



IESB University Center
Brasilia/DF - Brazil



André de Freitas Fernandes
andre.fernandes@serpro.gov.br

Grazielle A Viana Matias
grazielle@m2cloud.com.br

Fabiano Camilo Santiago de Brito
fabianocamilos@gmail.com

Mariana Sbaite Gonçalves
marianasbaite@gmail.com

Fátima Fernandes Periard
fatima.periard@crmbrasil.com.br

MSc. Reinaldo Gomes Balduino Filho
reinaldo.baldoino@iesb.edu.br

THE ISO 27000 FAMILY AND ITS APPLICABILITY IN LGPD ADAPTATION PROJECTS FOR SMALS AND MEDIUM-SIZED

*How the ISO 27000 family standards can help with the challenge of complying with the
General Data Protection Law for small and medium-sized businesses*



GRAZIELLE VIANA MATIAS

São Paulo/ SP - **Brazil**

2021 - **MBA** in Data Protection Officer

IESB University Center | Brasilia / DF – Brazil

2020 - **Data Protection Officer** - Exin

Entrepreneur

Founder of M2 Solution Company

More than 20 Years leading technology projects focused on business

LGPD Specialist - Compliance and information security projects for small and medium-sized enterprises

Member of ANPPD – National Association of Data Protection Professionals:

Ciber Security Advanced Group

Content Group

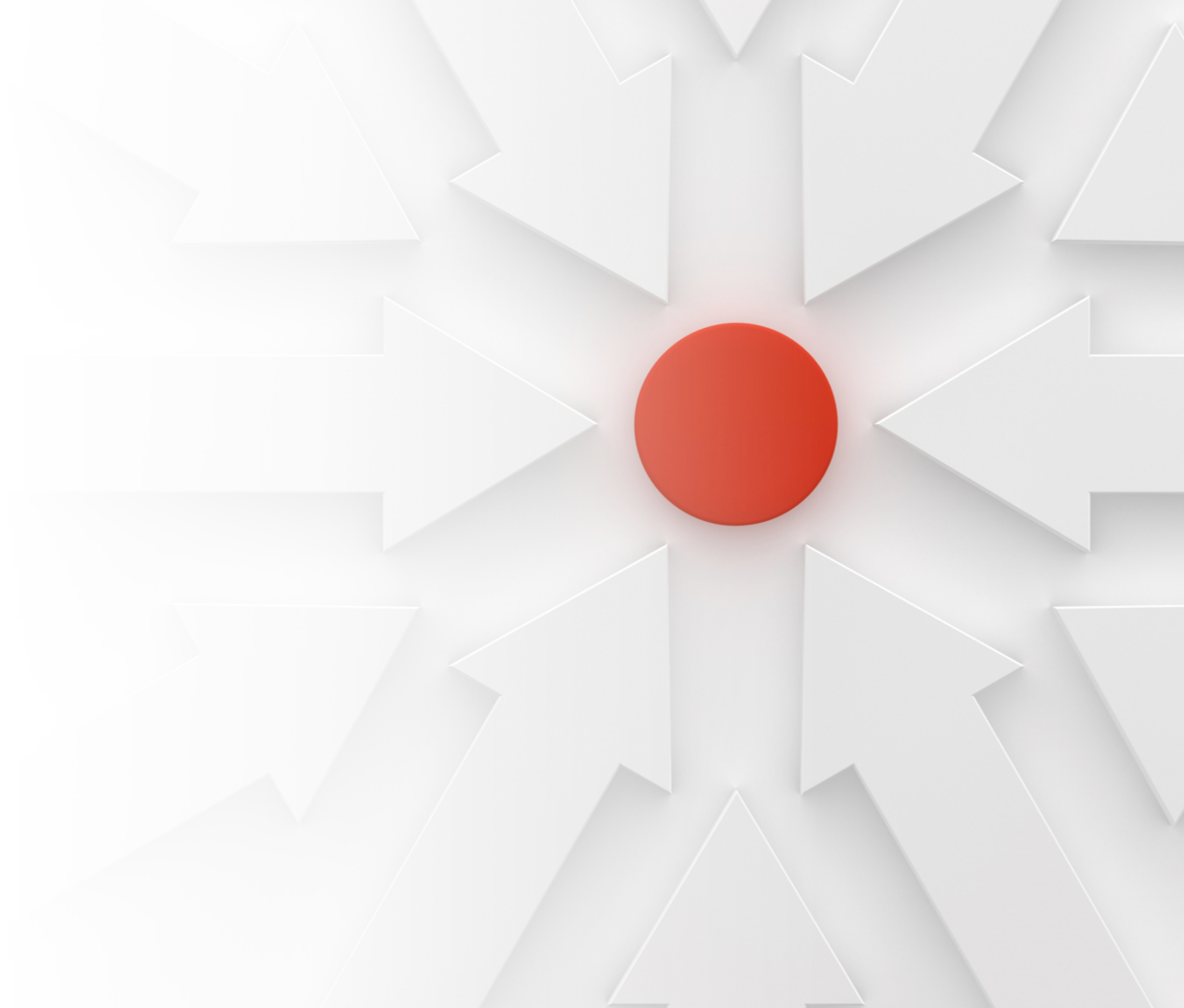
Woman in LGPD

Supervisor Group



OUR INTERESTS AND GOALS

- To work as propagators of privacy and data protection culture in Brazil
- Actively participate in compliance projects
- Act in study groups and exchange information
- Make the compliance process more practical, alive and real in people's and organization's daily routines





About the Brazilian Data Protection Regulation

Law 13.709/ 2018

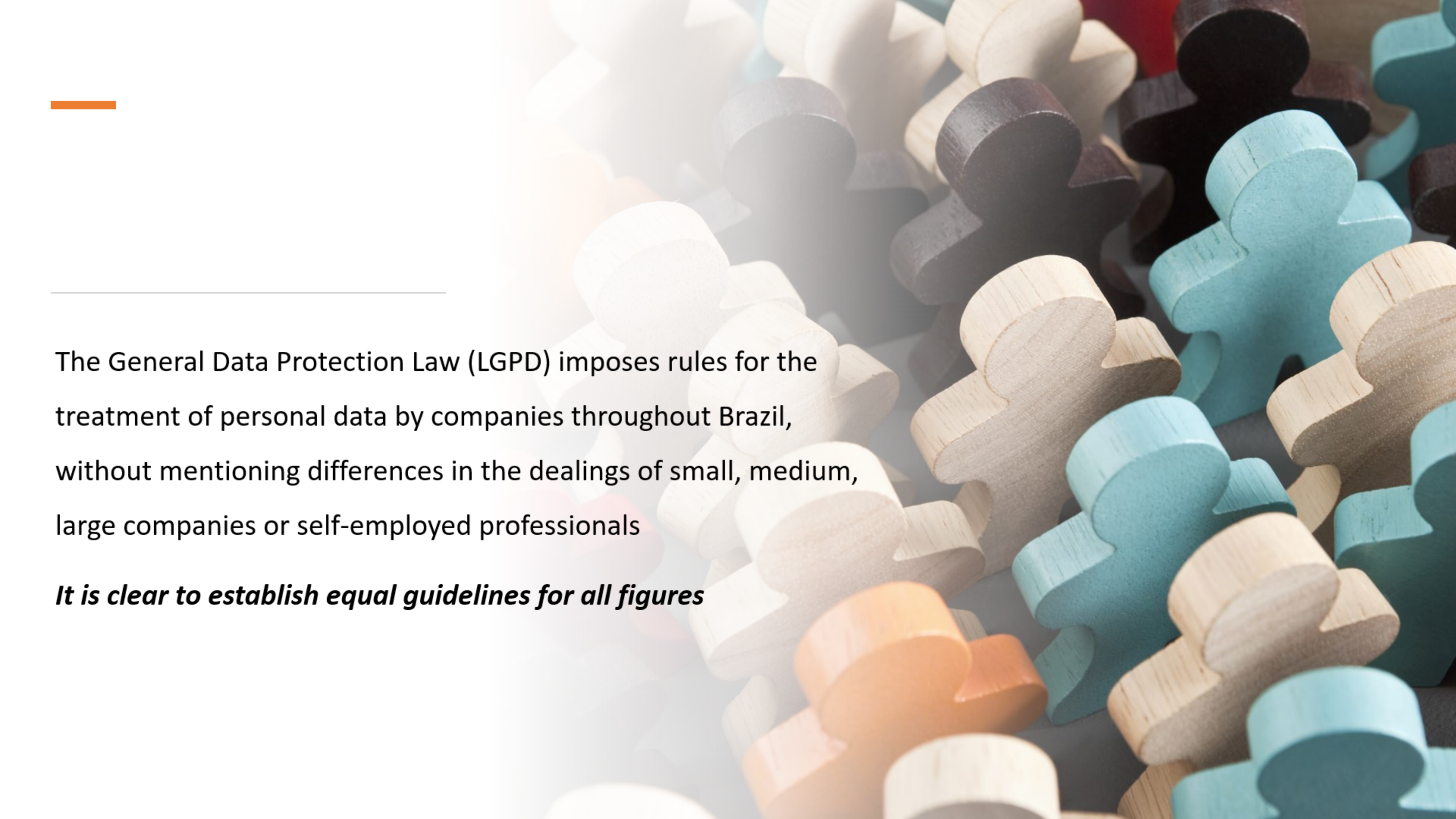
Based on GDPR – European

Sanctioned in 2018, august

Validity since 2020, September

Sanctions since 2021, august





The General Data Protection Law (LGPD) imposes rules for the treatment of personal data by companies throughout Brazil, without mentioning differences in the dealings of small, medium, large companies or self-employed professionals

It is clear to establish equal guidelines for all figures

The Brazilian SMEs

SME is an acronym for Small and Medium Enterprise

It is used to classify the size of a company in function of its number of employees and its annual income



Classifications according to the
number of workers employed

- **Industry**

- Microenterprise - up to 19 employees
- Small Business - from 20 to 99 employees
- Medium Company - from 100 to 499 employees
- Large Company - 500 or more employees

- **Trade and Services**

- Microenterprise - up to 9 employees
- Small Business - 10 to 49 employees
- Medium Company - 50 to 99 employees
- Large Company - more than 100 employees



Classification by billing

Individual Microentrepreneur:

Annual turnover up to USD 14.000

Microenterprise:

Annual turnover up to USD 66.000

Small Business:

Annual turnover between USD 1.980 and USD 828.000

Small Farmer:

Property with up to 4 fiscal modules or annual sales of up to USD 828.000



The economic Strenght of SMEs

19 million companyes in Brazil

7.5 million are SMEs

Toghether, the SMEs account for 29% of GDK – Gross Domestic

Products in Brazil Market

A close-up photograph of a complex knot made from several ropes. The ropes are multi-colored, featuring yellow, blue, red, and white. The knot is intricate, with multiple loops and crossings. The background is a soft, out-of-focus grey.

The Challenge

- It is neither easy nor cheap to adapting to the LGPD
- The companies need to structure themselves to have the budget and human resources to put into practice everything required by the Law
- Is a hard work for the SMEs , not only due to lack of investment, but also for lack of information
- The law requires a DPO figure in all companies





How to achieve the compliance?

According to the law:

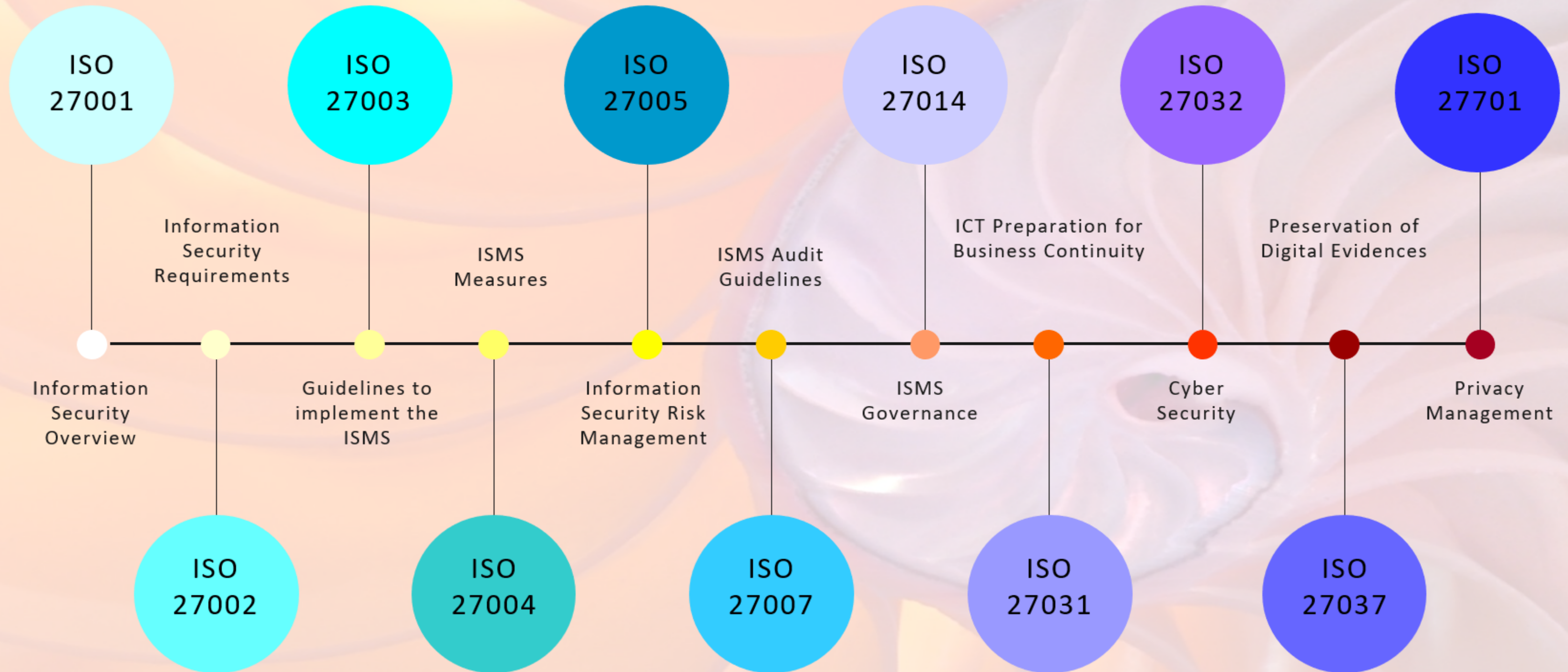
- Adopting **technical** and **administrative measures** to maintain the security and confidentiality of information
- Defining a **governance plan** and applying **good practices** in order to protect and maintain the security of all personal data involved in business flows and/or processes




ISO 27000 family of standards comes into play

- Address cybersecurity
- Brings a clarity on business process structure

A Tour into ISO 27000 standards





Security and privacy approach in ISO 27001 and ISO 27701 Standards

ABNT NBR ISO/IEC 27001	ABNT NBR ISO/IEC 27701
Information Security	Information Security and Privacy
Information Security Policies	Privacy and Information Security Policies
Information Security Management	Information Security Management and Information Privacy
Information Security Management System (ISMS)	Privacy Management System
Information Security Objectives	Information Security and Privacy Objectives
Information Security Performance	Information Security and Privacy Performance
Security Information Requirements	Security Information and Privacy Requirements
Information Security Risks	Information Security and Privacy Risks
Information Security Assessment	Security Risk Assessment of Information and Privacy
Treatment of Security Risks of Information	Treatment of Security Risks of the Information and Privacy



Escalation to compliance

From risk definition to business continuity and response plan, the ISO 27000 family provides a robust framework, and offers a guidance related on:

- How to identify risks related to the processing of personal data
- Reinforce the need for policies
- Internal and external contractual agreements

Items that are unknown to most small and medium-sized companies

The biggest cost is
**the non-investment in
information security**

90% of intrusions are directed to
the systems of small and
medium-sized companies



The background of the slide is a dark field filled with numerous light bulbs. Most of the bulbs are dark and unlit, but one bulb in the center-left area is brightly lit, creating a strong contrast with the dark background. This visual metaphor likely represents a single idea or conclusion standing out from many others.

Conclusion

The ISO 27000 Family standards can help small and mid-sized companies to achieve their compliance with the Data Protection Regulations not only in Brazil, but in the world, while helping these businesses to improve their information security.

A close-up, low-angle shot of a human hand reaching upwards, palm facing up. The hand is positioned in the lower-left quadrant of the frame. The background is a bright, hazy sky with a large, glowing sun in the upper-left corner, creating a strong lens flare effect. A faint rainbow is visible in the background, arching across the sky. The overall color palette is warm, dominated by yellows, oranges, and soft blues.

Thank You!