Centre for Information Policy Leadership (CIPL) and Brazil Institute of Public Policy (IDP) Joint Workshop

LGPD – Implementation and Harmonization with International Data Protection Regimes

25 September 2019, Brasilia
Opening Remarks

Bojana Bellamy
President, CIPL

Laura Mendes
Professor, IDP

Danilo Doneda
Lawyer and Professor, IDP
### Brazilian Data Protection Implementation and Effective Regulation – Project Objectives

#### Information Sharing
- Facilitating information sharing
- Relevant regulatory and political data protection developments in Brazil and the globe

#### LGPD Implementation
- Informing and advancing constructive and forward-thinking interpretation of key LGPD requirements
- Facilitating consistent LGPD application
- Drawing from global experiences

#### Industry Experience and Best Practices
- Providing a forum for discussion and reflections on LGPD implementation and challenges
- Contributing to, and learning from, best practices
- Streamlining implementation measures

#### Effective Regulation
- Promoting effective regulatory strategies – innovative regulatory methods and constructive engagement with organizations
- Drawing on international regulatory experiences
- Reflecting upon the essential role of the ANPD
**Additional local webinars may be organised on key LGPD topics. Timeline above is indicative.**
Opening Keynote I

Orlando Silva
LGPD Rapporteur, Brazil National Congress
Opening Keynote II

Justice Ricardo Cueva
Judge, Brazil Superior Court of Justice
Session I – Key issues in implementing the LGPD: Operationalizing accountability and compliance through comprehensive organizational privacy management programs
Session I (Compliance Programs) – Panelists

Moderator
Bojana Bellamy
President, CIPL

Sarah Saucedo
Senior Counsel, Privacy & Data Protection, Mastercard

Orrie Dinstein
Global Chief Privacy Officer, Marsh & McLennan Companies, Inc.

Damien Kieran
Global Data Protection Officer, Legal Director and Associate General Counsel, Twitter

Vitor de Andrade
Lawyer, LTSA Advogados

Sarah Godley
Senior Vice President of Privacy, Americas, Teleperformance

André Giacchetta
Partner, Pinheiro Neto
The LGPD includes an “accountability” requirement pursuant to which organizations must implement comprehensive privacy management programs that enable compliance with this law and that can **demonstrate the effectiveness of such a program (Article 6, X and Article 50, § 2º, I)**. In addition, the LGPD provides that organizations “may formulate rules for good practice and governance”, which include implementing a **risk-based privacy management program as specified in the law (Article 50)**. Experienced privacy experts and practitioners will explain the important role of this accountability requirement in global data protection and what it means in practice, and will share their experiences and practical examples of how to give effect to accountability within an organization through privacy compliance and management programs. Finally, the panelists will also address the **role of risk and privacy impact assessments (Article 38)**, touch on the role of the **controller-processor relationship (Article 39)**, as well as discuss formal accountability schemes, such as **global corporate rules, certificates and codes of conduct (Article 33)**.
Session I (Compliance Programs) – Relevant LGPD Provisions

- Article 6, X: Accountability
- Article 50: Privacy management programs
- Article 38: Risk-based approach
- Article 39: Controller-processor relationship
- Article 33: Global corporate rules, certifications, codes of conduct
Accountability requires comprehensive privacy programs that translate legal requirements into risk-based, verifiable and enforceable corporate practices and controls.

Organizations must be able to demonstrate accountability – internally and externally.

Accountability is not static, but dynamic, reiterative and a constant journey.

Company values and business ethics shape accountability.
Demonstrating Accountability – to Whom and How?

To Whom?

- **Internally** – executives, leadership, Board of Directors, shareholders
- **Externally** – business partners, regulators, individuals, and civil society

Models of Accountability require:

- Following substantive privacy rules
- Implementation infrastructure
- Verification
- Ability to demonstrate

Sample Models of Accountability

- Corporate Privacy Programs
- Binding Corporate Rules (BCRs)
- Codes of Conduct
- Certifications & Seals
- APEC Cross Border Privacy Rules (CBPR)
- ISO Standards
Accountability – Benefits for Organizations

Proactive data management is a business issue and accountability is beyond legal compliance

- Enable new business models, digitalisation, globalisation and data-driven innovation
- Address increased expectations of individuals for transparency, control and value exchange
- Ensure data protection, sustainability and digital trust
- Address regulatory change, impact and implementation
- Mitigate legal, commercial and reputational risks
Accountability – Benefits for DPAs and Individuals

**DPAs**
- Reduces enforcement and oversight burden of DPAs
- Promotes constructive engagement with accountable organizations
- Encourages race to the top rather than race to the bottom

**Individuals**
- Effective protection and reduced risk/harm
- Empowered, able to exercise rights and complaints
- Trust/ready to benefit from and participate in digital society
## LGPD and Accountability

| Leadership and Oversight | • Data protection officer  
|• Mandatory LGPD governance program integrated into the organization’s general governance structure |
|---|---|
| Risk Assessment | • Impact assessment report as requested by the ANPD  
|• Risk assessment of data incidents |
|• Risk-based approach to development of codes of conduct  
|• Systemic assessment of impact on, and risk to, privacy as part of LGPD governance program |
| Policies and Procedures | • Legal bases and fair processing  
|• Anonymization procedures  
|• Retention and deletion  
|• Review of automated decisions  
|• Data transfer mechanisms  
|• Internal technical and organisational measures to comply with LGPD |
|• Security measures for processors  
|• Further technical measures required by the ANPD  
|• Privacy by design  
|• Vendor/processor contracts  
|• Procedures for response to individual rights  
|• Codes of conduct |
| Transparency | • Access to information about data processing  
|• Special measures for transparency when processing is based on legitimate interests  
|• Special notices for children and elderly |
|• Goal of the LGPD governance program of building a trust relationship with individuals though transparency and participation mechanisms  
|• Publication of codes of conduct |
| Training and Awareness | • Ability to demonstrate commitment to adopt internal procedures and policies resulting from the LGPD governance program – training implied |
| Monitoring and Verification | • Evidencing consent  
|• Verifying parental consent  
|• Legitimate interest impact assessment  
|• Internal records of processing |
|• Internal and external compliance monitoring for the LGPD governance program  
|• Assessment of effectiveness of the LGPD governance program |
| Response and Enforcement | • Data incident response plans and remediation, breach notification  
|• Audit for discrimination resulting from automated decision-making  
|• Processor liability |
|• Demonstrating effectiveness of the LGPD governance program  
|• Sanctions for non-compliance  
|• Mandatory public consultation for ANPD guidance and requirements  
|• Public hearings organised by the National Council |
Session II – Key issues in implementing the LGPD: Bases for processing and operationalizing consent and legitimate interest
Session II (Bases for Processing) – Panelists

Moderator

Danilo Doneda
Lawyer and Professor, IDP

Daniel Arbix
Head of Legal – Brazil, Google

Antonio Muñoz Marcos
Data Protection Technical Director, Telefónica

Pablo Segura
Data Privacy Senior Manager, Mercado Libre

Vanessa Butalla
Legal Director for Experian/Serasa

Ana Paula Bialer
Partner, Bialer e Falsetti Advogados
The LGPD sets forth the specific circumstances under which personal data may be processed (Article 7). In this session, the panelists will focus on two of these circumstances – processing with the consent of the data subject and the “legitimate interest” of the controller or third party (Article 7, I and IX; Article 10), both of which raise unique problems with respect to their implementation in practice. Thus, the panelists will discuss data processing contexts where consent may be appropriate and practicable, as well as effective ways to operationalize it. The panelists will also discuss the issue of “consent fatigue” and why it is important to limit consent to situations where it is truly effective and meaningful for individuals. They will also discuss the important processing ground of “legitimate interest”, the balancing of benefits and risks it entails, the proper role of this processing ground, and how to operationalize it for specific data processing activities. The panelists will also discuss how legitimate interest-based processing relates to the risk-based approach to privacy under the LGPD (Article 38).
# Session II (Bases for Processing) – Relevant LGPD Provisions

<table>
<thead>
<tr>
<th>Article 7</th>
<th>Legal bases for processing personal data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 7, I</td>
<td>Legitimate interest</td>
</tr>
<tr>
<td>Article 7, X</td>
<td>Consent</td>
</tr>
<tr>
<td>Article 10</td>
<td></td>
</tr>
<tr>
<td>Article 38</td>
<td>Risk-based approach</td>
</tr>
</tbody>
</table>
Session III – Key issues in implementing the LGPD: The Impact on big data, AI and machine learning, other emerging technologies and automated decision making
Session III (Emerging Technologies) – Panelists

Andrlei Guerrero Gutierrez
Government Relations and Regulatory Affairs Manager, IBM

Flavia Mitri
Privacy Director for Latin America, Uber

Marcela Mattiuzzo
Partner, VMCA Advogados

Rafael Zanatta
Lawyer, Pereira Neto | Macedo Advogados

Moderator
Laura Schertel Mendes
Professor, IDP
The panelists will explore how various provisions of the LGPD interact with modern and emerging technologies and applications. The provisions and issues to be examined in this context will include rules relating to automated decision-making (Article 20), sensitive data (Article 11), consent (Article 7, I), legitimate interest (Article 7, IX), deletion rights (Article 17, IV and VI), purpose specification and compatible/incompatible purposes (Article 6, I), necessity (Article 6, III), transparency (Article 6, VI), anonymization (Article 12), children’s data (Article 14), scientific research (Article 7, IV, Article 11, I, c and Article 13), and processing personal data to the detriment of data subjects (Article 21). The panelists will highlight areas of potential tension between data protection principles and the effective application of modern technologies and business practices. They will also offer ways to minimize these tensions through both sensible interpretations of these principles and various accountability measures available under the LGPD.
### Session III (Emerging Technologies) – Relevant LGPD Provisions

<table>
<thead>
<tr>
<th>Article 20</th>
<th>Automated decision-making</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 17, IV and VI</td>
<td>Deletion rights</td>
</tr>
<tr>
<td>Article 6, VI</td>
<td>Transparency</td>
</tr>
<tr>
<td>Article 7, IV Article 11, I, c Article 13</td>
<td>Scientific research</td>
</tr>
<tr>
<td>Article 20</td>
<td>Automated decision-making</td>
</tr>
<tr>
<td>Article 11</td>
<td>Sensitive personal data</td>
</tr>
<tr>
<td>Article 6, I</td>
<td>Purpose specification and purpose compatibility</td>
</tr>
<tr>
<td>Article 12</td>
<td>Anonymization</td>
</tr>
<tr>
<td>Article 21</td>
<td>Processing of data to the detriment of data subjects</td>
</tr>
<tr>
<td>Article 7, I and IX</td>
<td>Consent and legitimate interests</td>
</tr>
<tr>
<td>Article 6, III</td>
<td>Necessity</td>
</tr>
<tr>
<td>Article 6, IX</td>
<td>Non-discrimination</td>
</tr>
<tr>
<td>Article 14</td>
<td>Children’s data</td>
</tr>
</tbody>
</table>
Session IV – Key issues in implementing the LGPD: The Roles and Responsibilities of the Data Protection Authority
Session IV (Data Protection Authority) – Panelists

Moderator
Bojana Bellamy
President, CIPL

José Antonio Ziebarth
Director, Brazil Ministry of Economy

Bruno Bioni
Founder, Data Privacy Brasil

Fabricio da Mota Alves
Lawyer and Professor, Garcia de Souza Advogados

Guilherme Roschke

José Alejandro Bermúdez
Advisor – LATAM, CIPL and former Deputy Superintendent for Data Protection, Colombian DPA

Paula Vargas
Head of Privacy Engagement - Latin America, Facebook
The LGPD establishes a national data protection authority (DPA) (Article 55-A and following Articles). This panel will examine the various DPA tasks under this law and discuss how to best implement them in light of globally recognized characteristics of an effective data protection authority and the experience of established international data protection authorities. Particular focus will be placed on the role of “constructive engagement” between the DPA and the regulated industry.
Session IV (Data Protection Authority) – Relevant LGPD Provisions

Article 55-A and following

Establishment of the ANPD
Effective regulators have to **act** in a connected world

**Strategic, prioritized, risk-based, transparent regulatory policy**
- Prioritized activities (leadership, enforcement, complaint handling, authorizer)
- Innovative regulatory methods (e.g. Regulatory sandbox)

**Constructive engagement with regulated organizations**
- Maximum consultation, participation and frank exchanges

**Incentivize and encourage accountability**
- E.g. Showcase best practices and accountability efforts; differentiating factor in enforcement

**Act in a connected way with other regulators**
- Regulatory guidance, approaches to enforcement, mutual cooperation

**Build bridges with different regimes**
- Accountability frameworks (e.g. APEC CBPR and EU BCR)
The Importance of a Central ANPD

- Centralized expertise to enable safe and reliable digital environment
- Ensures consistency and legal certainty for organizations and individuals
- Promotes uniform standards and best practices for organizations
- Prevents organizations engaging in "forum shopping"
- Consistent interpretation and application of DP law
- Consistent complaint, oversight and enforcement procedures
- International representation and cooperation (e.g. ICDPPC, RPID, APPA, GPEN, CPEA, etc.)
- Single contact in cross-border enforcement matters
- One national agenda for the development of data privacy law
- Single voice and point of contact internationally
- Harmonizes data protection across borders with other nations
- Single national agenda for the development of data privacy law

ANPD
Framework for Trusted Digital Age

Media  Market forces  Political forces  Civil Society  Certifiers  Redress Schemes

Effective Regulators  Constructive Engagement  Accountable Organizations

Effective Protection for Individuals and Benefits for Digital Society

Art. 55-J, §2, LGPD – Mandatory public consultation and hearings for ANPD regulation and rules
Session V – Key Issues in Implementing the LGPD: Extraterritorial application of the law, cross-border transfer mechanisms, and ensuring interoperability with international privacy regimes
Session V (Cross Border Issues) – Panelists

**Moderator**

Markus Heyder  
Vice President and Senior Policy Counselor, CIPL

**Panelists**

Carlos Affonso de Souza  
Director at Instituto de Tecnologia & Sociedade do Rio de Janeiro (ITS-Rio)

Jonathan Fox  
Director of Privacy Engineering, Cisco

Miriam Wimmer  
Director of Telecommunications Services, Brazil Ministry of Science, Technology, Innovation and Communication (MCTIC)

Josh Harris  
Director of International Regulatory Affairs, TrustArc

Cornelius Witt  
Manager Public Policy, SCOPE Europe
This panel will discuss sensible ways to interpret and implement the LGPD’s provisions on territorial scope (Article 3) and its provisions on the international transfers of personal data (Articles 33 to 35). Specifically, the panelists will discuss the respective benefits and downsides of the various transfer mechanisms, assess their current state of development and availability in Brazil, and suggest ways forward for Brazil to operationalize the full spectrum of transfer mechanisms enabled by the LGPD, particularly global corporate rules, certifications and codes of conduct (Article 33, II) that could become interoperable with similar schemes in the Asia-Pacific and the EU regions, thereby streamlining and supporting accountable global data flows.
Session IV (Cross Border Issues) – Relevant LGPD Provisions

- Article 3: Territorial scope
- Articles 33 to 35: International transfers
- Article 33, II: Global corporate rules, certifications, codes of conduct
Accountability

The cornerstone of corporate digital responsibility, sustainable privacy protection for individuals, responsible use of data, and the 4th Industrial Revolution

Enables compliance with local law requirements

Enables compliance with cross-border transfer requirements

Solutions = Interoperable Accountability Frameworks
- Global Corporate Rules
- Certifications
- Codes of Conduct
- CBPR & PRP
- ISO Standard

Accountability delivers benefits to organizations, regulators, individuals and society

Regulators, law and policymakers must incentivize accountability / accountable organizations
Core Elements of Accountability in Privacy

Accountability requires comprehensive privacy programs that translate legal requirements into risk-based, verifiable and enforceable corporate practices and controls.

Organizations must be able to demonstrate accountability – internally and externally.

Accountability is not static, but dynamic, reiterative and a constant journey.

Company values and business ethics shape accountability.

Effective Compliance and Protection for Individuals

Leadership and Oversight

Response and Enforcement

Risk Assessment

Policies and Procedures

Monitoring and Verification

Training and Awareness

Transparency
<table>
<thead>
<tr>
<th>Leadership and Oversight</th>
<th>LGPD</th>
<th>GDPR</th>
<th>CBPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data protection officer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mandatory LGPD governance program integrated into the organization’s general governance structure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executive oversight</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data privacy officer/Office of oversight and reporting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data privacy governance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy engineers</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Assessment</th>
<th>LGPD</th>
<th>GDPR</th>
<th>CBPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact assessment report as requested by the ANPD</td>
<td>At program level</td>
<td>Periodic risk assessments regarding data security measures</td>
<td></td>
</tr>
<tr>
<td>Risk assessment of data incidents</td>
<td>At product or service level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk-based approach to development of codes of conduct</td>
<td>In case of data breach incident</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systemic assessment of impact on, and risk to, privacy as part of LGPD governance program</td>
<td>DPIA for high-risk processing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk to organizations</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk to individuals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LGPD</td>
<td>GDPR</td>
<td>CBPR</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>• Legal bases and fair processing</td>
<td>• Internal privacy rules based on data protection principles</td>
<td>• Internal guidelines or policies covering all CBPR requirements</td>
<td></td>
</tr>
<tr>
<td>• Anonymization procedures</td>
<td>• Information security</td>
<td>• Contracts with service providers</td>
<td></td>
</tr>
<tr>
<td>• Retention and deletion</td>
<td>• Legal bases and fair processing</td>
<td>• Measures for compliance with applicable laws and regulations that ensure CBPR compliance</td>
<td></td>
</tr>
<tr>
<td>• Review of automated decisions</td>
<td>• Vendor/Processor management</td>
<td>• Measures to comply with codes of conduct that correspond to the CBPR</td>
<td></td>
</tr>
<tr>
<td>• Data transfer mechanisms</td>
<td>• Procedures for response to individual rights</td>
<td>• Procedures for responding to legal process</td>
<td></td>
</tr>
<tr>
<td>• Internal technical and organisational measures to comply with LGPD</td>
<td>• Other procedures (e.g., Marketing rules, HR rules, M&amp;A due diligence)</td>
<td>• Due diligence measures with respect to service providers</td>
<td></td>
</tr>
<tr>
<td>• Security measures for processors</td>
<td>• Data transfer mechanisms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Further technical measures required by the ANPD</td>
<td>• Privacy by design</td>
<td>• Information security policies</td>
<td></td>
</tr>
<tr>
<td>• Privacy by design</td>
<td>• Privacy by design</td>
<td>• Risk-based and proportionate information security safeguards</td>
<td></td>
</tr>
<tr>
<td>• Vendor/Processor contracts</td>
<td>• Privacy by default</td>
<td>• Policies for disposal of information</td>
<td></td>
</tr>
<tr>
<td>• Procedures for response to individual rights</td>
<td>• Templates and tools for privacy impact assessments</td>
<td>• Policies regarding accuracy and integrity of personal information</td>
<td></td>
</tr>
<tr>
<td>• Codes of conduct</td>
<td>• Crisis management and incident response</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LGPD</td>
<td>GDPR</td>
<td>CBPR</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>• Access to information about data processing</td>
<td>• Privacy policies and notices to individuals</td>
<td>• Statements and notices about privacy policies, practices and compliance with CBPR</td>
<td></td>
</tr>
<tr>
<td>• Special measures for transparency when processing is based on</td>
<td>• Innovative transparency – dashboards,</td>
<td>• Access and correction</td>
<td></td>
</tr>
<tr>
<td>legitimate interests</td>
<td>integrated in products/apps, articulate value exchange and benefits,</td>
<td>• Notice regarding choice/consent</td>
<td></td>
</tr>
<tr>
<td>• Special notices for children and elderly</td>
<td>part of the customer relationship</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Goal of the LGPD governance program of building a trust relationship with individuals through transparency and participation mechanisms</td>
<td>• Access to information portals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Publication of codes of conduct</td>
<td>• Notification of data breaches</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Transparency</strong></td>
<td></td>
<td><strong>Training and Awareness</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ability to demonstrate commitment to adopt internal procedures and policies resulting from the LGPD governance program – training implied</td>
<td></td>
</tr>
<tr>
<td><strong>Training and Awareness</strong></td>
<td></td>
<td>• Mandatory corporate training</td>
<td></td>
</tr>
<tr>
<td>• Ability to demonstrate commitment to adopt internal procedures and policies resulting from the LGPD governance program – training implied</td>
<td>• Ad hoc and functional training</td>
<td>• Mandatory corporate training on privacy and data security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Awareness raising campaigns and communication strategy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### LGPD, GDPR & CBPR Mapped to Elements of Accountability

<table>
<thead>
<tr>
<th></th>
<th>LGPD</th>
<th>GDPR</th>
<th>CBPR</th>
</tr>
</thead>
</table>
| **Monitoring and Verification** | • Evidencing consent  
  • Verifying parental consent  
  • Legitimate interest impact assessment  
  • Internal records of processing  
  • Internal and external compliance monitoring for the LGPD governance program  
  • Assessment of effectiveness of the LGPD governance program | • Internal records of processing  
  • Documentation and evidence – consent, legitimate interest and other legal bases, notices, PIA, processing agreements, breach response  
  • Compliance monitoring as appropriate, such as verification, self-assessments and audits  
  • Seals and certifications | • Measures to test effectiveness of data security  
  • Oversight over data security measures of service providers  
  • Annual re-certification to CBPR |
| **Response and Enforcement** | • Data incident response plans and remediation, breach notification  
  • Audit for discrimination resulting from automated decision-making  
  • Processor liability  
  • Demonstrating effectiveness of the LGPD governance program  
  • Sanctions for non-compliance  
  • Mandatory public consultation for ANPD guidance and requirements  
  • Public hearings organised by the National Council | • Individual requests and complaint-handling  
  • Breach reporting, response and rectification procedures  
  • Managing breach notifications to individuals and regulators  
  • Implementing response plans to address audit reports  
  • Internal enforcement of non-compliance subject to local laws  
  • Engagement/Co-operation with DPAs | • Procedures for internal compliance and enforcement of CBPR obligations  
  • Procedures for complaint handling and response  
  • Responding to security failures |
# Privacy Program Certification Interoperability

<table>
<thead>
<tr>
<th>Privacy Framework Category</th>
<th>Requirements</th>
<th>EU BCRs (pre-GDPR)</th>
<th>EU BCRs (under GDPR)</th>
<th>APEC CBPRs</th>
<th>Privacy Shield</th>
<th>Referential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Management</td>
<td>Governance and Oversight</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Complaint Handling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Audit Program / Verification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20</td>
</tr>
<tr>
<td>Substantive Privacy and Data Protection Standards</td>
<td>Transparency and Fairness</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>14, 17</td>
</tr>
<tr>
<td></td>
<td>Purpose Limitation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Data Quality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>13, 18</td>
</tr>
<tr>
<td></td>
<td>Individual Rights</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6, 7, 8</td>
</tr>
<tr>
<td></td>
<td>Onward Transfer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>15, 16</td>
</tr>
<tr>
<td></td>
<td>Basis for Processing Personal Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>12, 13</td>
</tr>
<tr>
<td></td>
<td>Necessity / Proportionality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Privacy by Design and Default</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>National Law Limitations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Relationship to National Law</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>26</td>
</tr>
<tr>
<td>Scope</td>
<td>Geographic Scope</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Yellow</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Material Scope</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Entity List</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Purposes of Transfer / Processing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Enforceability</td>
<td>Internally Binding - Entities</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Green</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Internally Binding - Employees</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Third Party Beneficiary Rights</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Liability of Applicant Entity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Sufficiency of Applicant Entity Assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Burden of Proof</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Access to the BCRs / Policy / Notice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Cooperation Duty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1, 25</td>
</tr>
<tr>
<td>Other</td>
<td>Definitions</td>
<td></td>
<td></td>
<td></td>
<td>Yellow</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Effective Date and Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>23, 27</td>
</tr>
</tbody>
</table>

**Legend:**
- **Green** - substantively interoperable / comparable requirements
- **Dark Green** - more stringent standard
- **Light Green** - comparable standard, but narrower application / scope
- **Yellow** - less stringent standard
- **Gray** - no known requirement

© 2016, TRUSTe All rights reserved
Concluding Remarks and Next Steps
### Next Steps for the Brazil Project

<table>
<thead>
<tr>
<th>2019</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug</td>
<td></td>
</tr>
<tr>
<td>Sep</td>
<td></td>
</tr>
<tr>
<td>Oct</td>
<td></td>
</tr>
<tr>
<td>Nov</td>
<td></td>
</tr>
<tr>
<td>Dec</td>
<td></td>
</tr>
<tr>
<td>Jan</td>
<td></td>
</tr>
<tr>
<td>Feb</td>
<td></td>
</tr>
<tr>
<td>Mar</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td></td>
</tr>
<tr>
<td>May</td>
<td></td>
</tr>
<tr>
<td>Jun</td>
<td></td>
</tr>
<tr>
<td>Jul</td>
<td></td>
</tr>
<tr>
<td>Aug</td>
<td></td>
</tr>
<tr>
<td>Sep</td>
<td></td>
</tr>
<tr>
<td>Oct</td>
<td></td>
</tr>
<tr>
<td>Nov</td>
<td></td>
</tr>
<tr>
<td>Dec</td>
<td></td>
</tr>
</tbody>
</table>

- **Project Launch**
- **Workshop 1**
- **Webinar 1**
- **Workshop 2**
- **Basic Training**
- **Webinar 2**
- **Workshop 3**
- **Basic Training**
- **Webinar 3**
- **Workshop 4**
- **Basic Training**
- **Webinar 4**
- **White Paper 1**
- **White Paper 2**
- **White Paper 3**

*Additional local webinars may be organised on key LGPD topics.*

*Timeline above is indicative.*