



X Marks the Spot

Using Privacy Framework
Regulatory Crosswalks to Integrate
Compliance and Risk
Management

December 1, 2021

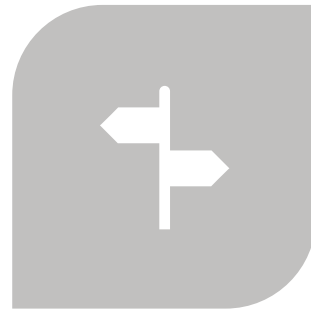
CCPA/CPRA/VCDPA Crosswalk

Jeewon Kim Serrato
BakerHostetler

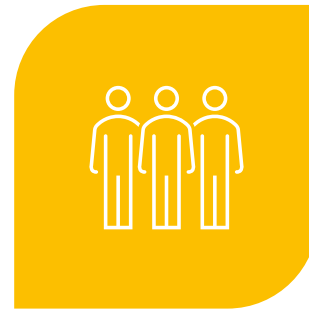
Key US Privacy Laws



CA. CONSUMER PRIVACY
ACT (CCPA) 2020



CA. PRIVACY RIGHTS ACT
(CPRA)
2023



VA. CONSUMER DATA
PROTECTION ACT (VCDPA)
2023



CO. PRIVACY ACT (COPA)
2023

How does the NIST Privacy Framework Help?

	CCPA	CPRA	VCDPA	COPA	GDPR
Status	01/20	01/23	01/23	07/23	5/18
Notice Requirement	✗	✗	✗	✗	✗
Right to Access	✗	✗	✗	✗	✗
Right to Delete	✗	✗	✗	✗	✗
Right to Correct		✗	✗	✗	✗
Right to Opt-Out of Sales	✗	✗	✗	✗	✗
Consent / Opt-in	✗	✗	✗	✗	✗
"Sensitive Data" Req.		✗	✗	✗	✗
Security Req.	✗	✗	✗	✗	✗
Private Right Of Action	✗	✗			✗
DPA Requirement		✗	✗	✗	✗
Enforcement (Fines)	✗	✗	✗	✗	✗
Cure	✗		✗	✗	

How to develop a governance structure

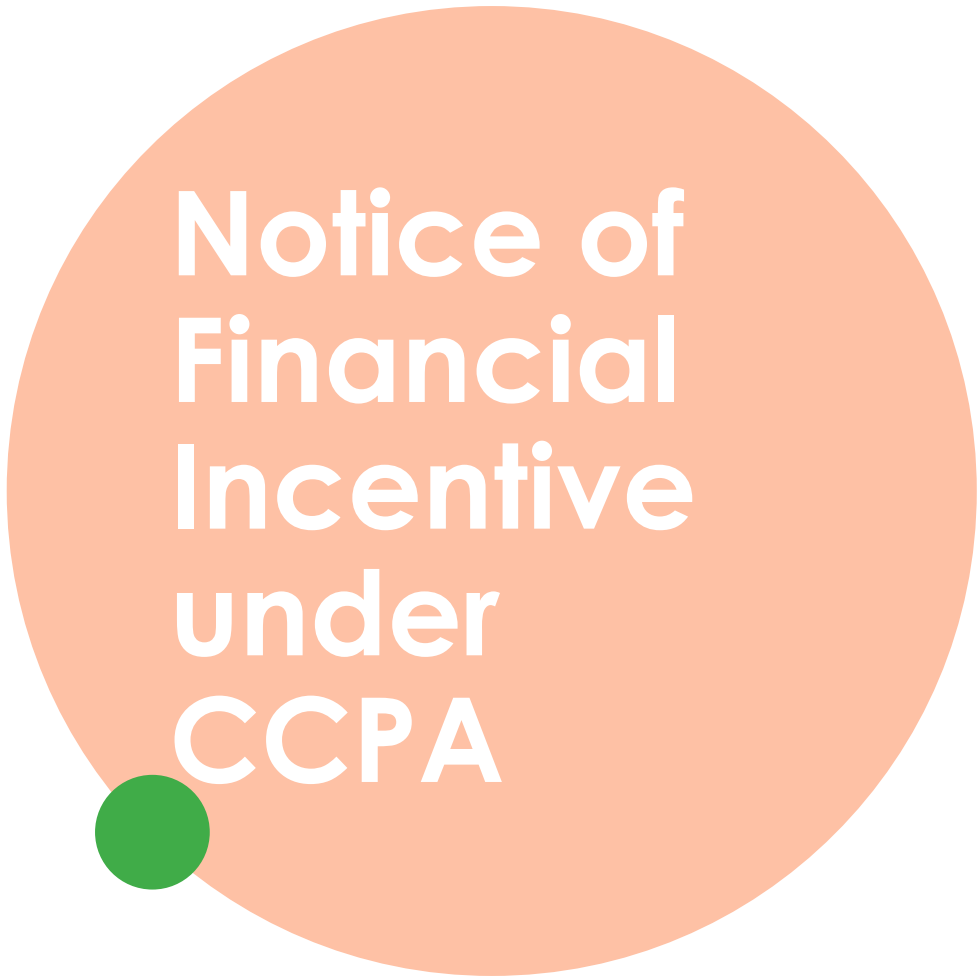
- GOVERN-P (GV-P): Develop and implement the organizational **governance** structure to enable an **ongoing** understanding of the organization's risk management **priorities** that are informed by privacy risk.





How to address legal risks

- GV.PO-P5: **Legal, regulatory, and contractual** requirements regarding privacy are understood and managed.



Notice of Financial Incentive under CCPA

1798.125(b)(1):


- A business may offer ***financial incentives***, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information.
- A business may also offer a ***different price, rate, level, or quality of goods or services*** to the consumer if that price or difference is directly related to the ***value*** provided to the business by the consumer's data.

Profiling under VCDPA

- The VCDPA explicitly forbids the processing of personal data in violation of state and federal anti-discrimination laws and specifically allows consumers to **opt-out** of data processing that involves profiling.
- Controllers must also undertake “**data protection assessments**” that judge the benefits of data processing along with risks to the consumer.
- Controllers must assess the processing of personal data used for profiling when there is a “**reasonably foreseeable risk**” that such profiling will lead to discriminatory impact; economic, reputational or actual harm; and invasions of privacy.



Consent under COPA

- The CoPA requires companies to obtain consent before processing “**sensitive data**,” which includes information “revealing”:
 - Racial or ethnic origin.
 - Religious beliefs.
 - A mental or physical health condition or diagnosis.
 - Sex life or sexual orientation.
 - Citizenship or citizenship status.
 - Genetic data.
 - Biometric data.
 - Personal data regarding a known child.
 - When analyzing whether they process sensitive data, controllers should evaluate **whether the data they process reveals any sensitive data**, even if no sensitive data will be collected directly.
 - Under CoPA, companies will have to obtain **express, affirmative consent** to process personal data if that data involves or reveals sensitive data.
- 

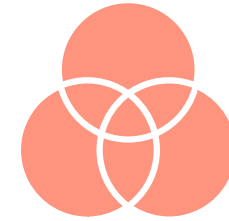
How Do You Make the Framework Work for You?



Inventory (ID.IM-P1):
Systems/products/services that process data are inventoried.



Data Mapping (ID.IM-P8):
Data processing is mapped.



Risk Prioritization (ID.RA-P4):
Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.

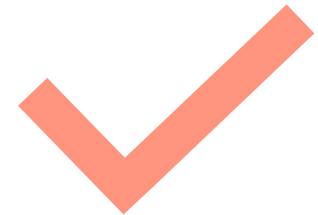
What does the Privacy Framework Not Do?



Create workflows for each legal regime



Operationalize legal requirements



Test and audit existing controls for effectiveness

Building a Future-Proof Privacy Program

Understand

Understand your data. Perform data mapping.

Communicate

Draft appropriate privacy policies and other disclosures regarding data use.

Govern

Ensure internal controls support public-facing disclosures.

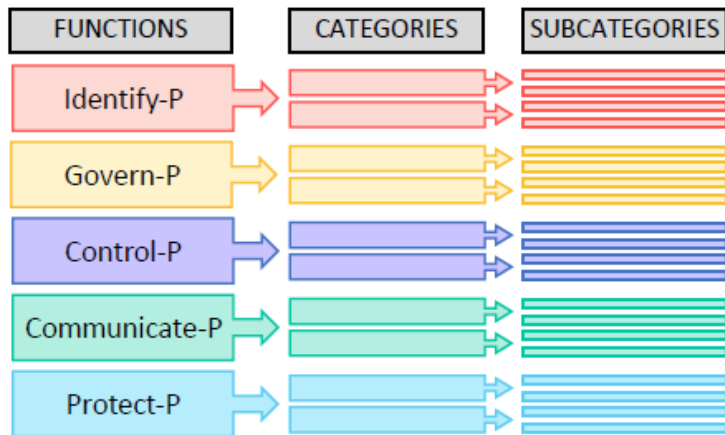
GPDR Crosswalk

R. Jason Cronk

Enterprivacy Consulting Group

GDPR Crosswalk

NIST Privacy Framework CORE



EU General Data Protection Regulation

Chapter II – Principles

Chapter III – Rights of the Data Subjects

- Section 1 Transparency and Modalities
- Section 2 Information and Access to Information
- Section 3 Rectification and Erasure
- Section 4 Right to object to automated decision making
- Section 5 Restrictions

Chapter IV – Controllers and Processors

- Section 1 General Obligations
- Section 2 Security of Personal Data
- Section 3 Data Protection Impact Assessments
- Section 4 Data Protection Officers
- Section 5 Certification and Codes of Conduct

Chapter V – Data Transfers

GDPR Crosswalk

NIST 800-53

AC-1

Control

Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more):
Organization-level; Mission/business process-level; Systemlevel] **access control policy** that:

ISO 27002

9.1.1 Access control policy

Control

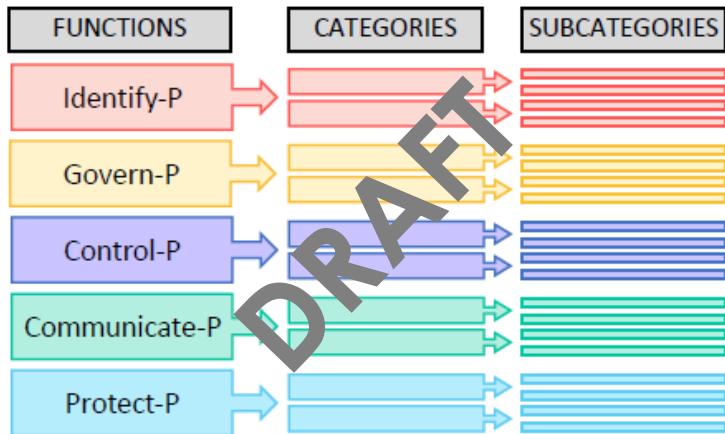
An access control policy should be established, documented and reviewed based on business and information security requirements.



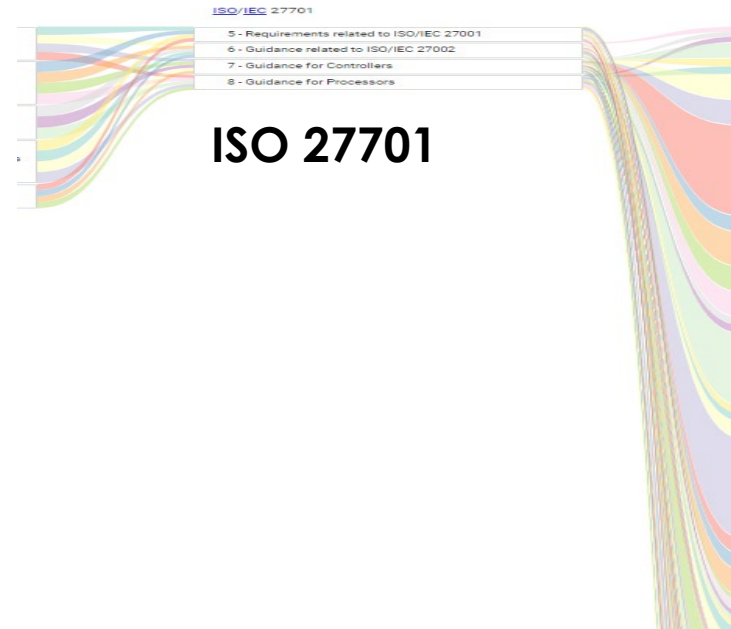
GDPR Crosswalk

Microsoft Data Protection/Privacy Mapping Project (dpmap.org)

NIST Privacy Framework CORE



ISO 27701



EU General Data Protection Regulation

Chapter II – Principles

Chapter III – Rights of the Data Subjects

- Section 1 Transparency and Modalities
- Section 2 Information and Access to Information
- Section 3 Rectification and Erasure
- Section 4 Right to object to automated decision making
- Section 5 Restrictions

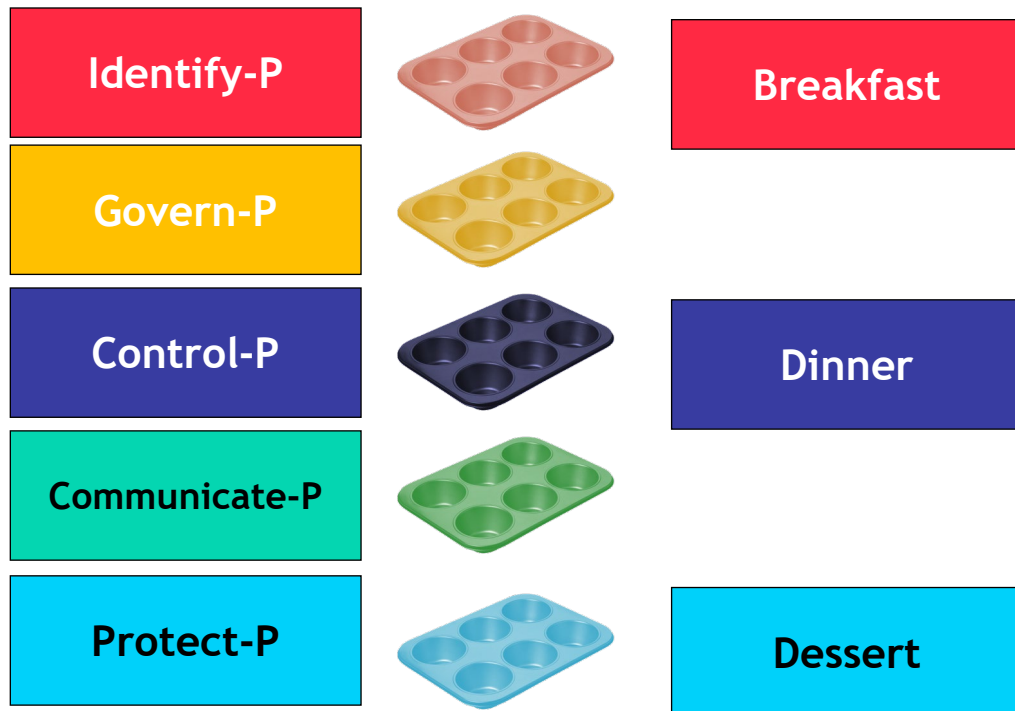
Chapter IV – Controllers and Processors

- Section 1 General Obligations
- Section 2 Security of Personal Data
- Section 3 Data Protection Impact Assessments
- Section 4 Data Protection Officers
- Section 5 Certification and Codes of Conduct

Chapter V – Data Transfers

GDPR Crosswalk

NIST Privacy Framework CORE



EU General Data Protection Regulation

GDPR Crosswalk

NIST Privacy Framework CORE



Company Profile

Blueberry Muffins

Blueberries
Flour
Water

Corn Bread

Corn Meal
Sugar
Salt
Milk
Jalapeños

Cupcakes

Sugar
Frosting
Strawberries

EU General Data Protection Regulation

GDPR Crosswalk

NIST Privacy Framework CORE

Identify-P



Govern-P



Control-P



Communicate-P



Protect-P



Breakfast

Dinner

Dessert

Company Profile

Blueberry Muffins

Blueberries ●
Flour
Water

Corn Bread

Corn Meal
Sugar ●
Salt
Milk
Jalapeños ●

Cupcakes

Sugar ●
Frosting ●
Strawberries ●

EU General Data Protection Regulation

○ Breakfast

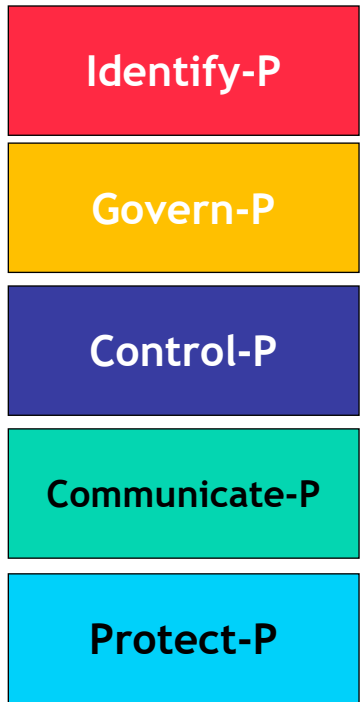
● Fruit

● Sweet

● Jalapeños

GDPR Crosswalk

NIST Privacy Framework CORE



ID.IM-P5: The purposes for the data actions are inventoried.

CT.PO-P1: Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, **individual consent**), revoking authorizations, and maintaining authorizations are established and in place.

EU General Data Protection Regulation

○ Article 35 DPIA

● Article 5(1)(b) Purpose Limitation

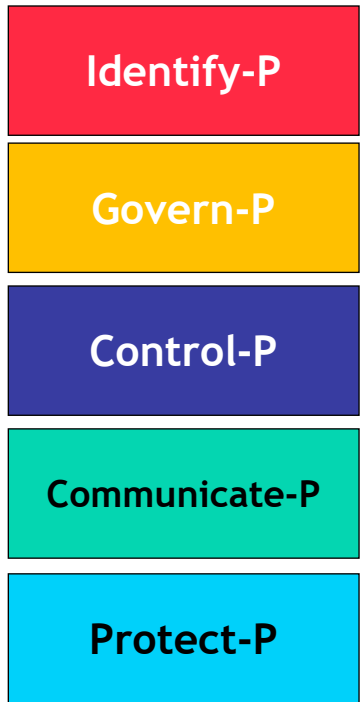
● Article 7 Conditions of Consent

● Article 32(4)

The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

GDPR Crosswalk

NIST Privacy Framework CORE



ID.IM-P5: The purposes for the data actions are inventoried.

CT.PO-P1: Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, **individual consent**), revoking authorizations, and maintaining authorizations are established and in place.

Profile

Procedure: systems requesting access to personal data ask, provide justification and be approved by internal data owners. Data owners review the request.

Policy: Principle of Least Privilege

EU General Data Protection Regulation

○ Article 35 DPIA

● Article 5(1)(b) Purpose Limitation

● Article 7 Conditions of Consent

● Article 32(4)

The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

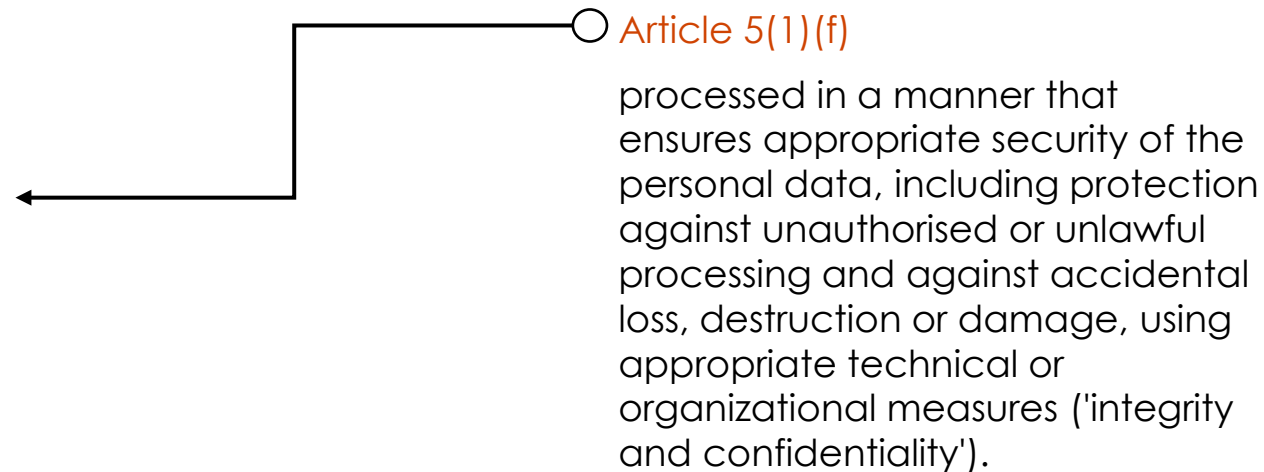
GDPR Crosswalk

NIST Privacy Framework CORE



CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.

EU General Data Protection Regulation



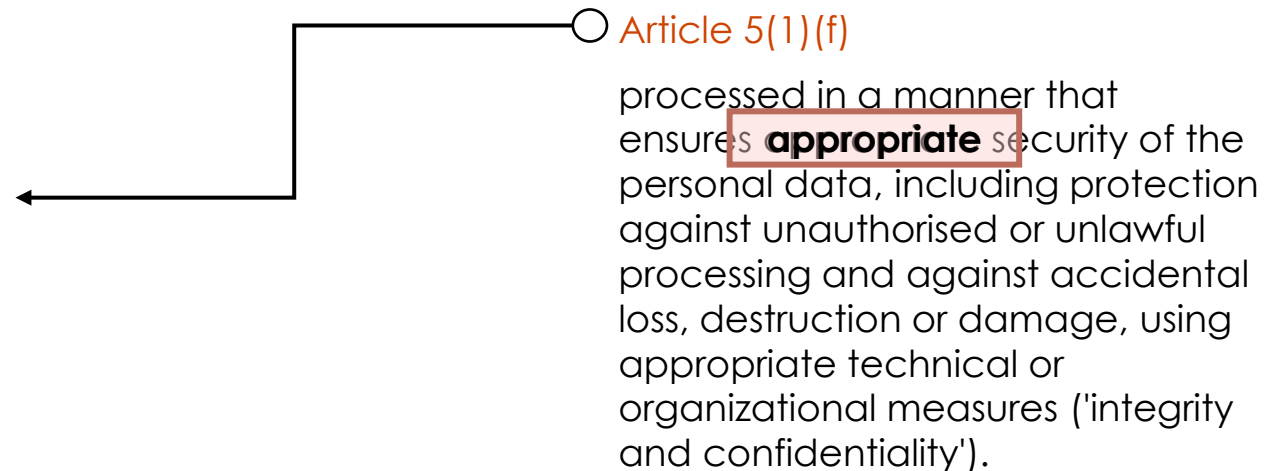
GDPR Crosswalk

NIST Privacy Framework CORE

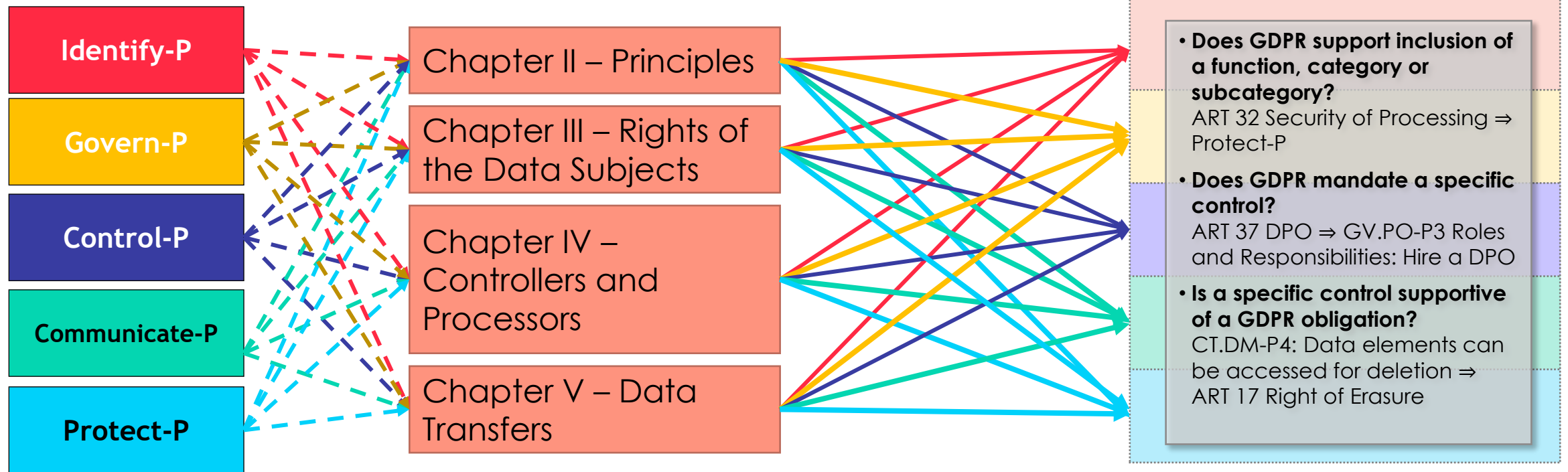


CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.

EU General Data Protection Regulation



Using the GDPR Crosswalk to develop your Target Profile



LGPD Crosswalk

Paulo Vidigal

Prado Vidigal Advogados

Dealing with the LGPD may feel like ...

PLAYING THE SQUID GAME

Just like in the TV Series, we may feel that:

- We are stuck in an unknown environment
- The rules are unclear and may change in the middle of the game
- We cannot rely on anyone: other participants are also new to the game
- We will soon be “eliminated”!



Can we pretend this is just like the GDPR?



Contracts:
Controllers – Processors



Record of Data Processing
Operations (ROPA)



Notification of Personal
Data Time Limits



DSAR Response Time Limits



Appointment of DPO

Contract provisions detailed in
Article 28

Content detailed in Article 30

72 hours

30 days +

Depending on the core
processing activities

Contract provisions are not
specified (implicit obligation)

Content not specified

Reasonable time

15 days

Mandatory to all data
controllers

Can the NIST Privacy Framework help?

The Privacy Framework can:

- help mitigate the principle-based nature of the LGPD and the lack of DPA regulations
- add credibility to the organization's privacy program
- act as the common language between different laws

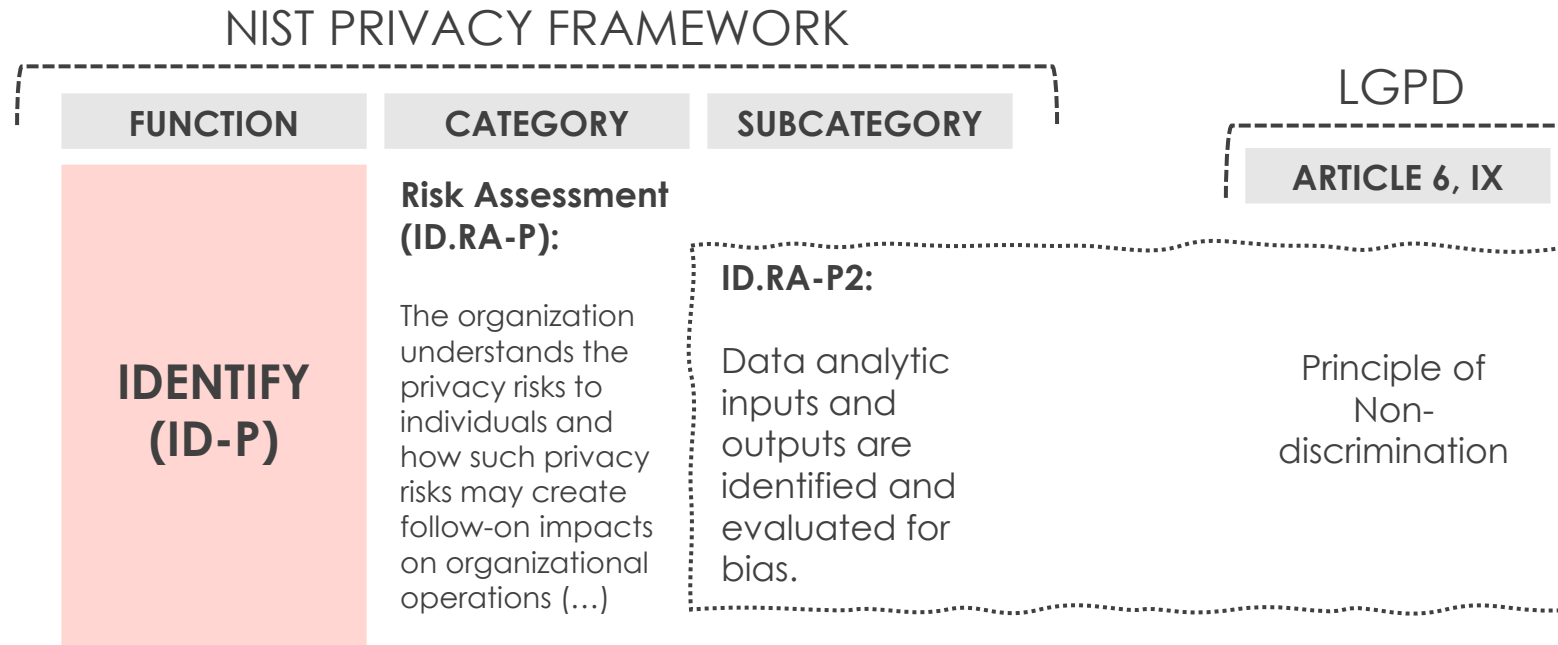
What about the LGPD Crosswalk?

Formula for the creation of the LGPD Crosswalk:

LGPD



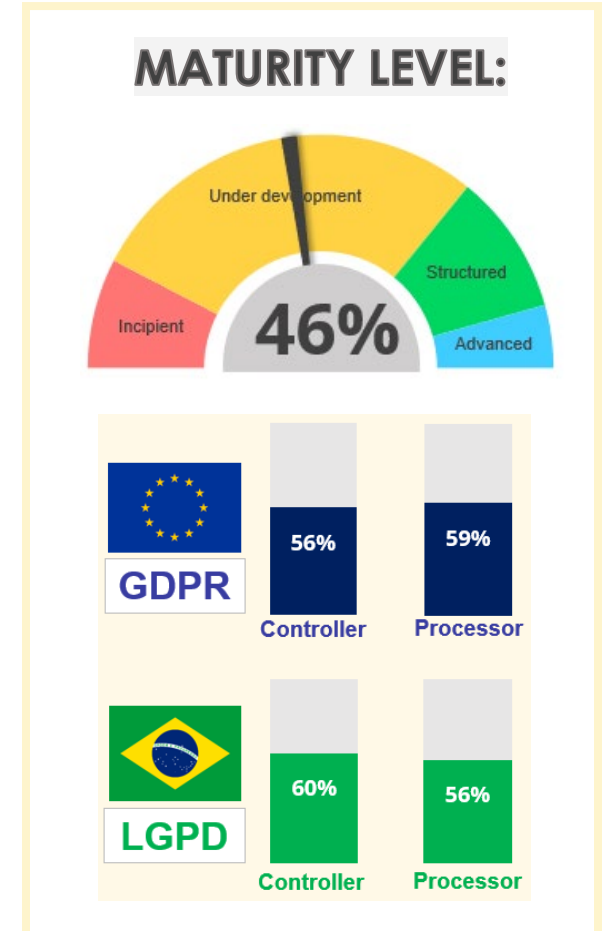
Example:



Was it ever used?

CASE STUDY

- Context: a Multinational organization that acquires small companies to fuel their growth
- What they did: Used the Privacy Framework to develop the preferable profile that a target should have and the Crosswalks (GDPR and LGPD) to ensure compliance
- Benefits: They have gained an increased perception of the real value of the targets and started to communicate risk more effectively



What's next?

Will we escape the Squid Game?

- Data privacy will continue to stay top of mind in Brazil
- LGPD will continue to evolve and be implemented by ANPD's regulations to come
- The Privacy Framework and the LGPD Crosswalk, which are living documents, can help us go beyond compliance

THANK YOU!

Resources



Website

<https://www.nist.gov/privacyframework>



Mailing List

<List.nist.gov/privacyframework>



Contact Us

PrivacyFramework@nist.gov

[@NISTcyber](#) [#PrivacyFramework](#)