

GDPR

O que é a nova lei europeia de privacidade e como se preparar?

Matheus Vanzella

Matheus Vanzella

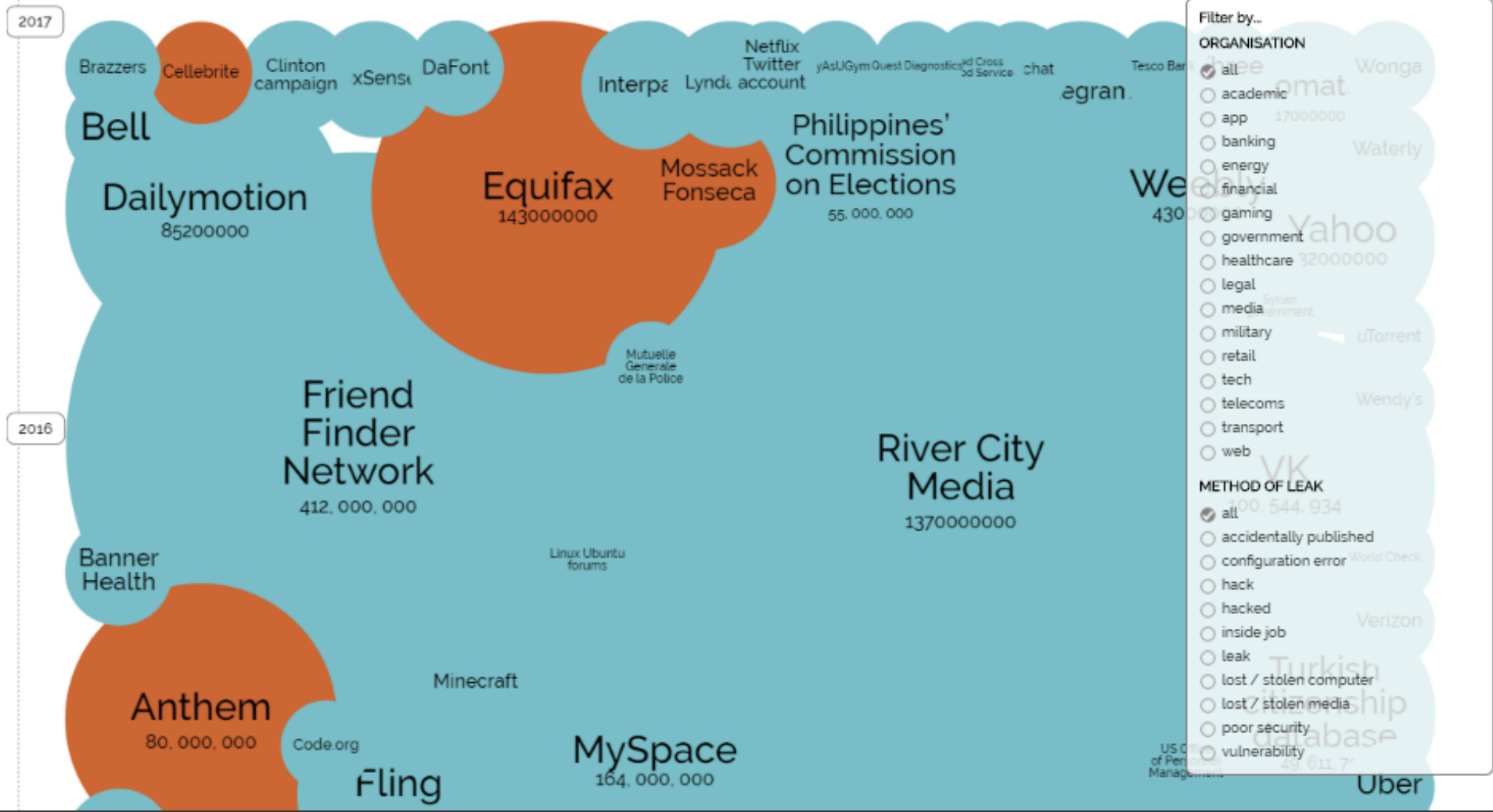
- Consultor de Segurança da Informação – iBLISS Digital Security
- Experiência em análise de Processos de Segurança e Pentester
- Palestrante iniciante:
 - Virada Tecnológica
 - Cryptoparty
 - Semana da FCI – Universidade Mackenzie
 - BsidesBDX - França

World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 10th Sep 2017)

interesting story



NEWS

Technology

Massive Equifax data breach hits 143 million

8 September 2017 Technology



Share



GETTY IMAGES

Top Stories

Irma will be 'devastating' to US

46 minutes ago

'Like nothing I have ever known'

3 hours ago

Strongest quake in century hits Mexico

43 minutes ago

Features



My brother's killer is now my friend

EDP, NOS e PT apanhadas a partilhar dados de clientes

18.09.2017 às 13h31



ILUSTRAÇÃO CRISTINA SAMPAIO

Contactos de novos clientes da elétrica cedidos ilegalmente a operadoras de comunicações. Empresas desmentem mas Comissão Nacional de Proteção de Dados confirma casos e abertura de processos-crime

PUBLICIDADE



Zendesk - Site oficial

O Zendesk facilita e otimiza a comunicação com os clientes. Experimente já.

Zendesk





22 SET 17

77

Exclusivo: atendentes da C&A vendem dados de clientes por R\$ 50 na internet

Agenda

- Privacidade de dados no Brasil
- Privacidade de dados na América Latina
- Privacidade de dados na Europa
- General Data Protection Regulation (GDPR)
- Desafios da GDPR
- Pontos-chave da GDPR
- Privacy Impact Assessment (PIA)
- Objetivos do PIA
- Transferência internacional de dados
- Como serei afetado?
- Como devo me preparar?
- Por onde devo começar?

Privacidade de Dados: Brasil, América Latina e Europa

Marco Civil da Internet

No Brasil, ainda não há uma lei específica sobre privacidade de dados que dite a forma como lidar com os dados, porém o Marco Civil, sancionado em 2015, define os deveres para operações que lidam com dados confidenciais.

Lei Carolina Dieckmann

Nome que ficou conhecida a lei 12.737/2012 que altera o código penal brasileiro e tipifica os delitos ou crimes informáticos.

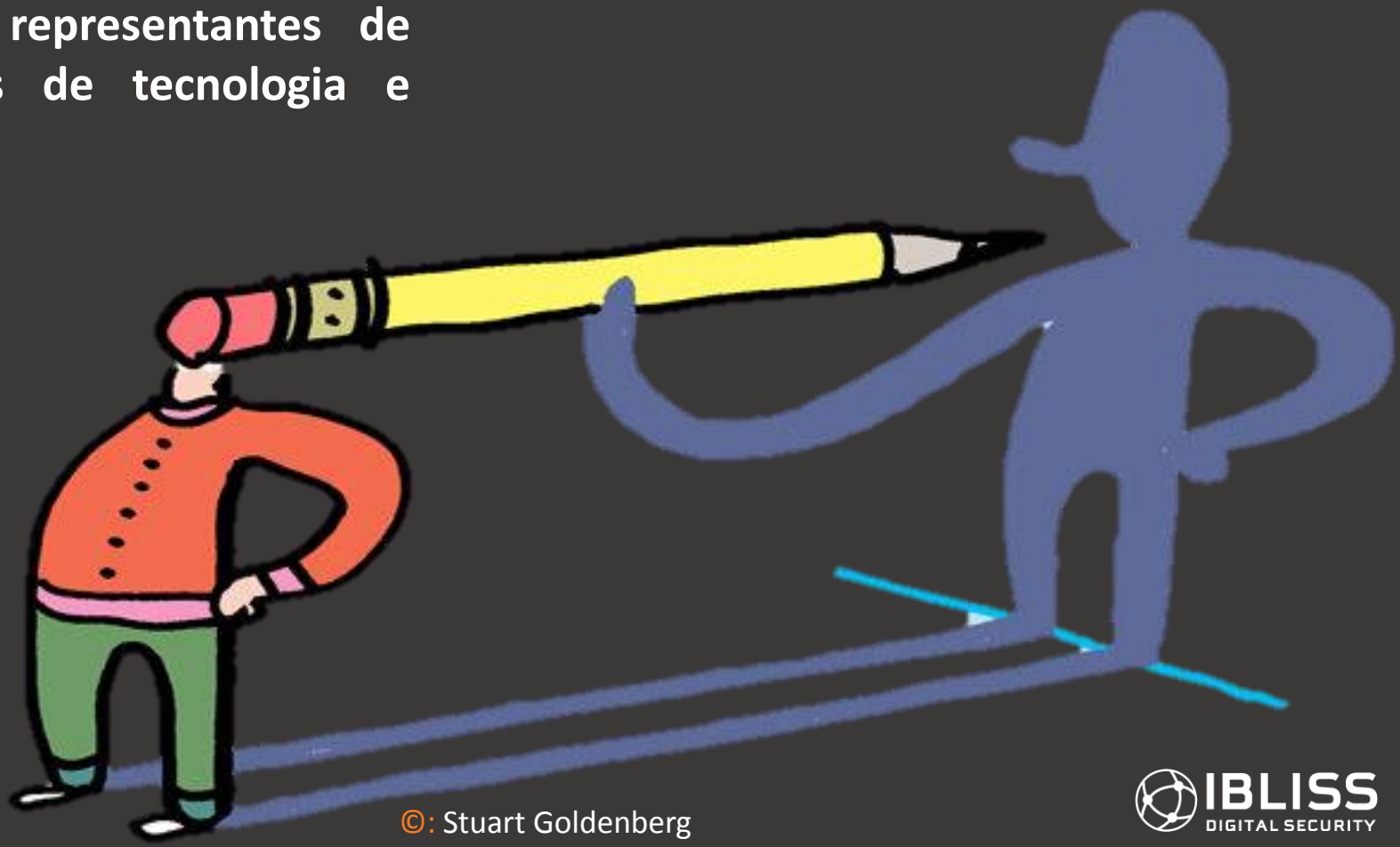
PL 5276/2016 - PL 4060/2012

PL 6291/2016 - PLS 330/2013

Projetos de leis que visam criar uma lei geral de proteção de dados brasileira.

Privacidade de Dados no Brasil

Em 12 de Junho de 2017 o *Direito ao esquecimento* começou a ser debatido pelo STF no Brasil, por meio de uma audiência pública que reuniu representantes de associações de jornalistas, empresas de tecnologia e especialistas.



Privacidade de Dados na América Latina



Ref: <https://www.dlapiperdataprotection.com/>

Privacidade de Dados na Europa

12

ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

23. 11. 95 EN Official Journal of the European Communities No L 281/31

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 24 October 1995
on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF
THE EUROPEAN UNION,

Having regard to the Treaty establishing the European
Community, and in particular Article 100a thereof,

Article 7a of the Treaty, the free movement of
goods, persons, services and capital is ensured
require not only that personal data should be able
to flow freely from one Member State to another,
but also that the fundamental rights of individuals
should be safeguarded;

General Data Protection Regulation (GDPR)

The screenshot shows the website ec.europa.eu/justice/data-protection/. The page features the European Commission logo and the word 'JUSTICE' with the tagline 'Building a European Area of Justice'. A green callout box indicates a 'Last update' on '24/11/16'. The main heading is 'Protection of personal data'. A sidebar on the left lists various topics under 'DATA PROTECTION', including 'Reform of the data protection legal framework', 'Data transfers outside the EU', 'Article 29 working party', 'Opinions and recommendations', 'Entities collecting data', 'Protecting your personal data', and 'Data protection bodies'. The main content area contains text about the reform, stating that in January 2012, the Commission proposed a comprehensive reform of data protection rules in the EU. It notes that the Regulation will enter into force on 24 May 2016, but apply from 25 May 2018, while the Directive enters into force on 5 May 2016. A highlighted sentence states: 'The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business.' The page also includes a search bar and navigation links like 'HOME' and 'ALL TOPICS'.

ec.europa.eu/justice/data-protection/

Glossary | About this site | Contact | Cookies | Legal notice | English (en)

European Commission

JUSTICE
Building a European Area of Justice

Last update
24/11/16

European Commission > Justice > Data protection

HOME ALL TOPICS Search

DATA PROTECTION

Protection of personal data

Reform of the data protection legal framework

Data transfers outside the EU < In January 2012, the European Commission proposed a comprehensive **reform of data protection rules in the EU**.

Article 29 working party < On 4 May 2016, the official texts of the Regulation and the Directive have been published in the EU Official Journal in all the official languages. While the **Regulation** will enter into force on 24 May 2016, it shall apply from **25 May 2018**. The **Directive** enters into force on 5 May 2016 and EU Member States have to transpose it into their national law by **6 May 2018**.

Opinions and recommendations <

Entities collecting data < **The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business.** The data protection reform is a key enabler of the Digital Single Market which the Commission has prioritised. The reform will allow European citizens and businesses to fully benefit from the digital economy.

Protecting your personal data <

Data protection bodies < **Take control of your personal data**

73%

OF DATA PRIVACY PROFESSIONALS BELIEVE THAT

The GDPR is the **MOST IMPORTANT CHANGE** IN DATA PRIVACY REGULATION IN THE PAST 20 YEARS²

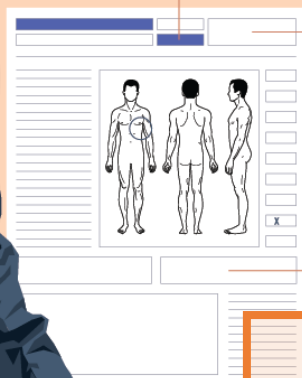
WHAT TYPES OF E.U. CITIZEN DATA

DOES THE GDPR AIM TO PROTECT?



Name
Location data
Identification numbers
IP addresses
Cookie data
RFID tags

Personal data Sensitive personal data



Health data
Genetic data
Biometric data
Racial or ethnic data
Political opinions
Sexual orientation

82%

OF DATA PRIVACY PROFESSIONALS BELIEVE THAT

The GDPR will have a **POSITIVE IMPACT** ON CONSUMER DATA PROTECTION²

PII e SPI

Qualquer informação sobre um indivíduo que pode ser utilizada para identificá-lo, seja por nome, RG ou até mesmo dados médicos e biométricos devem estar garantidamente protegidas.

Pontos-chave:

- Data subject
- Consent
- Data controller & Data processor
- O que acontece com quem não estiver em conformidade?
- Definição de um Data Protection Officer (DPO)
- Negócios com a Europa



Desafios da GDPR



©: [Http://slane.co.nz](http://slane.co.nz)

- Onde estão meus dados?
- O que você faz com meus dados?
- Quais são meus direitos?
- Quem será o DPO?
- Hackeado! E agora?!



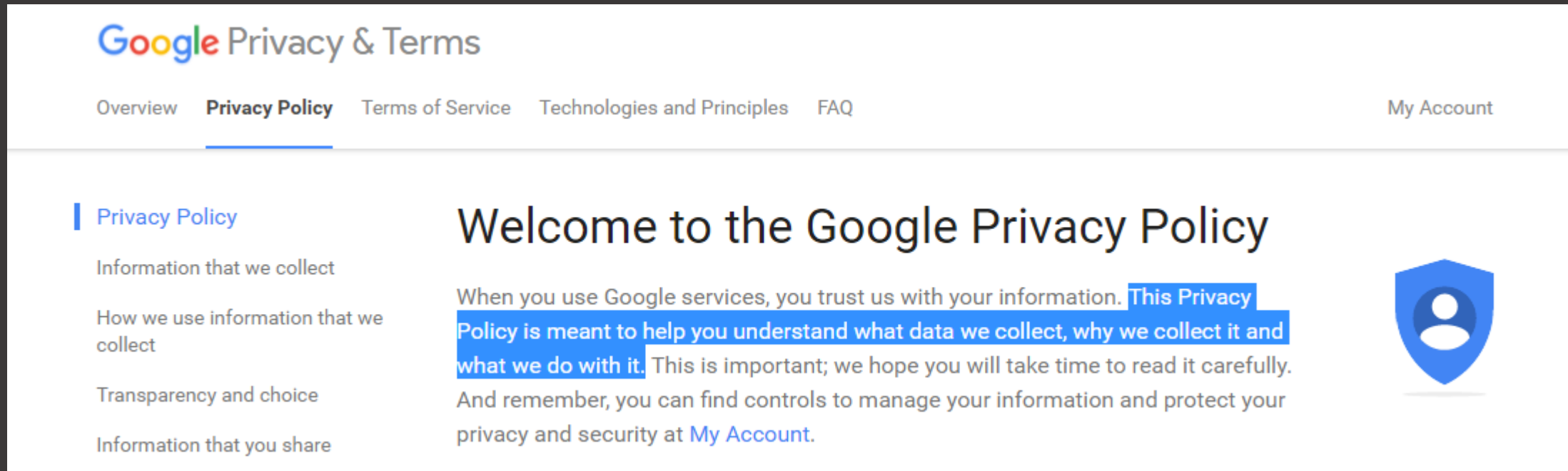
E em relação às crianças?

Princípios da GDPR

Princípios da GDPR

- 1** **Legalidade e transparência**
- 2** **Propósito e meios de coleta**
- 3** **Limitação de coleta (minimização)**
- 4** **Exatidão**
- 5** **Limitação de armazenamento**
- 6** **Segurança**

Política de Privacidade



The screenshot shows the Google Privacy & Terms page. At the top left is the Google logo followed by "Privacy & Terms". Below this is a navigation menu with "Overview", "Privacy Policy" (highlighted with a blue underline), "Terms of Service", "Technologies and Principles", and "FAQ". On the right side of the navigation menu is "My Account". On the left side of the main content area is a vertical list of links: "Privacy Policy" (with a blue vertical bar to its left), "Information that we collect", "How we use information that we collect", "Transparency and choice", and "Information that you share". The main content area features a large heading "Welcome to the Google Privacy Policy". Below the heading is a paragraph of text: "When you use Google services, you trust us with your information. This Privacy Policy is meant to help you understand what data we collect, why we collect it and what we do with it. This is important; we hope you will take time to read it carefully. And remember, you can find controls to manage your information and protect your privacy and security at My Account." To the right of the text is a blue shield icon with a white person silhouette inside. The "My Account" link in the text is highlighted in blue.

Como as empresas ficam em conformidade com a GDPR?

Privacy Impact Assessment (PIA)

Privacy Impact Assessment (PIA)

Avaliação geral para do tratamento de dados pessoas na empresa

- Identificar dados pessoais (SPI and PII)
- Categorizar os dados
- Avaliar o propósito da coleta de dados
- Avaliar o ciclo de vida dos dados

Objetivos do PIA

- Conformidade
- Mitigação de riscos
- Avaliar medidas de proteção atuais
- Deve ser conduzido periodicamente ou sempre que um novo sistema é implantado



©: [Http://slane.co.nz](http://slane.co.nz)

Transferência internacional de dados pessoais

- Como realizar?
- Propósito
- Quais são as vantagens?
- E na prática?



E minha empresa, como fica?

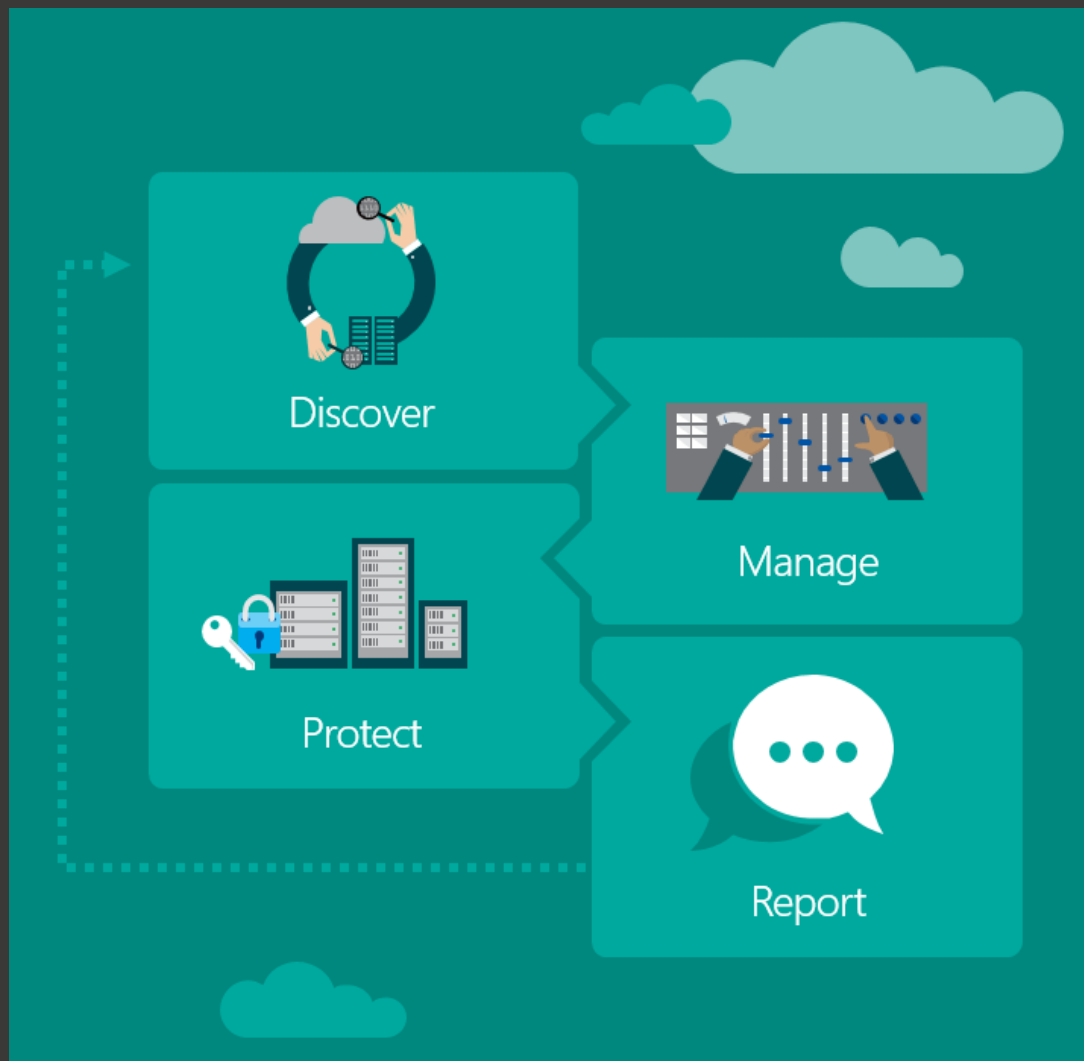
Como **serei** afetado?

A não-conformidade pode custar caro!

- Para meu bolso.
- Para minha imagem.



Como devo me preparar?



Conheça e controle seus dados!

Ref: <https://www.microsoft.com/en-us/trustcenter/privacy/gdpr>

Por onde devo começar?

- Defina um DPO (Data Protection Officer)
- Identifique PII e SPI nos sistemas
- Identifique os donos dos sistemas
- Implante medidas de segurança em todo o ciclo de dados (Coleta, armazenamento, processamento e destruição)
- Planeje os requisitos de transparência
- Treinamentos específicos



Preparing for the General Data Protection

Regulation (GDPR) 12 steps to take now

1 Awareness
You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.



5 Subject access requests
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Lawful basis for processing personal data
You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7 Consent
You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8 Children
You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9 Data breaches
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments
You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11 Data Protection Officers
You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 International
If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

Obrigado!

MATHEUS VANZELLA

Matheus.Vanzella@ibliss.com.br

www.ibliss.com.br

