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?

<table>
<thead>
<tr>
<th>Status</th>
<th>CCPA</th>
<th>CPRA</th>
<th>VCDPA</th>
<th>COPA</th>
<th>GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice Requirement</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Right to Access</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Right to Delete</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Right to Correct</td>
<td></td>
<td>✗</td>
<td></td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Right to Opt-Out of Sales</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Consent / Opt-in</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>“Sensitive Data&quot; Req.</td>
<td></td>
<td></td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Req.</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Private Right Of Action</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>DPA Requirement</td>
<td></td>
<td></td>
<td></td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>Enforcement (Fines)</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>Cure</td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.
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

<table>
<thead>
<tr>
<th>Understand</th>
<th>Communicate</th>
<th>Govern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand your data. Perform data mapping.</td>
<td>Draft appropriate privacy policies and other disclosures regarding data use.</td>
<td>Ensure internal controls support public-facing disclosures.</td>
</tr>
</tbody>
</table>
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
Control Define, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more):
Organization-level; Mission/business process-level; System-level] 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

NIST Privacy Framework CORE

<table>
<thead>
<tr>
<th>FUNCTIONS</th>
<th>CATEGORIES</th>
<th>SUBCATEGORIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify-P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Govern-P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control-P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communicate-P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect-P</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

- Identify-P
- Govern-P
- Control-P
- Communicate-P
- Protect-P

EU General Data Protection Regulation

- Breakfast
- Dinner
- Dessert
# GDPR Crosswalk

<table>
<thead>
<tr>
<th>NIST Privacy Framework CORE</th>
<th>EU General Data Protection Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify-P</td>
<td>Company Profile</td>
</tr>
<tr>
<td></td>
<td>Blueberry Muffins</td>
</tr>
<tr>
<td></td>
<td>Flour</td>
</tr>
<tr>
<td></td>
<td>Water</td>
</tr>
<tr>
<td>Govern-P</td>
<td>Corn Bread</td>
</tr>
<tr>
<td></td>
<td>Corn Meal</td>
</tr>
<tr>
<td></td>
<td>Sugar</td>
</tr>
<tr>
<td>Control-P</td>
<td>Salt</td>
</tr>
<tr>
<td></td>
<td>Milk</td>
</tr>
<tr>
<td>Communicate-P</td>
<td>Jalapeños</td>
</tr>
<tr>
<td>Protect-P</td>
<td>Cupcakes</td>
</tr>
<tr>
<td></td>
<td>Sugar</td>
</tr>
<tr>
<td></td>
<td>Frosting</td>
</tr>
<tr>
<td></td>
<td>Strawberries</td>
</tr>
</tbody>
</table>
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.

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.
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.
Article 5(1)(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

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.
Article 5(1)(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

NIST Privacy Framework CORE

- Identify-P
- Govern-P
- Control-P
- Communicate-P
- Protect-P

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.
Using the GDPR Crosswalk to develop your Target Profile

Chapter II – Principles
Chapter III – Rights of the Data Subjects
Chapter IV – Controllers and Processors
Chapter V – Data Transfers

• Does GDPR support inclusion of a function, category or subcategory?
  ART 32 Security of Processing ⇒ Protect-P

• Does GDPR mandate a specific control?
  ART 37 DPO ⇒ GV.PO-P3 Roles and Responsibilities: Hire a DPO

• Is a specific control supportive of a GDPR obligation?
  CT.DM-P4: Data elements can be accessed for deletion ⇒ ART 17 Right of Erasure
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?

<table>
<thead>
<tr>
<th>Contracts: Controllers – Processors</th>
<th>Record of Data Processing Operations (ROPA)</th>
<th>Appointment of DPO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller provisions are specified</td>
<td>Content not specified (implicit obligation)</td>
<td>Content not specified</td>
</tr>
<tr>
<td>Content detailed in Article 30</td>
<td>Reasonable time</td>
<td>Reasonable time</td>
</tr>
<tr>
<td>72 hours</td>
<td>15 days</td>
<td>15 days</td>
</tr>
<tr>
<td>30 days +</td>
<td>Mandatory to all data controllers</td>
<td>Mandatory to all data controllers</td>
</tr>
<tr>
<td>Depending on the core processing activities</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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:

Example:

<table>
<thead>
<tr>
<th>NIST PRIVACY FRAMEWORK</th>
<th>LGPD</th>
</tr>
</thead>
<tbody>
<tr>
<td>FUNCTION</td>
<td>CATEGORY</td>
</tr>
<tr>
<td>IDENTIFY (ID-P)</td>
<td>Risk Assessment (ID.RA-P):</td>
</tr>
<tr>
<td>The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations (...)</td>
<td>Data analytic inputs and outputs are identified and evaluated for bias.</td>
</tr>
</tbody>
</table>
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