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

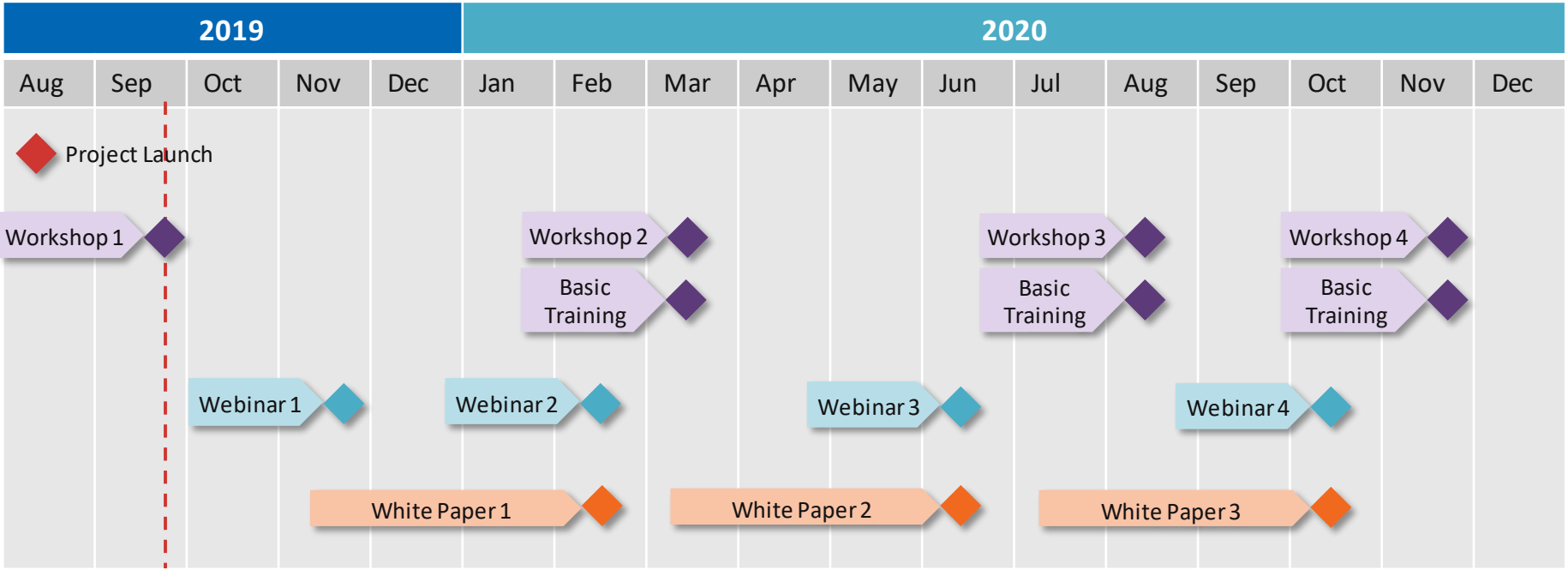
Industry Experience and Best Practices

- 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

Next Steps for the Brazil Project



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

Session I (Compliance Programs) – Description

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

Core Elements of Accountability in Privacy

Organizations must be able to demonstrate accountability – internally and externally

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

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

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

Vanessa Butalla

Legal Director for Experian/Serasa

Antonio Muñoz Marcos

Data Protection Technical Director, Telefónica

Ana Paula Bialer

Partner, Bialer e Falsetti Advogados

Pablo Segura

Data Privacy Senior Manager, Mercado Libre

Session II (Bases for Processing) – Description

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

Article 7	Legal bases for processing personal data
Article 7, I	Legitimate interest
Article 7, X Article 10	Consent
Article 38	Risk-based approach

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

Moderator

Laura Schertel Mendes

Professor, IDP

Andriei Guerrero Gutierrez

Government Relations and Regulatory Affairs Manager, IBM

Marcela Mattiuzzo

Partner, VMCA Advogados

Flavia Mitri

Privacy Director for Latin America, Uber

Rafael Zanatta

Lawyer, Pereira Neto | Macedo Advogados

Session III (Emerging Technologies) – Description

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

Article 20	Automated decision-making
Article 17, IV and VI	Deletion rights
Article 6, VI	Transparency
Article 7, IV Article 11, I, c Article 13	Scientific research
Article 11	Sensitive personal data
Article 6, I	Purpose specification and purpose compatibility
Article 12	Anonymization
Article 21	Processing of data to the detriment of data subjects
Article 7, I and IX	Consent and legitimate interests
Article 6, III	Necessity
Article 6, IX	Non-discrimination
Article 14	Children's data

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

Guilherme Roschke

Counsel for International Consumer Protection, US Federal Trade Commission

Bruno Bioni

Founder, Data Privacy Brasil

José Alejandro Bermúdez

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

Fabricio da Mota Alves

Lawyer and Professor, Garcia de Souza Advogados

Paula Vargas

Head of Privacy Engagement - Latin America, Facebook

Session IV (Data Protection Authority) – Description

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 and Results-Based Regulators in the Digital World

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

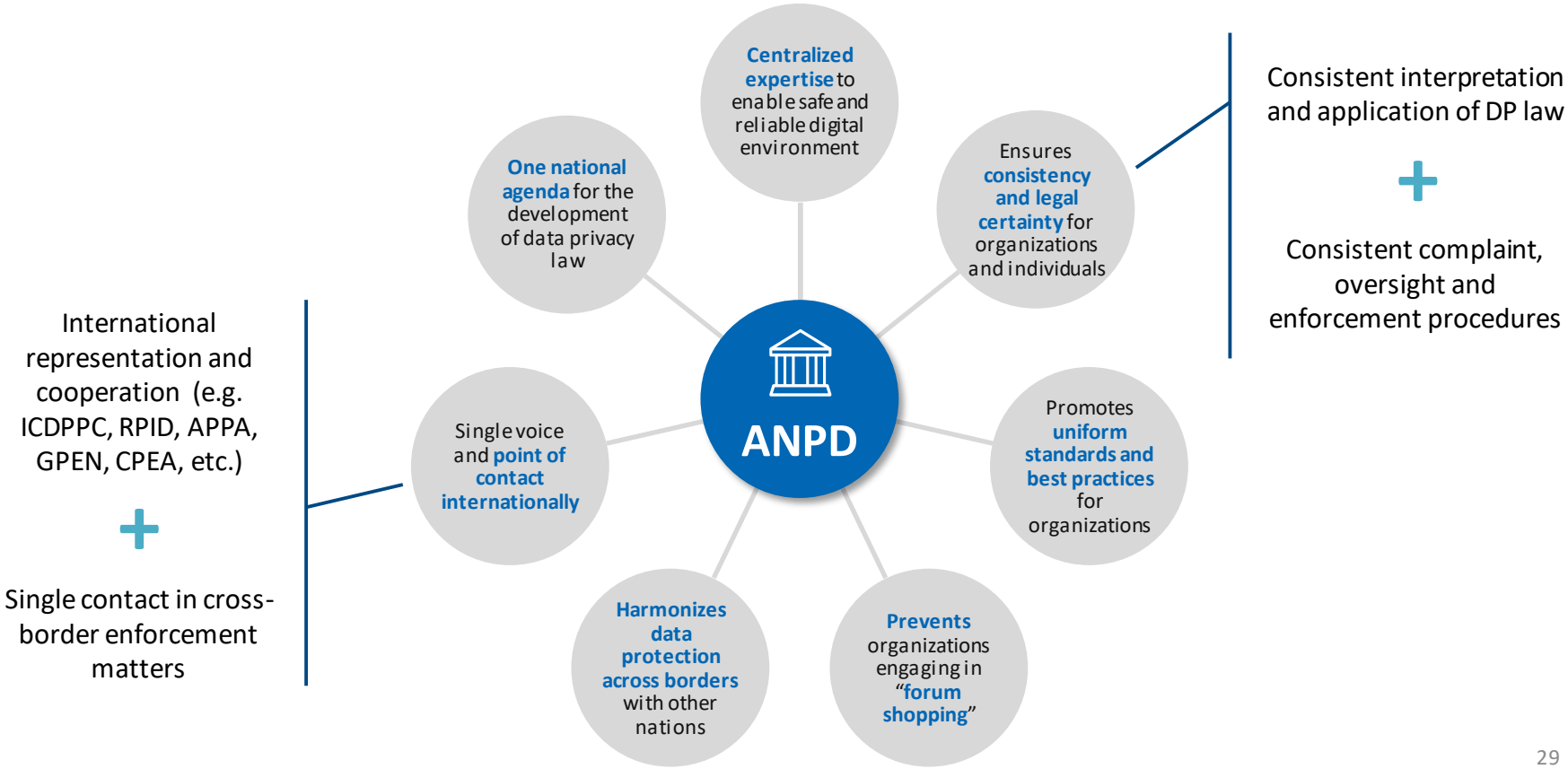
Act in a connected way with other regulators

- 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



Framework for Trusted Digital Age

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

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

Session V (Cross Border Issues) – Description

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 and Interoperable Cross-border Data Flows

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

Organizations must be able to demonstrate accountability – internally and externally

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

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

Company values and business ethics shape accountability

LGPD, GDPR & CBPR Mapped to Elements of Accountability

	LGPD	GDPR	CBPR
Leadership and Oversight	• Data protection officer • Mandatory LGPD governance program integrated into the organization's general governance structure	• Executive oversight • Data privacy officer/Office of oversight and reporting • Data privacy governance • Privacy engineers	• Individual responsible for compliance with CBPR
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	• At program level • At product or service level • In case of data breach incident • DPIA for high-risk processing • Risk to organizations • Risk to individuals	• Periodic risk assessments regarding data security measures

LGPD, GDPR & CBPR Mapped to Elements of Accountability

	LGPD	GDPR	CBPR
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	• Internal privacy rules based on data protection principles • Information security • Legal bases and fair processing • Vendor/Processor management • Procedures for response to individual rights • Other procedures (e.g., Marketing rules, HR rules, M&A due diligence) • Data transfer mechanisms • Privacy by design • Privacy by default • Templates and tools for privacy impact assessments • Crisis management and incident response	• Internal guidelines or policies covering all CBPR requirements • Contracts with service providers • Measures for compliance with applicable laws and regulations that ensure CBPR compliance • Measures to comply with codes of conduct that correspond to the CBPR • Procedures for responding to legal process • Due diligence measures with respect to service providers • Information security policies • Risk-based and proportionate information security safeguards • Policies for disposal of information • Policies regarding accuracy and integrity of personal information

LGPD, GDPR & CBPR Mapped to Elements of Accountability

	LGPD	GDPR	CBPR
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	• Privacy policies and notices to individuals • Innovative transparency – dashboards, integrated in products/apps, articulate value exchange and benefits, part of the customer relationship • Access to information portals • Notification of data breaches	• Statements and notices about privacy policies, practices and compliance with CBPR • Access and correction • Notice regarding choice/consent
Training and Awareness	• Ability to demonstrate commitment to adopt internal procedures and policies resulting from the LGPD governance program – training implied	• Mandatory corporate training • Ad hoc and functional training • Awareness raising campaigns and communication strategy	• Mandatory corporate training on privacy and data security

LGPD, GDPR & CBPR Mapped to Elements of Accountability

	LGPD	GDPR	CBPR
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

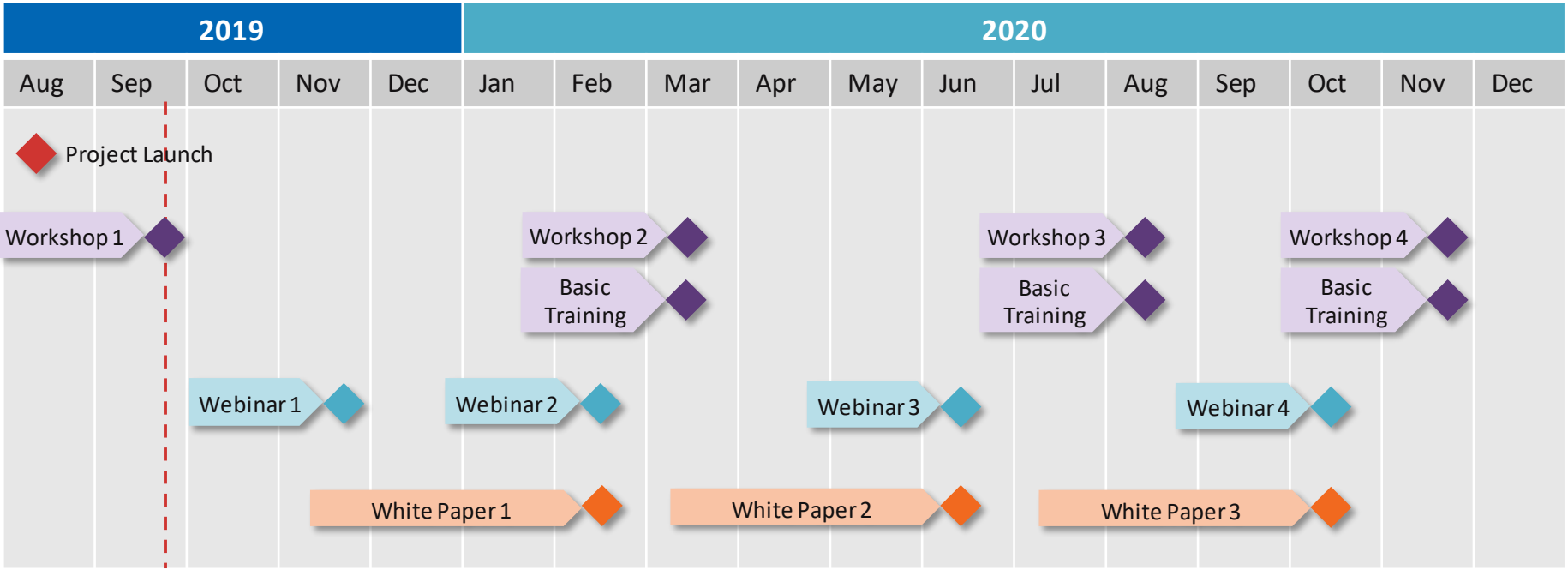
Privacy Framework Category	Requirements	EU BCRs (pre-GDPR)	EU BCRs (under GDPR)	APEC CBPRs	Privacy Shield	Referential
Program Management	Governance and Oversight					21
	Training					19
	Complaint Handling					22
	Audit Program / Verification					20
Substantive Privacy and Data Protection Standards	Transparency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

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

Concluding Remarks and Next Steps

Next Steps for the Brazil Project



Additional local webinars may be organised on key LGPD topics.
Timeline above is indicative.

Thank You

Bojana Bellamy

President

bbellamy@HuntonAK.com

Markus Heyder

Vice President & Senior Policy Advisor

mheyder@HuntonAK.com

Giovanna Carloni

Global Privacy Policy Manager

gcarloni@HuntonAK.com

Laura Schertel Mendes

Professor, IDP

lauraschertel@hotmail.com

Danilo Doneda

Lawyer and Professor, IDP

danilo@doneda.net

Centre for Information Policy Leadership
www.informationpolicycentre.com

Hunton's Information Security Law Blog
www.huntonprivacyblog.com

@THE_CIPL

linkedin.com/company/centre-for-information-policy-leadership

Instituto Brasiliense de Direito Público
http://www.idp.edu.br

@SejaIDP

https://www.linkedin.com/company/idp-brasilia/about/