Brazil general data protection law
LGPD

SÉRGIO LUÍS RIBEIRO
sribeiro@cpqd.com.br
Historical

- Early 2010 - Brazil starts the discussion in the congress.
- August 2018 - Brazil approved the General Data Protection Law.
- December 2018 - Brazil establish the National Authority Data Protection.
- December 2020 - Transition and adaptation period.
LGPD creates a new legal framework for the use of personal data in Brazil. Brazil already has more than 40 legal rules at the federal level. LGPD is replacing and supplementing this sectorial regulatory framework. The LGPD is the result of a broad discussion. Foster economic, technological and innovation development.

Brazil enters the roll of more than 100 countries that today may be considered to have an adequate level of protection of privacy and the use of personal data.
Like the GDPR, the LGPD ensures and define:
- a number of rights for data subjects;
- several lawful bases for data processing.

Introduces requirements for:
- processing of sensitive personal data;
- international transfer of data.

Concepts of privacy by design and privacy by default.
Challenges

- Controllers and processors of personal data in Brazil face a number of challenges. There is a general unawareness of the importance of the protection of privacy and data subjects' rights.
- The country only began discussing comprehensive data protection legislation in 2008.
- LGPD is a fairly recent regulation, controllers and processors lack appropriate technology systems, data governance mechanisms, and ways to allow data subjects to exercise their rights.

General lack of clear rules on data protection.
Challenges

- There are also general difficulties in:
  - obtaining consent;
  - identifying the legal bases for data treatments;
  - ways to ensure employees and stakeholders are properly involved with data flows and comply with the rules.

Will have to keep finding creative ways to enhance technology, and foster free competition
**What we expect**

- The LGPD will have an impact on society as few laws have had before.
- Companies from all sectors will have to adapt in a new culture.
- Appropriate use of data has to be formed.
- Companies need to conform to today’s rules and understand that anticipating future regulation is an investment and a competitive advantage.

Protection of personal data should not be seen as a cost, but as a competitive advantage, a market differential.
Excluding multinationals, only 15% of Brazilian companies are in compliance with LGPD.

For that companies 64% do not know where their sensitive content is located and who can access it.

At least 30% of organizations will spend on LGDP-related consultancies and implementations.

Risk and privacy management related to digital transformation initiatives will drive spending on security services by 2020 in more than 40% of organizations.

Gartner
Approach

**DATA FLOW MAPPING**
Mapping of personal data that is used in the company's activities.

**RISK ASSESSMENT**
Risk assessment in the scope of personal data and potential risks of leakage.

**LGPD COMPLIANCE STRATEGY**
Action plan definition to adjust the company in the LGPD.
Risk Management
LGPD Compliance Strategy

- Secure channel
- Development security
- Access control
- Security operations
- Pseudonymization & Anonymization
- Cryptography

Data leak protection
- Security architecture
- Risk management

Identity protection
- Pseudonymization
- Anonymization

Confidentiality protection
- Cryptography
- Obfuscation
Objective: promote the improvement of eating and physical disorders and also the prevention of the obesity onset for children 224 million school-age children in the world; more than one in three in Brazil, Greece and Spain.

Solution: IoT-based personalised coaching solution guiding children to adopt healthy eating and physical activity behaviour.

Pilots: three pilot sites - Spain, Greece and Brazil.
OCARIoT: Privacy and Security Framework

- Consent permission for processing personal information;
- Start the project applying the principles of *Privacy by Design* and *Security by Design*;
- Clear, enforceable policies for both collection and usage of information;
- Formal processes for risk assessment; and
- Stronger security assurance of the data at rest, in use and in transit.
Risk Assessment

- Context
- Points of Attacks
- Threat
- Security Objective
- Vulnerabilities
- Probabilities
- Impact
- Risk Matrix
- Security Controls
- Action Plan


- Threat Agents: Cracker, User, External agent, Internal agent, OCARIoT Platform

- Assets and Information: Information subject to GDPR and LGPD

- OCARIoT Dashboard

- Security Controls: SC01, SC02, SC03, SC04, SC05, SC06, SC07, SC08, SC10, SC11, SC12, SC13, SC14, SC15, SC16, SC17, SC18, SC19, SC20, SC21, SC22, SC23, SC24

- RISKS: High (R01, R03), Low (R02, R04, R05)

- Threats: Failure, Destruction, Unavailability, Modification, Leakage
LGPD Compliance Strategy

Application and Service Support and Application Support Layer

Network Layer

Device Layer

Management Capabilities

Security Controls

Risk Matrix

Impact

Probabilities

Vulnerabilities

Security Objective

Threat

Points of Attacks

Context

P1

P2

P3

P4

P5

P6

P7

P8

P9

P10

Action Plan

Development Security

Identification

Authorization

Authentication

Network Security

Cryptography

Asset Security

Security Assessment

Site and Safety Security

Monitoring

Sec. Risk Man.

Security Policy

Privacy Policy

Sec. Operat.

Incident Resp.

LGPD Compliance Strategy
Remarks and Conclusion

**Project**: use the security by *design* and privacy by *design*, since the start. The project should be planned and developed using these approaches for a product life cycle (design, deploy, maintain, update, retire and replace) always thinking in security and privacy.

**Devices**: design security and access policies for each device type (risk based) to determine the best and correct protection mode (controls).

**Applications**: follow authentication best practices.

**Data**: design security policies for each type of data (risk based), considering the data in use, in rest and in transit.

**Connections**: use secure network infrastructure, secure protocols and encryption data when needed (risk based).
Thanks!

Connect to the new

SÉRGIO LUÍS RIBEIRO
sribeiro@cpqd.com.br
www.cpqd.com.br