Webinar 2 – Applying the LGPD’s Risk-Based Approach: How Can Organizations Prioritize Compliance and Accountability Based on Risk?

23 April 2020
Welcome and Introductions

Bojana Bellamy, President, CIPL
The Centre for Information Policy Leadership (CIPL) is a global privacy and security think tank. Based in Washington, DC, Brussels and London, CIPL was founded in 2001 by leading companies and Hunton Andrews Kurth LLP. It works with industry leaders, regulatory authorities and policy makers to develop global solutions and best practices for data privacy and responsible use of data to enable the modern information age.
## CIPL-CEDIS Joint Brazil Project

### Project Objectives

**Effective Implementation and Regulation Under the New Brazilian Data Protection Law (LGPD)**

<table>
<thead>
<tr>
<th>Information Sharing</th>
<th>LGPD Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Facilitating information sharing</td>
<td>• Informing and advancing constructive and forward-thinking interpretation of key LGPD requirements</td>
</tr>
<tr>
<td>• Relevant regulatory and political data protection developments in Brazil and the globe</td>
<td>• Facilitating consistent LGPD application</td>
</tr>
<tr>
<td></td>
<td>• Drawing from global experiences</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Industry Experience and Best Practices</th>
<th>Effective Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Providing a forum for discussion and reflections on LGPD implementation and challenges</td>
<td>• Promoting effective regulatory strategies – innovative regulatory methods and constructive engagement with organizations</td>
</tr>
<tr>
<td>• Contributing to, and learning from, best practices</td>
<td>• Drawing on international regulatory experiences</td>
</tr>
<tr>
<td>• Streamlining implementation measures</td>
<td>• Reflecting upon the essential role of the ANPD</td>
</tr>
</tbody>
</table>

For more info about the project, visit: https://www.informationpolicycentre.com/brazilian-data-protection-implementation-and-effective-regulation.html
**CIPL-CEDIS Joint Brazil Project**

**Project achievements so far**

- **Workshop 1** held in Brazilian, with additional side meetings with regulators and policymakers
  - Testimony of Bojana Bellamy at the House of Representatives public hearing on the proposed Constitutional Amendment No. 17-A of 2019

- **Webinar 1** on Top Priorities for Organisations when Implementing the LGPD
  - CIPL response to the Brazilian MCTIC's Consultation on a National AI Strategy for Brazil

- **Workshop 2**
  - Paper on the Role and Priorities of the ANPD
  - Webinar 2 on Applying the LGPD's Risk-Based Approach

- **Workshop 3** (online)
  - Papers on COVID-19 and data protection; Top LGPD Implementation Priorities; LGPD Risk-based Approach

- **Coming**
The Notion of a Risk-Based Approach

Conceptual Elements

Goals of a risk-based approach:
1. Facilitate and improve organizational accountability and legal compliance
2. Enable consistent approach to regulatory oversight and law enforcement
3. Support effective privacy legislation and rule making

- Assessment of the **likelihood and severity of risk** of the data processing operations to individuals
- Notion of **proportionality** – taking into account the nature, scope, context and purposes of the processing operations
- **Consistency** in the identification and classification of risks, threats and harms (material or non-material; risks to individuals, society and the organization; etc.)
- **Flexibility** for organisations to address risks in a contextual manner
Different Types of Risk Assessments

**Calibrating privacy programmes and compliance**

### At privacy programme level
- Determines the programme and its elements
- Adjusts the programme elements
- Periodic programme assessment

### At legal requirement level
- Data Protection Impact Assessments (DPIAs) and privacy by design
- Legitimate interests assessment
- Purpose limitation
- Security
- Data breaches

### Other product/service risk assessments
- Product or service reviews
- Assessments of processors/vendors
- M&A due diligence
- Compliance approvals
- AI impact assessments
- Audits
- Information security assessments
- Approval of new IT systems and databases
Initial considerations

Risk-Based Approach in the LGPD

Horizontal – accountability obligation
- Calibrating the privacy governance programme based on:
  - the structure, scale and volume of processing
  - the sensitivity of the personal data processed
  - the probability and seriousness of damages to data subjects

Implied consideration of risk
- Legitimate interest impact assessment
- Risk of re-identification of anonymous data
- ANPD may assess whether automated decisions result in discrimination
- Exemption from appointing Data Protection Officers

Specific obligations based on risk
- Processing is “irregular” when organisations do not take into account the risks reasonably expected
- Managing security incidents and data breaches
- ANPD may issue technical standards for data security, throughout the product/service lifecycle, considering the nature of personal data processed

Specific requirements for high-risk processing
- Data Protection Impact Assessments (DPIAs)
- Communication to the ANPD and data subjects of security incidents/data breaches that may result in “relevant damage” to data subjects
- ANPD may propose mitigation measures relating to the security incident/data breach

Further guidance to be provided by the Agência Nacional de Proteção de Dados – ANPD
Speaker Presentations

Two sessions:
(1) LGPD provisions
(2) Sharing experiences

Open Discussions

All participants are encouraged to submit questions and comments through the Q&A box in the Zoom Application
Speakers

Bruno Bioni  
*Founder, Data Privacy Brasil*

Tatiana Campello  
*Partner, Demarest Advogados*

Bojana Bellamy  
*President, CIPL*

Alisa Bergman  
*Chief Privacy Officer, Adobe*

Orrie Dinstein  
*Chief Privacy Officer, Marsh & McLennan Companies Group*

Clarissa Yoshino  
*Counsel – Privacy and Data Protection, Brazil Data Protection Officer, Mastercard*

Danilo Doneda  
*Lawyer and Professor, IDP*
Updates on the latest privacy developments in Brazil

Danilo Doneda, Lawyer and Professor, IDP
LGPD provisions on risk-based approach

Bruno Bioni, Founder, Data Privacy Brasil
Tatiana Campello, Partner, Demarest Advogados
LGPD provisions
Bruno Bioni, Founder, Data Privacy Brasil

Horizontal – accountability obligation
- Calibrating the privacy governance programme based on:
  - the structure, scale and volume of processing
  - the sensitivity of the personal data processed
  - the probability and seriousness of damages to data subjects
  Art. 50

Implied consideration of risk
- Legitimate interest impact assessment
- Risk of re-identification of anonymous data
- ANPD may assess whether automated decisions result in discrimination
- Exemption from appointing Data Protection Officers
  Art.10, §3
  Art. 12, §1 and §2
  Art. 20, §1 and §2
  Art. 41, §3
Specific obligations based on risk

- **Processing is “irregular”** when organisations do not take into account the risks reasonably expected
- Managing **security incidents and data breaches**
- ANPD may issue technical standards for **data security**, throughout the product/service lifecycle, considering the nature of personal data processed

Art. 44, II
Art. 46
Art. 46, §1 and §2

Specific requirements for high-risk processing

- Data Protection Impact Assessments (DPIAs)
- **Communication to the ANPD and data subjects** of security incidents/data breaches that may result in “relevant damage” to data subjects
- ANPD may propose **mitigation measures** relating to the security incident/data breach

Art. 38
Art. 48
Art. 48, §2
Processing is irregular

- No compliance of the law (legal grounds)
- No security
  - the way it is performed
  - result and risk reasonably expected
  - use of processing techniques available

Principles:
- Transparency
- Security
- Prevention (controller shall create measures to mitigate risk)

Processing agents responsibility if security measures are not adopted and there are damages

Reasonability and case by case analysis
Managing security incidents and data breaches

Processing agents shall adopt security, technical and administrative measures to protect personal data from inappropriate or unlawful processing

• Potential administrative sanctions and civil responsibility

Security – references such as National Institute of Standards and Technology (NIST)

• Confidentiality / Availability / Integrity
  • On-line and Off-line

Technical and administrative

• Compliance / Best Practices

Possibility of creation of minimum technical requirements (use of Internet Civil Act Regulation?)

• Access control and responsibility definitions
  • Authentication
  • Inventory
  • Inviolability

Privacy by design - new mindset - privacy experts will be included on team work to develop new products or services.
DPIA – Data Protection Impact Assessment

Risk - description of event and its consequences severity and likelihood

Risk management: coordination of activities to direct and control an organization with regard to risk

- potential reduction of sanctions in case of incidents (good faith)
- increase organization value - good risk assessment and control

DPIAs should consider:

- compliance risks
- risks to the rights and freedom of individuals
- significant social or economic disadvantage to individuals or to society (physical, material or non-material risks)
- one or several processing activities
DPIA – Data Protection Impact Assessment

Source: http://ec.europa.eu/justice/data-protection/index_eg.htm
Security incidents/data breaches that may result in relevant risk or damage to data subjects

Subjective criteria (economic, moral, individual rights, all of them?)

Case by cases

- nature, sensitivity, and volume of personal data
- type of breach
- ease of identification of individuals
- severity of consequences for individuals
- special characteristics of the individual and/or the data controller
- number of affected individuals
- expectation by data subject
- industry/activity consideration

Risk assessment and management
Sharing experiences on prioritizing compliance and applying a risk-based approach

Clarissa Yoshino, Counsel – Privacy and Data Protection, Brazil Data Protection Officer, Mastercard

Orrie Dinstein, Chief Privacy Officer, Marsh & McLennan Companies Group

Alisa Bergman, Chief Privacy Officer, Adobe
What is Mastercard? The importance of developing a detailed understanding of your business and its data processing activities in order to take risk-based decisions to implement the LGPD

Design Sessions: A practical approach to identifying high-risk processing activities and defining actions to bring them into compliance with the LGPD

Sharing Regional Experiences and Best Practices: The key to scaling an accountability based Privacy Program
Privacy Risk Assessments – core elements:

• Centralized / global solution

• Preliminary risk assessment – Triage of cases:
   • Low risk – ignore
   • Medium risk – self service
   • High risk – focus

• Understand the risk and conduct your balancing test – focus on mitigation actions and also on PbD controls

• Examples:
  • Use of Zoom
  • COVID19 contact tracing app
Defining data protection risks
Data Protection Impact Assessments
Open Discussions

All participants are encouraged to submit questions and comments through the Q&A box in the Zoom Application.
• What does it mean to have a risk-based approach for data processing activities?
• What is the relationship between a risk-based approach and accountability?
• How can organizations apply a risk-based approach to the development and implementation of their LGPD compliance programs?
• How can organizations measure risks related to the processing of personal data? What kind of risks and harms should be considered, and how should they be weighted and measured?
• What is the difference between general risk assessments, Privacy Impact Assessments (PIAs) and a formal DPIA?
• What is the business opportunity/benefit in undertaking across-the-board risk assessments as a routine business activity, even when the ANPD may not have required a formal DPIA?
• What is expected from the ANPD when issuing rules and procedures concerning DPIAs and high-risk processing?
For more information about the CIPL & CEDIS-IDP Brazil project, visit:

Portuguese – CEDIS-IDP’s website: http://www.idp.edu.br/centro-de-pesquisa-cepes/centro-de-estudos-de-direito-internet-e-sociedade-cedis/