Building Infrastructure with Privacy in mind

Natalia Grybovska

Who am I

Natalia Grybovska

Software Engineer
3 years in Big Tech Privacy


protection
pseudonymization
policy
regulation
controls
breach
data
lineage
legislation
purpose
gdpr
retention
compliance
privacy
security
safeguards
minimization
mitigation
ethics
anonymization
surveillance
consent
deletion
evidence
encryption
ccpa
remediation

Objective

A high level overview of the privacy domain with respect to the infrastructure design.

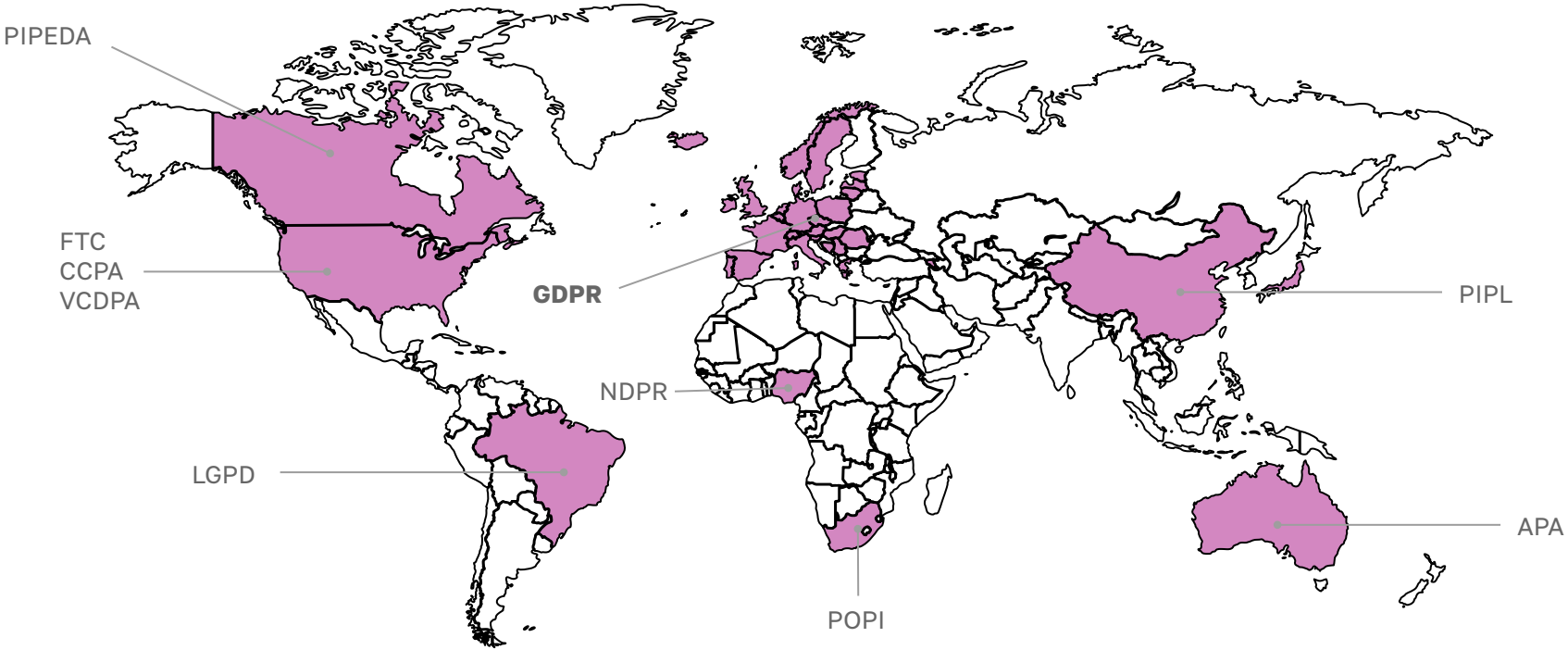
Why Privacy?

Ethics

Building
User Trust

Regulatory
compliance

Regulations



What is Privacy

Privacy > Security

Principles

Data Protection

personal data is protected against unauthorized processing, loss or damage

Transparency

users are informed about the data collection and processing activities

Control

users can access, rectify, erase or restrict their personal data

Deletion

(The right to be forgotten) users have a simple means to delete data related to them

Principles

Data Minimisation

Only the necessary data should be collected and processed

Purpose limitation

Data cannot be used for anything other than the original purpose

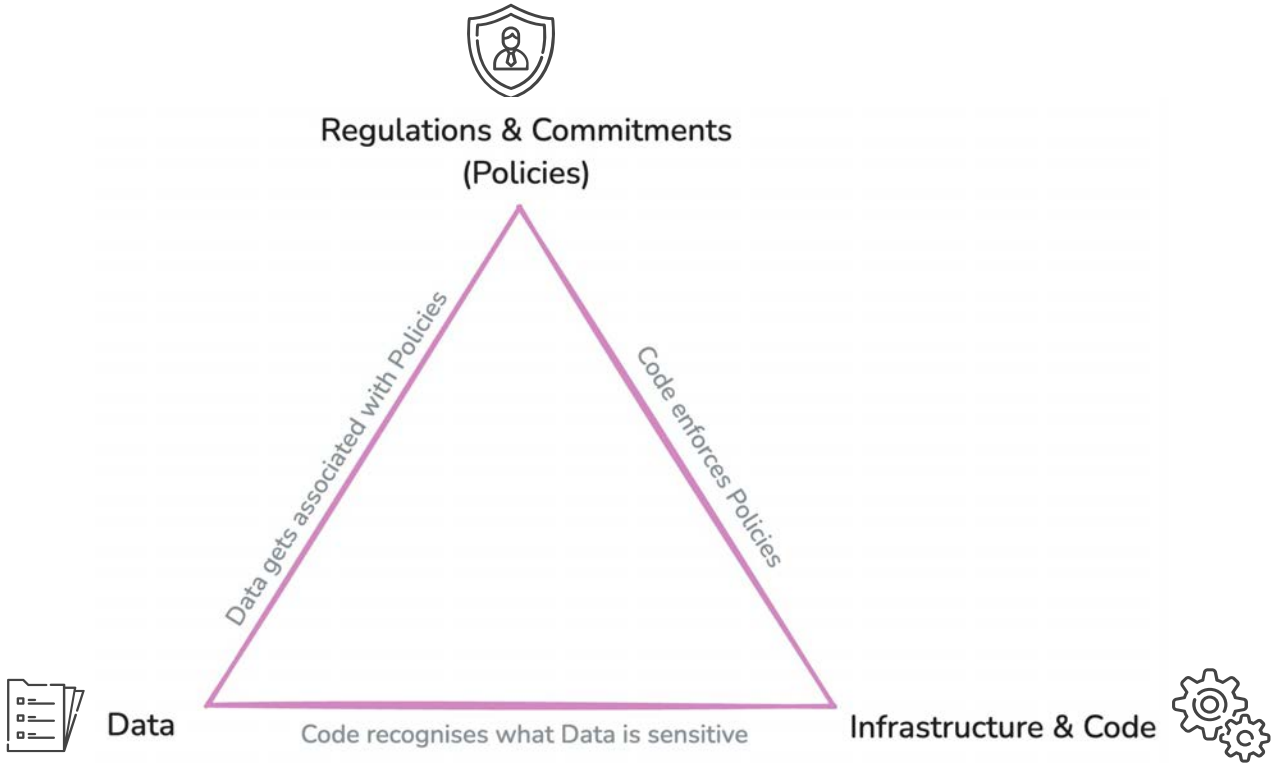
Retention

Data is stored only for as long as necessary and is disposed when no longer required

Accountability

organizations must be able to demonstrate compliance

Privacy And Infrastructure


Regulations & Commitments
(Policies)
Data gets associated with Policies
Code enforces Policies
Data
Code recognises what Data is sensitive
Infrastructure & Code

Regulations & Commitments

Translated into Policies consisting of

1. Scope (where does this policy apply)
2. Enforcement logic
3. Associated with Data

Examples:

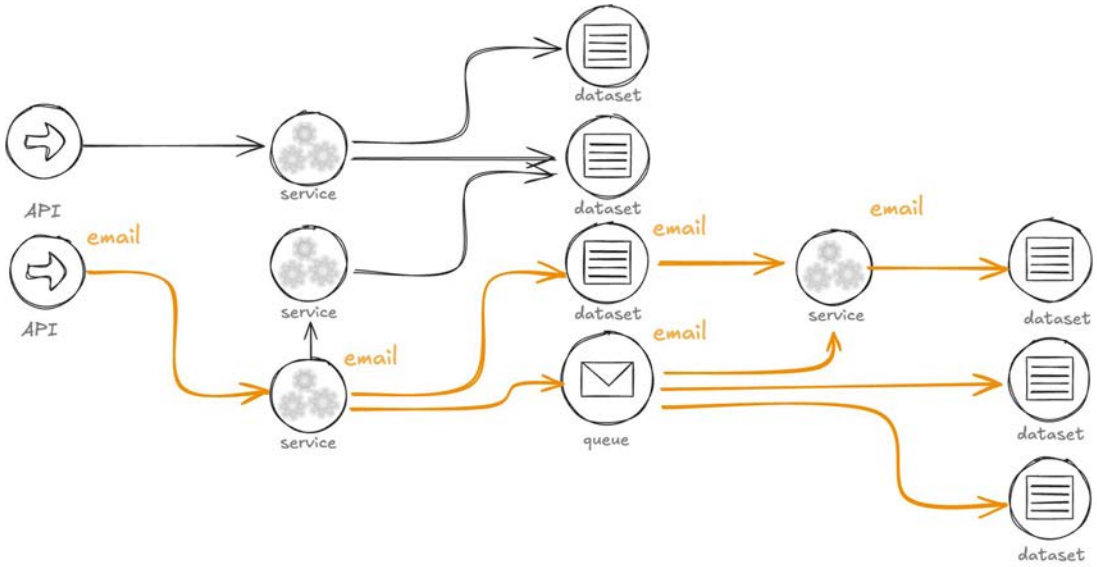
- Consent Policy: *Email shouldn't be used for marketing without consent in the EU*
- Retention Policy: *Bank Statements shouldn't be retained for longer than 7 years in the US*

Data

Data Understanding

1. Defining and registering sensitive data
2. Annotating data (API, DTOs, Data Sink schemas etc)
3. Building Data Lineage

Data Lineage



Infrastructure & Code

Integrates a policy layer

1. Code associated sensitive data with a set of policies
2. Code propagates policy context
3. Code enforces policies where applicable

Examples:

- Code respects the Consent Policy with regards to Email
- An automated process in place to ensure that *Bank Statement* data is deleted after retention period

Privacy Practises

Prevention practises

Access Controls

Ensures data is protected from unauthorised access

Encryption

Protected data in case of unauthorised access

Anonymisation

Removing personal information from data before sharing with third-party companies or analytics layer

Data Coarsening

Reducing the granularity of data making it more challenging to identify individuals

Organisational measures

Privacy Policies

Establishing clear policies that outline data handling practises

Employee Training

Ensuring employees are aware of privacy regulations and internal privacy policies

Privacy Reviews

Establishing review processes on feature releases.

Risk Assessments and Compliance Audits

Conducting regular risk assessments and audits to assess compliance, potential privacy risks and vulnerabilities

Continuous compliance

Automated Breach Detection

Implementing continuous policy compliance verification processes.

Incident Response Process

Having a well-defined process for addressing privacy incidents.

Privacy Investments

Small company

1. Context Propagation
2. Distributed tracing
3. Consent implementation
4. Encryption
5. Access Controls

Growing company

1. Established Privacy Policies
2. Employee Training
3. Data Understanding
4. Data Annotation
5. Policy Propagation
6. Policy Enforcement implementation

Bigger company

1. Data Lineage
2. Continuous Compliance
   a. Automated Breach Detection
   b. Evidence generation
3. Risk Assessments
4. Compliance Audits

Conclusions

- Invest early
- Understand your data
- Establish clear policies

Thank you!


We have updated our GLOBAL
PRIVACY TERMS. Your trust is
important to us. As part of our
ongoing commitment to
transparency, and in preparation