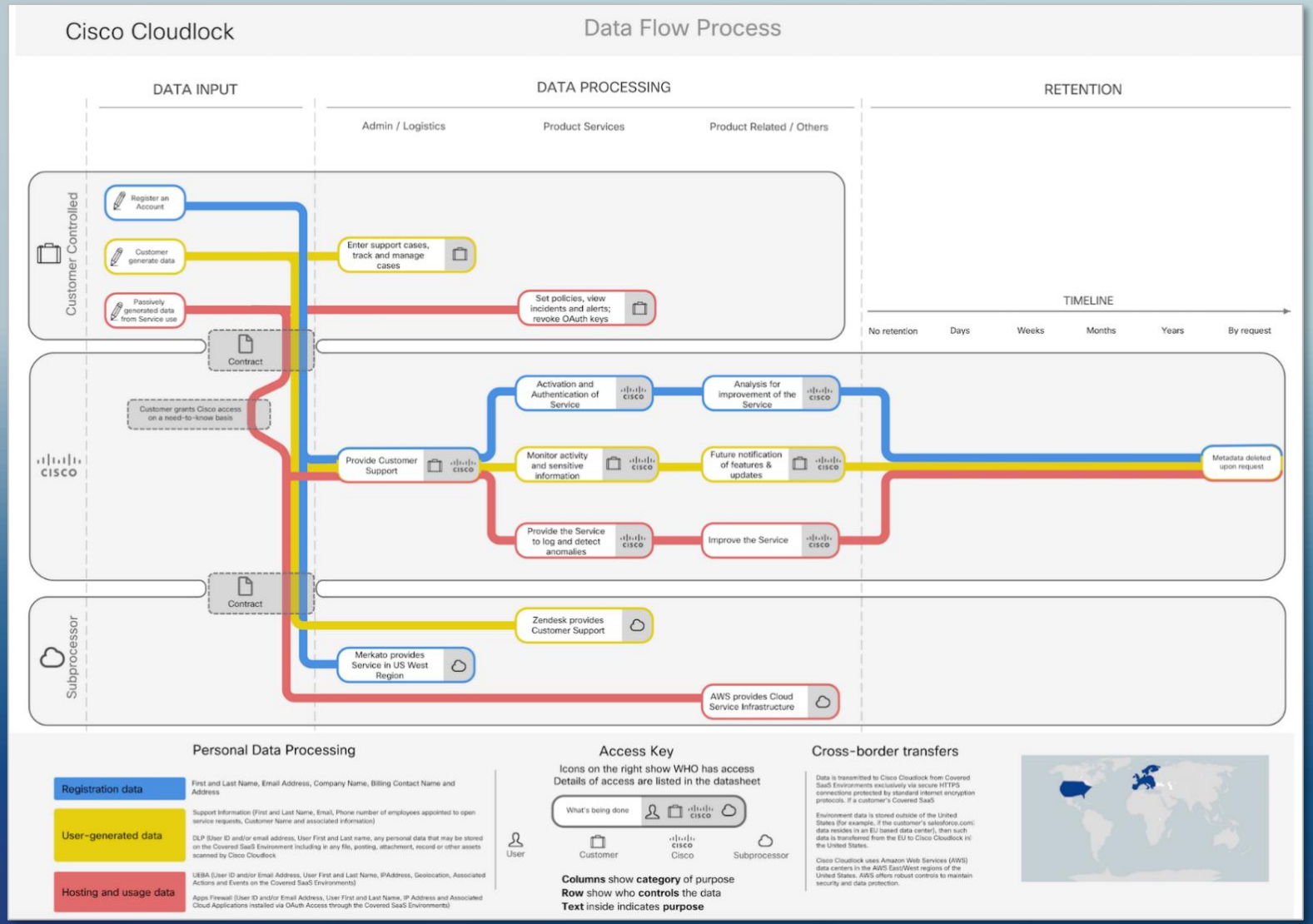
You may access Webex Messenger through Jabber for Windows, Jabber for Mac, Jabber for iPhone and iPad, and Jabber for Android ("Cisco Jabber Clients"). Cisco Jabber Clients can connect you to additional Cisco cloud-based services, as well as Cisco on-premise services. When you access Cisco services through Cisco Jabber clients, three sections in this Privacy Data Sheet apply to your use of such services: Section 2 – Data for Analytics, Section 2 – Technical Support Assistance, and Section 6 – Data Deletion and Retention. This means that Cisco may collect certain personal data related to analytics and technical support when you use Cisco Jabber Clients to access Cisco services, regardless of whether those services are cloud-based or on-premise.

If you choose to enable the interoperability setting that allows Cisco Webex Teams and Cisco Jabber to communicate with each other (also called Cisco Webex Teams/Jabber Interop), the Cisco Webex Teams Privacy Data Sheet will govern the processing of personal data related to the interoperating features.

**2. Personal Data Processing**

If you are a user and your employer is the Customer that purchased the Service, all of the information described in this Privacy Data Sheet is subject to your employer's policies regarding retention, monitoring, deletion, and export of information. *Note that Cisco has no control over and is not responsible nor liable for the privacy of any information that you have shared with others. Copies of messages may remain viewable elsewhere to the extent they have been shared with others.*

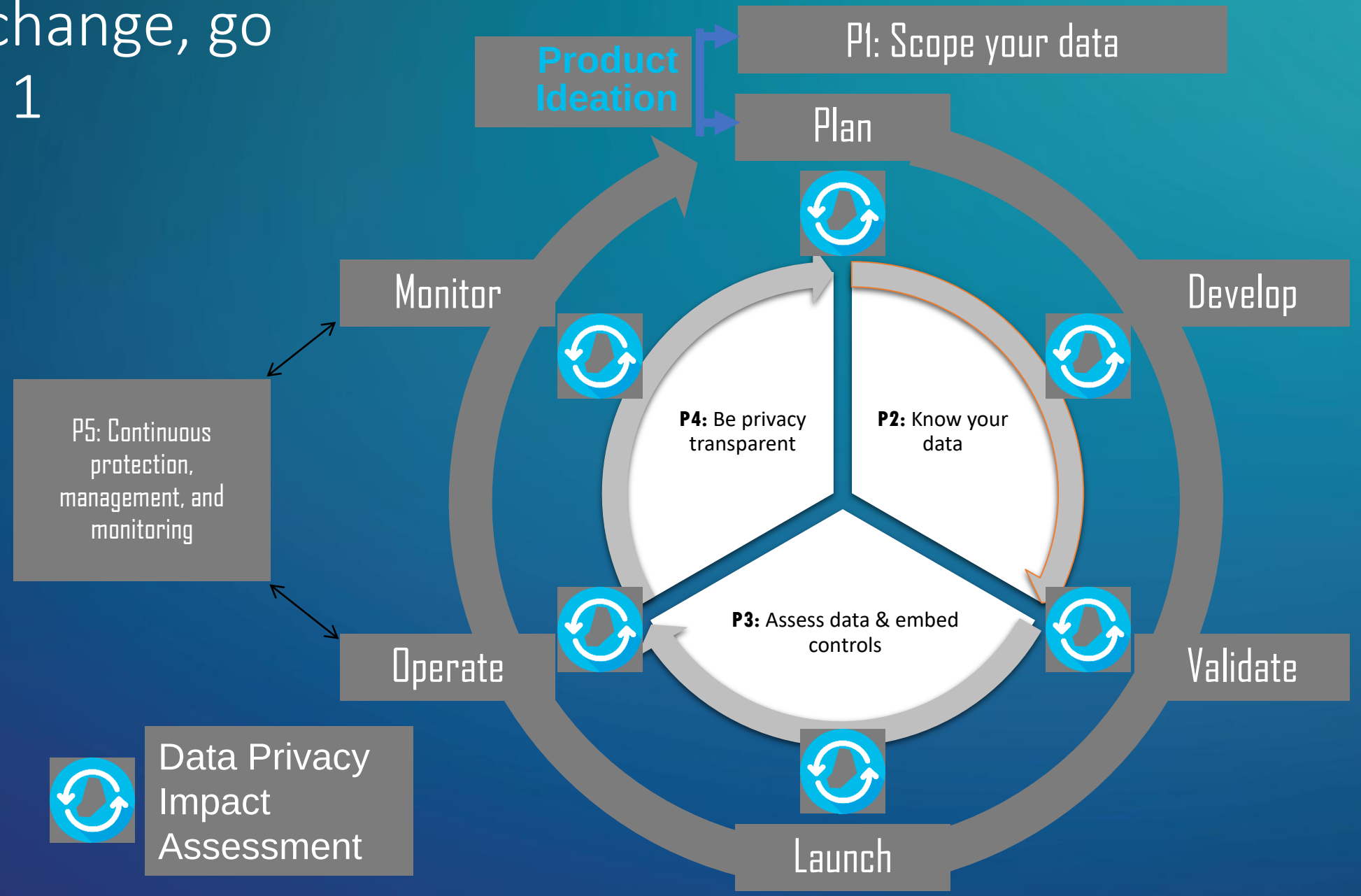
The tables below list the personal data used by Cisco Webex Messenger to carry out the services and describes why we process that data.



# Step 5: Operate & Monitor Controls

- **Establish a monitoring cadence** for all your processes including updating your PIA, checking on third-party processing, and measuring your response to requests re individual rights
- **Verify your technology controls** across solutions such as encryption at rest and in transit, identity and role-based access, and retention periods. Establish exceptions and automate where you can to monitor this

# Step 6: Any change, go back to Step 1



# As the data owner/steward/custodian, you are the control point who knows…

- If data **should** be used by others
  - Data **sensitivity**
  - **Risk** to person/customer
- If data **can** be used by others
  - **Legal** basis
  - P**urpose** for which data was created/collected

- **You establish** procedure methods for new purposes
  - Determine if data can be anonymized, de-identified, tokenized, summarized
  - Determine if data can be shared externally or internally per legal basis or value to the organization