Designing for Data Privacy on AWS

Carl Mathis
Senior Privacy Architect

Dan Nieters
Senior Privacy Architect

AWS Security Assurance Services (SAS)

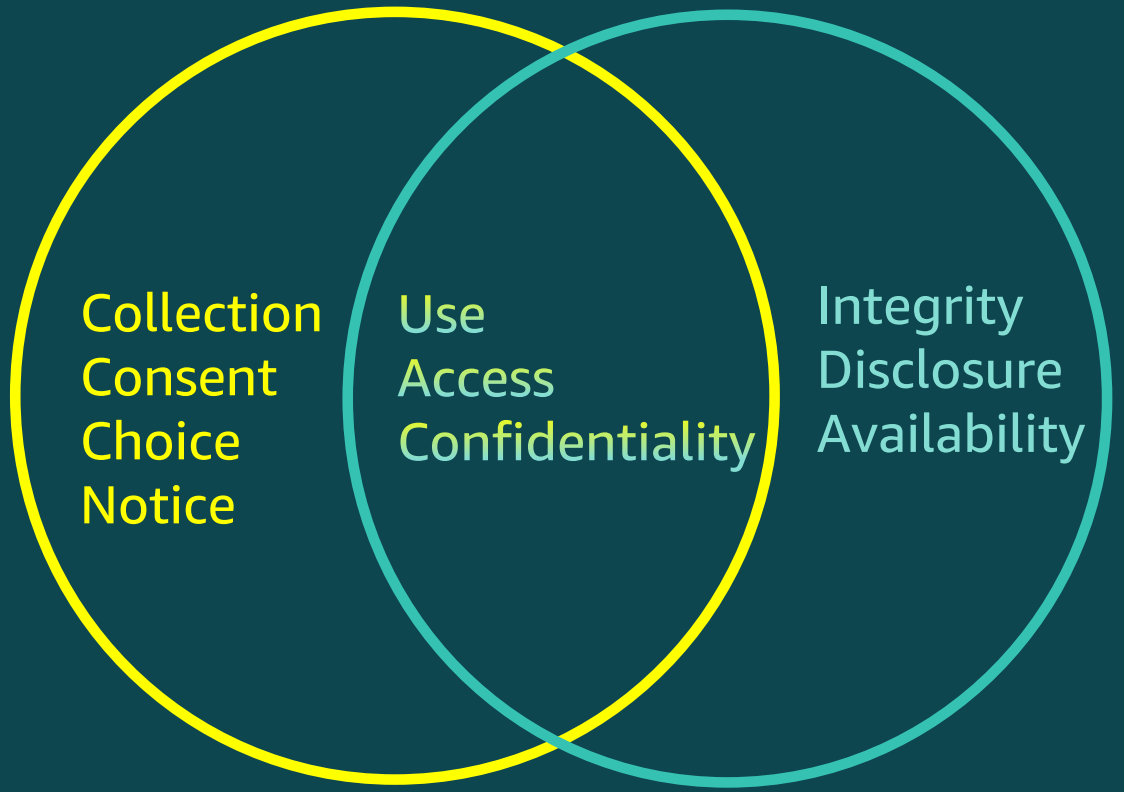
Legal Disclaimer

This presentation is provided for the purposes of information only; it is not legal advice, and should not be relied on as legal advice. As each customer's requirements will differ, AWS encourages its customers to obtain appropriate advice on their implementation of privacy and data protection environments, and more generally, applicable laws relevant to their business.

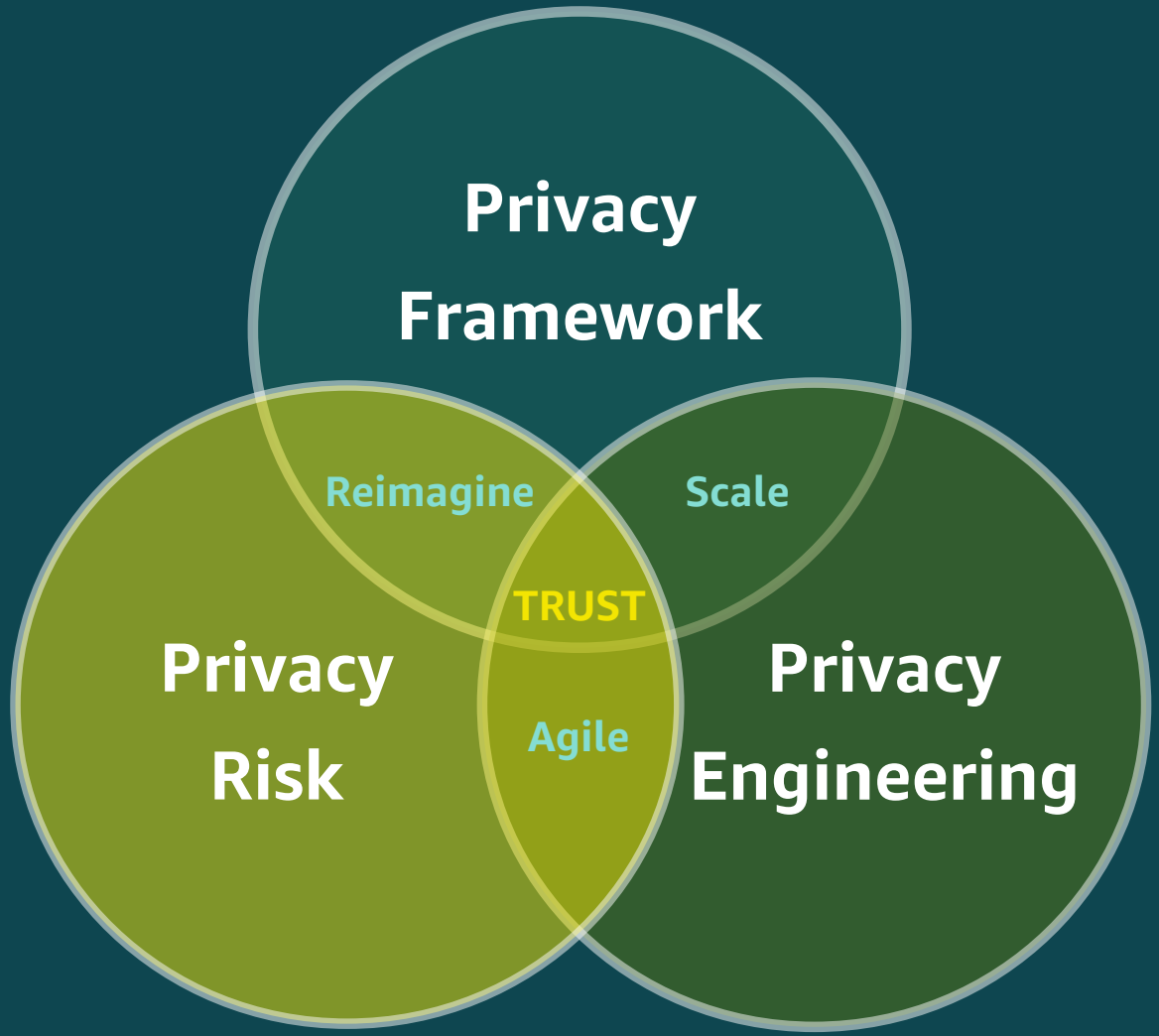
Agenda

- Security and Privacy
- Our Mental Model
- Privacy Principles
- Privacy Engineering Patterns

Are Privacy and Security equal?



Privacy Mental Model



Framework Principles – People/Process/Technology

Organizational

- Privacy Governance
- Risk Management
- Third-Party Management
- Openness
- Consent, Choice, and Notice
- Purpose Identification and Specification
- Information Sharing and Disclosure

+

Engineering

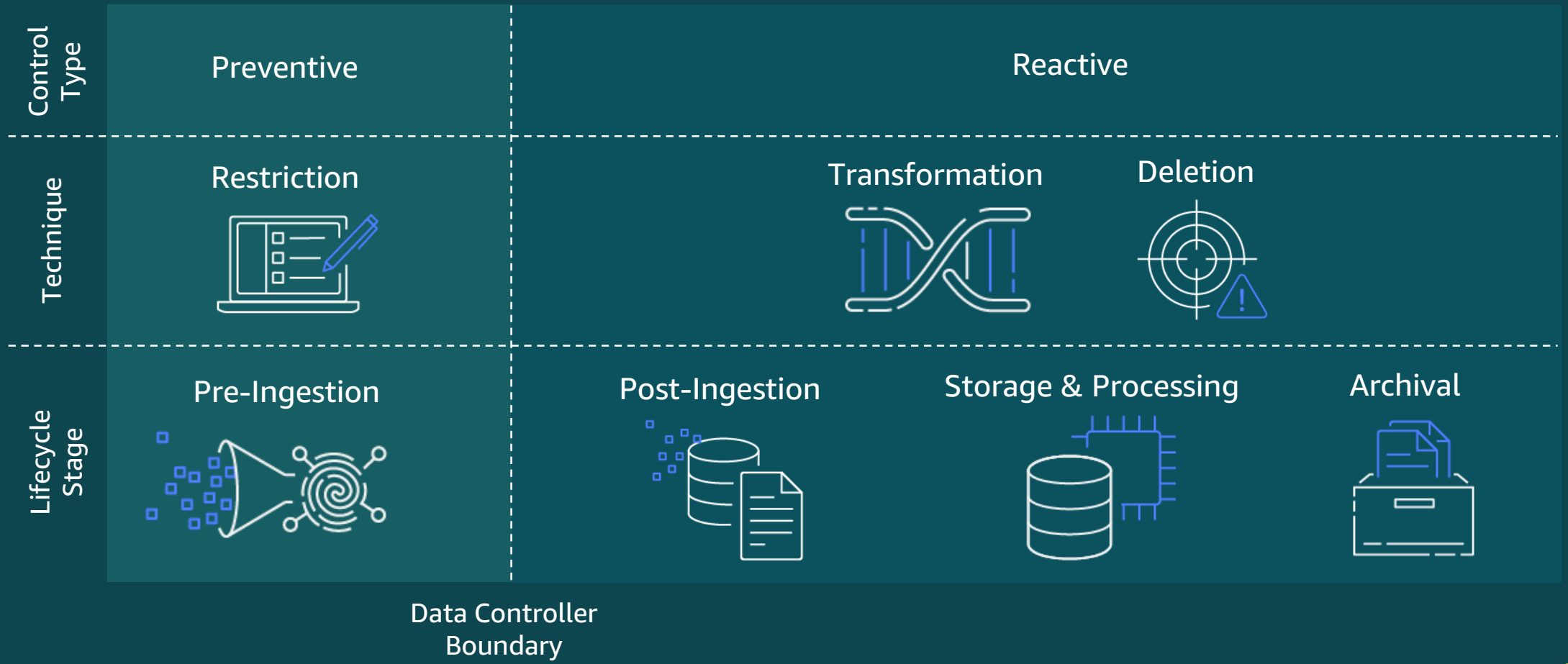
- Data Minimization
- Data-Centric Design
- Security
- Auditability
- Individual Participation

=

Control Set

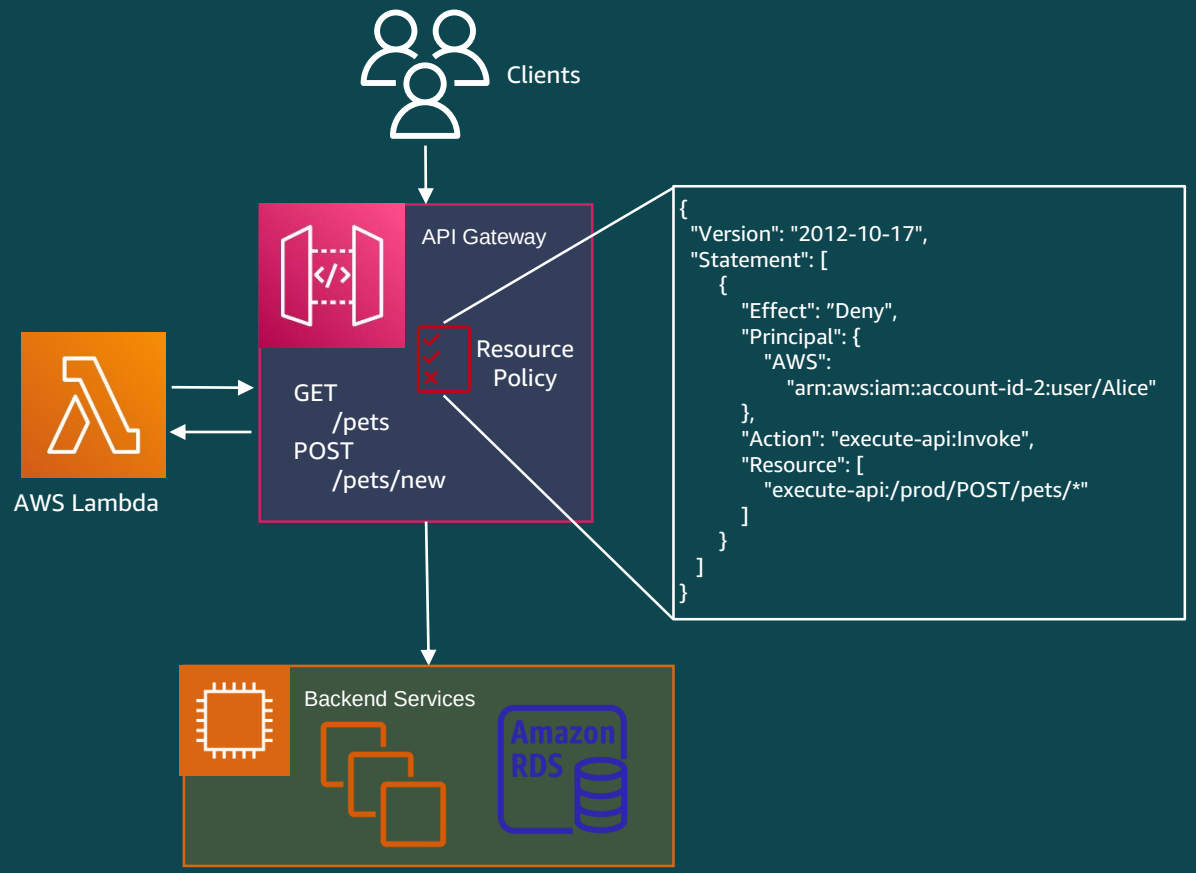
Privacy Engineering Patterns

Data Minimization – Overall Techniques



Data Minimization – Restriction

- Limit input options for your end-users
  - Checkboxes rather freeform text
- Determine and document the minimum level of identifiability required for each input
  - Utilize fuzzing/ranging
  - Instead of asking for a user's birth date, ask for an age range
- If PI is only required at ingestion, ensure it is not stored after completion and caches are cleansed
- Design application to store PI on the user's device, i.e. in a cookie



Data Minimization – Transformation

Non-reversible

Anonymization

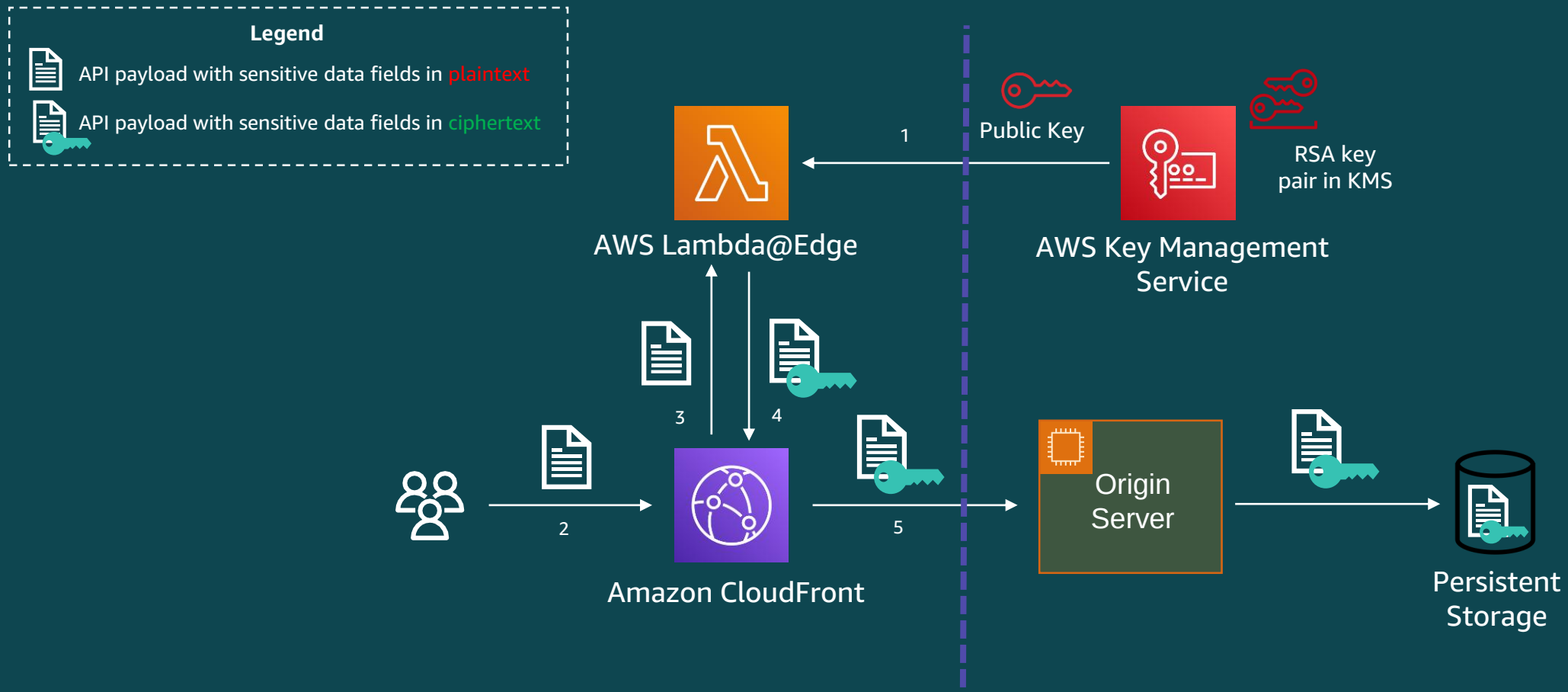
Reversible

Pseudonymization

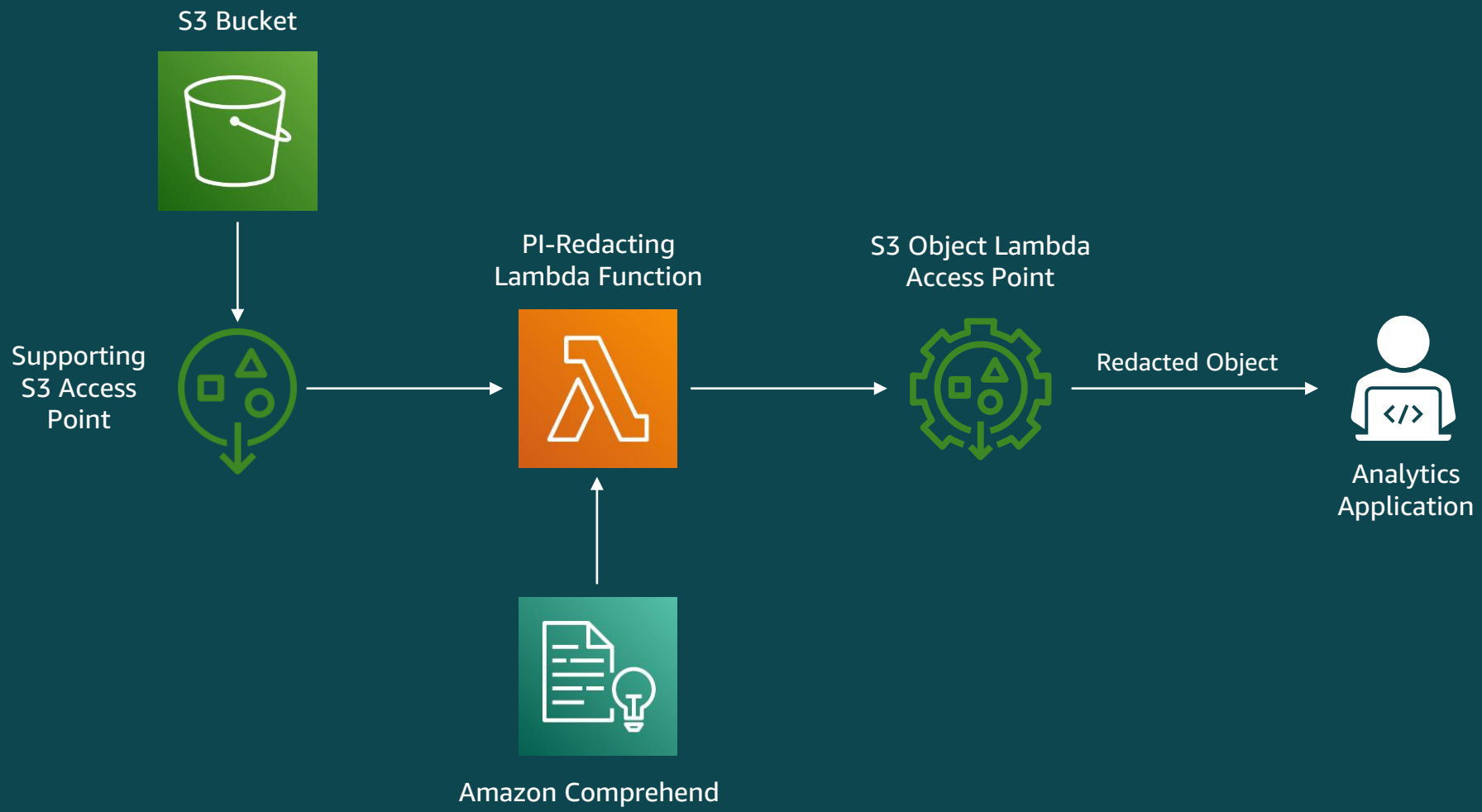
or

Encryption

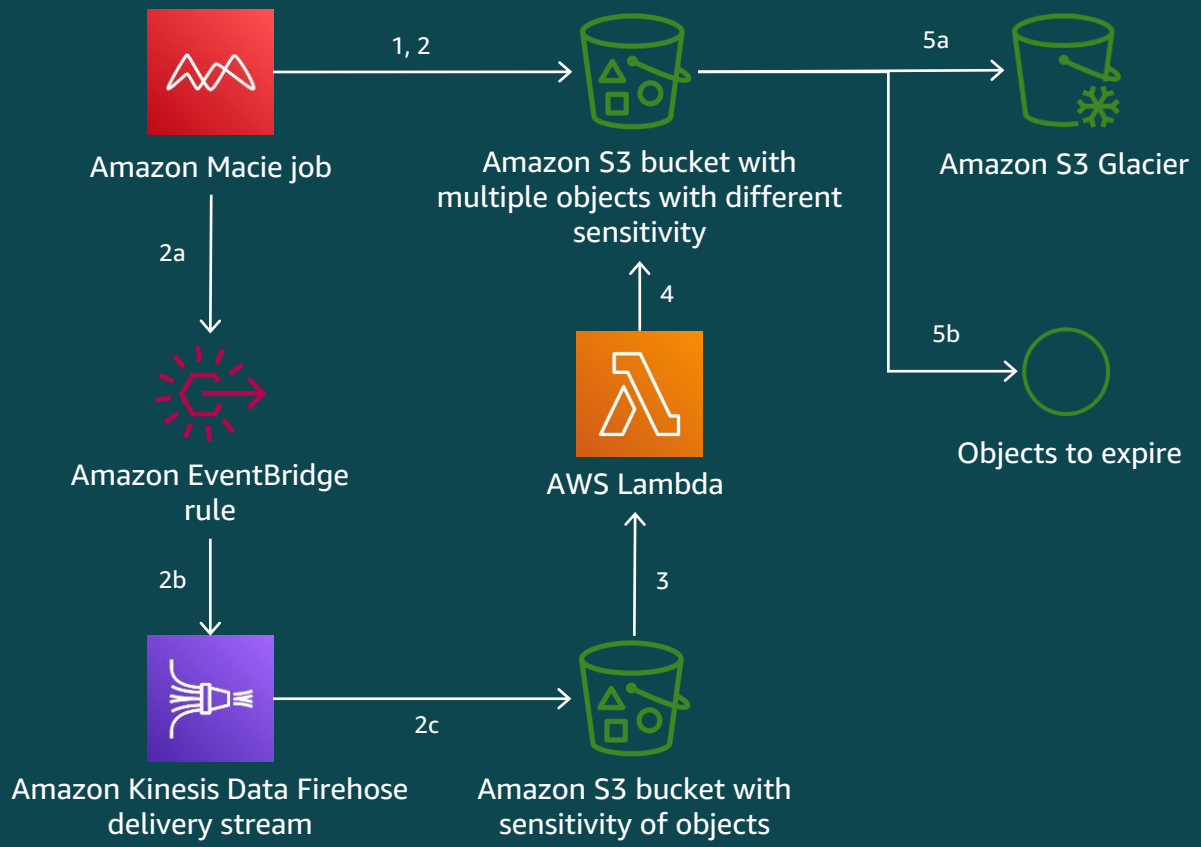
Data Minimization – Transformation with Encryption



Data Minimization – Transformation with Anonymization



Data Minimization – Archival and Deletion

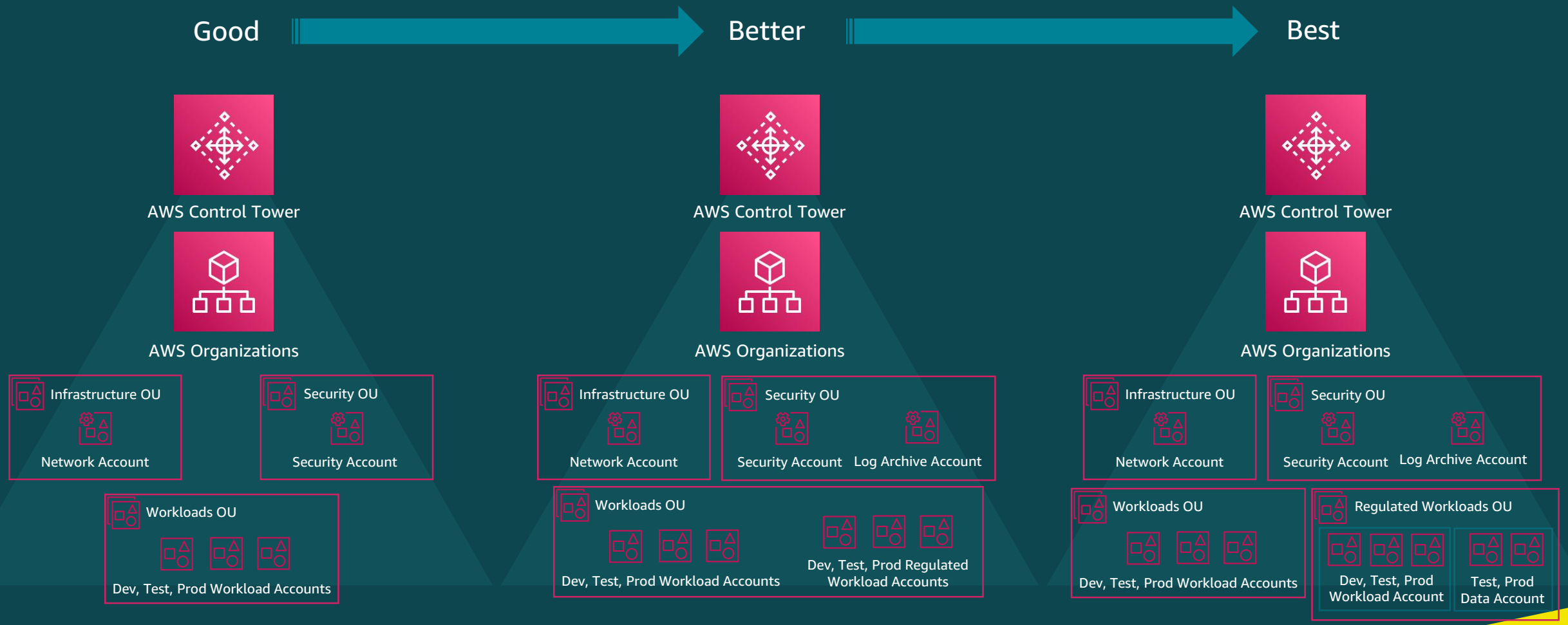


Data-Centric Design – Data Map

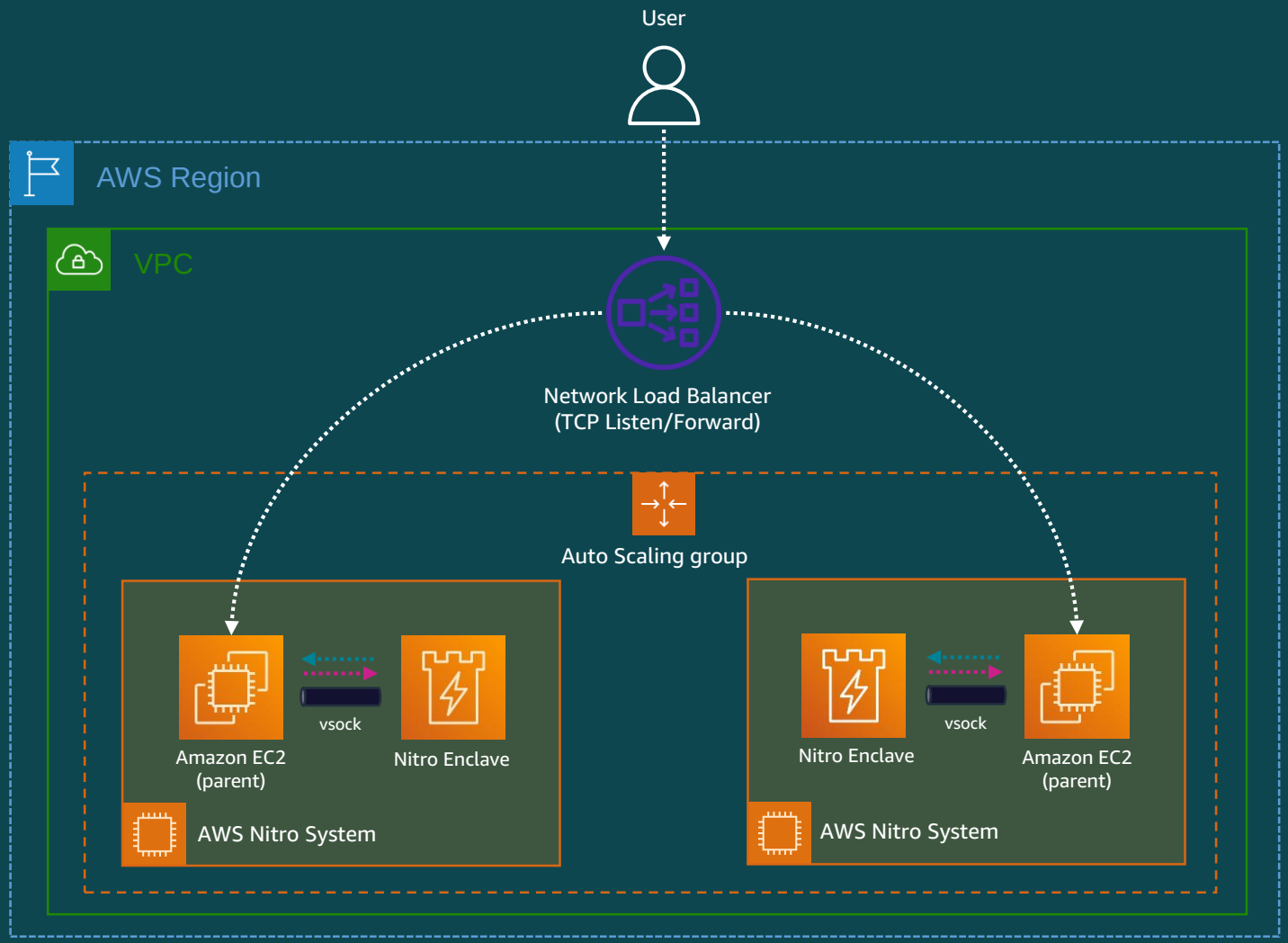
Once you understand the architecture and the data lifecycle, work with your data processing officer (DPO) to insert this information into a data map

Personal Information	Source	Justification	Processing	Access	Disposal	Consent
What personal information is being collected? Any sensitive PI?	How and where was this data collected?	What are the legal reasons for collecting this data?	How is this data being stored and processed?	Who has access to it? What is the justification for access?	For how long is the data retained? When and how is it disposed?	How is consent obtained for the collection of this data?
Email address	Contact form	Marketing	AWS services (S3, etc..)	Site admins	S3 Lifecycle policy, removed after 60 days	Explicit opt-in via a pop-up
…	…	…	…	…	…	…
…	…	…	…	…	…	…

Data-Centric Design – Account Segmentation



Data-Centric Design – Processing Segmentation



Data-Centric Design – Cross-Border Data Flows

Residency

Sovereignty

Localization

Least rigorous

Most rigorous

Data-Centric Design – Restricting Cross-Region Flows

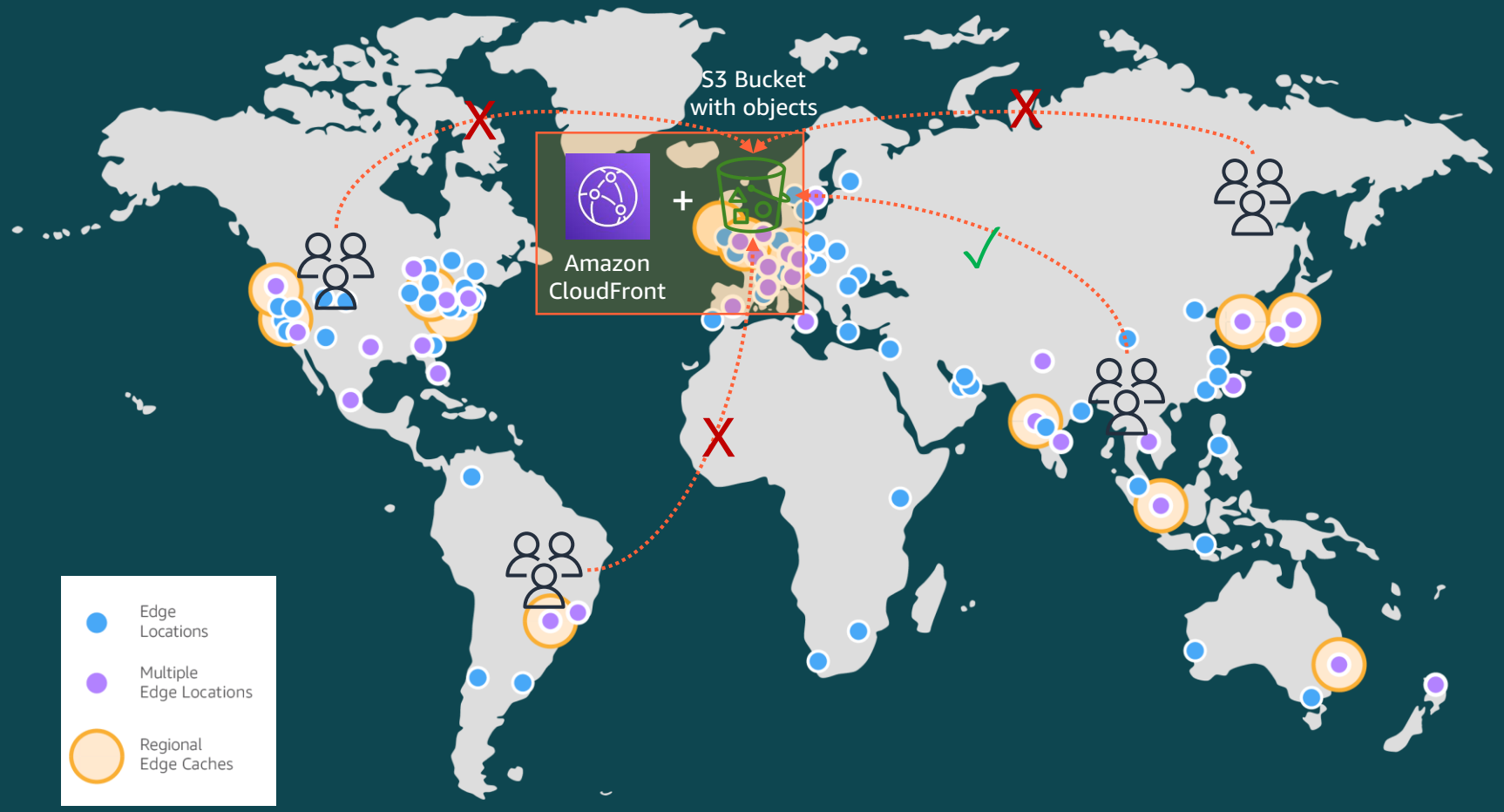
Service Control Policies (SCPs)
Deny access to AWS based on the requested AWS Region

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                ...
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
            }
        }
    ]
}
```

AI Services Opt-Out Policies
Control data collection for AWS AI services

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Data-Centric Design – Front-End Geo-Restriction



Security – Privacy Best Practices for Encryption

- Use KMS Customer-Managed Keys for greater control over strength, rotation, expiration, etc. required for GDPR, the Schrems II ruling, et. al.
  - AWS-Managed keys are regional!
  - Do not use cross-region KMS keys
- Ensure usage of CMKs to protect PI and secrets that allow access to PI
- Define data classification levels and have at least one dedicated CMK per level
- Prevent unknown cross-account access to keys
- Implement separation of duties in IAM
  - Key administration
  - Key usage
- Enforce automatic key rotation

Auditability – Centralizing Logs

You can create two types of Cloud “trails”

- A trail that applies to all regions
- A trail that applies to one region

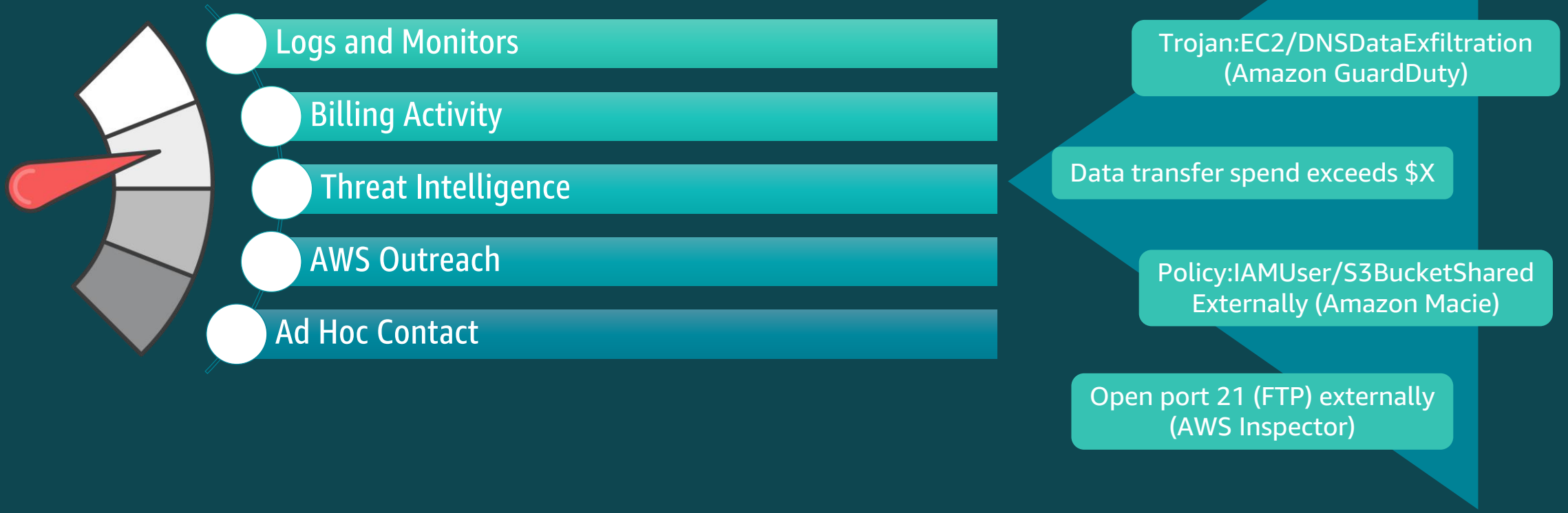
When you create a trail that applies to all regions, CloudTrail creates the same trail in each region, records the log files in each region, and delivers the log files to the single S3 bucket

Many-to-one centralization

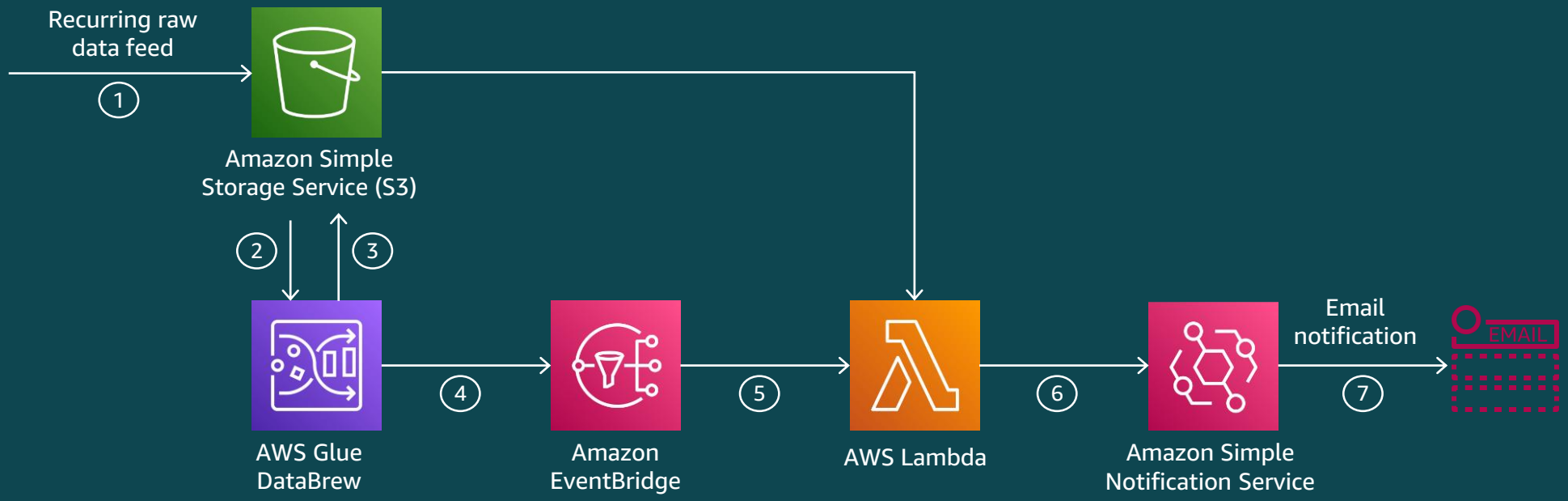
- From multiple regions into one S3 bucket (described before)
- From multiple accounts into one account’s S3 bucket

Is there a potential privacy violation?

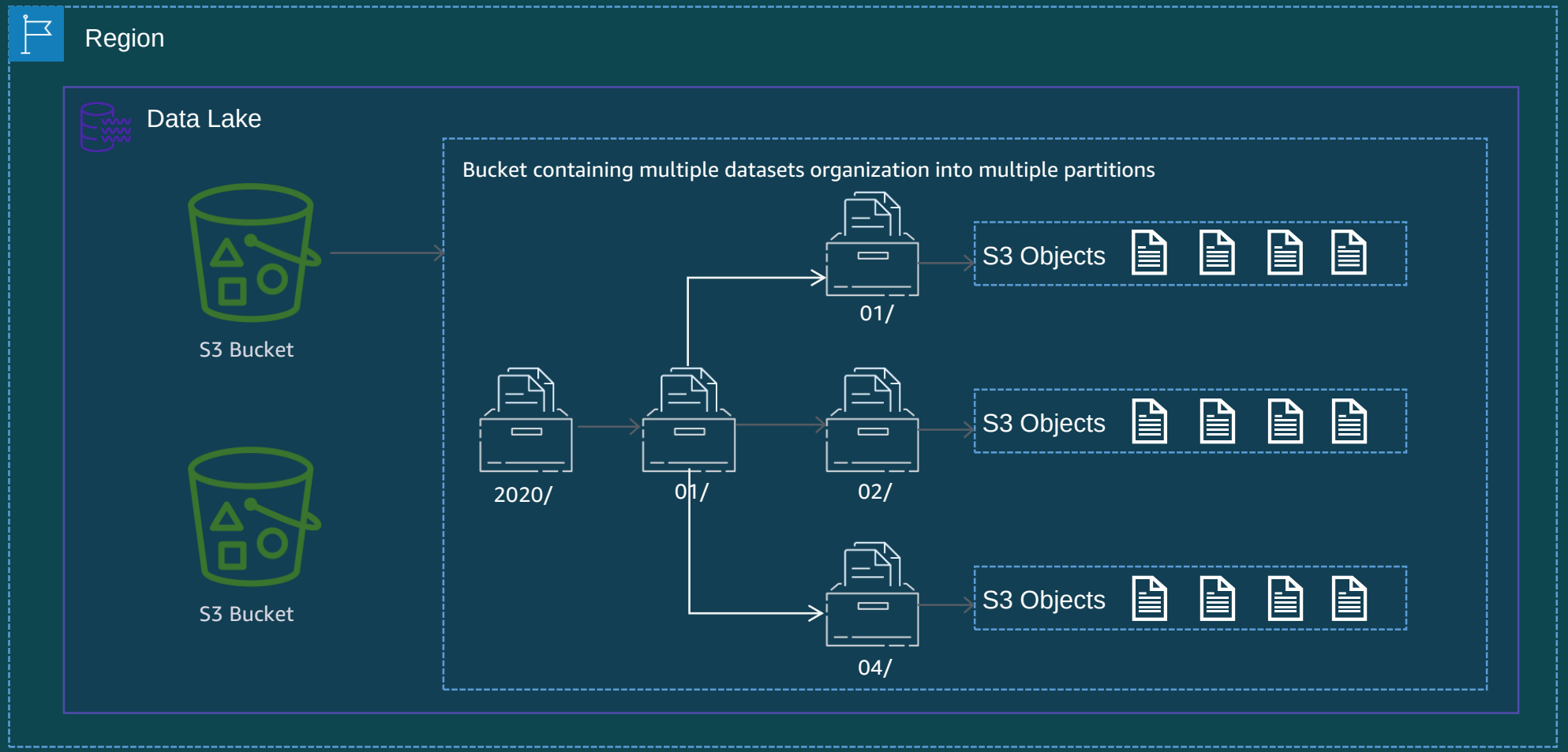
Auditability - Privacy Indicators of Compromise



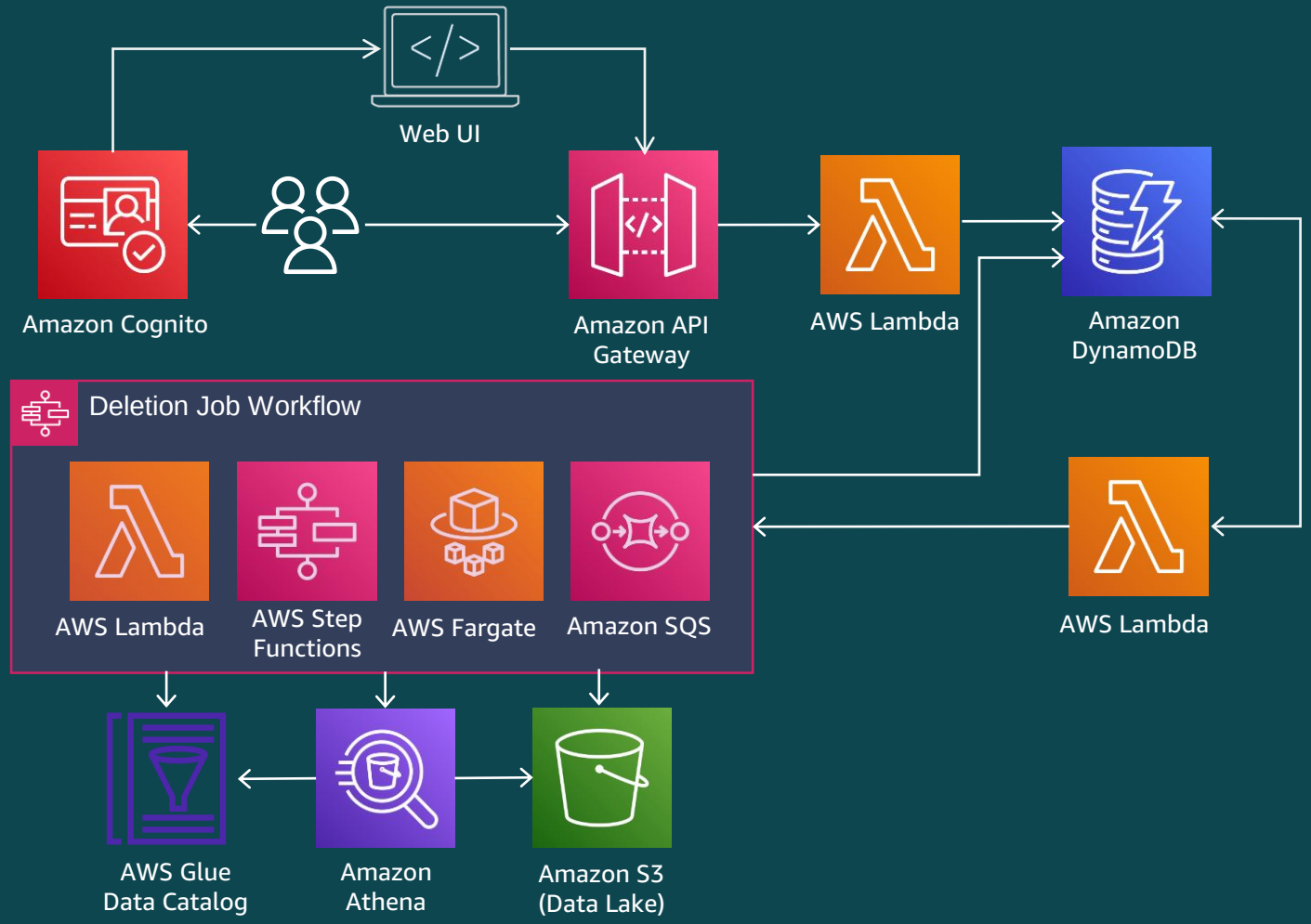
Individual Participation – Data Quality Automation



Individual Participation – Right to Erasure



Individual Participation – Right to Erasure



Come and Partner with us for Privacy Innovation

Contact Us: AWS Security Assurance Services

Helpful Links:

Privacy Features of AWS Services

Data Privacy Center

Using AWS in the Context of Common Privacy and Data Protection Considerations

Thank you!