Webinar 4
Practical Steps to Implement the LGPD Effectively (plus launch of the new CIPL & CEDIS-IDP paper and of OneTrust LGPD tool)

29 September 2020
10:00 AM   Welcome and Introductions

Bojana Bellamy
President, CIPL

10:20 AM   CIPL & CEDISO-IDP new paper: Top 12 Priorities for Effective LGPD Implementation

Laura Schertel
Lawyer, Professor and Director of CEDIS-IDP

10:40 AM   OneTrust’s New LGPD Tool

Danilo Doneda
Lawyer, Professor and Director of CEDIS-IDP

11:00 AM   Questions and Answers

11:30 AM   End of webinar

Alex Bermudez
Offering Manager, Latin America at OneTrust
About CIPL

Global Privacy and Security Think Tank

ACTIVE GLOBAL REACH

- **90+** Member companies
- **5+** Active projects & initiatives
- **20+** Events annually
- **15+** Principals and Advisors

We

**INFORM**
through publications and events

**NETWORK**
with global industry and government leaders

**SHAPE**
privacy policy, law and practice

**CREATE**
and implement best practices

ABOUT US

- The Centre for Information Policy Leadership (CIPL) is a global privacy and security think tank
- Based in Washington, DC, Brussels and London
- Founded in 2001 by leading companies and Hunton Andrews Kurth LLP
- CIPL 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
IDP’s Center for Law, Internet and Society (CEDIS) is a dynamic space devoted to foster the debate of legal and social challenges regarding new technologies and the implementation of new legal frameworks.

- Based in Brasília, DF
- Founded in 2014
- The purpose of CEDIS is to promote research and debates through events, workshops, papers, research groups and partnerships with other institutions, in order to contribute to the consolidation of mechanisms that promote privacy and protection of personal data, stimulate competition and innovation and strengthen the multi-sectoral Internet governance system.

CEDIS wishes to promote the development of a network to guarantee privacy and freedom on the Internet, acting as a hub to academics and representatives of the public, private and civil society sectors.
CIPL-CEDIS Joint Brazil Project Objectives

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

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

CIPL-CEDIS Joint Brazil Project Elements

Events

• Workshops, webinars and roundtables organized with Brazilian and international data privacy experts, organizations and public sector stakeholders

• Various topics addressed include: the establishment of the ANPD, accountability, risk-based approach, legal bases for processing, DPOs, DSR, international data transfers, artificial intelligence and emerging tech, and others

Publications

• White Papers, including on the role of the ANPD and on the top priorities for LGPD implementation (and more coming)

• Blog posts, OpEds, news articles on various LGPD and ANPD legal and regulatory developments

• Visual infographics

Additional debates

• Additional meetings with key stakeholders

• Parallel discussions with project participants

• Ad hoc speaking engagements and events
CIPL-CEDIS Joint Brazil Project Timeline

**Workshop 1**, in Brazil, and side meetings with regulators and policymakers

**Sep 2019**
- **Bojana Bellamy’s testimony at the House of Representatives** public hearing on the proposed Constitutional Amendment No. 17-A of 2019

**Nov 2019**
- **Webinar 1** on Top Priorities for Organizations when Implementing the LGPD & CIPL response to the Brazilian MCTIC’s Consultation on a National AI Strategy for Brazil

**Jan 2020**
- **Paper on the Role and Priorities of the ANPD** & **Webinar 2** on Applying the LGPD’s Risk-Based Approach

**April 2020**
- **Virtual Industry Roundtable** on the legal bases for processing

**Jul 2020**
- **Open webinar 3** to launch the ANPD paper

**Aug 2020**
- **Paper on Top LGPD Implementation Priorities**

**Sep 2020**
- **Series of webinars and roundtables** on multiple topics & Future project papers

**Coming**
CIPL & CEDIS-IDP new paper: Top 12 Priorities for Effective LGPD Implementation

Bojana Bellamy, President, CIPL
Danilo Doneda, Lawyer, Professor and Director of CEDIS-IDP
The LGPD applies to both public and private sector organizations, regardless of where they are located, if they fall within the scope of the law.

Some organizations have already made notable progress towards LGPD compliance, but many are still in the very early stages of implementing the LGPD’s requirements.

The CIPL and CEDIS-IDP new paper:
• Describes 12 practical priorities and specific related steps that public and private organizations need to take to implement the LGPD effectively.
• Is based on the extensive data privacy compliance experience of numerous Brazilian and international privacy experts and professionals.

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-idp_white_paper_on_top_priorities_for_public_and_private_organizations_to_effectively_implement_the_lgpd__1_september_2020__.pdf
Checklist: Priority Steps for LGPD Compliance

One-Page Checklist in the Paper

1. Understand the LGPD’s impact on the organization and obtain buy-in from top management
2. Explain and demonstrate privacy compliance and request support from resources.

Infographic Version

**Top Priorities for LGPD Implementation**

1. Understand the LGPD impact on the organization and obtain buy-in from top management
2. Designate a person in charge of data protection, and identify and engage key stakeholders
3. Identify the organization’s processing activities and the data that the organization handles
4. Determine the organization’s role and obligations as a controller or operator
5. Assess the privacy risks associated with the organization’s data processing
6. Design and implement a data privacy management program covering the LGPD requirements
7. Define the legal bases for the organization’s data processing activities
8. Define technical and organizational measures for effective data security and internal reporting and management of security incidents
9. Identify all third parties with which the organization shares personal data and establish a third party management process
10. Identify the organization’s cross-border data flows (inbound and outbound) and put in place appropriate data transfer mechanisms and safeguards
11. Build effective processes for transparency and data subject rights
12. Train employees on LGPD requirements and create an awareness-raising program
Once established, the ANPD is expected to issue guidance, regulations and standards on a number of LGPD implementation topics.

ANPD Priorities

**Priorities to support organizations with LGPD implementation**

- **Interpreting the LGPD**
  To clarify provisions relating to its scope, consent, processing of children's data.

- **Providing guidance**
  On topics such as data sharing, portability, timeframes for responding to data subject rights.

- **Providing technical standards**
  And encouraging the adoption of industry standards that will enable LGPD implementation.

- **Enabling international data transfers**
  Through recognizing adequacy of third countries and establishing the various data transfer mechanisms.

- **Acknowledging good practice**
  Recognizing best in class examples of accountable privacy governance programs.

**Other priorities**

- **Defining its strategy**
  Preparing the National Policy for the Protection of Personal Data and Privacy.

- **Educating on data protection**
  Educating individuals about their data protection rights, and organizations about their obligations.

- **Preparing for LGPD enforcement**
  By establishing enforcement procedures and implementing mechanisms to receive complaints.

[https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[en]_cipl-idp_paper_on_the_role_of_the_anpd_under_the_lgpd__0_4.16.2020__3_.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[en]_cipl-idp_paper_on_the_role_of_the_anpd_under_the_lgpd__0_4.16.2020__3_.pdf)
OneTrust’s New LGPD Tool

Alex Bermudez, Offering Manager, Latin America at OneTrust
CIPL Priorities | How OneTrust Helps

CIPL Priority 1
Understand the LGPD's impact on the organization and obtain buy-in from top management

Maturity & Planning | Program Benchmarking
Data Discovery | Data Mapping | DataGuidance

CIPL Priority 2
Designate a person in charge of data protection and identify and engage key stakeholders

Assessment Automation | Enterprise Policy Management

CIPL Priority 3
Identify the organization's processing activities and the data that the organization handles

Data Discovery
Data Mapping

CIPL Priority 4
Determine the organization's role and obligations as a controller or operator

Maturity & Planning | Enterprise Policy Management | Data Mapping

CIPL Priority 5
Assess the privacy risks associated with the organization's data processing

Assessment Automation
Vendor Risk Management

CIPL Priority 6
Design and implement a data privacy management program covering the LGPD requirements

Enterprise Policy Management
<table>
<thead>
<tr>
<th>CIPL Priority 7</th>
<th>Define the legal bases for the organization’s data processing activities</th>
<th>Data Mapping</th>
<th>Assessment Automation</th>
<th>Consent</th>
<th>Cookie Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIPL Priority 8</td>
<td>Define technical and organizational measures for effective data security and internal reporting and management of security incidents</td>
<td>Enterprise Policy Management</td>
<td>IT Risk Management</td>
<td>Incident Response</td>
<td>Awareness Training</td>
</tr>
<tr>
<td>CIPL Priority 9</td>
<td>Identify all third parties with which the organization shares personal data and establish a third-party management process</td>
<td>Vendor Risk Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIPL Priority 10</td>
<td>Identify the organization’s cross-border data flows (inbound and outbound) and put in place appropriate data transfer mechanisms and safeguards</td>
<td>Data Mapping</td>
<td>Vendor Risk Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIPL Priority 11</td>
<td>Build effective processes for transparency and data subject rights</td>
<td>Policy &amp; Notice Management</td>
<td>Cookie Compliance</td>
<td>Consent</td>
<td>Data Subject Requests</td>
</tr>
<tr>
<td>CIPL Priority 12</td>
<td>Train employees on LGPD requirements and create an awareness-raising program</td>
<td>Awareness Training</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Conduct a Personal Data and System Inventory

**Assets:** Define systems/services processing data, location, access

**Business Processes:** create organizational context, informing RoPA

**Vendors:** profile data categories, transfers both domestic and international
Controllers and operators must maintain records of processing activities (registro das operações de tratamento de dados pessoais)

- Include Legal Basis for Processing
- Define Business Group/Brand Responsible
- Ensure business is indicated as controller or operator
<table>
<thead>
<tr>
<th>Nome</th>
<th>Base legal para o tratamento</th>
<th>Titulares de dados - Dados pessoais</th>
<th>Categoria dos dados - Dados pessoais</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lead Generation</td>
<td>Consentimento do indivíduo</td>
<td>Clientes, Futuros funcionários</td>
<td>Clientes - informações de contato</td>
</tr>
<tr>
<td>User Account Authentication</td>
<td>É necessário para as finalidades dos nossos interesses legítimos (da organização...</td>
<td>Funcionários</td>
<td>Funcionários - identificação de propósito...</td>
</tr>
<tr>
<td>Onboarding</td>
<td>É necessário para a execução de um contrato com o indivíduo</td>
<td>Funcionários, Contratante</td>
<td>Funcionários - identificação de propósito...</td>
</tr>
<tr>
<td>Account Management</td>
<td>É necessário para a execução de um contrato com o indivíduo</td>
<td>Clientes, Contratante, Funcionários, Futuros funcionários</td>
<td>Clientes - informações das contratações</td>
</tr>
<tr>
<td>Contract Submission</td>
<td>É necessário para as finalidades dos nossos interesses legítimos (da organização...</td>
<td>Funcionários</td>
<td>Funcionários - informações de contrato</td>
</tr>
<tr>
<td>Online Advertising</td>
<td>Consentimento do indivíduo</td>
<td>Clientes</td>
<td>Clientes - informações de navegação</td>
</tr>
<tr>
<td>Customer Service</td>
<td>Consentimento do indivíduo</td>
<td>Clientes, Contratante</td>
<td>Clientes - informações das contratações</td>
</tr>
<tr>
<td>Events and Trade Shows</td>
<td>Consentimento do indivíduo</td>
<td>Clientes</td>
<td>Clientes - informações de navegação</td>
</tr>
<tr>
<td>Marketing CRM</td>
<td>É necessário para as finalidades dos nossos interesses legítimos (da organização...</td>
<td>Clientes</td>
<td>Clientes - informações de navegação</td>
</tr>
<tr>
<td>SaaS Products Procurement</td>
<td>É necessário para o cumprimento de uma obrigação jurídica</td>
<td>Clientes</td>
<td>Clientes - informações de navegação</td>
</tr>
<tr>
<td>HR Recruiting</td>
<td>É necessário para as finalidades dos nossos interesses legítimos (da organização...</td>
<td>Futuros funcionários</td>
<td>Futuros funcionários - informações de navegação</td>
</tr>
<tr>
<td>SAP ERP Access</td>
<td>É necessário para o cumprimento de uma obrigação jurídica, É necessário par...</td>
<td>Clientes, Funcionários, Contratante, Futuros funcionários</td>
<td>Clientes - informações das contratações</td>
</tr>
<tr>
<td>Active Directory Service</td>
<td></td>
<td>Funcionários, Contratante</td>
<td>Funcionários - informações de navegação</td>
</tr>
</tbody>
</table>
International Transfers of Data

ADEQUACY

INTERNATIONAL COMMITMENT

Other Lawful Methods of International Data Transfers

- Global Corporate Rules
- Standard Contractual Clauses
- Contractual Clauses Specific to a Particular Transfer
- Seals/Stamp, Certificates and Codes of Conduct
- Data Holder’s Specific, Separate, Informed Consent

NECESSITY
(e.g., contract performance; compliance with legal obligation; international legal cooperation)
Transfronteiriço
Privacy Impact Assessments

Privacy Impact Assessments are essential for a proper privacy governance program

PIAs help you verify that the processing of personal data satisfies the LGPD’s Processing Principles
Whenever the ANPD requires the RIPD (arts. 4 §3, 10, 38)

**Bests practices** – perform an RPID when there could be a privacy impact resulting from:

- Processing based on your legitimate interests (art. 10, § 3)
- Tracking individuals or creating behavioral profiles of individuals (art. 12 § 2)
- Use of a new technology or product/service
- Processing sensitive personal data (art. 5º, II)
- Processing to make automated decisions that affect data subjects’ interests or might have legal effects (art. 20)
- Processing children's or adolescent's’ personal data (art. 14)
- Processing that may cause material/physical or moral harm to individuals or society at large (art. 42)
- A material change in the business or operations, such as an acquisition or merger
- Legal or regulatory changes that impact privacy, processing activities, data handling, etc.
ANPD may determine the controller to prepare a RIPD

Documentation describing the processes of processing personal data that may generate risks to civil liberties and fundamental rights, as well as measures, safeguards and risk mitigation mechanisms

The RIPD must contain, as a minimum:
1. Description of the types of data collected
2. Methodology used to collect and guarantee the security of information
3. Analysis regarding measures, safeguards and risk mitigation mechanisms adopted
DATA SUBJECT RIGHTS

- **Confirmation of existence of processing**
- **Access to personal data**
- **Correction of incomplete, inaccurate or outdated data**
- **Anonymization, blocking or elimination of unnecessary, excessive or unlawfully processed data**
- **Information about the ability to deny consent and the consequences of such denial**
- **Portability of personal data to another provider**
- **Revocation of consent**
- **Review of automated decision-making (no human review)**
- **Information about the public and private entities with which the controller has shared personal data**
- **Deletion of personal data processed with consent, unless an exception applies**
Implement a Privacy Governance Program to demonstrate Accountability

- Map and inventory personal data based on processing activities, assets, and processors
- Implement policies and procedures to manage data subjects' rights requests
- Define the parties responsible for handling the requests and train them on how to do so
- Establish adequate policies and safeguards based on a systematic impacts on and risks to privacy
- Establish measures to safeguard against any risks to privacy, such as fraudulent requests
- Ensure that data subjects can exercise their rights easily
- Regularly update and revise policies and procedures to facilitate data subjects rights process
- track any requirements or recommendations issued by the ANPD
Consent: free, informed and unequivocal manifestation by which the holder agrees to the processing of his personal data for a given purpose.

Consent is waived where the data subject makes the personal data publicly available.

Specific consent required to transfer or disclose personal data to other third-party controllers (except in cases of a waiver).
When is Consent Required?

**Sensitive Personal Data**

Specific and distinct consent is *required* for a specific purpose, unless an exception applies.

**Children Personal Data**

- Consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, unless an exception applies
- Controllers must use reasonable efforts to verify the parent or legal representative

**Optional – Consent is one lawful basis for International Transfers**

Specific and informed consent, distinct for the transfer purpose
Lawful Consent

Consent Must

- Be written or by any other means that demonstrates the holder's expression of will
- Refer to particular purposes → no generic authorizations

Controller bears burden of proof

Consent is void if the information about processing is
- misleading or abusive
- not presented in a transparent, clear and unambiguous way

Changes to processing purpose, type or duration, or controller’s identity or sharing of personal data

Changes to purpose of processing incompatible with initial consent
## Consent & Data Subject Rights

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request deletion of personal data where processing is based on consent</td>
<td>Request deletion of personal data where processing is based on consent.</td>
</tr>
<tr>
<td>Request information on the possibility of denying consent and the consequences of a denial</td>
<td>Request information on the possibility of denying consent and the consequences of a denial.</td>
</tr>
<tr>
<td>Revoke consent for free at any time</td>
<td>Revoke consent for free at any time.</td>
</tr>
<tr>
<td>Oppose processing based on a waiver of consent where the processing does not comply with the LGPD</td>
<td>Oppose processing based on a waiver of consent where the processing does not comply with the LGPD.</td>
</tr>
<tr>
<td>Data portability: electronic portable, readily useable format</td>
<td>Data portability: electronic portable, readily useable format.</td>
</tr>
</tbody>
</table>
Questions and Answers