ethyca

European AI Act unpacked for Governance, Data & Engineering

Session

01 / Privacy & Governance engineering benefits

02 / EU AI Acts Requirements and Technical Impacts

03 / Technical deep dive: Risk management systems

04 / Technical deep dive: Data governance

05 / Embedded engineering solution to AI governance

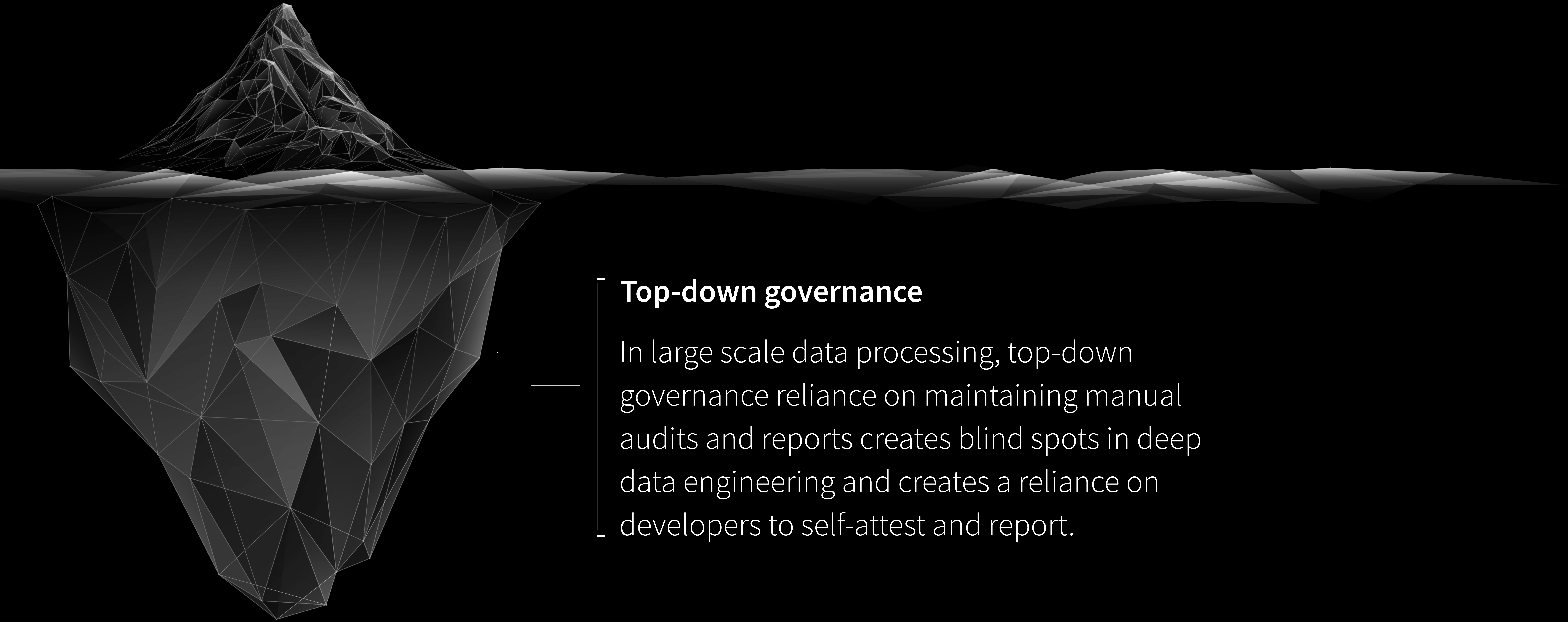
06 / Key Takeaways

ethyca

Privacy & governance engineering approach to AI

Top-down governance

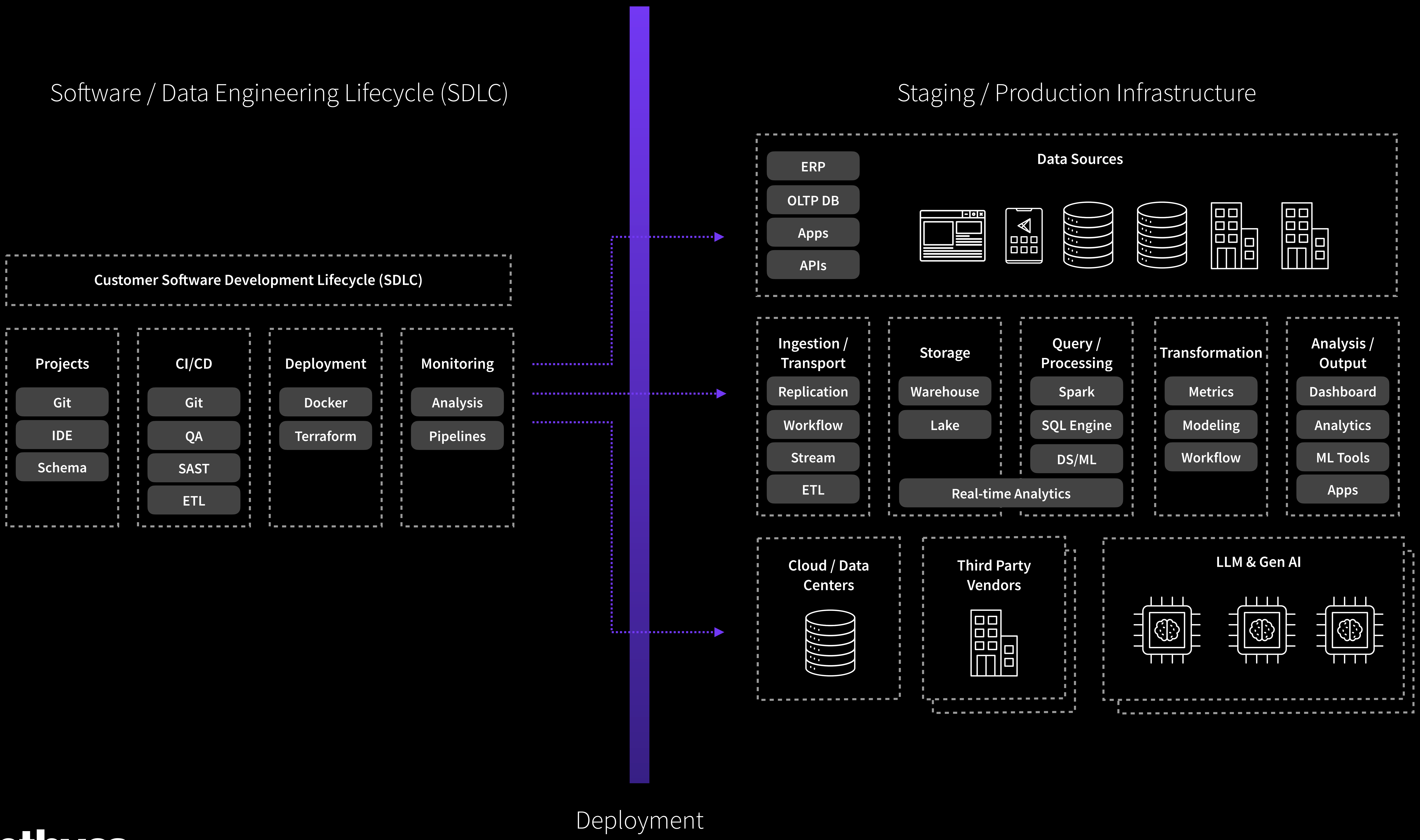
Is vital to an organizations success, yet managing workflows and maintaining inventories is a traditional approach facing an increasingly complex data landscape.



Top-down governance

In large scale data processing, top-down governance reliance on maintaining manual audits and reports creates blind spots in deep data engineering and creates a reliance on developers to self-attest and report.

Modern Data & AI Enterprise Architecture



Software / Data Engineering Lifecycle (SDLC)

Customer Software Development Lifecycle (SDLC)

Projects
- Git
- IDE
- Schema

CI/CD
- Git
- QA
- SAST
- ETL

Deployment
- Docker
- Terraform

Monitoring
- Analysis
- Pipelines

Deployment

Staging / Production Infrastructure

Data Sources
- ERP
- OLTP DB
- Apps
- APIs

Ingestion / Transport
- Replication
- Workflow
- Stream
- ETL

Storage
- Warehouse
- Lake

Query / Processing
- Spark
- SQL Engine
- DS/ML

Real-time Analytics

Transformation
- Metrics
- Modeling
- Workflow

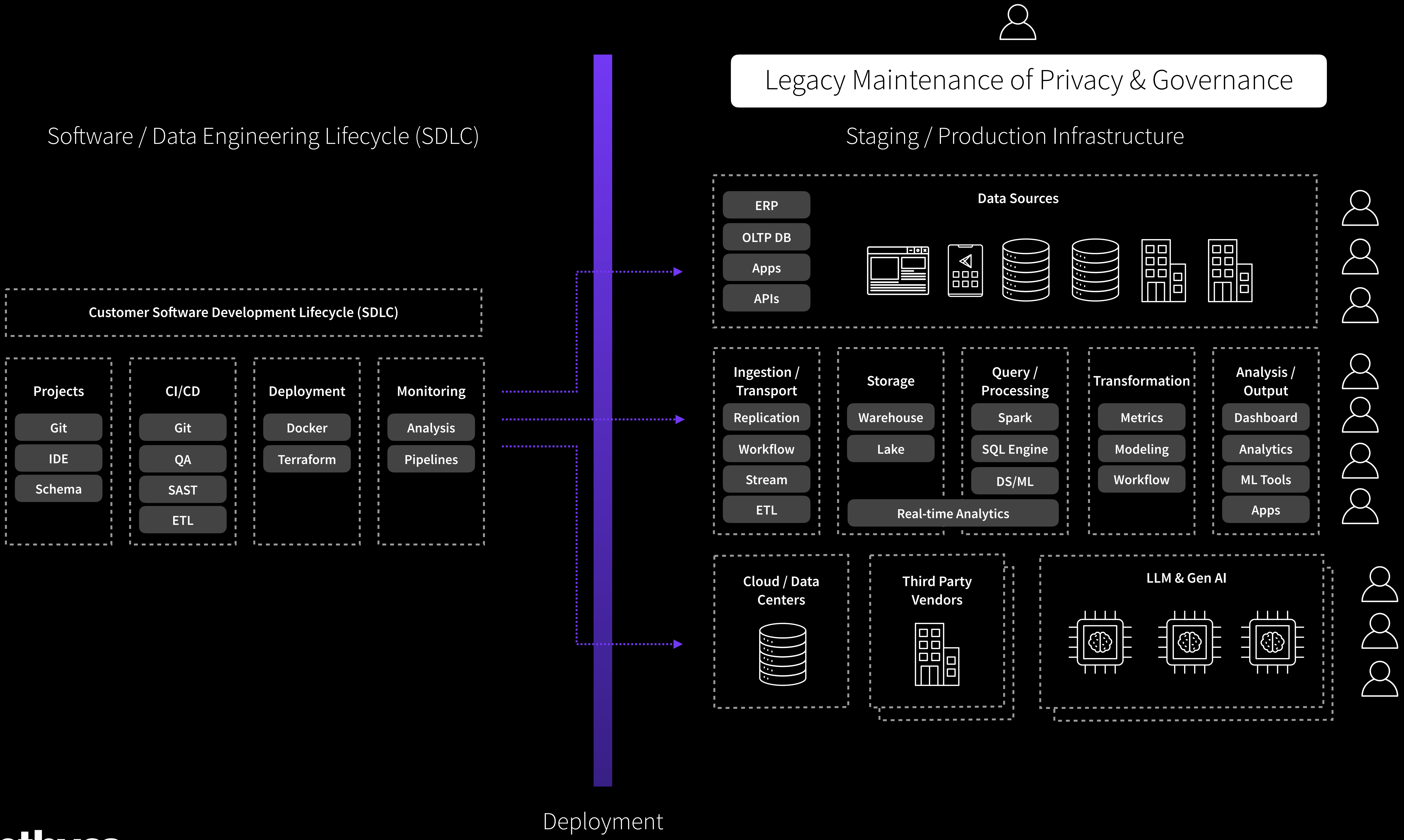
Analysis / Output
- Dashboard
- Analytics
- ML Tools
- Apps

Cloud / Data Centers

Third Party Vendors

LLM & Gen AI

Modern Data & AI Enterprise Architecture



Legacy Maintenance of Privacy & Governance

Software / Data Engineering Lifecycle (SDLC)

Customer Software Development Lifecycle (SDLC)

Projects
- Git
- IDE
- Schema

CI/CD
- Git
- QA
- SAST
- ETL

Deployment
- Docker
- Terraform

Monitoring
- Analysis
- Pipelines

Deployment

Staging / Production Infrastructure

Data Sources
- ERP
- OLTP DB
- Apps
- APIs

Ingestion / Transport
- Replication
- Workflow
- Stream
- ETL

Storage
- Warehouse
- Lake

Query / Processing
- Spark
- SQL Engine
- DS/ML

Real-time Analytics

Transformation
- Metrics
- Modeling
- Workflow

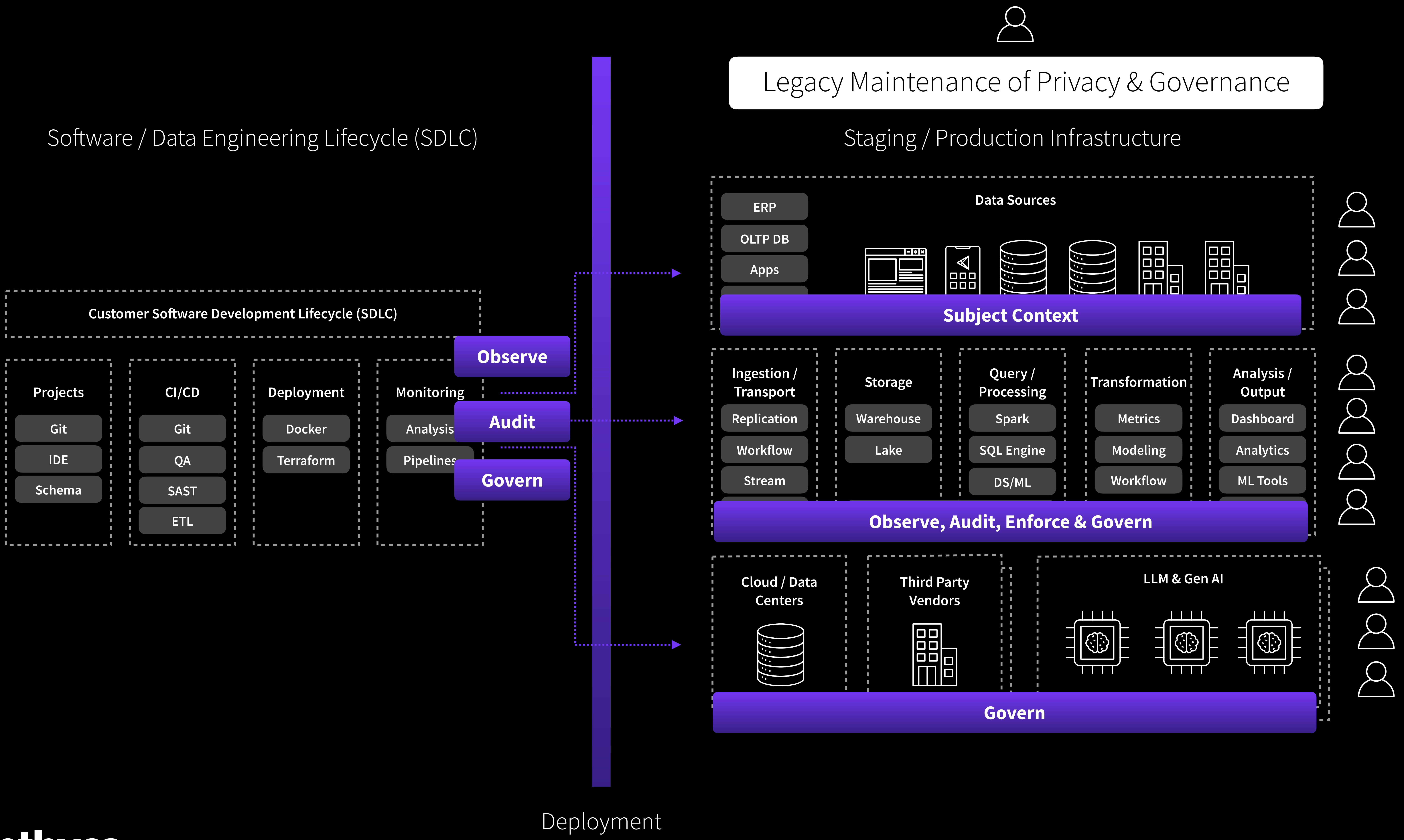
Analysis / Output
- Dashboard
- Analytics
- ML Tools
- Apps

Cloud / Data Centers

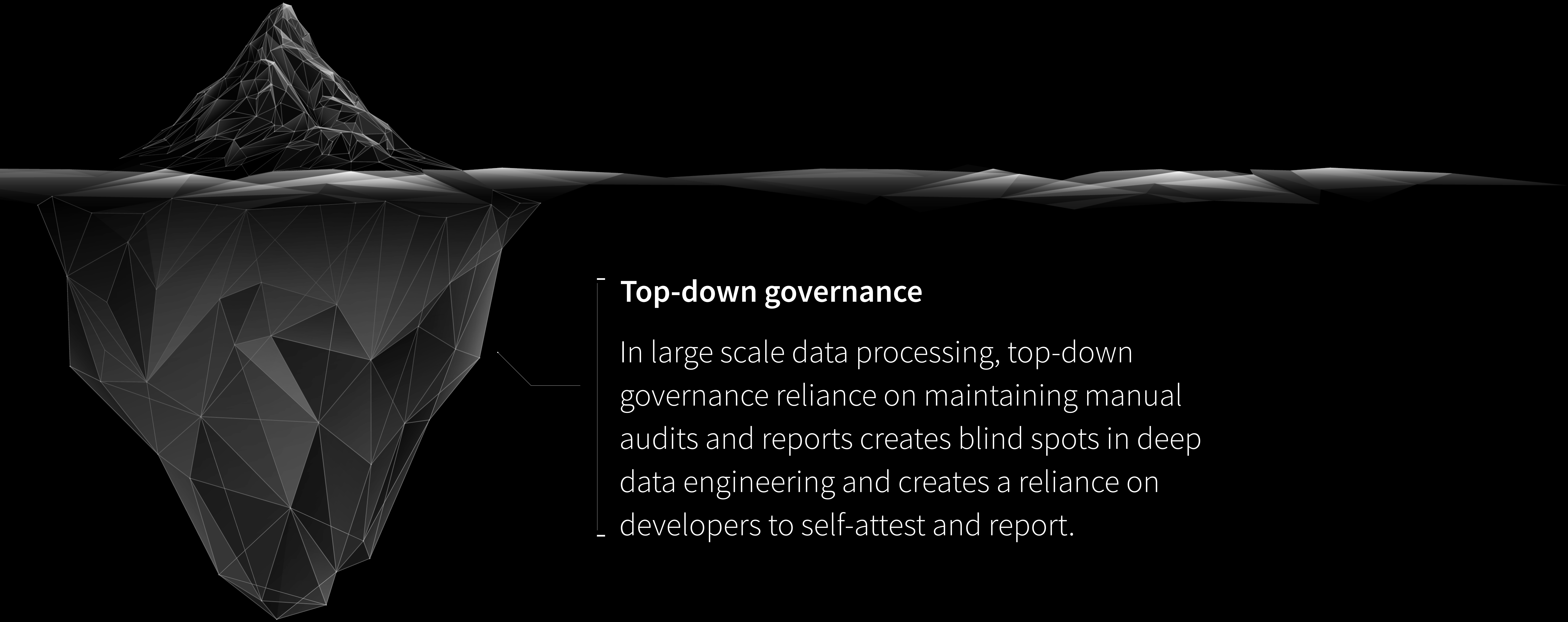
Third Party Vendors

LLM & Gen AI

Modern Data & AI Enterprise Architecture



ethyca



Top-down governance

In large scale data processing, top-down governance reliance on maintaining manual audits and reports creates blind spots in deep data engineering and creates a reliance on developers to self-attest and report.

Engineering Operating System for Governance of Data & AI

Seamlessly integrate data governance with software development, data engineering and AI for data-driven enterprise. Confidently observe, audit and govern the risks of modern data.

ethyca

EU AI Acts Requirements and Technical Impacts

EU AI Act Risk Thresholds

Majority of AI with negligible risk can continue without regulation.

Minimal or No Risk

Limited Risk

High Risk

Unacceptable Risk

EU AI Act Risk Thresholds

Minimal or No Risk

Limited Risk

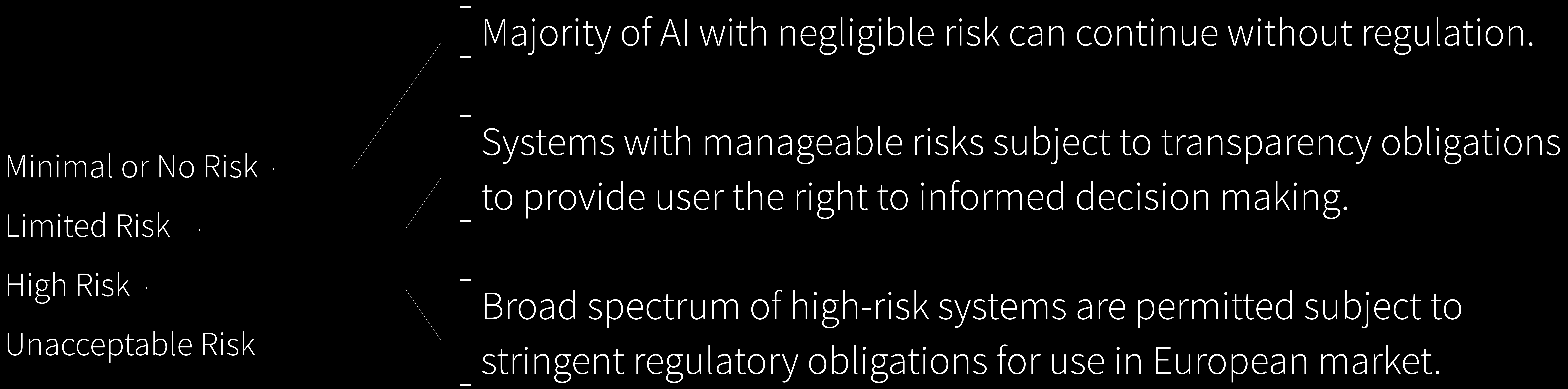
High Risk

Unacceptable Risk

Majority of AI with negligible risk can continue without regulation.

Systems with manageable risks subject to transparency obligations to provide user the right to informed decision making.

EU AI Act Risk Thresholds



Minimal or No Risk

Limited Risk

High Risk

Unacceptable Risk

Majority of AI with negligible risk can continue without regulation.

Systems with manageable risks subject to transparency obligations to provide user the right to informed decision making.

Broad spectrum of high-risk systems are permitted subject to stringent regulatory obligations for use in European market.

EU AI Act Risk Thresholds

Minimal or No Risk

Majority of AI with negligible risk can continue without regulation.

Limited Risk

Systems with manageable risks subject to transparency obligations to provide user the right to informed decision making.

High Risk

Broad spectrum of high-risk systems are permitted subject to stringent regulatory obligations for use in European market.

Unacceptable Risk

Systems teemed to have unacceptable risks such as cognitive manipulation, predictive policing, social scoring are broadly banned with some limited government, military and law enforcement use cases.

EU AI Act Risk Thresholds

Minimal or No Risk

Limited Risk

High Risk

Unacceptable Risk

Broad spectrum of high-risk systems are permitted subject to stringent regulatory obligations for use in European market.

EU AI Act's 10 Technical Requirements

Quality management systems

Conformity assessment

Corrective action

Risk management

Data governance

Technical documentation

Record-keeping

Transparency

Human oversight

Accuracy, robustness and security

EU AI Act’s 10 Technical Requirements

Quality management systems

Conformity assessment

Corrective action

Risk management

Data governance

Technical documentation

Record-keeping

Transparency

Human oversight

Accuracy, robustness and security

Continuous risk management system run throughout the lifecycle of a high-risk AI system, requiring regular updates.

EU AI Act’s 10 Technical Requirements

- Quality management systems
- Conformity assessment
- Corrective action
- Risk management
- Data governance
- Technical documentation
- Record-keeping
- Transparency
- Human oversight
- Accuracy, robustness and security

Continuous risk management system run throughout the lifecycle of a high-risk AI system, requiring regular updates.

Define and enforce organizational policies for AI and govern the use of data processing activity in AI systems.

EU AI Act’s 10 Technical Requirements

- Corrective action
- **Risk management**
- Data governance
- ▻ Technical documentation
- Record-keeping
- Transparency
- Human oversight
- Accuracy, robustness and security
- Quality management systems
- Conformity assessment

Prepare and maintain technical documentation prior to an AI system’s deployment and processing of data.

EU AI Act’s 10 Technical Requirements

Risk management

Data governance

Technical documentation

▻ Record-keeping

Transparency

Human oversight

Accuracy, robustness and security

Quality management systems

Conformity assessment

Corrective action

Maintain continuous records of the data processing lifecycle of AI systems, from data collection, ingestion, outcome and failure/risk.

ethyca

EU AI Act’s 10 Technical Requirements

- Data governance
- Technical documentation
- Record-keeping
- ▻ Transparency
- Human oversight
- Accuracy, robustness and security
- Quality management systems
- Conformity assessment
- Corrective action
- Risk management

Provide transparent notices to a person when they are interacting with AI and what purpose it is performing.

EU AI Act’s 10 Technical Requirements

Technical documentation

Record-keeping

Transparency

▻ Human oversight

Accuracy, robustness and security

Quality management systems

Conformity assessment

Corrective action

Risk management

Data governance

AI sytems should be designs with “humans in the loop”, to assure accountability, dignity, human agency, trust and transparency.

ethyca

EU AI Act’s 10 Technical Requirements

- Record-keeping
- Transparency
- Human oversight
- ▻ Accuracy, robustness and security
- Quality management systems
- Conformity assessment
- Corrective action
- Risk management
- Data governance
- Technical documentation

High-risk AI systems must achieve an appropriate level or accuracy, prevent bias in continuous learning and have appropriate security controls in place.

EU AI Act’s 10 Technical Requirements

Transparency

Human oversight

Accuracy, robustness and security

▻ Quality management systems

Conformity assessment

Corrective action

Risk management

Data governance

Technical documentation

Record-keeping

Providers of high-risk AI systems must implement a comprehensive quality management system that adequately documents, records and enforces the regulations.

EU AI Act's 10 Technical Requirements

- Human oversight
- Accuracy, robustness and security
- Quality management systems
- ▻ Conformity assessment
- Corrective action
- Risk management
- Data governance
- Technical documentation
- Record-keeping
- Transparency

A pro-deployment conformity assessment must be conducted for high risk AI systems to evidence that a system meets the regulatory requirements. Includes testing, inspection, certification.

EU AI Act Technical a EU AI Act’s 10 Technical Requirements

Accuracy, robustness and security

Quality management systems

Conformity assessment

▻ Corrective action

Risk management

Data governance

Technical documentation

Record-keeping

Transparency

Human oversight

Where a provider becomes aware that an AI system deployed in the market may not be in conformity, or create a new risk, they must withdraw the system and take immediate measures to remediate.

Webinar focus area: Risk Management & Data Governance

Quality management systems

Conformity assessment

Corrective action

Risk management

Data governance

Technical documentation

Record-keeping

Transparency

Human oversight

Accuracy, robustness and security

Continuous risk management system run throughout the lifecycle of a high-risk AI system, requiring regular updates.

Define and enforce organizational policies for AI and govern the use of data processing activity in AI systems.

ethyca

Deep dive
AI Risk Management

EU AI Act Technical Risk Management

Quality management systems

Conformity assessment

Corrective action

▻ Risk management

Data governance

Technical documentation

Record-keeping

Transparency

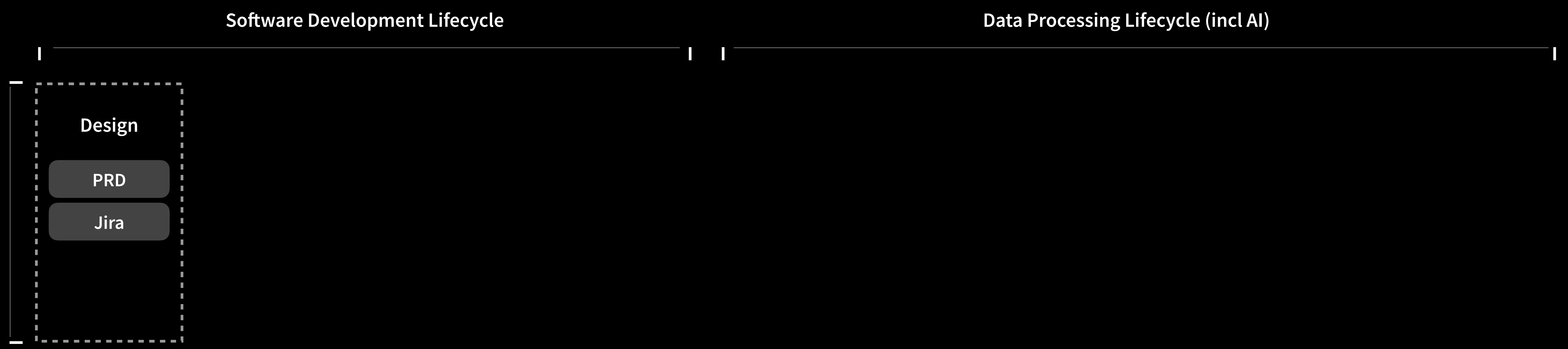
Human oversight

Accuracy, robustness and security

Continuous, end-to-end identification, mitigation and recording of risks in AI design, development and operations.

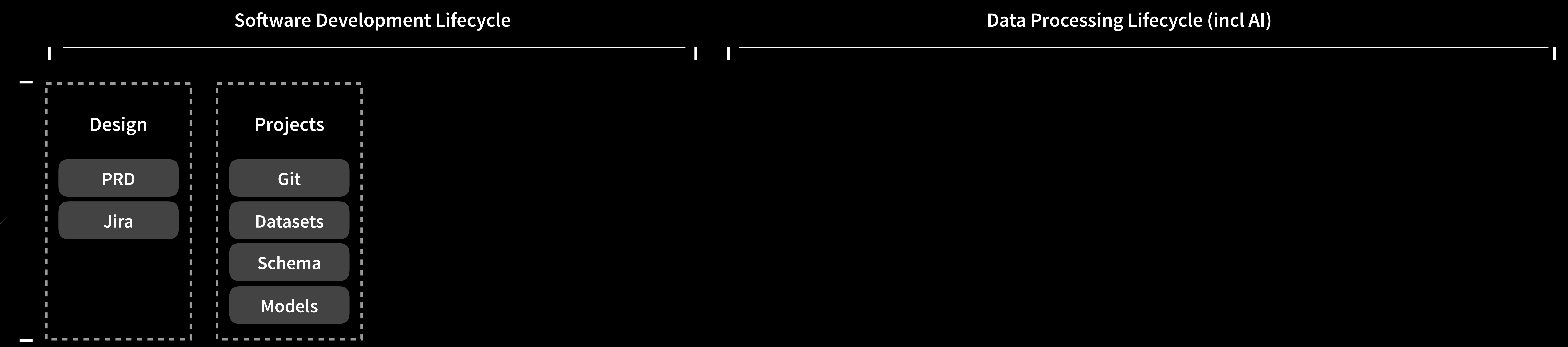
EU AI Act Technical Risk Management

- Quality management systems
- Conformity assessment
- Corrective action
- ▻ Risk management
- Data governance
- Technical documentation
- Record-keeping
- Transparency
- Human oversight
- Accuracy, robustness and security


Software Development Lifecycle
Data Processing Lifecycle (incl AI)
Design
PRD
Jira

EU AI Act Technical Risk Management

- Quality management systems
- Conformity assessment
- Corrective action
- ▻ **Risk management**
- Data governance
- Technical documentation
- Record-keeping
- Transparency
- Human oversight
- Accuracy, robustness and security


Software Development Lifecycle
Data Processing Lifecycle (incl AI)
Design
PRD
Jira
Projects
Git
Datasets
Schema
Models

EU AI Act Technical Risk Management

Quality management systems

Conformity assessment

Corrective action

▻ Risk management

Data governance

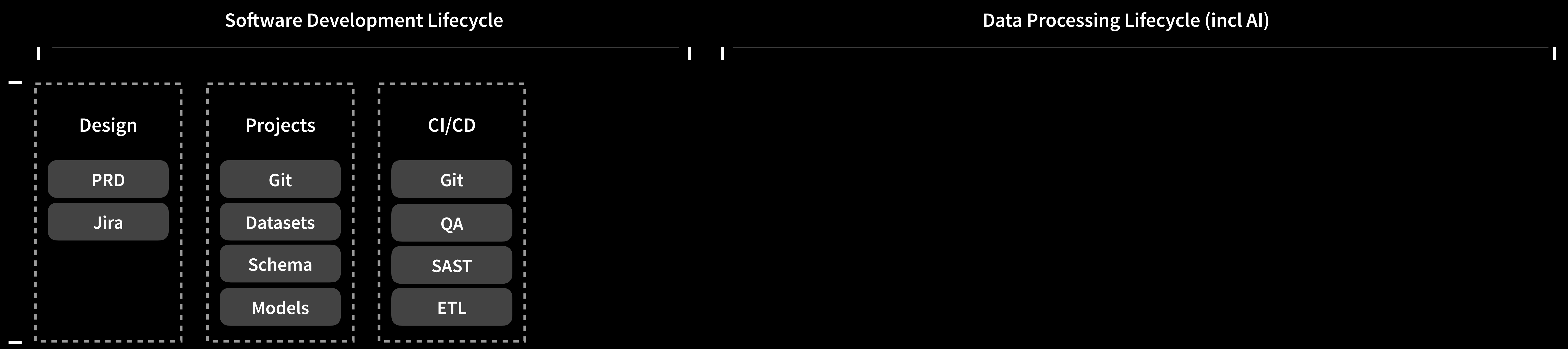
Technical documentation

Record-keeping

Transparency

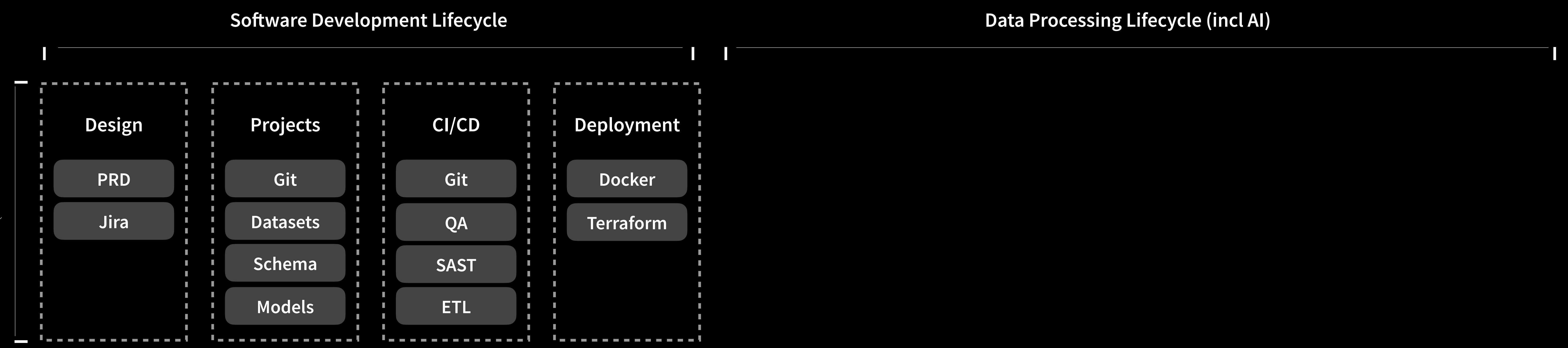
Human oversight

Accuracy, robustness and security


Software Development Lifecycle
Data Processing Lifecycle (incl AI)
Design
PRD
Jira
Projects
Git
Datasets
Schema
Models
CI/CD
Git
QA
SAST
ETL

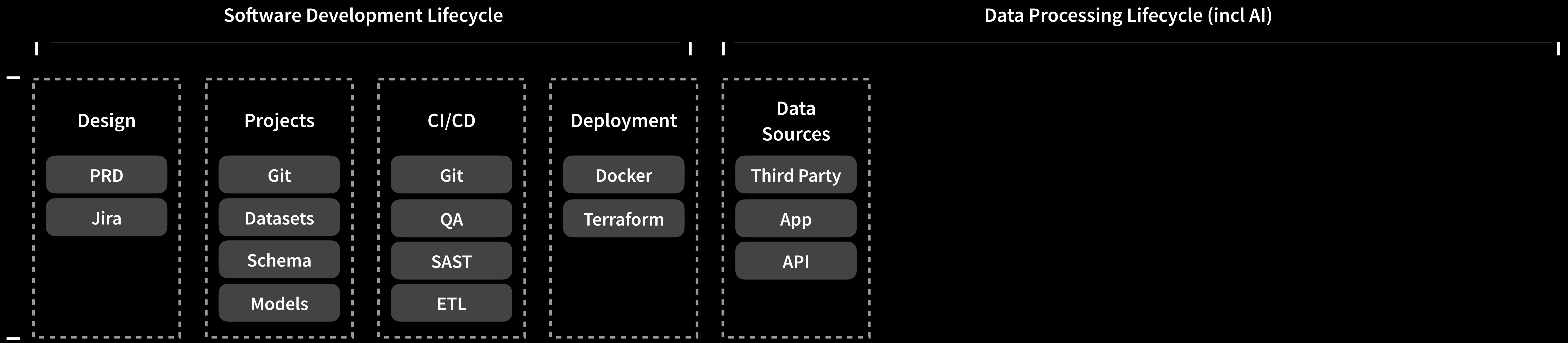
EU AI Act Technical Risk Management

- Quality management systems
- Conformity assessment
- Corrective action
- ▻ Risk management
- Data governance
- Technical documentation
- Record-keeping
- Transparency
- Human oversight
- Accuracy, robustness and security



EU AI Act Technical Risk Management

- Quality management systems
- Conformity assessment
- Corrective action
- ▻ Risk management
- Data governance
- Technical documentation
- Record-keeping
- Transparency
- Human oversight
- Accuracy, robustness and security



ethyca

EU AI Act Technical Risk Management

Quality management systems

Conformity assessment

Corrective action

▻ Risk management

Data governance

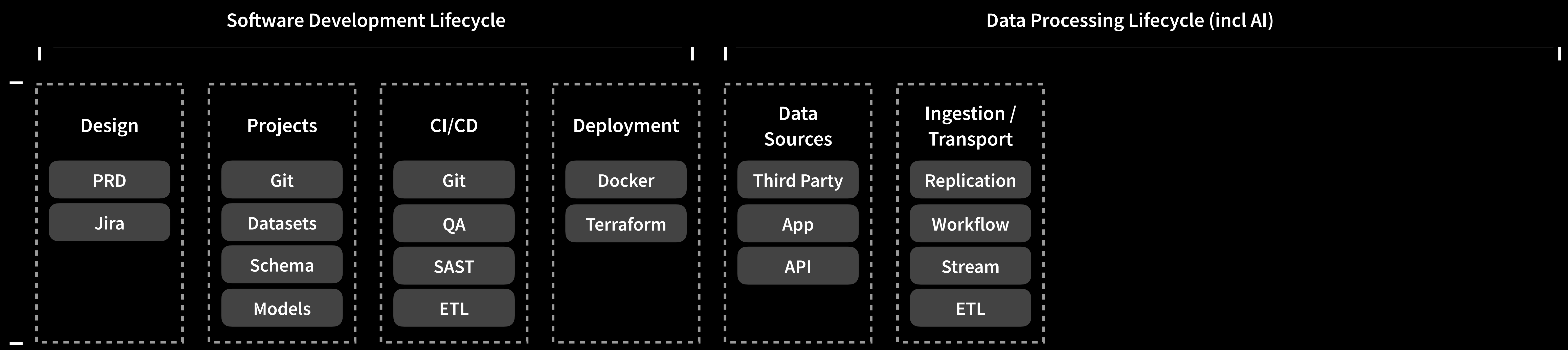
Technical documentation

Record-keeping

Transparency

Human oversight

Accuracy, robustness and security



Software Development Lifecycle				Data Processing Lifecycle (incl AI)	
Design	Projects	CI/CD	Deployment	Data Sources	Ingestion / Transport
PRD	Git	Git	Docker	Third Party	Replication
Jira	Datasets	QA	Terraform	App	Workflow
	Schema	SAST		API	Stream
	Models	ETL			ETL

ethyca

EU AI Act Technical Risk Management

Quality management systems

Conformity assessment

Corrective action

▻ Risk management

Data governance

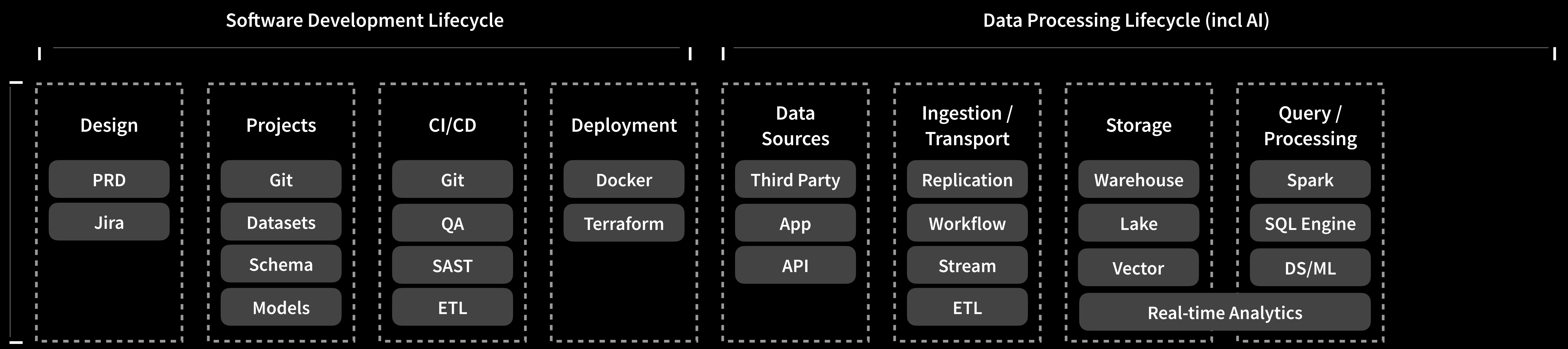
Technical documentation

Record-keeping

Transparency

Human oversight

Accuracy, robustness and security



Software Development Lifecycle

- Design: PRD, Jira
- Projects: Git, Datasets, Schema, Models
- CI/CD: Git, QA, SAST, ETL
- Deployment: Docker, Terraform

Data Processing Lifecycle (incl AI)

- Data Sources: Third Party, App, API
- Ingestion / Transport: Replication, Workflow, Stream, ETL
- Storage: Warehouse, Lake, Vector
- Query / Processing: Spark, SQL Engine, DS/ML
- Storage, Query / Processing: Real-time Analytics

EU AI Act Technical Risk Management

Quality management systems

Conformity assessment

Corrective action

▻ Risk management

Data governance

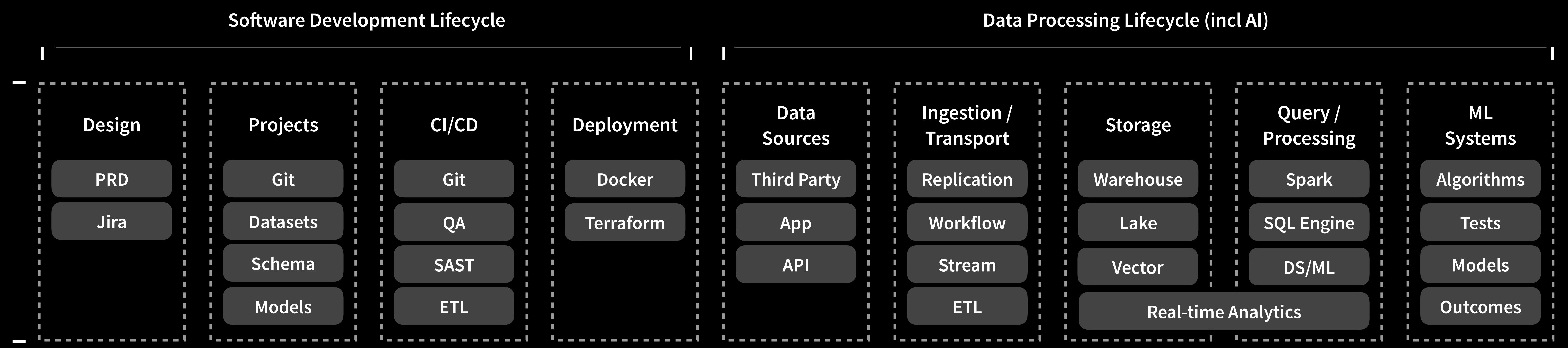
Technical documentation

Record-keeping

Transparency

Human oversight

Accuracy, robustness and security



Software Development Lifecycle				Data Processing Lifecycle (incl AI)				
Design	Projects	CI/CD	Deployment	Data Sources	Ingestion / Transport	Storage	Query / Processing	ML Systems
PRD	Git	Git	Docker	Third Party	Replication	Warehouse	Spark	Algorithms
Jira	Datasets	QA	Terraform	App	Workflow	Lake	SQL Engine	Tests
	Schema	SAST		API	Stream	Vector	DS/ML	Models
	Models	ETL			ETL	Real-time Analytics		Outcomes

EU AI Act Technical Risk Management

Quality management systems

Conformity assessment

Corrective action

▻ Risk management

Data governance

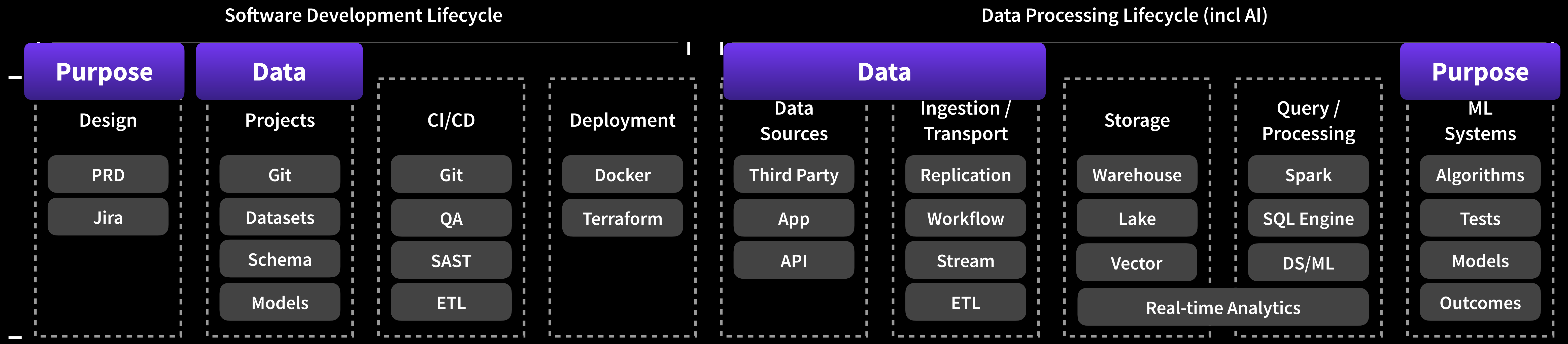
Technical documentation

Record-keeping

Transparency

Human oversight

Accuracy, robustness and security



ethyca

EU AI Act Technical Risk Management

Quality management systems

Conformity assessment

Corrective action

▻ Risk management

Data governance

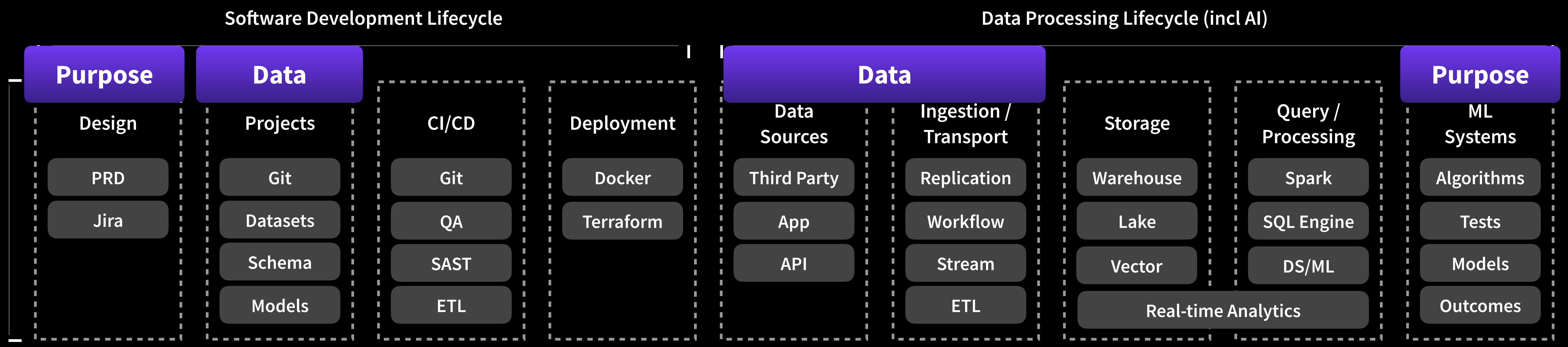
Technical documentation

Record-keeping

Transparency

Human oversight

Accuracy, robustness and security



Software Development Lifecycle				Data Processing Lifecycle (incl AI)				
Purpose	Data			Data				Purpose
Design	Projects	CI/CD	Deployment	Data Sources	Ingestion / Transport	Storage	Query / Processing	ML Systems
PRD	Git	Git	Docker	Third Party	Replication	Warehouse	Spark	Algorithms
Jira	Datasets	QA	Terraform	App	Workflow	Lake	SQL Engine	Tests
	Schema	SAST		API	Stream	Vector	DS/ML	Models
	Models	ETL			ETL	Real-time Analytics		Outcomes

Technical Requirements

- Ontology for purposes, data categories and risks
- Method to inventory AI systems and purposes
- Catalogue of data categories processed

ethyca

EU AI Act Technical Risk Management

Quality management systems

Conformity assessment

Corrective action

▻ **Risk management**

Data governance

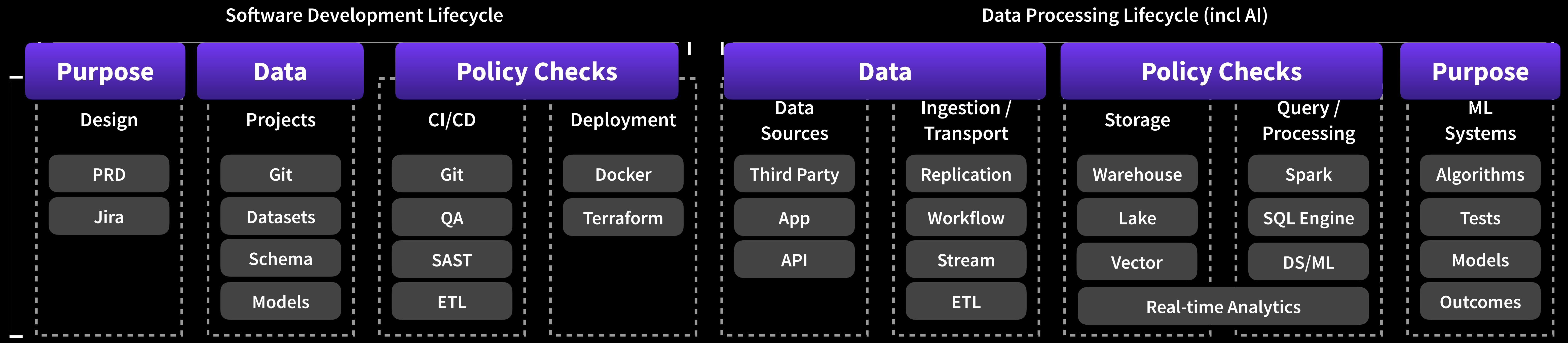
Technical documentation

Record-keeping

Transparency

Human oversight

Accuracy, robustness and security



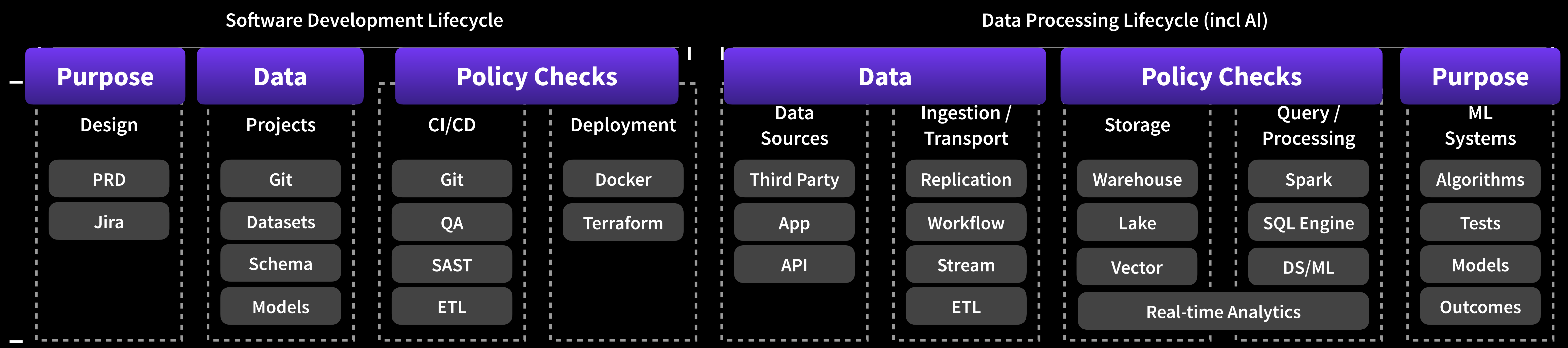
Software Development Lifecycle				Data Processing Lifecycle (incl AI)					
Purpose	Data	Policy Checks		Data		Policy Checks		Purpose
Design	Projects	CI/CD	Deployment	Data Sources	Ingestion / Transport	Storage	Query / Processing	ML Systems
PRD	Git	Git	Docker	Third Party	Replication	Warehouse	Spark	Algorithms
Jira	Datasets	QA	Terraform	App	Workflow	Lake	SQL Engine	Tests
	Schema	SAST		API	Stream	Vector	DS/ML	Models
	Models	ETL			ETL	Real-time Analytics		Outcomes

Technical Requirements

- Ontology for purposes, data categories and risks
- Method to inventory AI systems and purposes
- Catalogue of data categories processed

EU AI Act Technical Risk Management

- Quality management systems
- Conformity assessment
- Corrective action
- ▻ Risk management
- Data governance
- Technical documentation
- Record-keeping
- Transparency
- Human oversight
- Accuracy, robustness and security



Software Development Lifecycle				Data Processing Lifecycle (incl AI)				
Purpose	Data	Policy Checks		Data		Policy Checks		Purpose
Design	Projects	CI/CD	Deployment	Data Sources	Ingestion / Transport	Storage	Query / Processing	ML Systems
PRD	Git	Git	Docker	Third Party	Replication	Warehouse	Spark	Algorithms
Jira	Datasets	QA	Terraform	App	Workflow	Lake	SQL Engine	Tests
	Schema	SAST		API	Stream	Vector	DS/ML	Models
	Models	ETL			ETL	Real-time Analytics		Outcomes

Technical Requirements

- Ontology for purposes, data categories and risks
- Method to inventory AI systems and purposes
- Catalogue of data categories processed
- Analysis during SDLC as part of, or prior to pull requests
- Policy enforcement in production data pipelines

EU AI Act Technical Risk Management

Quality management systems

Conformity assessment

Corrective action

▻ **Risk management**

Data governance

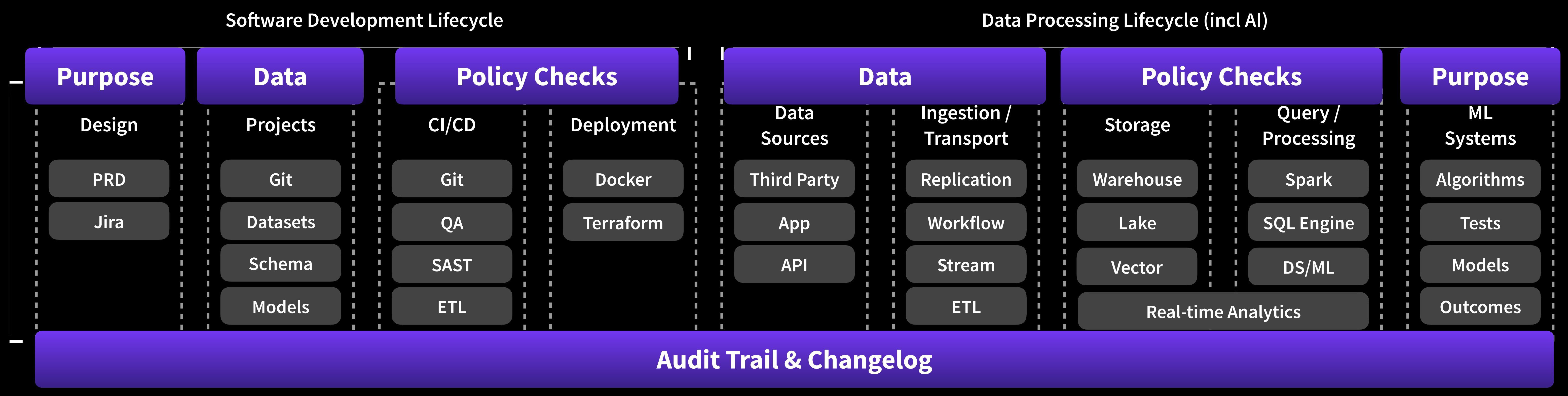
Technical documentation

Record-keeping

Transparency

Human oversight

Accuracy, robustness and security



Software Development Lifecycle

- **Purpose** – Design: PRD, Jira
- **Data** – Projects: Git, Datasets, Schema, Models
- **Policy Checks** – CI/CD: Git, QA, SAST, ETL; Deployment: Docker, Terraform

Data Processing Lifecycle (incl AI)

- **Data** – Data Sources: Third Party, App, API; Ingestion / Transport: Replication, Workflow, Stream, ETL
- **Policy Checks** – Storage: Warehouse, Lake, Vector; Query / Processing: Spark, SQL Engine, DS/ML; Real-time Analytics
- **Purpose** – ML Systems: Algorithms, Tests, Models, Outcomes

Audit Trail & Changelog

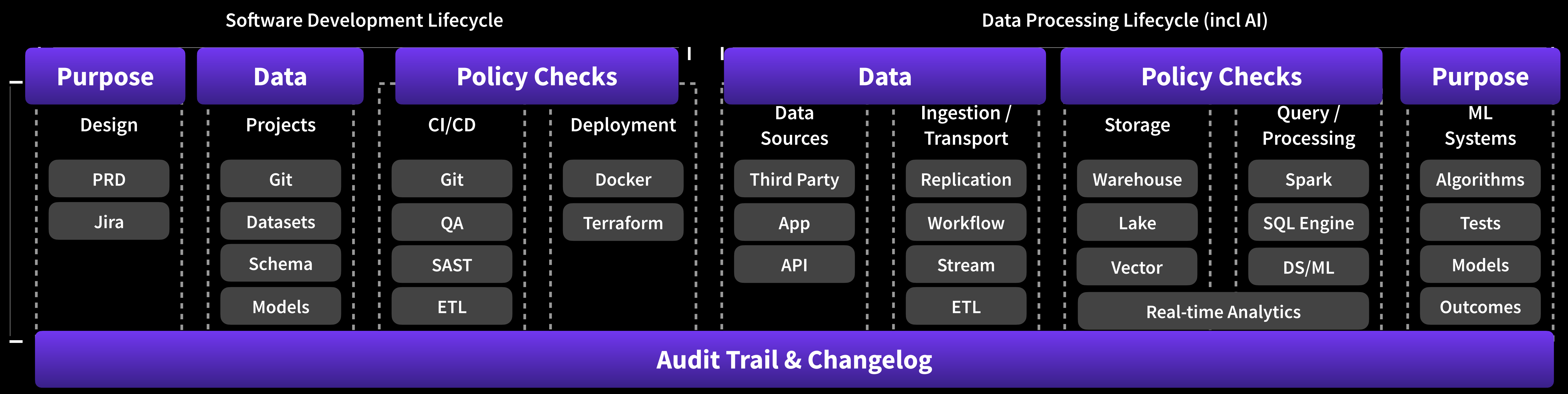
Technical Requirements

- Ontology for purposes, data categories and risks
- Method to inventory AI systems and purposes
- Catalogue of data categories processed
- Analysis during SDLC as part of, or prior to pull requests
- Policy enforcement in production data pipelines

ethyca

EU AI Act Technical Risk Management

- Quality management systems
- Conformity assessment
- Corrective action
- ▻ Risk management
- Data governance
- Technical documentation
- Record-keeping
- Transparency
- Human oversight
- Accuracy, robustness and security



Software Development Lifecycle

Purpose: Design: PRD, Jira

Data: Projects: Git, Datasets, Schema, Models

Policy Checks: CI/CD: Git, QA, SAST, ETL; Deployment: Docker, Terraform

Data Processing Lifecycle (incl AI)

Data: Data Sources: Third Party, App, API; Ingestion / Transport: Replication, Workflow, Stream, ETL

Policy Checks: Storage: Warehouse, Lake, Vector; Query / Processing: Spark, SQL Engine, DS/ML; Real-time Analytics

Purpose: ML Systems: Algorithms, Tests, Models, Outcomes

Audit Trail & Changelog

Technical Requirements

- Ontology for purposes, data categories and risks
- Method to inventory AI systems and purposes
- Catalogue of data categories processed
- Analysis during SDLC as part of, or prior to pull requests
- Policy enforcement in production data pipelines
- Audit trail of risks and changelog of remediation

ethyca

Deep dive
AI Data Governance

EU AI Act Technical Data Governance

Conformity assessment

Corrective action

Risk management

▻ Data governance

Technical documentation

Record-keeping

Transparency

Human oversight

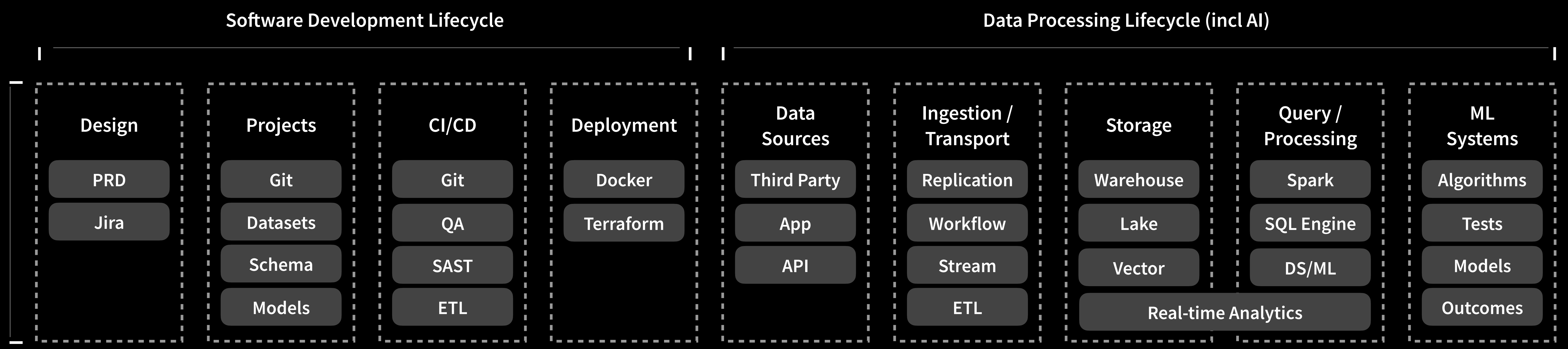
Accuracy, robustness and security

Quality management systems

Manage and enforce AI policies, and govern the use of data in data pipelines and AI systems.

EU AI Act Technical Data Governance

- Conformity assessment
- Corrective action
- Risk management
- ▻ Data governance
- Technical documentation
- Record-keeping
- Transparency
- Human oversight
- Accuracy, robustness and security
- Quality management systems



Software Development Lifecycle				Data Processing Lifecycle (incl AI)				
Design	Projects	CI/CD	Deployment	Data Sources	Ingestion / Transport	Storage	Query / Processing	ML Systems
PRD	Git	Git	Docker	Third Party	Replication	Warehouse	Spark	Algorithms
Jira	Datasets	QA	Terraform	App	Workflow	Lake	SQL Engine	Tests
	Schema	SAST		API	Stream	Vector	DS/ML	Models
	Models	ETL			ETL	Real-time Analytics		Outcomes

EU AI Act Technical Data Governance

Conformity assessment

Corrective action

Risk management

▻ Data governance

Technical documentation

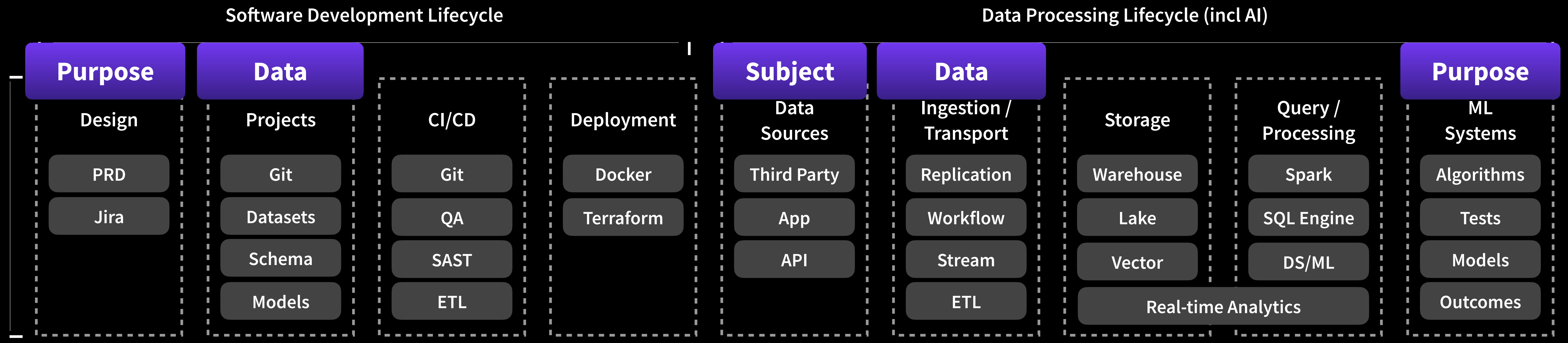
Record-keeping

Transparency

Human oversight

Accuracy, robustness and security

Quality management systems



Software Development Lifecycle				Data Processing Lifecycle (incl AI)				
Purpose	Data			Subject	Data			Purpose
Design	Projects	CI/CD	Deployment	Data Sources	Ingestion / Transport	Storage	Query / Processing	ML Systems
PRD	Git	Git	Docker	Third Party	Replication	Warehouse	Spark	Algorithms
Jira	Datasets	QA	Terraform	App	Workflow	Lake	SQL Engine	Tests
	Schema	SAST		API	Stream	Vector	DS/ML	Models
	Models	ETL			ETL	Real-time Analytics		Outcomes

EU AI Act Technical Data Governance

Conformity assessment

Corrective action

Risk management

▻ Data governance

Technical documentation

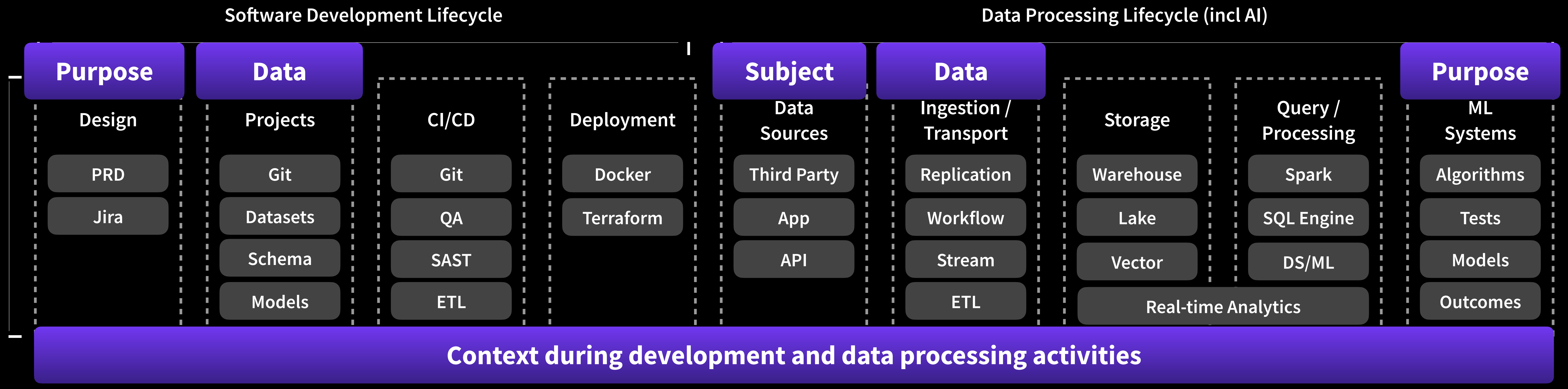
Record-keeping

Transparency

Human oversight

Accuracy, robustness and security

Quality management systems



Technical Requirements

- Aggregate system context (purpose, data, subject, etc.)

ethyca

EU AI Act Technical Data Governance

Conformity assessment

Corrective action

Risk management

▻ Data governance

Technical documentation

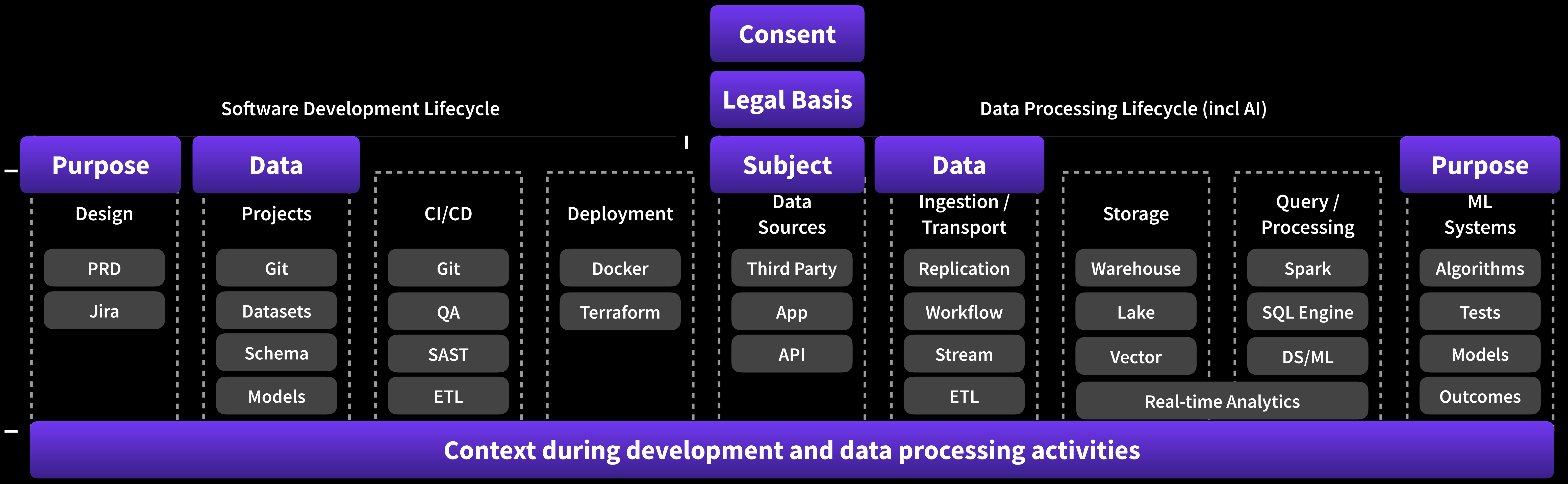
Record-keeping

Transparency

Human oversight

Accuracy, robustness and security

Quality management systems



Technical Requirements

- Aggregate system context (purpose, data, subject, etc.)

EU AI Act Technical Data Governance

Conformity assessment

Corrective action

Risk management

▻ Data governance

Technical documentation

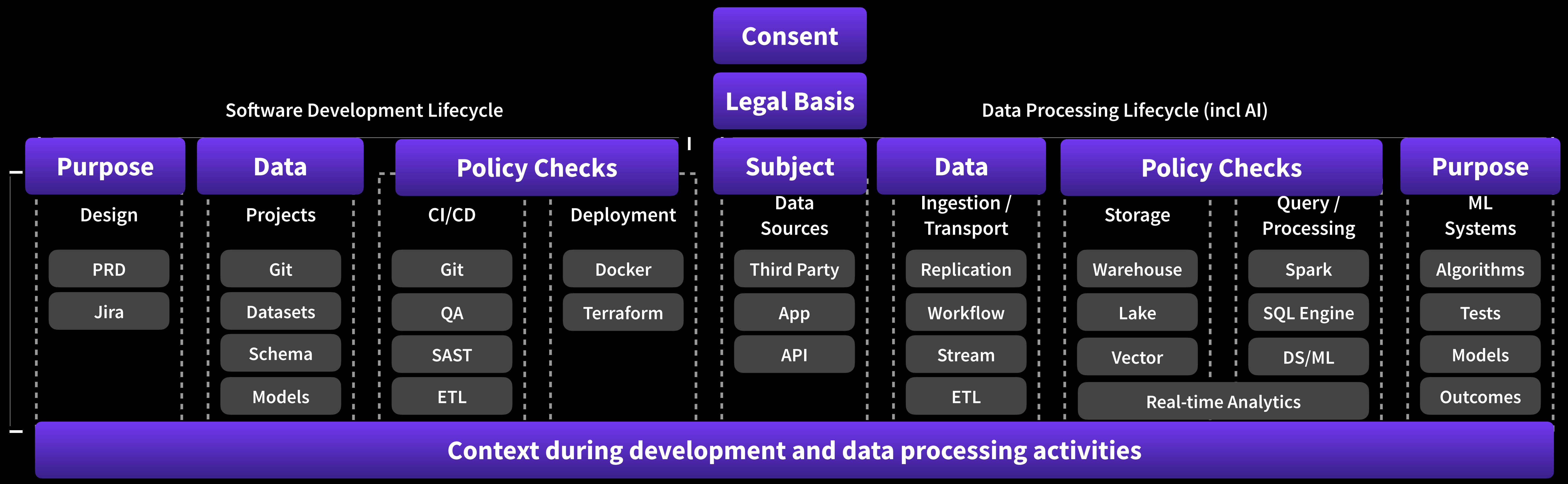
Record-keeping

Transparency

Human oversight

Accuracy, robustness and security

Quality management systems



Consent

Legal Basis

Software Development Lifecycle

Purpose
- Design: PRD, Jira

Data
- Projects: Git, Datasets, Schema, Models

Policy Checks
- CI/CD: Git, QA, SAST, ETL
- Deployment: Docker, Terraform

Data Processing Lifecycle (incl AI)

Subject
- Data Sources: Third Party, App, API

Data
- Ingestion / Transport: Replication, Workflow, Stream, ETL

Policy Checks
- Storage: Warehouse, Lake, Vector
- Query / Processing: Spark, SQL Engine, DS/ML
- Real-time Analytics

Purpose
- ML Systems: Algorithms, Tests, Models, Outcomes

Context during development and data processing activities

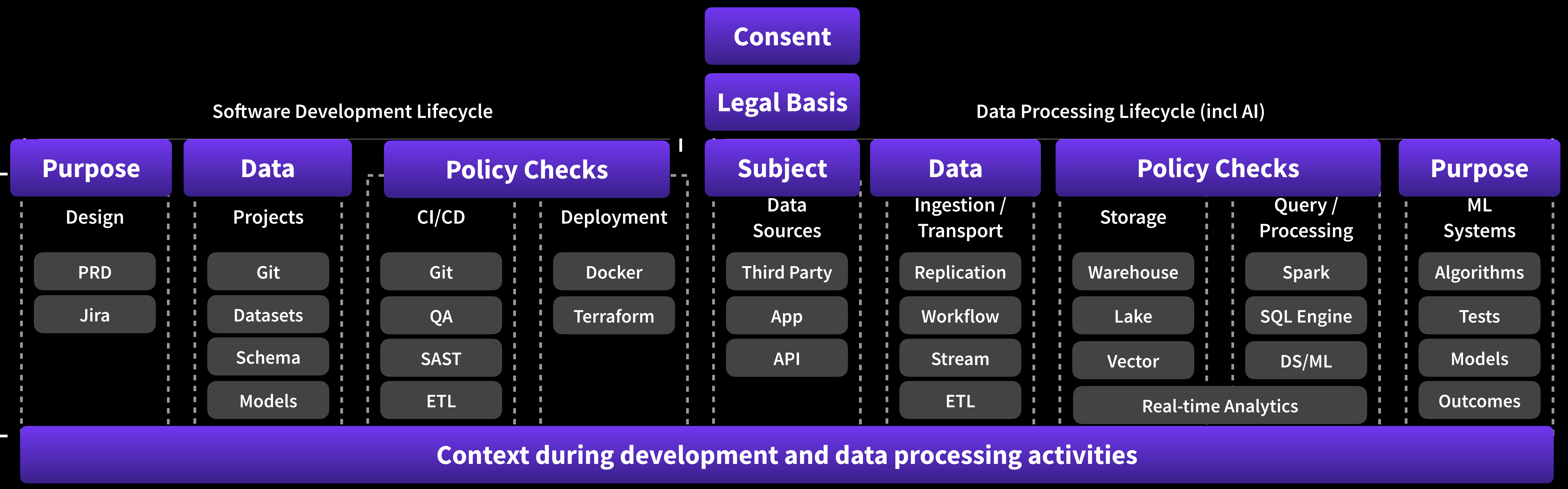
Technical Requirements

- Aggregate system context (purpose, data, subject, etc.)

ethyca

EU AI Act Technical Data Governance

- Conformity assessment
- Corrective action
- Risk management
- ▻ Data governance
- Technical documentation
- Record-keeping
- Transparency
- Human oversight
- Accuracy, robustness and security
- Quality management systems



Consent

Legal Basis

Software Development Lifecycle

- Purpose — Design: PRD, Jira
- Data — Projects: Git, Datasets, Schema, Models
- Policy Checks — CI/CD: Git, QA, SAST, ETL; Deployment: Docker, Terraform

Data Processing Lifecycle (incl AI)

- Subject — Data Sources: Third Party, App, API
- Data — Ingestion / Transport: Replication, Workflow, Stream, ETL
- Policy Checks — Storage: Warehouse, Lake, Vector; Query / Processing: Spark, SQL Engine, DS/ML; Real-time Analytics
- Purpose — ML Systems: Algorithms, Tests, Models, Outcomes

Context during development and data processing activities

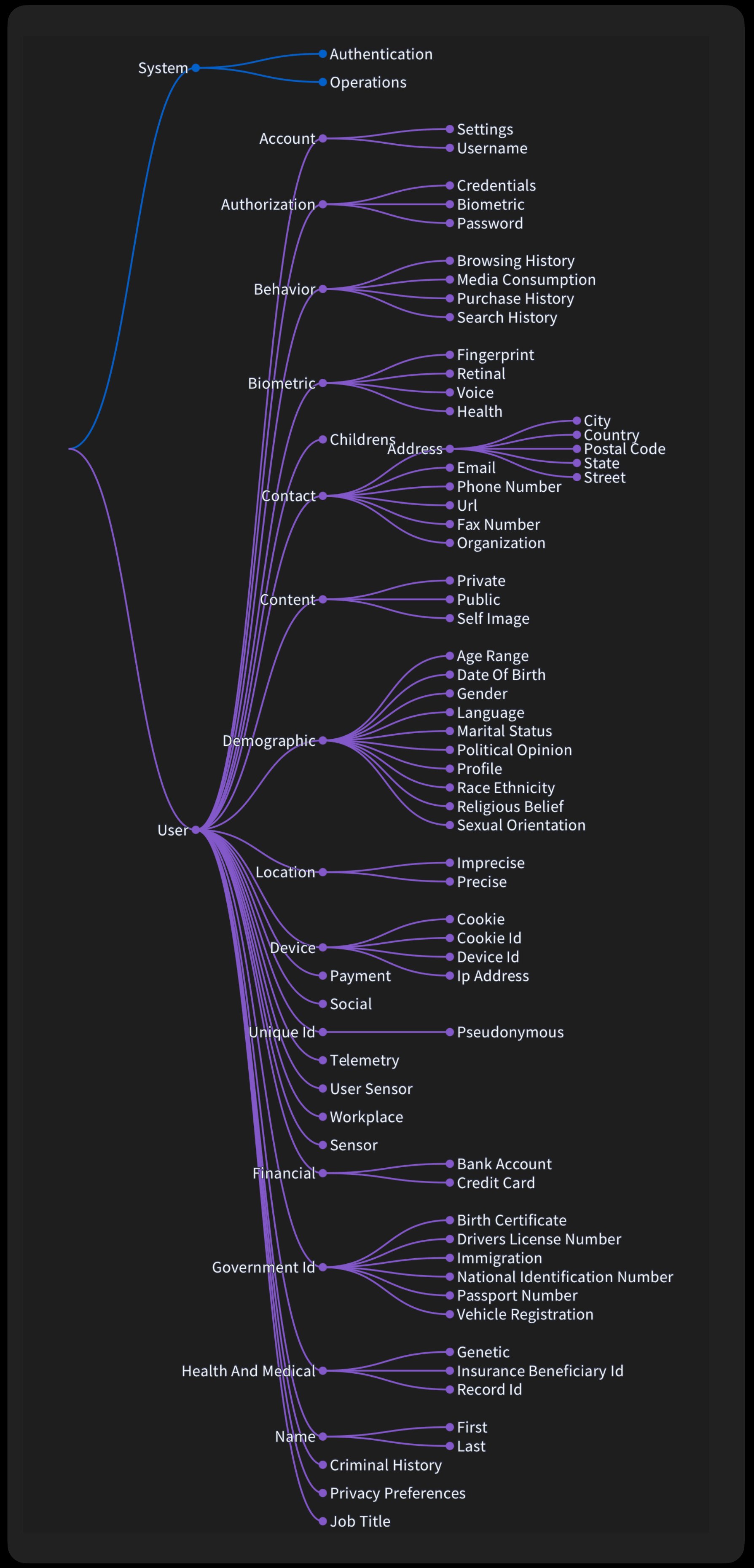
Technical Requirements

- Aggregate system context (purpose, data, subject, etc.)
- Enforce just-in-time policies in design and development
- Enforce policies at point of data processing

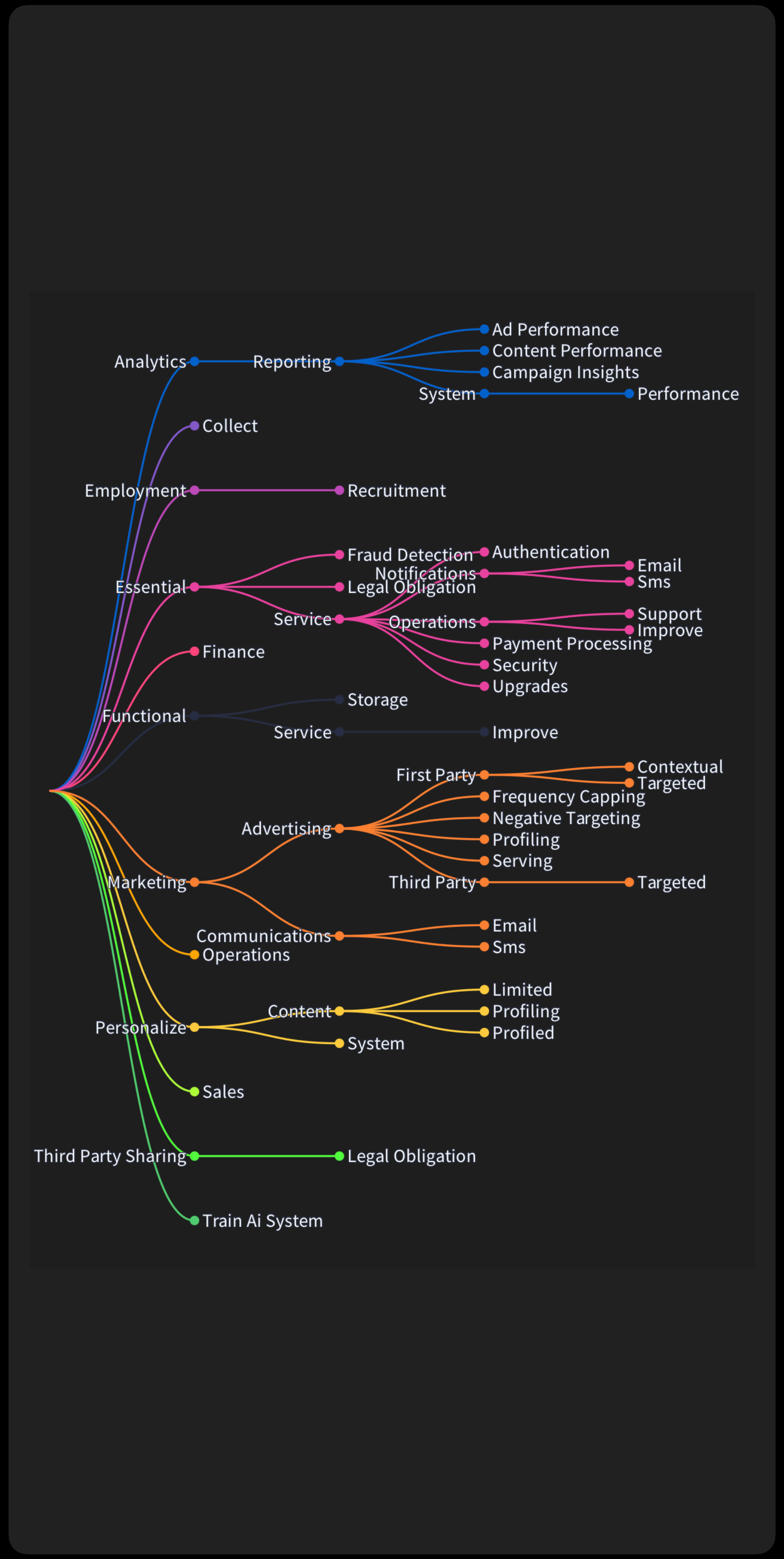
ethyca

Embedded engineering solution to AI governance

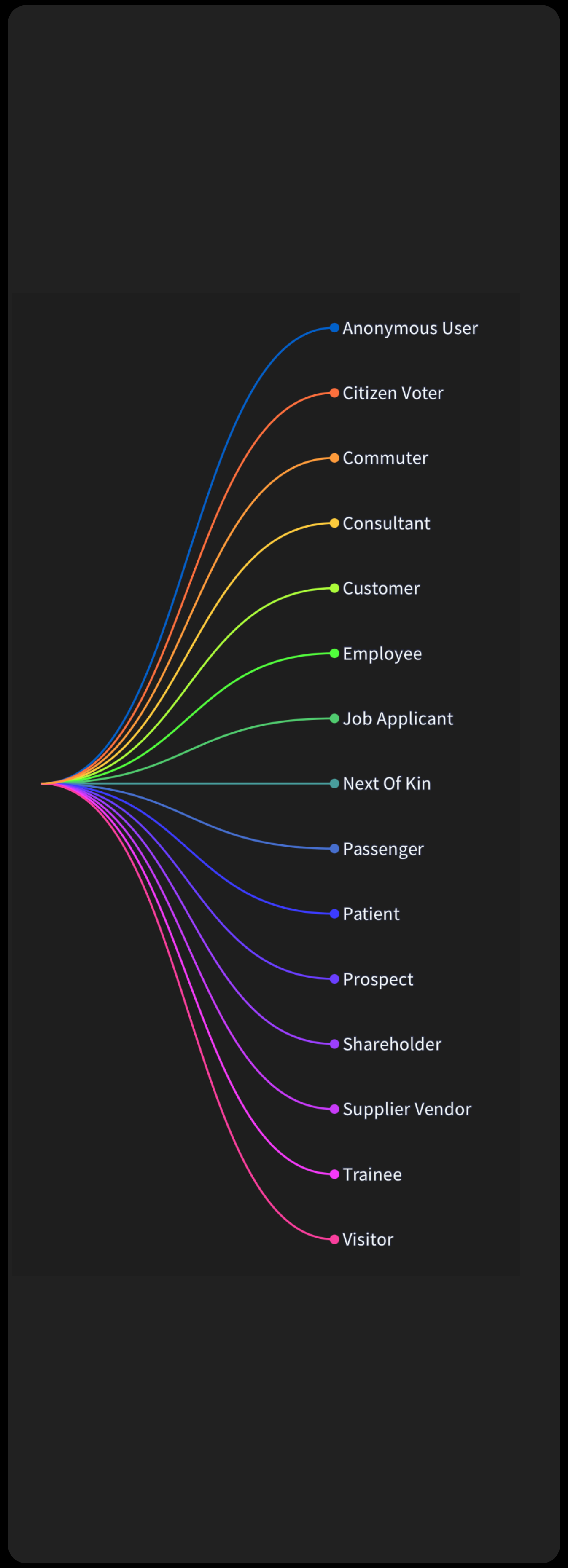
Fides Ontology for Risk, Policy & Governance



Data Categories



Purposes, Risks, Harms



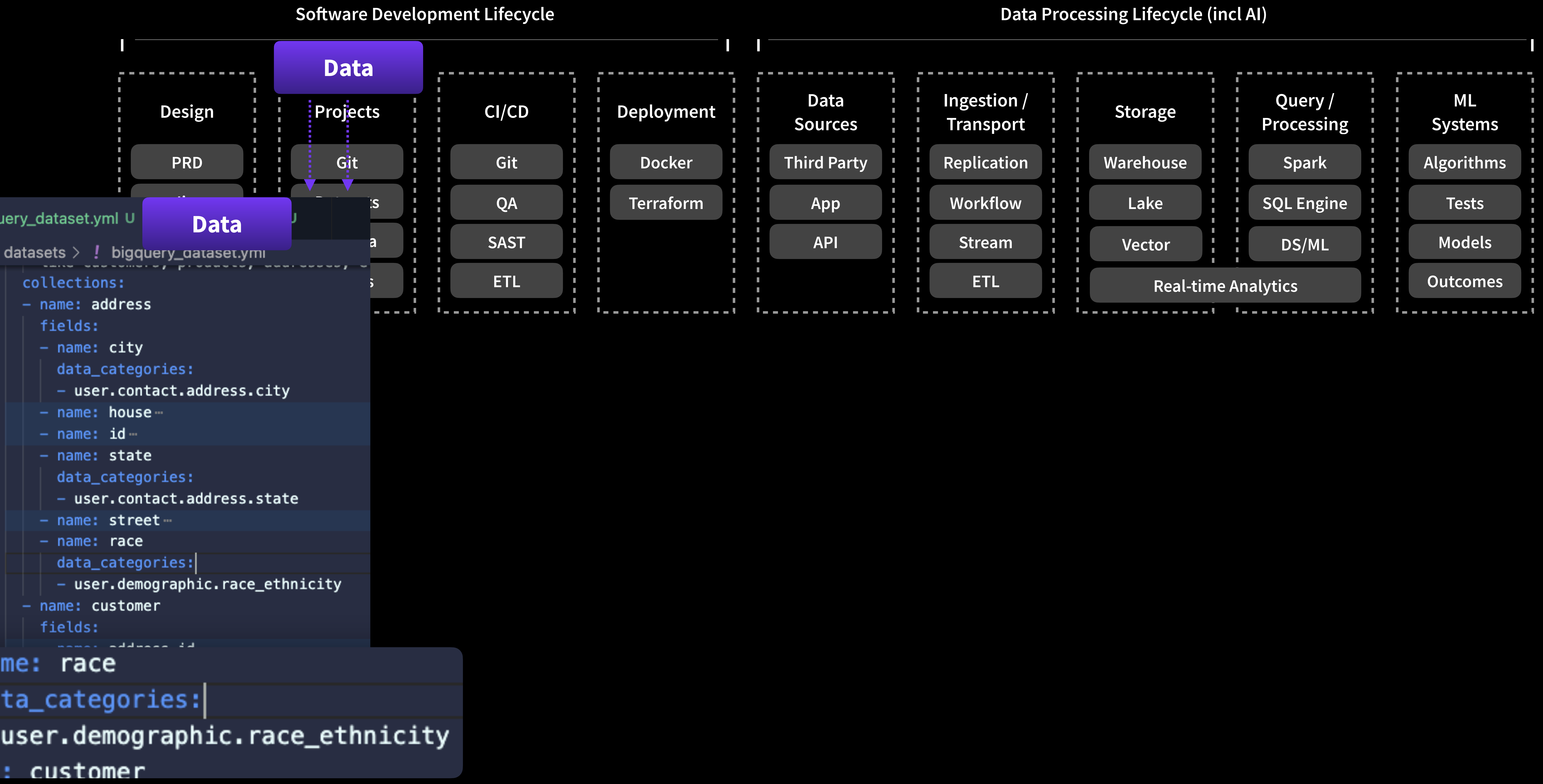
Data Subject

Fides Semantic policies

We do not permit the use of data_category(s) that belong to data_subject(s) for the purpose of data_use(s) which may result in harm(s) .

We do not permit the use of user.demographic.race , user.location.precise belonging to customers for the purpose of train_ai_system for personalized.profiling.racial .

Example: identifying risks and enforcing policies

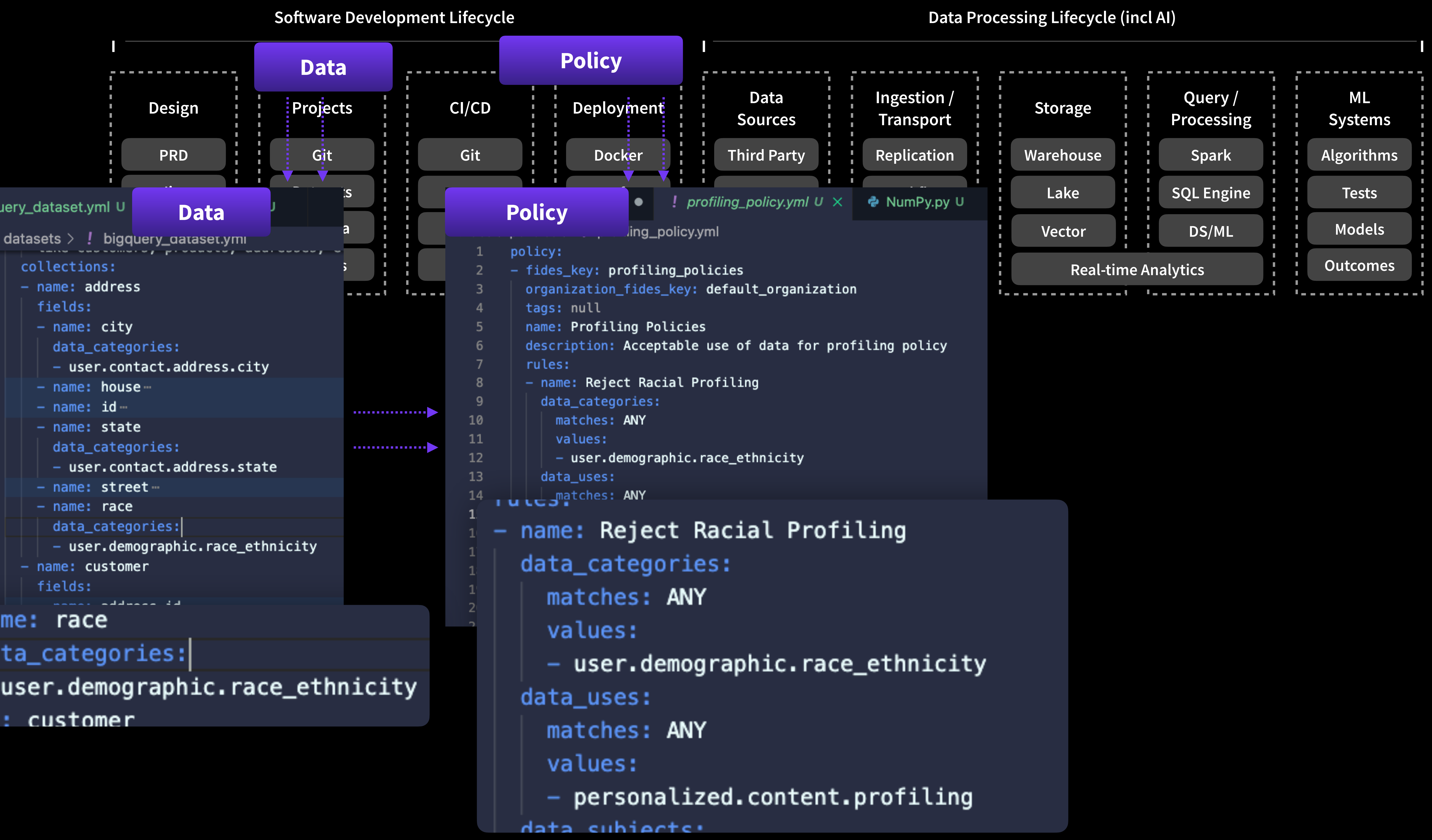


```
collections:
- name: address
  fields:
  - name: city
    data_categories:
    - user.contact.address.city
  - name: house ⋯
  - name: id ⋯
  - name: state
    data_categories:
    - user.contact.address.state
  - name: street ⋯
  - name: race
    data_categories:
    - user.demographic.race_ethnicity
- name: customer
  fields:
```

```
me:  race
ta_categories:
user.demographic.race_ethnicity
: customer
```

ethyca

Example: identifying risks and enforcing policies



```yaml
collections:
- name: address
  fields:
  - name: city
    data_categories:
    - user.contact.address.city
  - name: house⋯
  - name: id⋯
  - name: state
    data_categories:
    - user.contact.address.state
  - name: street⋯
  - name: race
    data_categories:
    - user.demographic.race_ethnicity
- name: customer
  fields:
```

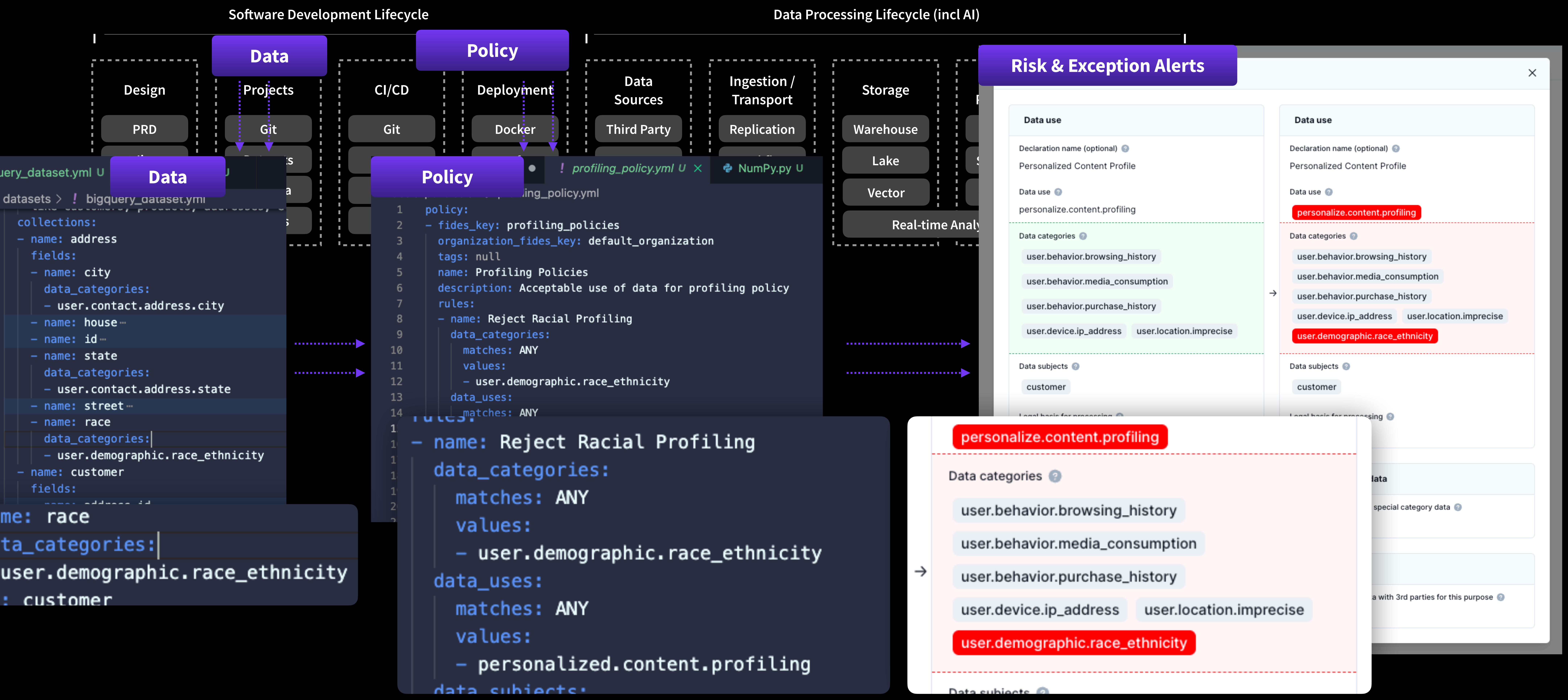
```yaml
me: race
ta_categories:
user.demographic.race_ethnicity
: customer
```

```yaml
policy:
- fides_key: profiling_policies
  organization_fides_key: default_organization
  tags: null
  name: Profiling Policies
  description: Acceptable use of data for profiling policy
  rules:
  - name: Reject Racial Profiling
    data_categories:
      matches: ANY
      values:
      - user.demographic.race_ethnicity
    data_uses:
      matches: ANY
```

```yaml
rules:
- name: Reject Racial Profiling
  data_categories:
    matches: ANY
    values:
    - user.demographic.race_ethnicity
  data_uses:
    matches: ANY
    values:
    - personalized.content.profiling
  data_subjects:
```

ethyca

Example: identifying risks and enforcing policies



ery_dataset.yml U

datasets > ! bigquery_dataset.yml

```
collections:
- name: address
  fields:
  - name: city
    data_categories:
    - user.contact.address.city
  - name: house ⋯
  - name: id ⋯
  - name: state
    data_categories:
    - user.contact.address.state
  - name: street ⋯
  - name: race
    data_categories:
    - user.demographic.race_ethnicity
- name: customer
  fields:
```

```
me:  race
ta_categories:
user.demographic.race_ethnicity
: customer
```

! profiling_policy.yml U ×   NumPy.py U

ing_policy.yml

```
policy:
- fides_key: profiling_policies
  organization_fides_key: default_organization
  tags: null
  name: Profiling Policies
  description: Acceptable use of data for profiling policy
  rules:
  - name: Reject Racial Profiling
    data_categories:
      matches: ANY
      values:
      - user.demographic.race_ethnicity
    data_uses:
      matches: ANY
```

```
rules:
- name: Reject Racial Profiling
  data_categories:
    matches: ANY
    values:
    - user.demographic.race_ethnicity
  data_uses:
    matches: ANY
    values:
    - personalized.content.profiling
  data_subjects:
```

Data use

Declaration name (optional)
Personalized Content Profile

Data use
personalize.content.profiling

Data categories
user.behavior.browsing_history
user.behavior.media_consumption
user.behavior.purchase_history
user.device.ip_address user.location.imprecise

Data subjects
customer

Legal basis for processing

→

Data use

Declaration name (optional)
Personalized Content Profile

Data use
personalize.content.profiling

Data categories
user.behavior.browsing_history
user.behavior.media_consumption
user.behavior.purchase_history
user.device.ip_address user.location.imprecise
user.demographic.race_ethnicity

Data subjects
customer

Legal basis for processing

data

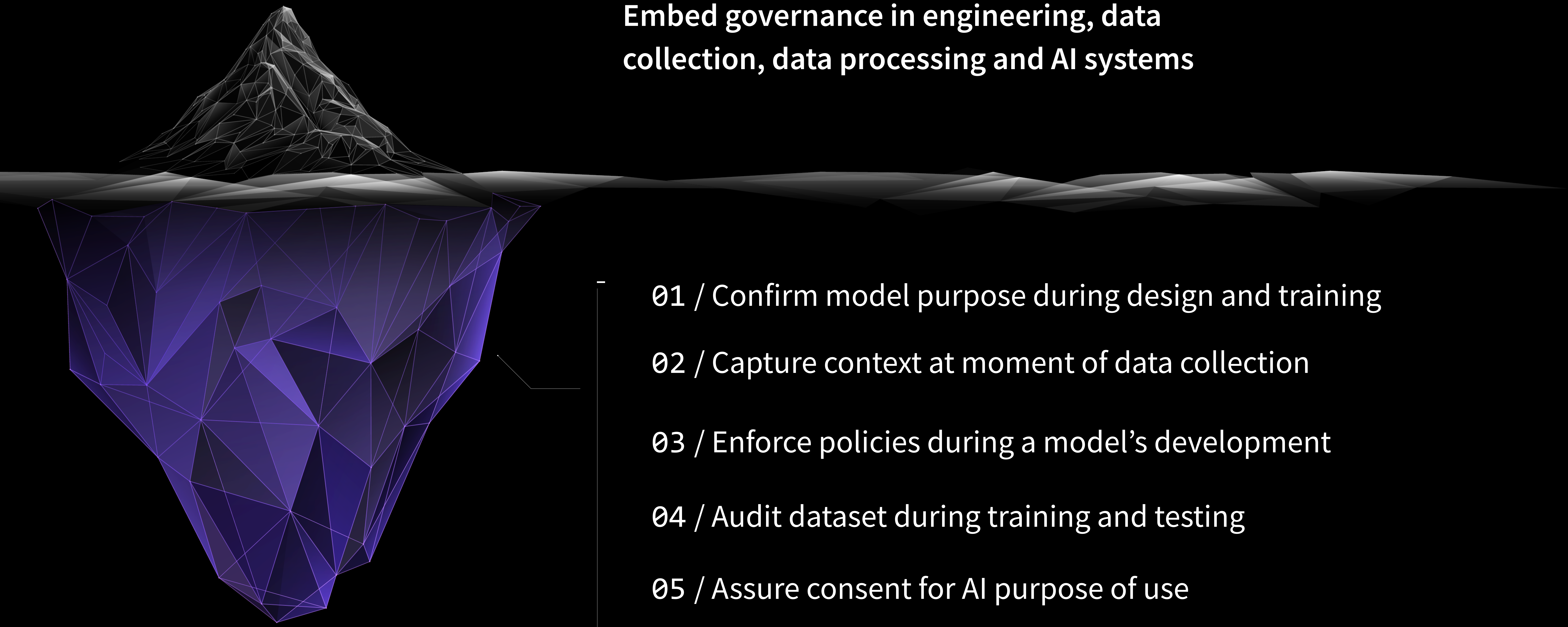
special category data

a with 3rd parties for this purpose

personalize.content.profiling

Data categories
user.behavior.browsing_history
user.behavior.media_consumption
user.behavior.purchase_history
user.device.ip_address user.location.imprecise
user.demographic.race_ethnicity

Data subjects



Embed governance in engineering, data collection, data processing and AI systems

01 / Confirm model purpose during design and training

02 / Capture context at moment of data collection

03 / Enforce policies during a model’s development

04 / Audit dataset during training and testing

05 / Assure consent for AI purpose of use

06 / Generate continuous audit trail of data & AI processes

EU AI Act Takeaways

01 / EUAI Act defines low, medium, high and unacceptable risk framework.

02 / Where models are high-risk there are 10 requirements to operationalize.

03 / Two key items; AI risk management and data governance will require deeper instrumentation of data pipelines and model purposes.

04 / Robust governance will require an ontology jointly defined by legal, data and engineering teams for categories, purposes, risks and harms.

ethyca

European AI Act unpacked for Governance, Data & Engineering

fid.es/strategist

fid.es/docs