Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CEDIS Centro de Direito, Internet e Sociedade

idp

OneTrust
PRIVACY, SECURITY & TRUST

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

Agenda and Speakers

10:00 AM	**Welcome and Introductions**
10:20 AM	**CIPL & CEDISO-IDP new paper: Top 12 Priorities for Effective LGPD Implementation**
10:40 AM	**OneTrust's New LGPD Tool**
11:00 AM	**Questions and Answers**
11:30 AM	**End of webinar**

Bojana Bellamy

President, CIPL

Laura Schertel

Lawyer, Professor and Director of CEDIS-IDP

Danilo Doneda

Lawyer, Professor and Director of CEDIS-IDP

Alex Bermudez

Offering Manager, Latin America at OneTrust

CIPL Centre for Information Policy Leadership HUNTON ANDREWS KURTH

CEDIS

OneTrust PRIVACY, SECURITY & TRUST

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

About CIPL

Global Privacy and Security Think Tank

BRIDGING REGIONS | BRIDGING INDUSTRY & REGULATORS | BRIDGING PRIVACY AND DATA DRIVEN INNOVATION

ACTIVE GLOBAL REACH

90+
Member companies

5+
Active projects & initiatives

20+
Events annually

15+
Principals and Advisors

We **INFORM** through publications and events

We **NETWORK** with global industry and government leaders

We **SHAPE** privacy policy, law and practice

We **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

Twitter.com/the_cipl

https://www.linkedin.com/company/centre-for-information-policy-leadership

www.informationpolicycentre.com

2200 Pennsylvania Ave NW
Washington, DC 20037

Park Atrium, Rue des Colonies 11
1000 Brussels, Belgium

30 St Mary Axe
London EC3A 8EP

About CEDIS

CEDIS | Centro de Direito, Internet e Sociedade

ABOUT US

- 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.

twitter.com/CedisIdp

https://www.idp.edu.br/cedis/

SGAS Quadra 607 - Módulo 49 - Via L2 Sul - Brasília - DF CEP 70.200-670

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 Centre for Information Policy Leadership HUNTON ANDREWS KURTH | CEDIS | OneTrust PRIVACY, SECURITY & TRUST

https://www.informationpolicycentre.com/brazilian-data-protection-implementation-and-effective-regulation.html

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 Centre for Information Policy Leadership
HUNTON ANDREWS KURTH
CEDIS
OneTrust
PRIVACY, SECURITY & TRUST

CIPL-CEDIS Joint Brazil Project Timeline

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CEDIS

OneTrust
PRIVACY, SECURITY & TRUST

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

Bojana Bellamy, President, CIPL

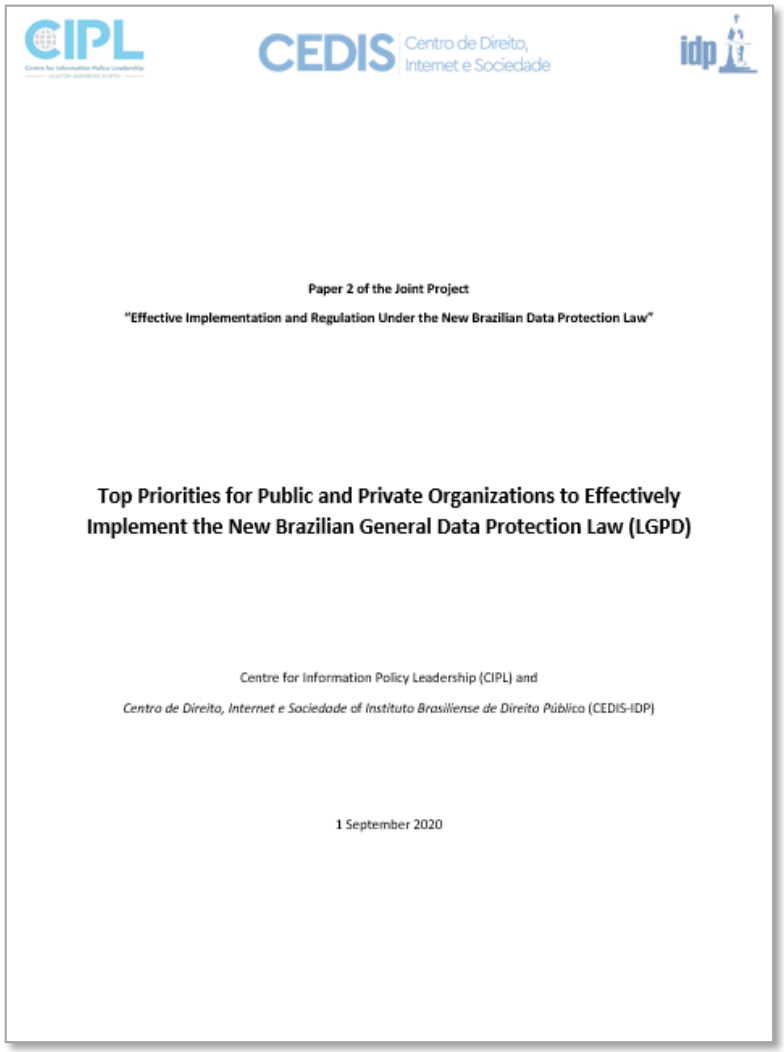
Danilo Doneda, Lawyer, Professor and Director of CEDIS-IDP

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CEDIS

OneTrust
PRIVACY, SECURITY & TRUST

Project Paper: Top Priorities for LGPD Implementation



CIPL Centre for Information Policy Leadership HUNTON ANDREWS KURTH

CEDIS Centro de Direito, Internet e Sociedade

idp

Paper 2 of the Joint Project

"Effective Implementation and Regulation Under the New Brazilian Data Protection Law"

Top Priorities for Public and Private Organizations to Effectively Implement the New Brazilian General Data Protection Law (LGPD)

Centre for Information Policy Leadership (CIPL) and

Centro de Direito, Internet e Sociedade of Instituto Brasiliense de Direito Público (CEDIS-IDP)

1 September 2020

- 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

CIPL Centre for Information Policy Leadership HUNTON ANDREWS KURTH CEDIS OneTrust PRIVACY, SECURITY & TRUST

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

CIPL Centre for Information Policy Leadership HUNTON ANDREWS KURTH | CEDIS Centro de Direito, Internet e Sociedade | idp

Checklist: Priority Steps for LGPD Compliance

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

- ☐ Understand the impact of the LGPD rules on the organization and its use of personal data as a controller and/or operator.
- ☐ Explain and demonstrate to senior management the importance of privacy compliance and the benefits of accountability.
- ☐ Request support from senior management, including budget and resources.

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

- ☐ Designate the organization's DPO and document and communicate their role and responsibilities internally.
- ☐ Identify and engage key internal stakeholders and senior leaders who will sponsor the data privacy management program and who will own program implementation activities.
- ☐ Identify and engage with key external stakeholders.

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

- ☐ Define the methodology to map and record the organization's processing activities (as controller and/or operator) and periodically review the data lifecycle.
- ☐ Map the organization's data and processing activities as soon as possible.
- ☐ Consider anonymization and data minimization to reduce the organization's risk and compliance burden.

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

- ☐ Determine the organization's role and obligations as a controller or operator.
- ☐ Communicate these obligations to the relevant individuals and teams within the organization.
- ☐ Consider any updates needed to standard customer contracts to reflect the organization's role.

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

- ☐ Implement a data privacy risk assessment process that includes consideration of risks to individuals.
- ☐ Prioritize compliance measures related to data processing that carries the highest risks for individuals and the organization.

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

- ☐ Design a data privacy management program and an action plan for implementing it based on the identified risks.
- ☐ Identify easier tasks and implement them as soon as possible.
- ☐ Maintain and review the data privacy management program on an ongoing basis.

Priority 7. Define the legal bases for the organization's data processing activities

- ☐ Identify the individuals or team that will be responsible for determining the legal bases for processing—they should define the legal bases the organization relies upon as a priority.
- ☐ Consider what processes should be put in place and/or adapted for ongoing maintenance of the legal bases for processing activities.

Priority 8. Define technical and organizational measures for effective data security and internal reporting and management of security incidents

- ☐ Work with the information security and systems/data architecture teams to determine the changes needed to implement appropriate data security measures.
- ☐ Establish a process for internal reporting and managing of security incidents and personal data breaches and notifying the ANPD if necessary.

Priority 9. Identify all third parties with which the organization shares personal data and establish a third party management process

- ☐ Identify the third parties that process personal data on the organization's behalf, and determine whether it processes personal data on behalf of another organization.
- ☐ Assess and adopt third party management mechanisms, including due diligence and entering into data processing agreements.

Priority 10. Identify the organization's cross-border data flows (inbound and outbound) and put in place appropriate data transfer mechanisms and safeguards

- ☐ Identify whether the organization transfers personal data to third countries, for what purposes and in what capacity (as controllers and/or operators).
- ☐ Assess and implement the transfer mechanisms that are most appropriate for the organization.

Priority 11. Build effective processes for transparency and data subject rights

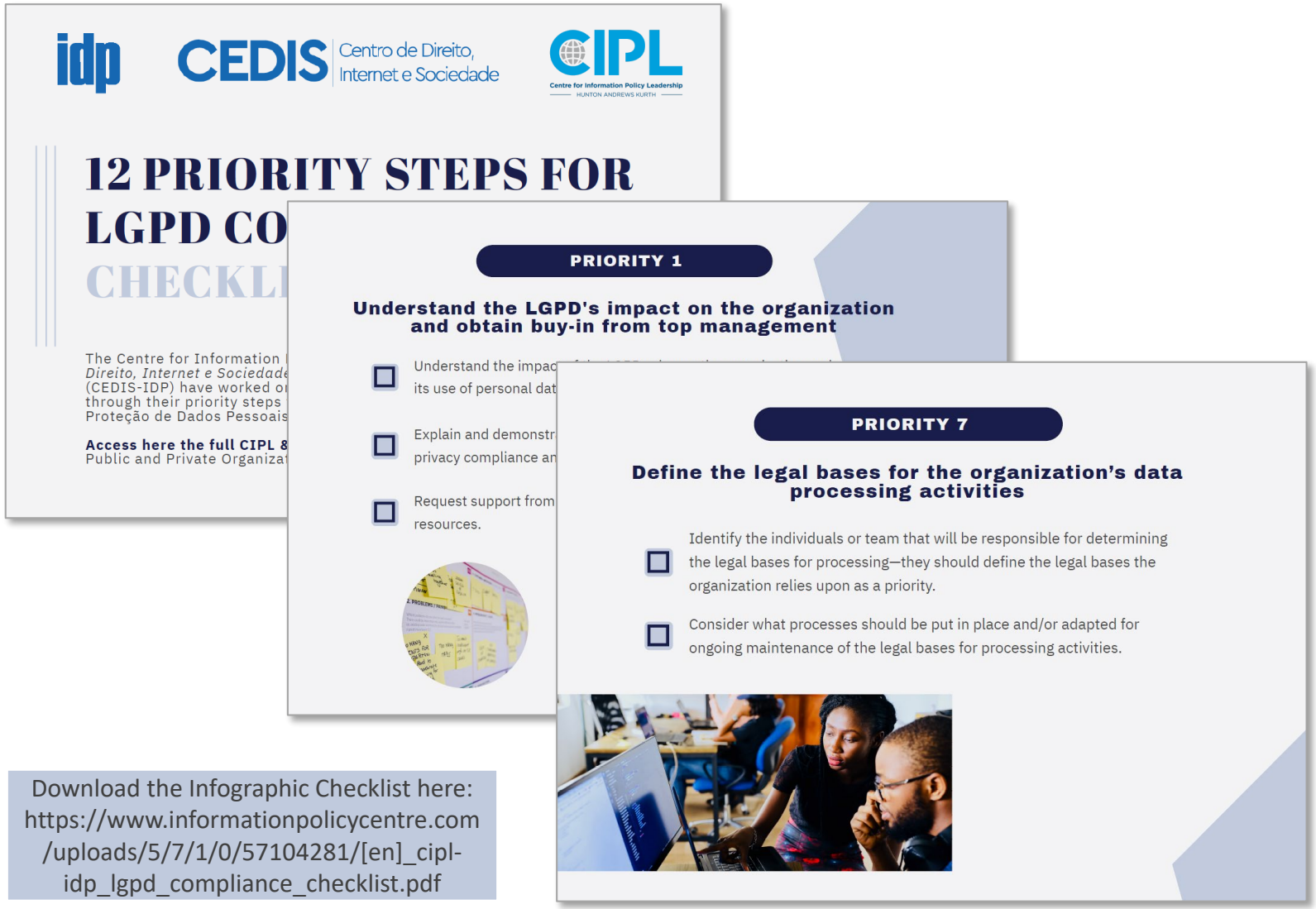
- ☐ Prepare privacy notices and other relevant resources to provide easily accessible information to individuals about the organization's data processing.
- ☐ Map the various case scenarios for data subject rights requests and assess the organization's response time to requests to develop the relevant processes.
- ☐ Develop processes to respond to such requests.

Priority 12. Train employees on LGPD requirements and create an awareness-raising program

- ☐ Implement ongoing training for all existing employees, contractors and new-joiners.
- ☐ Plan training and communications activities both in the beginning of the organization's data privacy management program and on an ongoing basis.

3

Infographic Version



Download the Infographic Checklist here: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[en]_cipl-idp_lgpd_compliance_checklist.pdf

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

ANPD Priorities

Once established, the ANPD is expected to issue guidance, regulations and standards on a number of LGPD implementation topics

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

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[en]_cipl-idp_paper_on_the_role_of_the_anpd_under_the_lgpd__04.16.2020__3_.pdf

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

OneTrust's New LGPD Tool

Alex Bermudez, Offering Manager, Latin America at OneTrust

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CEDIS

OneTrust
PRIVACY, SECURITY & TRUST

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

CIPL Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CEDIS

OneTrust
PRIVACY, SECURITY & TRUST

CIPL Priorities | How OneTrust Helps

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

CIPL Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CEDIS

OneTrust
PRIVACY, SECURITY & TRUST

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

CIPL Centre for Information Policy Leadership HUNTON ANDREWS KURTH

CEDIS

OneTrust PRIVACY, SECURITY & TRUST

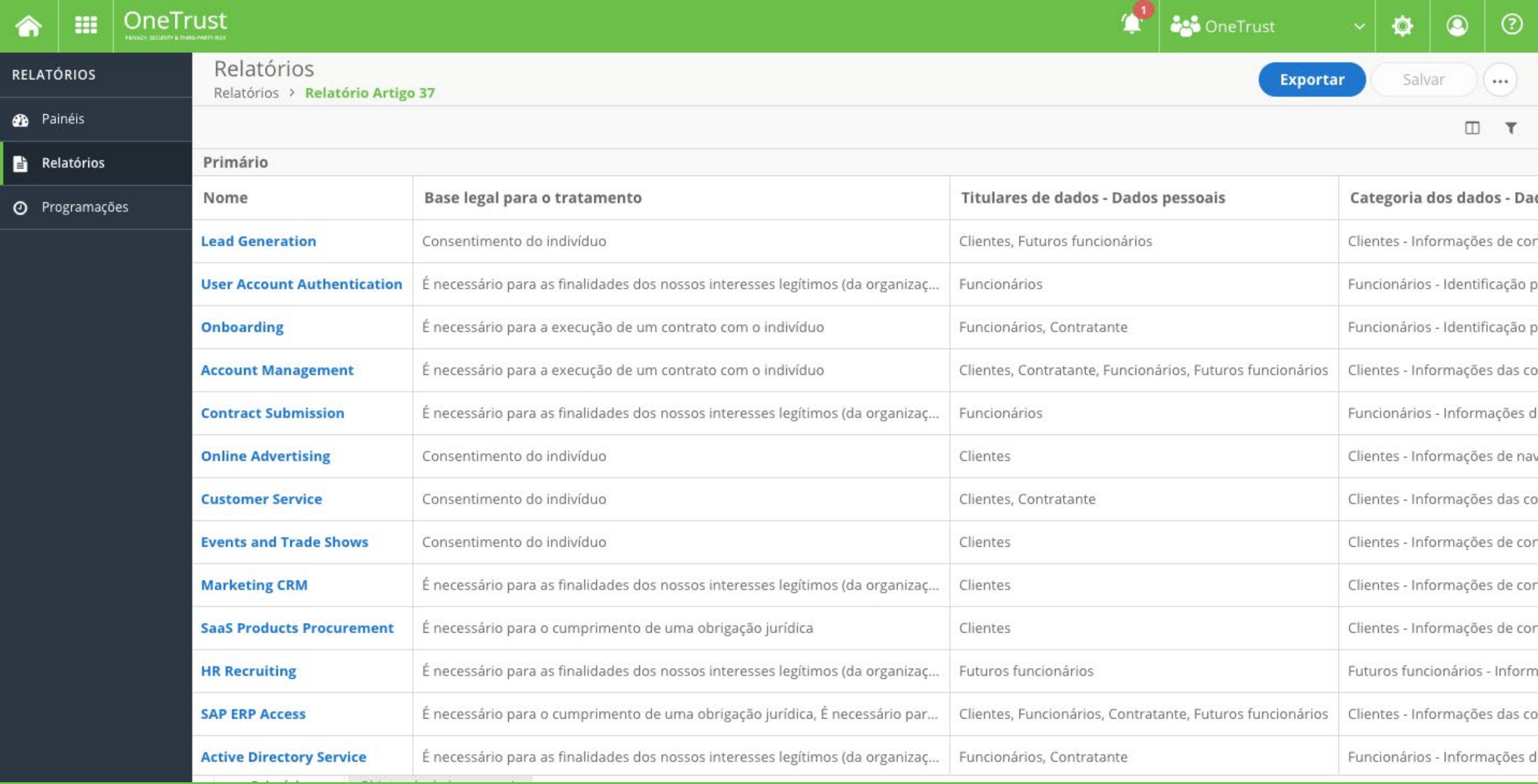
Records of Processing Activities

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



REPORTS| ART. 37

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)

CIPL Centre for Information Policy Leadership — HUNTON ANDREWS KURTH

CEDIS

OneTrust PRIVACY, SECURITY & TRUST

MAPEAMENTO DE DADOS
Painel
Avaliações
Registro dos riscos
Inventário
Ativos
Atividades de tratamento
Entidades
Fornecedores
Reportar
Mapa de ativos
Transfronteiriço
Linhagem de dados
Relatórios
Configuração
Definições de Mapeam...

Mapa de ativos

Filtros

Grupo da organização

OneTrust

Interno ou de terceiros

De terceiros

Interno

DATA MAPPING | ASSETS MAP

OneTrust | Portal de Privacidade

OneTrust

MAPEAMENTO DE DADOS

- Painel
- Avaliações
- Registro dos riscos
- Inventário
  - Ativos
  - Atividades de tratamento
  - Entidades
  - Fornecedores
- Reportar
  - Mapa de ativos
  - Transfronteiriço
  - Linhagem de dados
  - Relatórios
- Configuração
- Definições de Mapeam...

Transfronteiriço

Filtrar por atividade de tratamento: Todas

DATA MAPPING| CROSS BOARDER

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

Identify the Need to Prepare the RIPD

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.

Personal Data Protection Impact Report (RIPD)

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

CIPL Centre for Information Policy Leadership HUNTON ANDREWS KURTH CEDIS OneTrust PRIVACY, SECURITY & TRUST

General Information on Consent

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

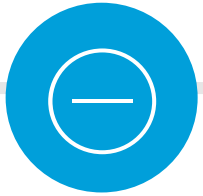
Specific and informed consent, distinct for the transfer purpose

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

Request deletion of personal data where processing is based on consent

Request information on the possibility of denying consent and the consequences of a denial

Revoke consent for free at any time

Oppose processing based on a waiver of consent where the processing does not comply with the LGPD

Data portability: electronic portable, readily useable format

Questions and Answers

Thank You

Centre for Information Policy Leadership
www.informationpolicycentre.com

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

@THE_CIPL

@centre-for-information-policy-leadership

Centro de Direito, Internet e Sociedade of Instituto Brasiliense de Direito Público (CEDIS-IDP)
https://www.idp.edu.br/cedis/

@CedisIDP

@SEJAIDP

OneTrust Privacy Software
https://www.onetrust.com/

@OneTrust

@OneTrust