Open-Source Taxonomy for Ex-ante Privacy

fides

CONTENTS

The challenge of Privacy and Software Development
What is Fides?
Benefits of Privacy-as-Code
Real Example 1: Enforcing policies during development
Real Example 2: Programmatic Individual Rights

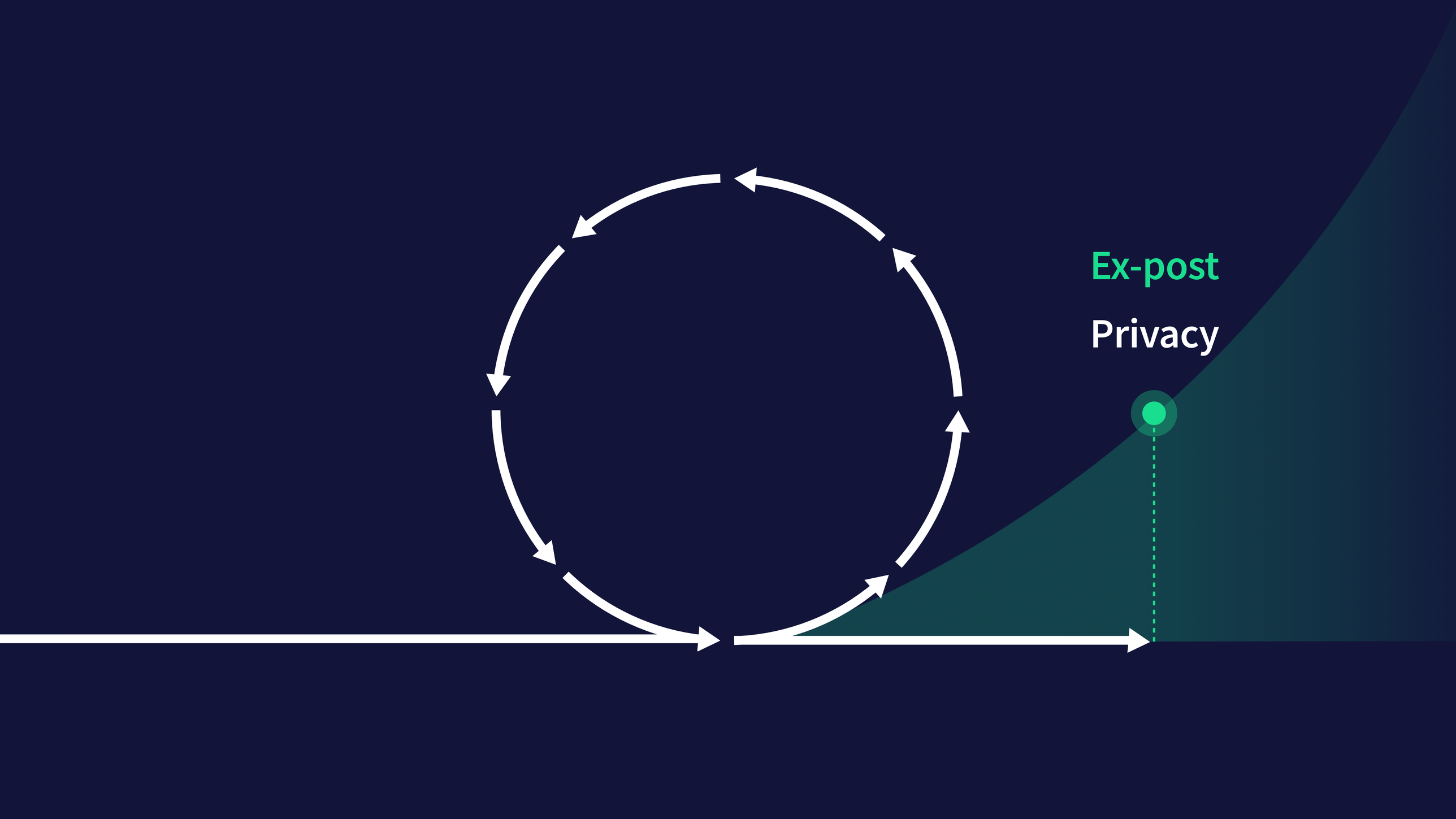
Privacy and Software Development

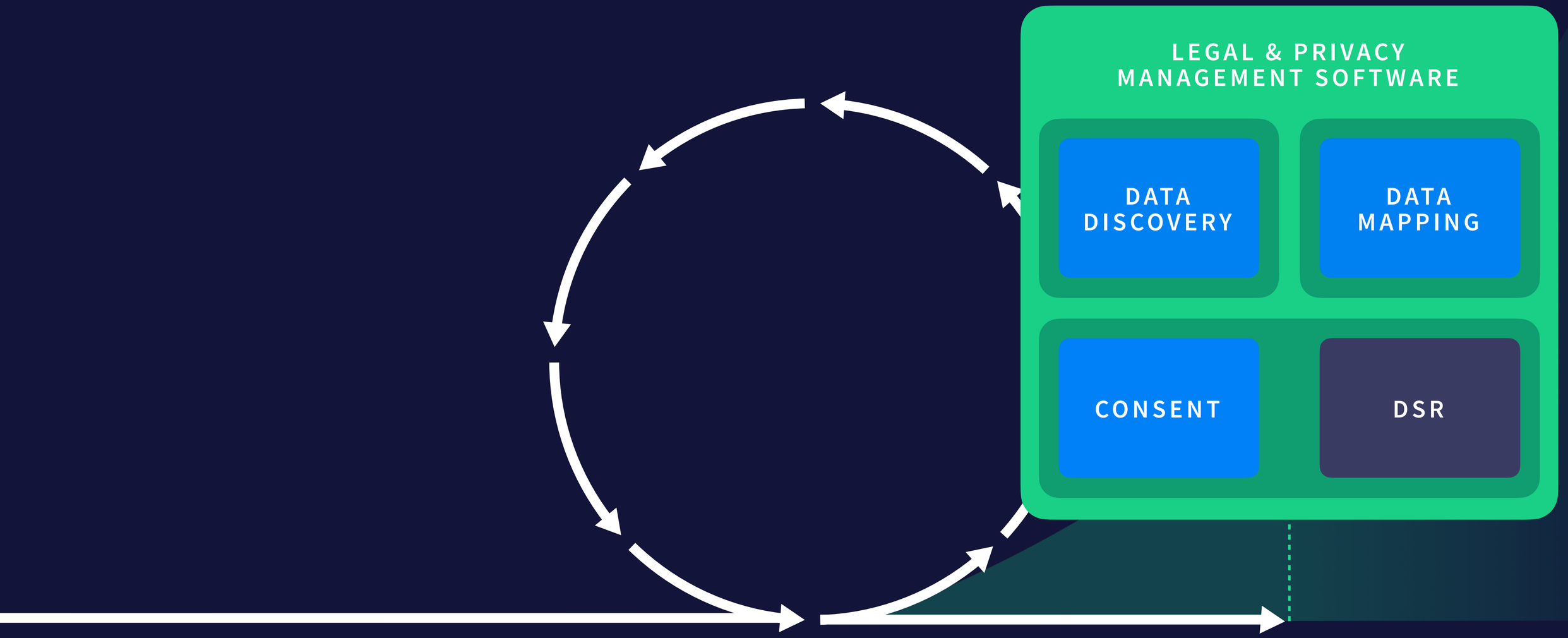
BELIEF

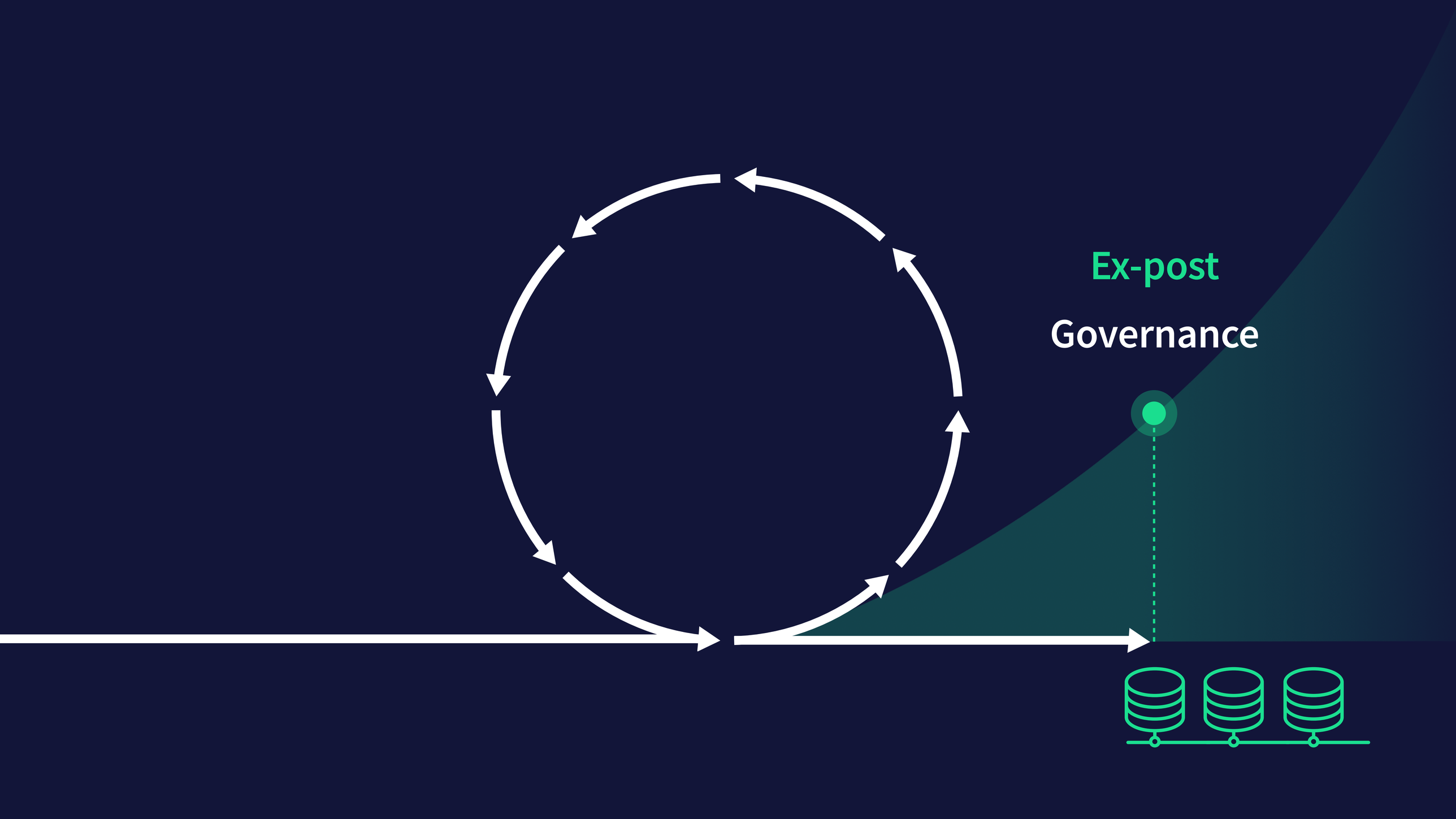
Privacy should be a feature of every tech stack.

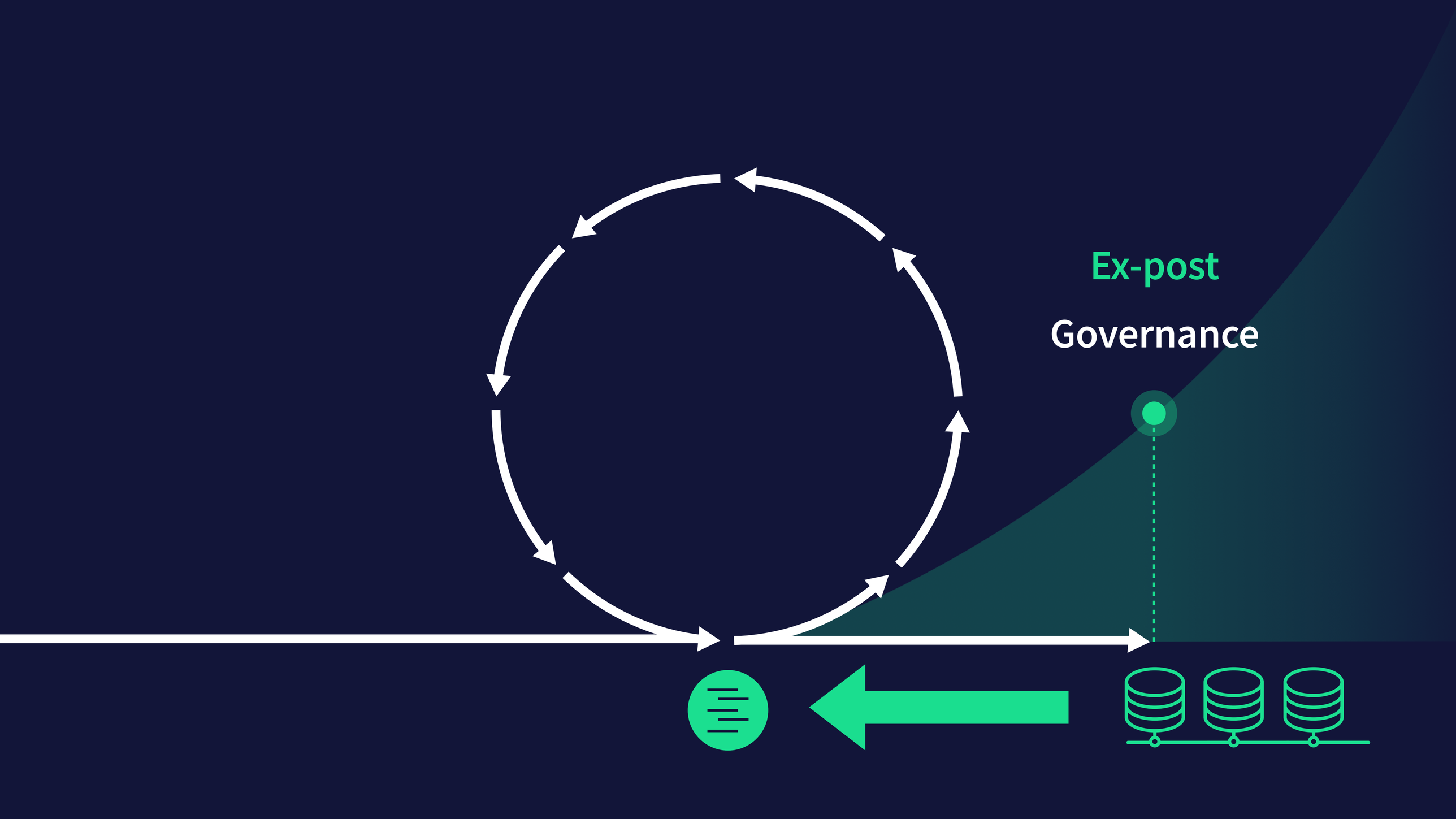
CHALLENGE

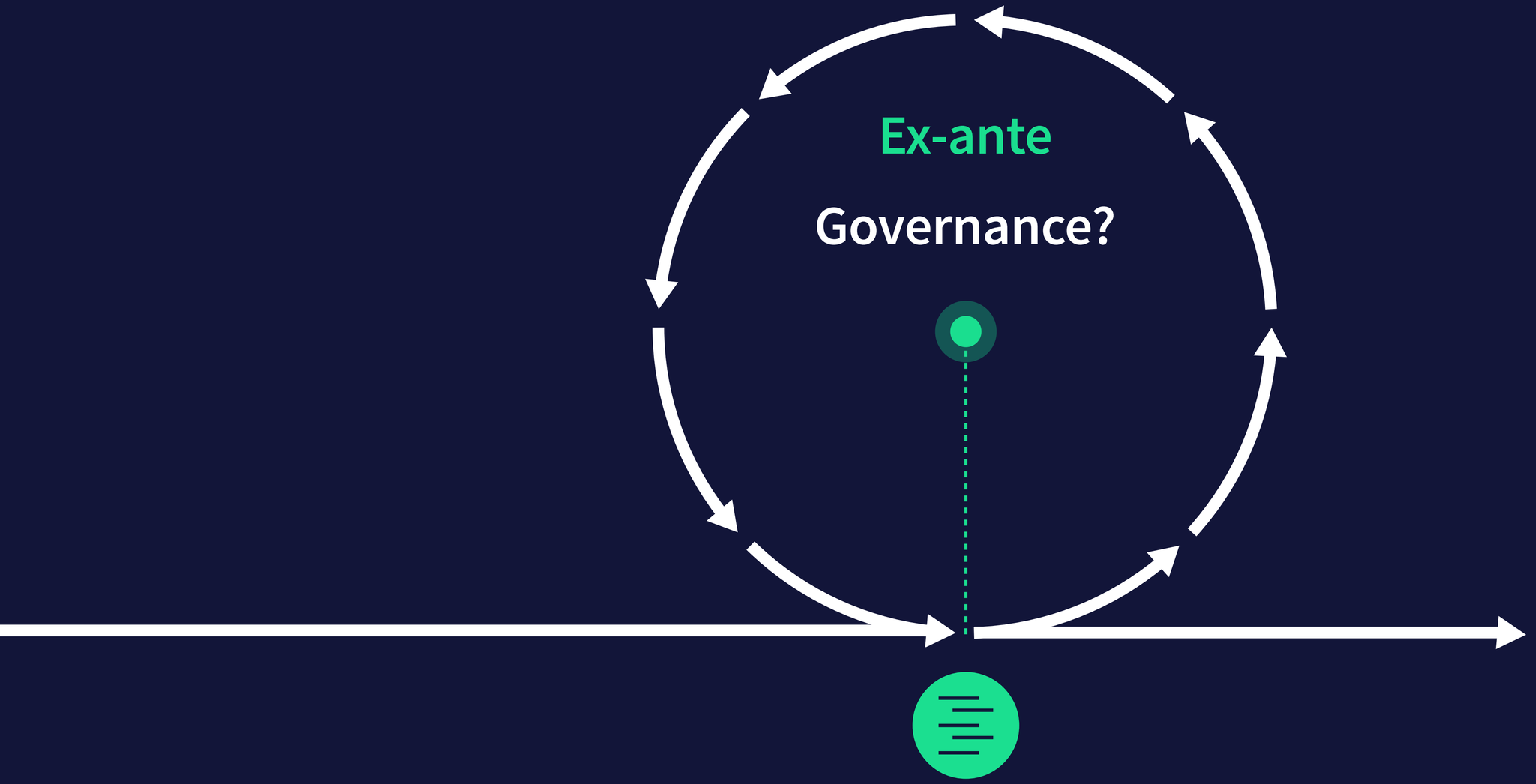
Instead for most developers, privacy creates added complexity and friction.

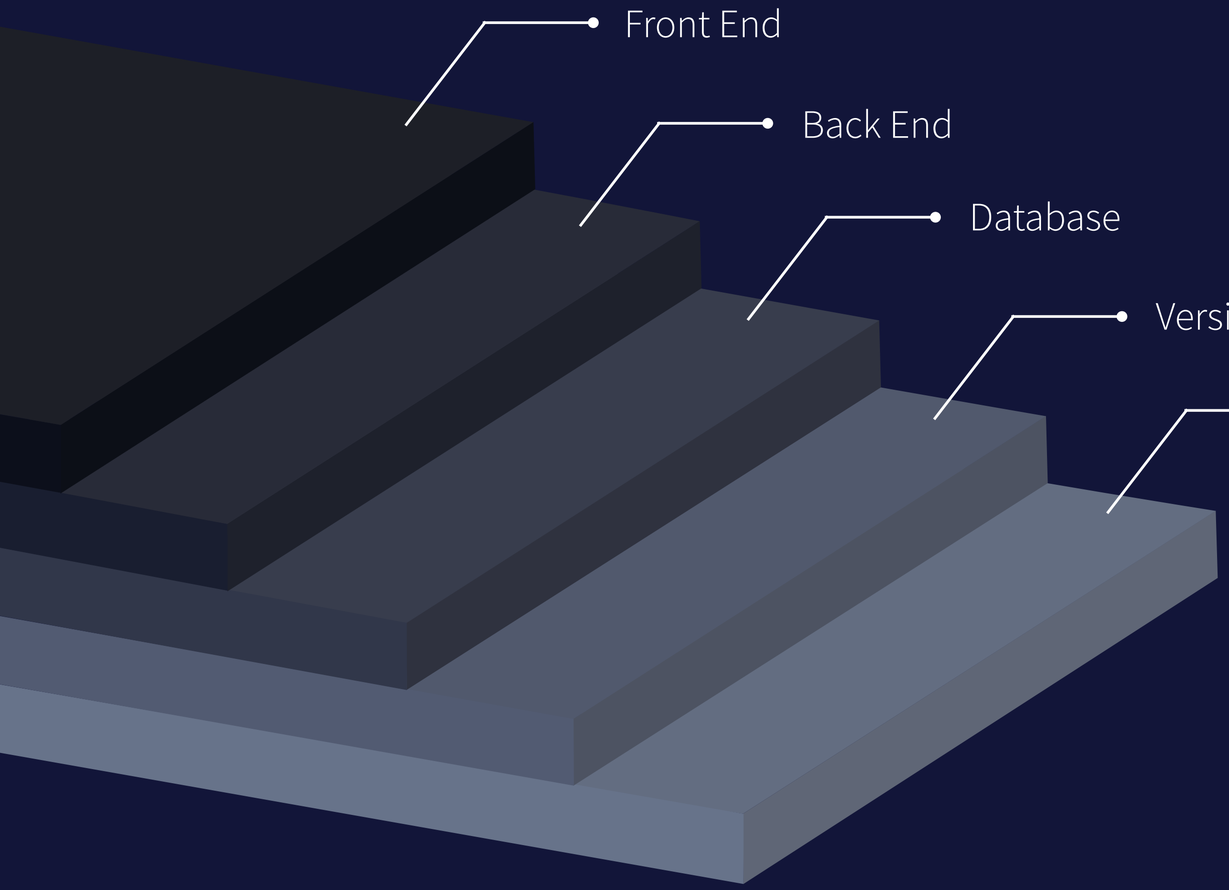

Ex-post
Privacy


LEGAL & PRIVACY
MANAGEMENT SOFTWARE
DATA
DISCOVERY
DATA
MAPPING
CONSENT
DSR

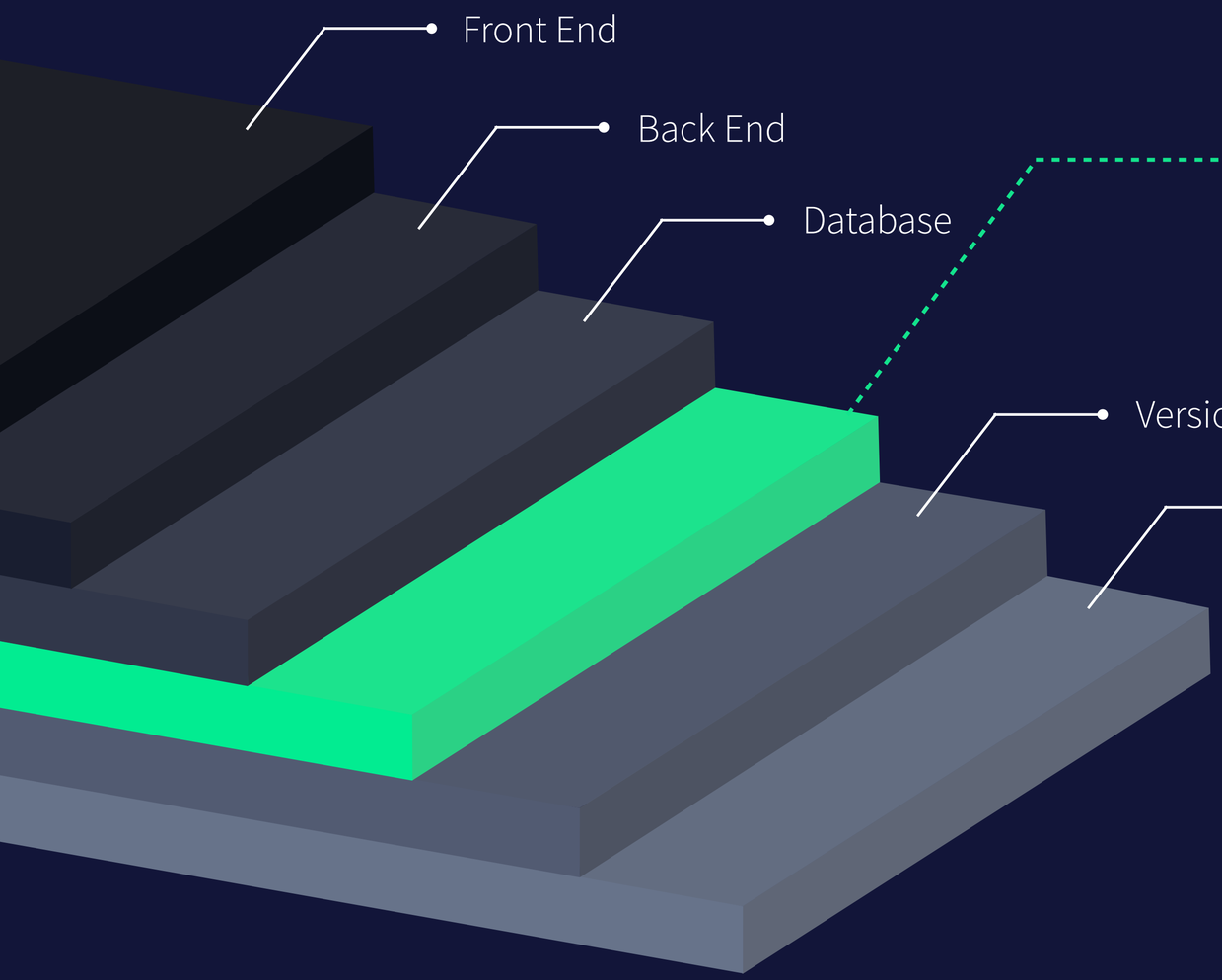

Ex-post
Governance


Ex-post
Governance


Ex-ante
Governance?



Privacy, Policy & GRC
Governance, Manual Workflows,
Risk Evaluation, Auditing



Privacy as code

Governance in the Stack
Proactive, dynamic, low
Friction part of SDLC

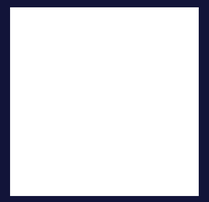
With an open-source standard for
Privacy-as-Code we can begin to solve this.
Let’s see how…

What is Fides?

fides

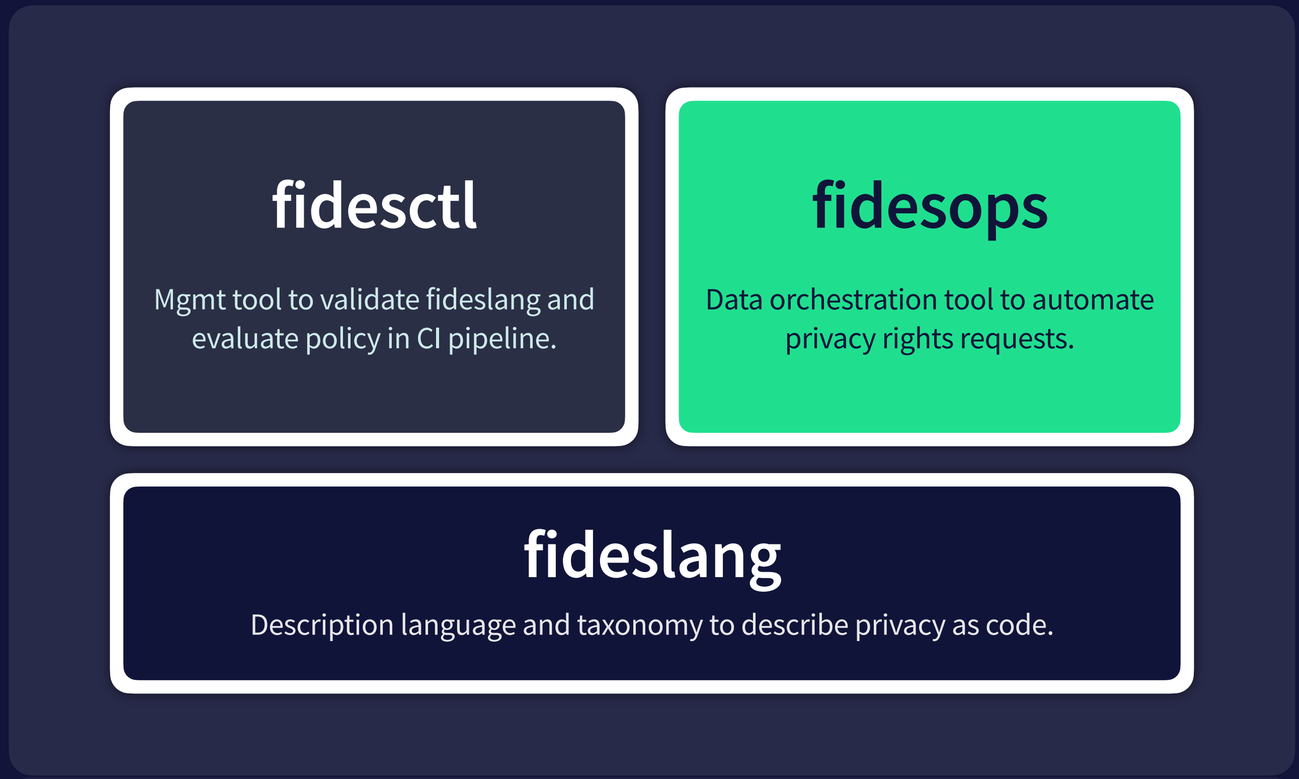
License Apache 2 License CC BY 4.0

An open-source description language and tools to add privacy to the CI pipeline and runtime.



fides benefits

- # Dev friendly language to describe data (privacy)
- # Integrate privacy checks in Git and CI
- # Build automated privacy tasks in runtime
- # Configurable data de-identification in analysis


fidesctl
Mgmt tool to validate fideslang and evaluate policy in CI pipeline.
fidesops
Data orchestration tool to automate privacy rights requests.
fideslang
Description language and taxonomy to describe privacy as code.

Benefits of Privacy-as-Code

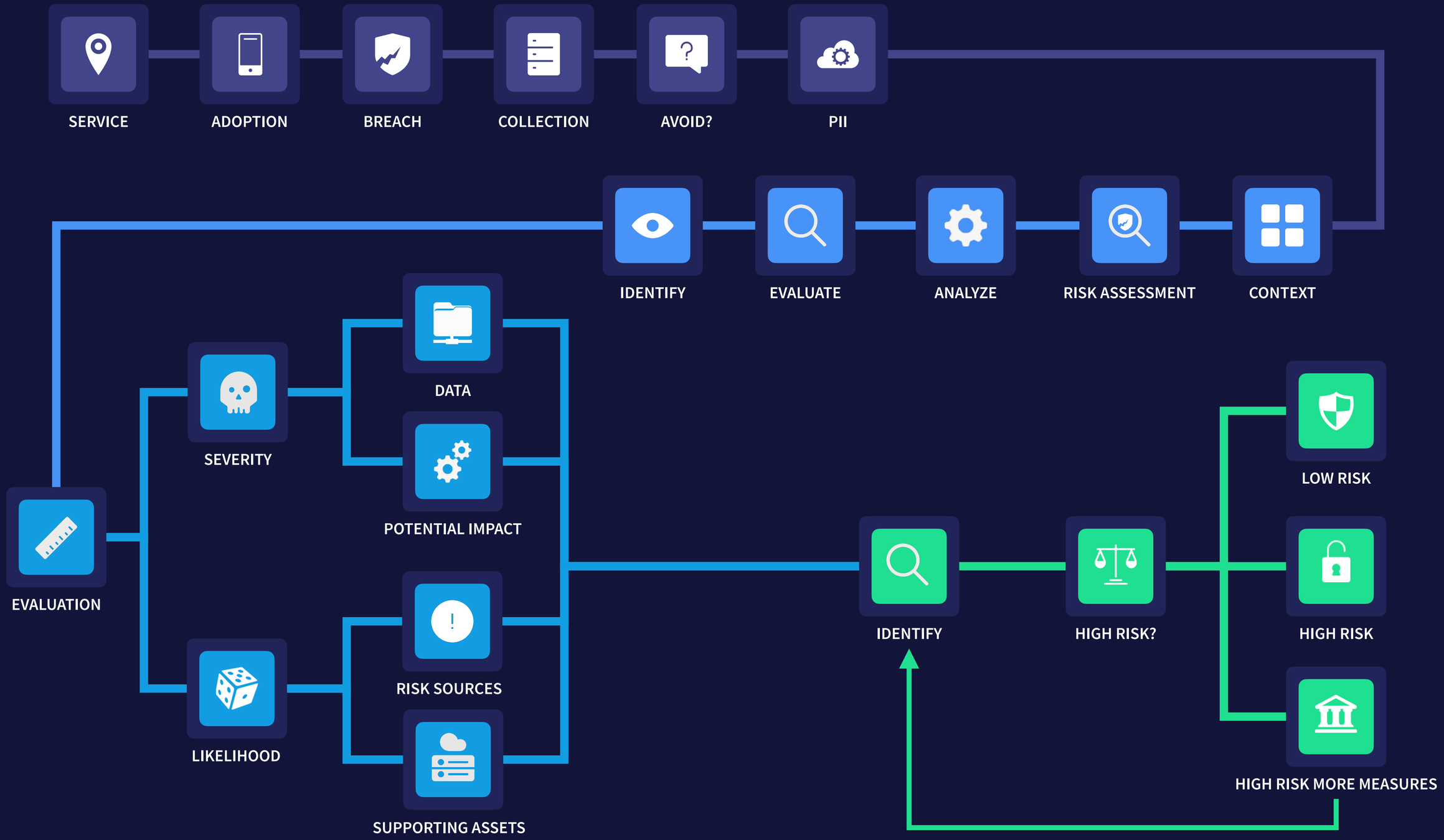
3. Enforce
4. Audit
2. Evaluate
Ex-ante
In SDLC
5. Map
1. Declare

Risks mitigated in SDLC
Audit trail of SDLC
Consistent Data Inventory
Built-in Governance

Context & Control

Use Case 1

Enforcing Policies in Development


SERVICE
ADOPTION
BREACH
COLLECTION
AVOID?
PII
IDENTIFY
EVALUATE
ANALYZE
RISK ASSESSMENT
CONTEXT
DATA
SEVERITY
POTENTIAL IMPACT
EVALUATION
RISK SOURCES
LIKELIHOOD
SUPPORTING ASSETS
IDENTIFY
HIGH RISK?
LOW RISK
HIGH RISK
HIGH RISK MORE MEASURES

CODE MANAGEMENT (DEV)
RUNTIME (PRODUCTION)
GRC, Legal, Exec
DETERMINE SENSITIVE DATA
WRITE PRIVACY POLICIES
WRITE RISK MANAGEMENT POLICIES
PRIVACY REQUEST REPORTING
Feature / Product Owner
DATA USAGE REQUIREMENTS
DESCRIBE DATA USES
WRITE RISK MANAGEMENT POLICIES
PRIVACY REQUEST MANAGEMENT
Eng, Tech
DESIGN
CODE
DEPLOY
APP MAINTENANCE
PRIVACY REQUEST FULFILLMENT
fidesctl
fidesops

PRIVACY CHECK IN CI

Describe our systems

“What, why, who and how”

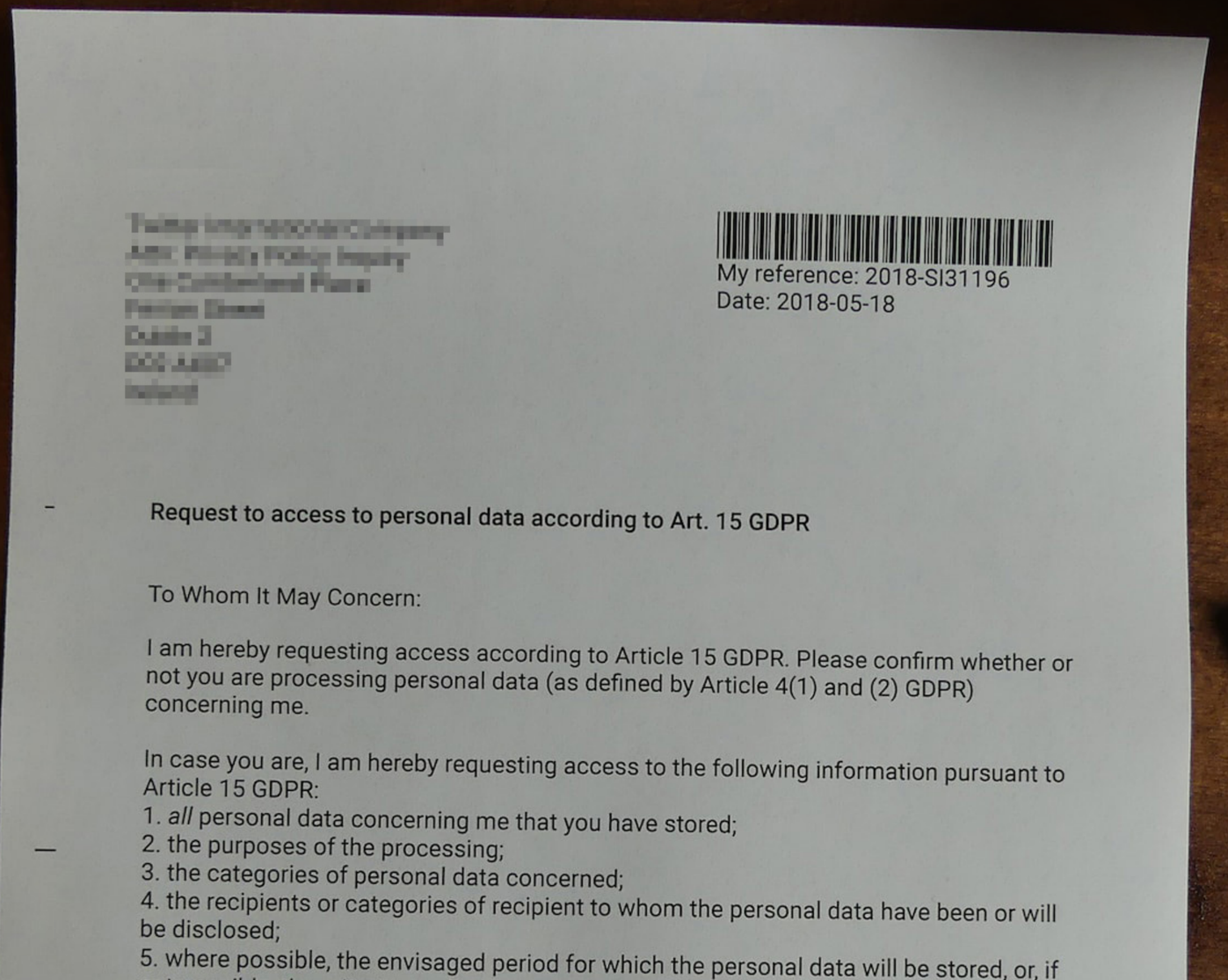
Check our system against policies

Update our system to comply

Use Case 2

Programmatic Individual Rights

Data Subject Access Requests look like this…



[redacted]

My reference: 2018-SI31196
Date: 2018-05-18

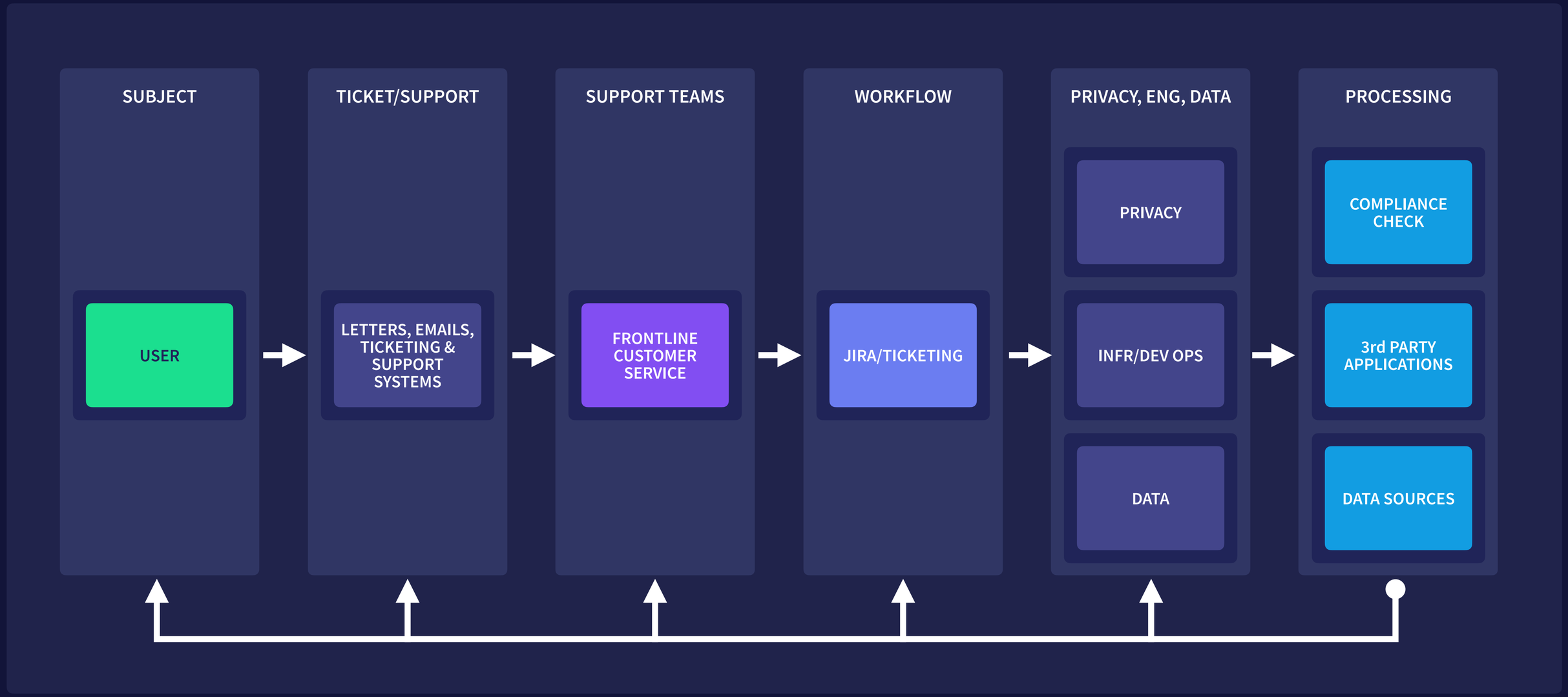
Request to access to personal data according to Art. 15 GDPR

To Whom It May Concern:

I am hereby requesting access according to Article 15 GDPR. Please confirm whether or not you are processing personal data (as defined by Article 4(1) and (2) GDPR) concerning me.

In case you are, I am hereby requesting access to the following information pursuant to Article 15 GDPR:

1. *all* personal data concerning me that you have stored;
2. the purposes of the processing;
3. the categories of personal data concerned;
4. the recipients or categories of recipient to whom the personal data have been or will be disclosed;
5. where possible, the envisaged period for which the personal data will be stored, or, if


SUBJECT
TICKET/SUPPORT
SUPPORT TEAMS
WORKFLOW
PRIVACY, ENG, DATA
PROCESSING
USER
LETTERS, EMAILS, TICKETING & SUPPORT SYSTEMS
FRONTLINE CUSTOMER SERVICE
JIRA/TICKETING
PRIVACY
INFR/DEV OPS
DATA
COMPLIANCE CHECK
3rd PARTY APPLICATIONS
DATA SOURCES

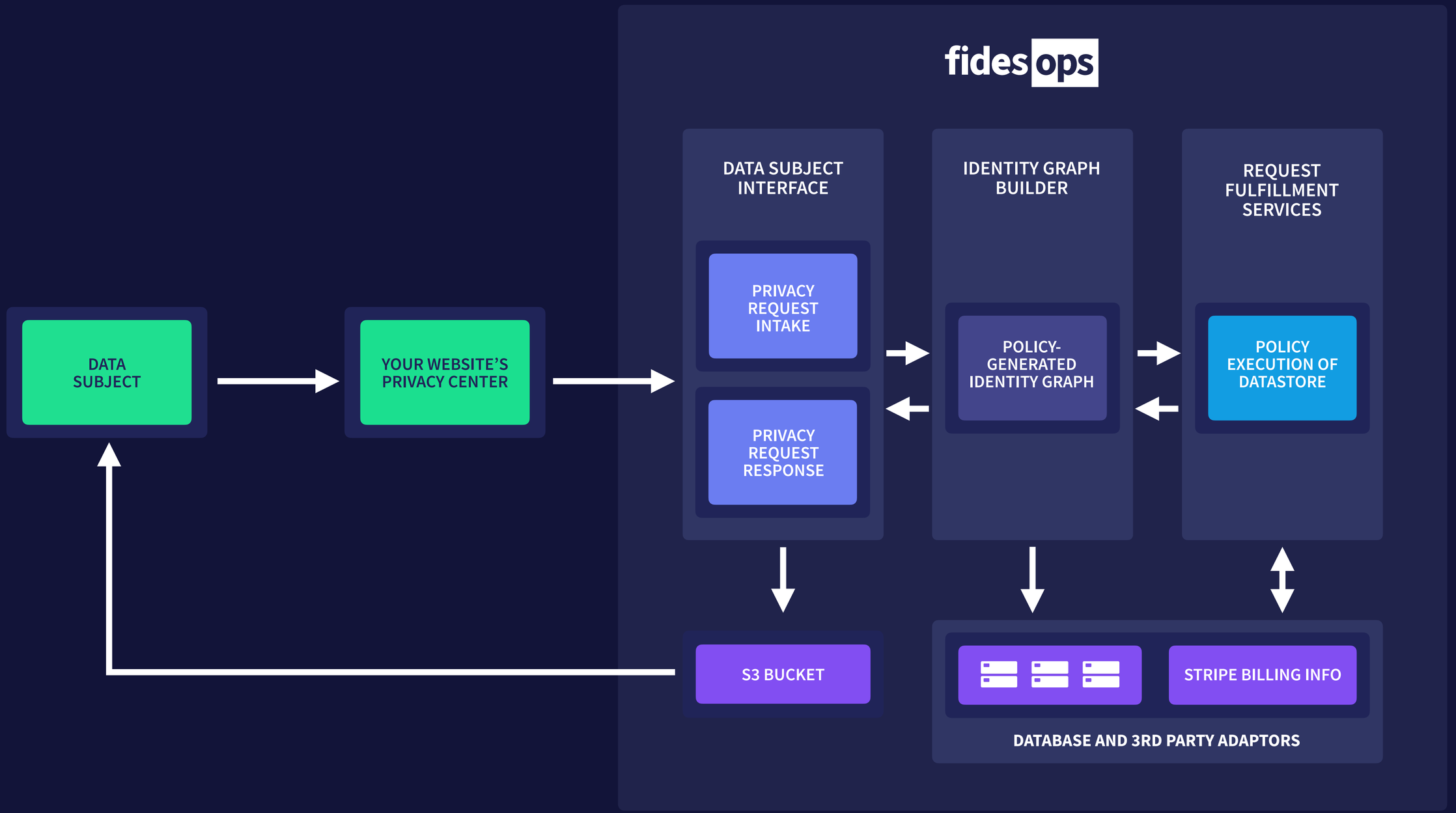
PRIVACY REQUEST IN RUNTIME

Construct a request policy

Retrieve all data for a user

Modify our request policy

Retrieve only contact data for user


fidesops
DATA SUBJECT INTERFACE
IDENTITY GRAPH BUILDER
REQUEST FULFILLMENT SERVICES
DATA SUBJECT
YOUR WEBSITE'S PRIVACY CENTER
PRIVACY REQUEST INTAKE
PRIVACY REQUEST RESPONSE
POLICY-GENERATED IDENTITY GRAPH
POLICY EXECUTION OF DATASTORE
S3 BUCKET
STRIPE BILLING INFO
DATABASE AND 3RD PARTY ADAPTORS

CONTENTS

The challenge of Privacy and Software Development
What is Fides?
Benefits of Privacy-as-Code
Real Example 1: Enforcing policies during development
Real Example 2: Programmatic Individual Rights

fides

fidesctl

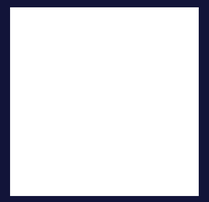
Mgmt tool to validate fideslang and evaluate policy in CI pipeline.

fidesops

Data orchestration tool to automate privacy rights requests.

fideslang

Description language and taxonomy to describe privacy as code.



fides

License Apache 2 License CC BY 4.0

Join the community and contribute to help define an open standard for Trust and Respect.

ethyca.com/fides