General Data Protection Regulation (GDPR)

Renato Leite Monteiro

CGI.br – 27.04.18

Doutorando em Filosofia do Direito na Universidade de São Paulo e Mestre em Direito Constucional plela UFC. LL.M em Technology Law pela NYU e NUS. Foi consultor do Ministério da Justiça para o Anteprojeto de Proteção de Dados e study visitor do Departamento de Proteção de Dados Pessoais do Conselho da Europa.
Fundador do Data Privacy.br

AGENDA

1. O que é a GDPR e o seu contexto?

2. A espinha dorsal da GDPR: um sobrevoo

a) Aplicação Extraterritorial;

b) Escopo de Aplicação – dados pessoais, anonimizados e pseudoanonimizados

c) Direitos dos Titulares;

d) Controllers e Processors

e) Enforcement;

f) Transferência internacional

3. Estrutura da GDPR

O que é a GDPR?

Contextualizando...

Progresso Geracional de Proteção de Dados Pessoais na Europa

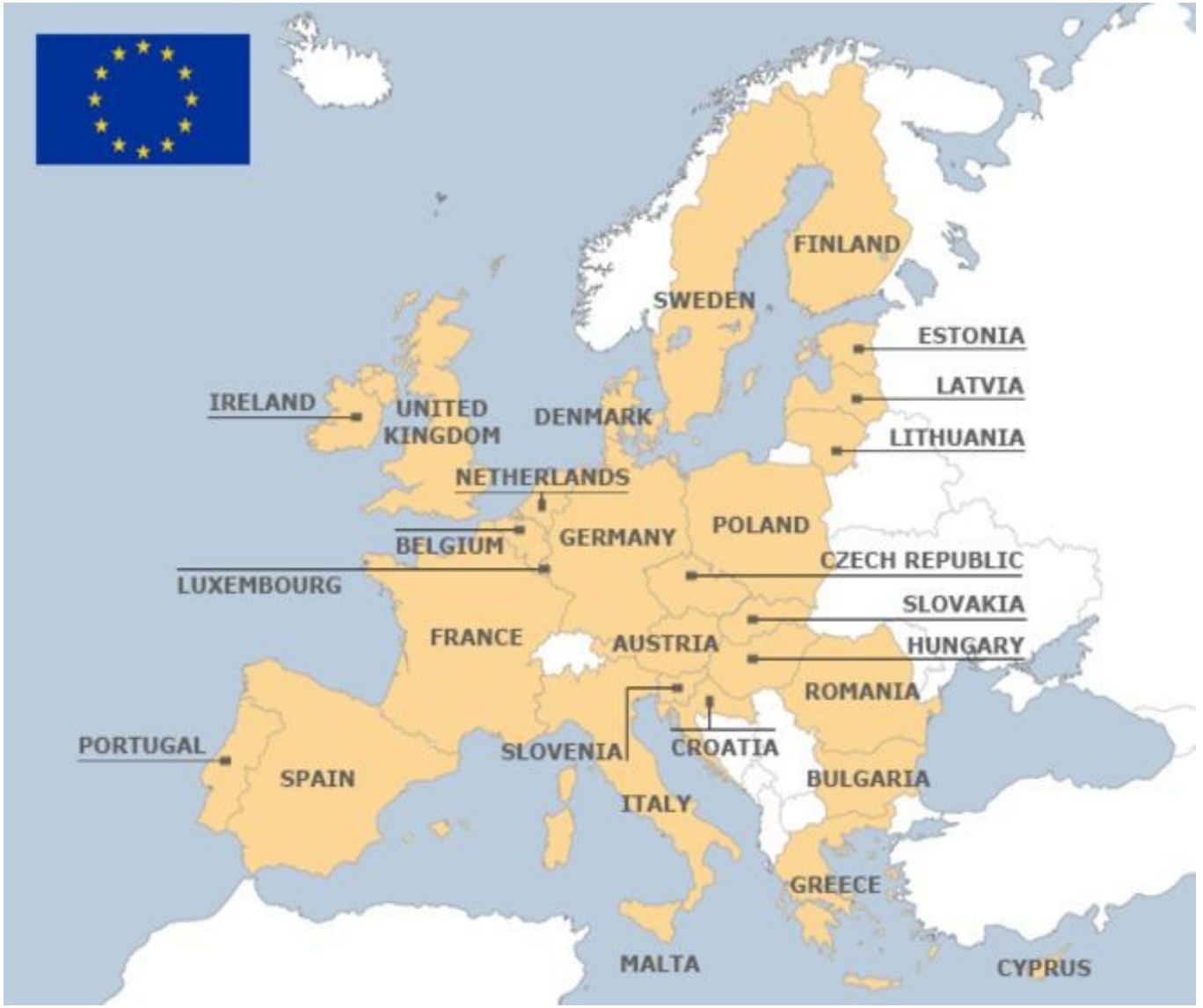
Confiança

(Economia e Sociedade baseada em dados)

DATA-DRIVEN SOCIETY

União Europeia

- **Bloco: integração econômica e política**
  - Livre Fluxo de Informação
  - Uniformidade normativa
- **Diretiva versus regulamento**
  - Aplicação indireta *vs* direta
  - Fragmentação
  - Transposição nacional e pluralidade de normas
- Considerandas (2), (3), (5), (8), (10), (41)




European Commission
Why we need a
Digital Single Market
315 million
Europeans
use the
Internet
every day
A Digital Single Market
can create up to
€340 billion in additional growth,
hundreds of thousands of new jobs,
and a vibrant knowledge-based society

Aplicação extraterritorial

aplicação extraterritorial – além da UE

- aplicação extraterritorial que alcança empresas brasileiras com filiais na União Europeia ou que ofertem serviços ao mercado europeu
- Aplica-se: empresa com filial ou representação na União Europeia ("EU")
- Aplica-se: empresa, mesmo sem presença física na EU, mas que oferece serviços ao mercado europeu
- Aplica-se: empresa, mesmo sem presença física na EU, que coleta dados de pessoas naturais localizadas na EU, independente da nacionalidade.
- Aplica-se: empresa, mesmo sem presença física na EU, que monitora pessoas naturais localizadas na EU, independente da nacionalidade.
- Aplica-se: empresa, mesmo sem presença física na EU, que terceiriza o processamento de dados para empresas localizadas na EU

aplicação extraterritorial – além da UE

Pessoa natural

Empresa localizada fora UE

Pessoa natural localizada fora na UE

Monitora/fornece serviços ou produtos

A pessoa natural está na UE durante o processamento (coleta ou outro tratamento)?

Os dados da pessoa natural são processados por Controller/Processor estabelecido na UE?

Fornece serviços/produtos/monitora/ perfilha/processa/ dados de pessoas naturais localizadas na UE?

Sim

Sim

Sim

Aplica-se a GDPR

Não

Não

Não se aplica a GDPR

Escopo de Aplicação
Dado Pessoal

Conceito de Dado Pessoal

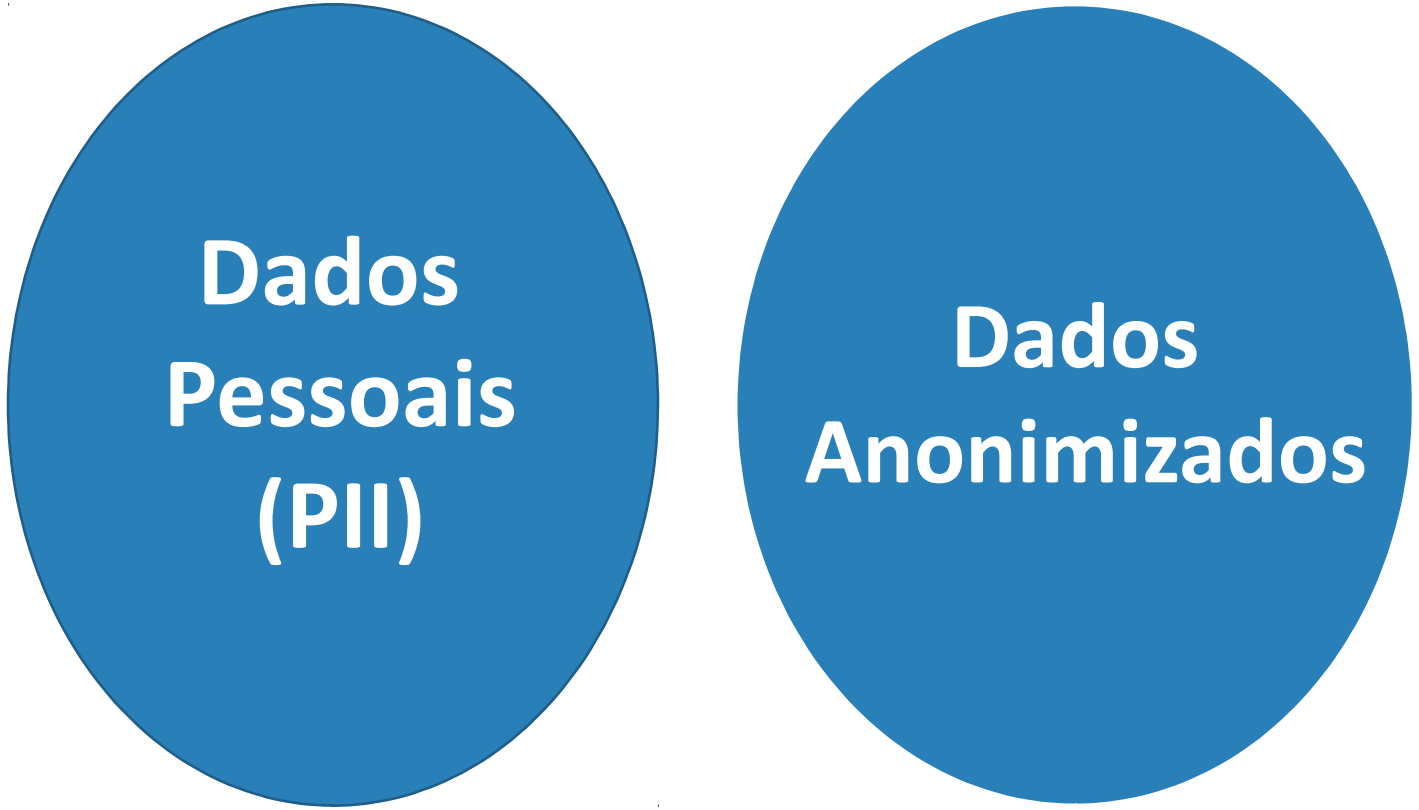
Vocabulário Analítico

Expansionista	Reducionista
Pessoa identificável	**Pessoa identificada**
Pessoa indeterminada	**Pessoa específica/determinada**
Vínculo mediato, indireto, impreciso ou inexato	**Vínculo imediato, direto, preciso ou exato**
Alargamento da qualificação do dado como pessoal	**Retração da qualificação do dado como pessoal**

Definição de Dado Pessoal

Artigo 4 (1) - GDPR	Artigo 2 (1) - Diretiva
personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;	'personal data' shall mean any information relating to an identified or identifiable natural person (' data subject'); an identifiable person is one who can be identified , directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical , physiological , mental, economic, cultural or social identity
Expansionista (com rol exemplificativo mais extenso)	Expansionista (com rol exemplificativo menos extenso)

Dicotomia



O que é anonimização?

TABELA 1
BASE DE DADOS RELACIONAIS

NOME	CPF	CEP	IDADE	CLASSIFICAÇÃO | SEGMENTAÇÃO
Bruno dos Santos	123.456-77	04055-000	18	Jovem hipster
Bruno dos Santos	234.567-88	04055-111	17	Jovem poupador
Bruno dos Santos	345.678-99	04055-222	17	Jovem consumista
Bruno Souza	456.789-10	01201-000	65	Idoso com rentabilidade
Bruno Souza	567.891-01	04201-111	66	Idosa sem rentabilidade
Bruna Schonberg	222.333.44-55	04201-222	70	Idosa com rentabilidade
Maria Silva	157.890.88-66	09201-000	40	Adulto desempregado
Maria Silva	666.666.66-66	09201-111	38	Adulto perfil executivo
Maria Silva	987.354.22-99	09201-222	16	Jovem hipster

TABELA 2
BASE DE DADOS RELACIONAIS ANONIMIZADA

NOME	CPF	CEP	IDADE	CLASSIFICAÇÃO | SEGMENTAÇÃO
Bruno [redacted]	[redacted]	04055-[redacted]	18 >	Jovem hipster
Bruno [redacted]	[redacted]	04055-[redacted]	18 >	Jovem poupador
Bruno [redacted]	[redacted]	04055-[redacted]	18 >	Jovem consumista
Bruno [redacted]	[redacted]	01201-[redacted]	60 <	Idoso com rentabilidade
Bruno [redacted]	[redacted]	04201-[redacted]	60 <	Idosa sem rentabilidade
Bruna [redacted]	[redacted]	04201-[redacted]	60 <	Idosa com rentabilidade
Maria [redacted]	[redacted]	09201-[redacted]	18 <	Adulto desempregado
Maria [redacted]	[redacted]	09201-[redacted]	18 <	Adulto perfil executivo
Maria [redacted]	[redacted]	09201-[redacted]	18 >	Jovem hipster

33 Bits of Entropy

The End of Anonymous Data and what to do about it

Dado Pessoal Dado Anonimizado

PBS NEWSHOUR

THE RUNDOWN

A BLOG OF NEWS AND INS

HEALTH SUPREME CO

NATION

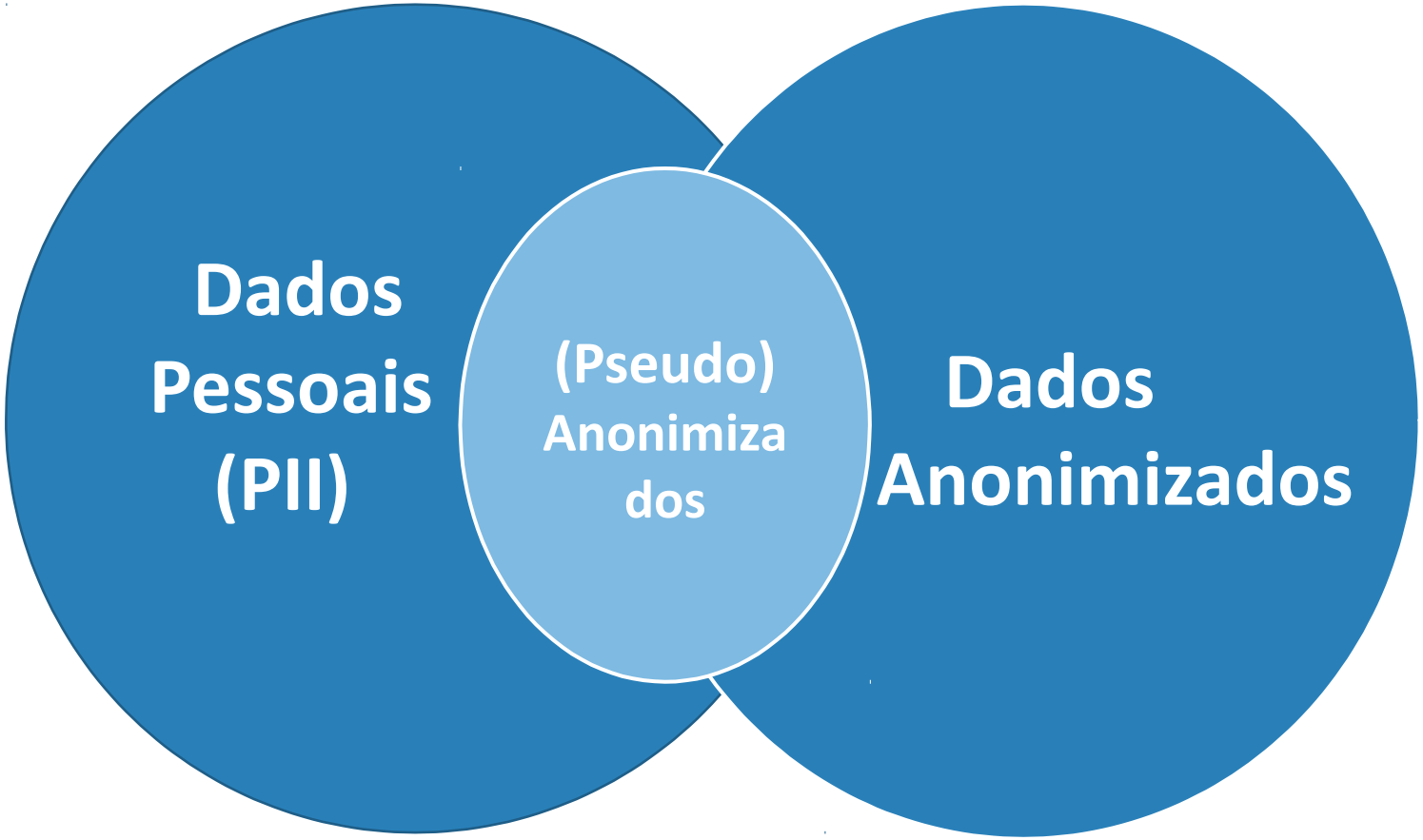
Your ‘anonymous’ credit card data is not so anonymous, study finds

14

EMAIL

BY REBECCA JACOBSON, INSIDE ENERGY *January 29, 2015 at 5:54 PM EDT*

Zona Cinzenta



(Pseudo)Anonimização Artigo 4 (5) GDPR	(Pseudo) Anonimização Consideranda 26	Dados Anônimos Consideranda 26
‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;	Personal data which have undergone pseudonymisation (…) should be considered to be information on an identifiable natural person whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used (...)To ascertain whether means are reasonably (...) should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology	(..) not apply to anonymous information, in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Filtro: Razoabilidade

O que é razoável?

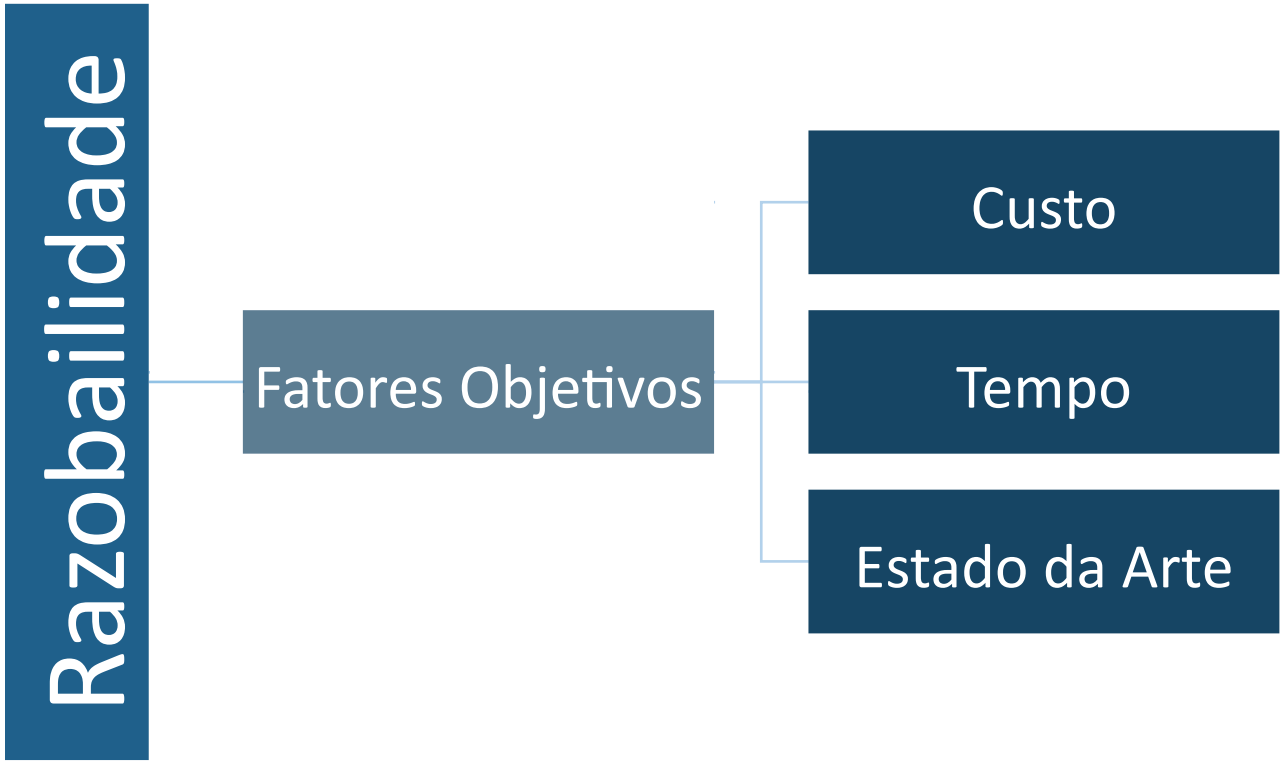
GDPR

Art. 4 (5) ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject

(...)

Recitalas 26 To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used (...)To ascertain whether means are reasonably (...) should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology

Meios Razoáveis



(Pseudo) Anonimização

Consideranda 28

The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

Instrumento de Mitigação de Risco (Segurança da Informação)

The Risk-Based Approach in the GDPR: Interpretation and Implications

By Gabriel Maldoff, CIPP/US, IAPP Westin Fellow

iapp

Anonymization and Risk

Ira S. Rubinstein and Woodrow Hartzog

Anonymous versus personal data: from a binary view to a rigorous risk-based approach*

Gergely Ács† Claude Castelluccia‡ Daniel Le Métayer§
Inria, France

October 30, 2015

Exemplo Prático

Segregação da Base de Dados

Consideranda 29

In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

Instrumento Típico de Segurança da Informação

Direitos dos Titulares dos Dados

direitos do titular e deveres do Controller

- Direito à transparência e à informação **(explicação)**
- Direito ao acesso
- Direito à retificação
- Direito ao apagamento (”**Direito de ser esquecido**”)
- Direito à restrição de processamento
- **Direito a portabilidade de dados**
- Direito à objeção
- **Direito a não estar sujeito a decisões automatizadas com efeitos legais ou similares sobre os titulares**

transparência e informação aos titulares:

- Detalhes de **identidade** e contato do **Controller**
- Detalhes do **contato do DPO**
- **Finalidades** para o processamento dos dados pessoais
- **Base legal** para o processamento dos dados
- **Interesses legítimos** do *controller*, se aplicável
- Destinatários **com quem os dados serão compartilhados**, se aplicável
- **Informações** sobre qualquer **transferência** dos dados para **fora da EU**
- **Tempo** pelo qual os dados serão **armazenados**
- Existência de direito a acesso e retificação, direito a retirar o consentimento
- Informações sobre práticas de análise do perfil, se houver (***profiling***)

Controller e Processor

responsabilização

data controller

- determina o motivo, as finalidades e como os dados pessoais serão processados
- devem estabelecer uma base legal para o tratamento dos dados
- devem fiscalizar os *processors*, pois podem ser responsabilizados conjuntamente
- responsabilidade pode ser limitada em caso de conformidade provada (*accountability*)
- termo pode ser impreciso

data processor

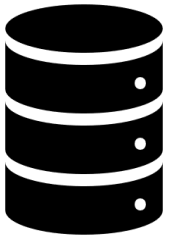
- processam os dados pessoais por conta do *data controller,* em nome deste
- devem seguir as diretrizes do GDPR no processamento, incluindo as relativas a padrões de segurança
- incidentes podem levar a altas penalidades
- termo pode ser impreciso

responsável pelo tratamento (controller)

- utilização das melhores técnicas para proteção dos dados
- registro de toda atividade de tratamento
- notificação sobre violações (data breach notification)
- avaliação de riscos e consulta prévia à autoridade de proteção de dados (DPIA)

deveres do Controller

princípio da responsabilização e da precaução: a norma exige proteção de dados *by design* (***privacy by design***) e ***privacy by default***. Isso significa que as empresas devem tomar medidas e documentá-las para cumprir as diretrizes da regulação. (*risk based approach*)



dever de guarda: controladores de dados e quaisquer contratantes devem **registrar e guardar seus processos** e práticas de tratamento de dados, **incluindo motivação e período previsto**, para apresentarem para as autoridades quando solicitados.

DPO (Data Protection Officer): cargo que deve existir dentro de empresas e órgãos que lidem com **grande fluxo de dados** (hospitais, bancos, seguradoras, etc.), **categorias especiais de dados** ou **tratamentos de risco**. O DPO é o responsável pelo monitoramento e processamento de dados nesses estabelecimentos.

Officer by Anwer Hossain

Enforcement

Autoridades de Proteção de Dados

Poderes das autoridades supervisoras

- Investigações, em particular fornecimento de documentos e auditorias, incluindo acesso aos locais físicos
- Ordens para obedecer: fazer ou deixar de fazer, incluindo transferência internacionais, para Controllers e Processors
- Banir o processamento
- Ordens para informar titulares dos dados
- Revogar certificações
- Avisos e multas

Data Breach Notification

A Autoridade de Proteção de Dados responsável deve ser informada em até no máximo 72hrs sobre o incidente de segurança da informação. Os titulares dos dados também podem ter que ser informados.

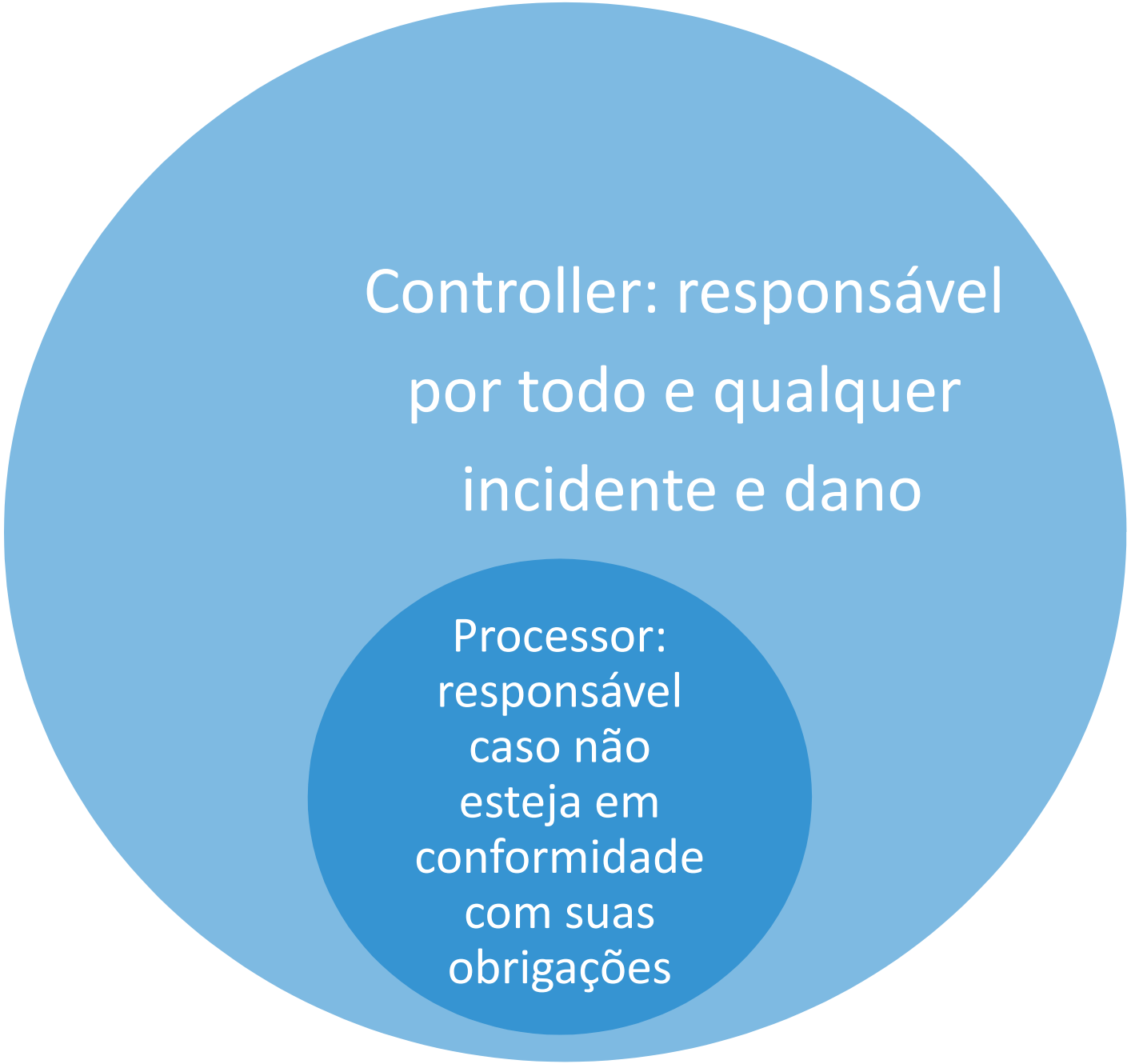
- Destruição
- Perda
- Alteração
- Vazamento
- Acesso

Multas – princípios

- Todo uso indevido e vazamento de dados deve ser multado (a exceção de pequenos incidentes);
- Deve ser efetiva, proporcional e dissuasiva;
- Critério:
  - Gravidade, quantidade, duração, dano, categorias de dados
  - Benefícios financeiros do responsável pelo incidente;
  - Intenção ou negligência, histórico de conformidade;
  - Aderência a código de conduta ou cerificação aprovada;
  - Atos de mitigação aplicados, cooperação com as autoridades

Penas de até €20 milhões ou 4% do faturamento global

enforcement



Transferência Internacional

Transferência Internacional

Article 46 GDPR

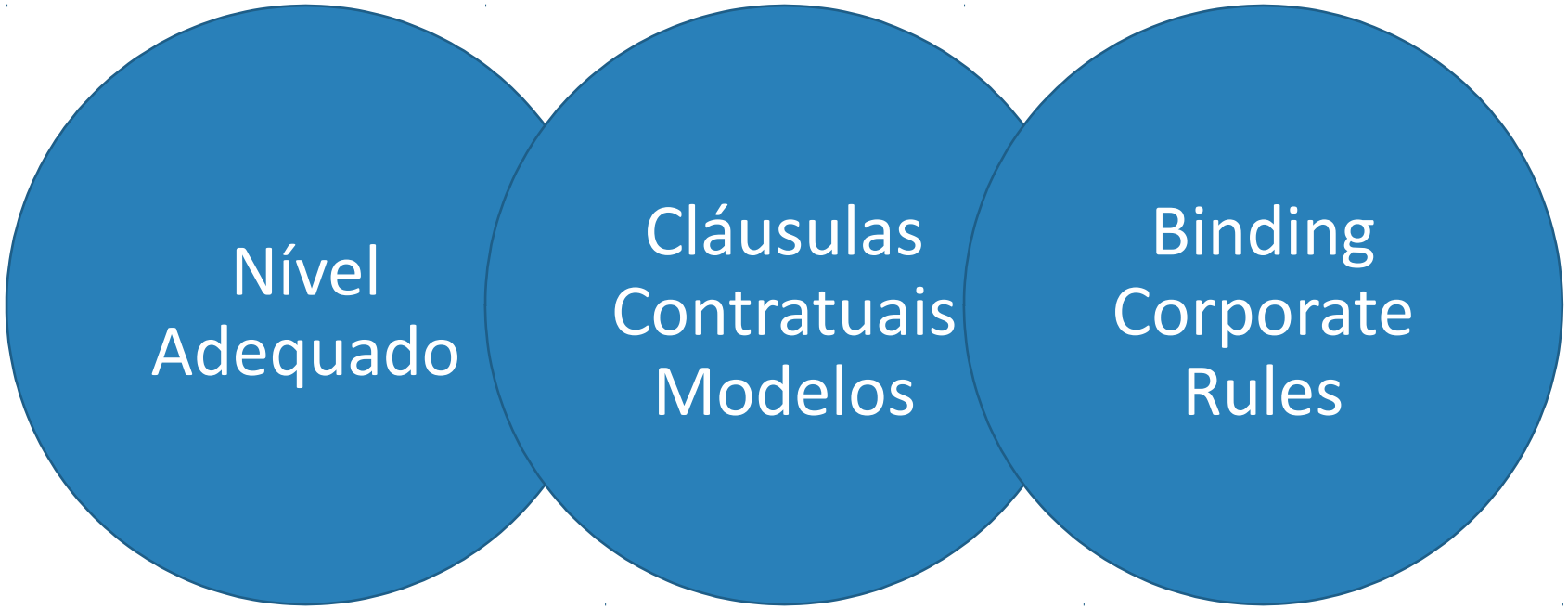


Exhibit E2

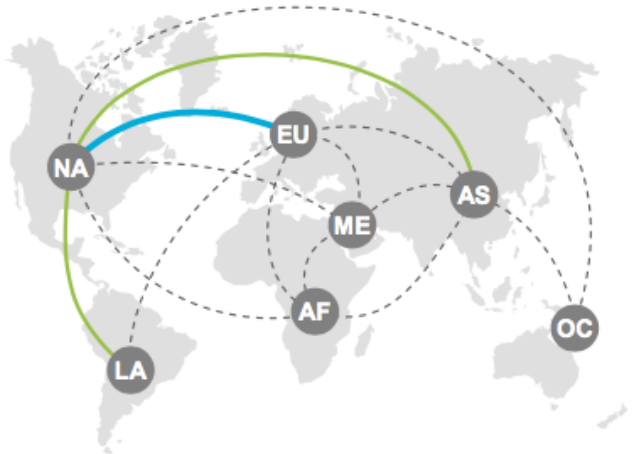
Cross-border data flows are surging and connecting more countries

Used cross-border bandwidth

Regions	NA United States and Canada	EU Europe	AS Asia	LA Latin America	ME Middle East	AF Africa	OC Oceania

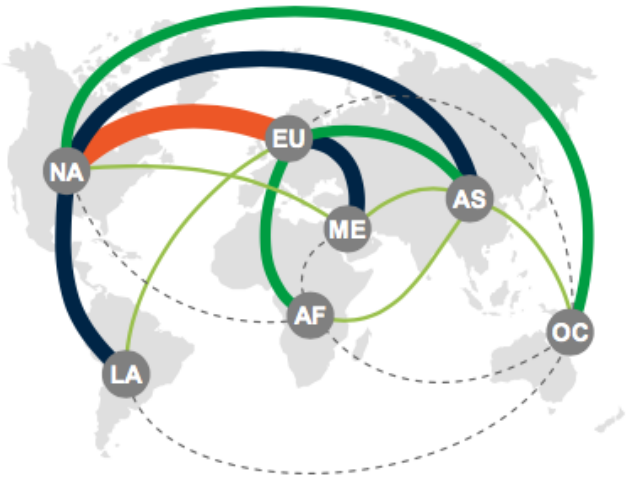
Bandwidth Gigabits per second (Gbps)	<50	50–100	100–500	500–1,000	1,000–5,000	5,000–20,000	>20,000

2005
100% = 4.7 Terabits per second (Tbps)



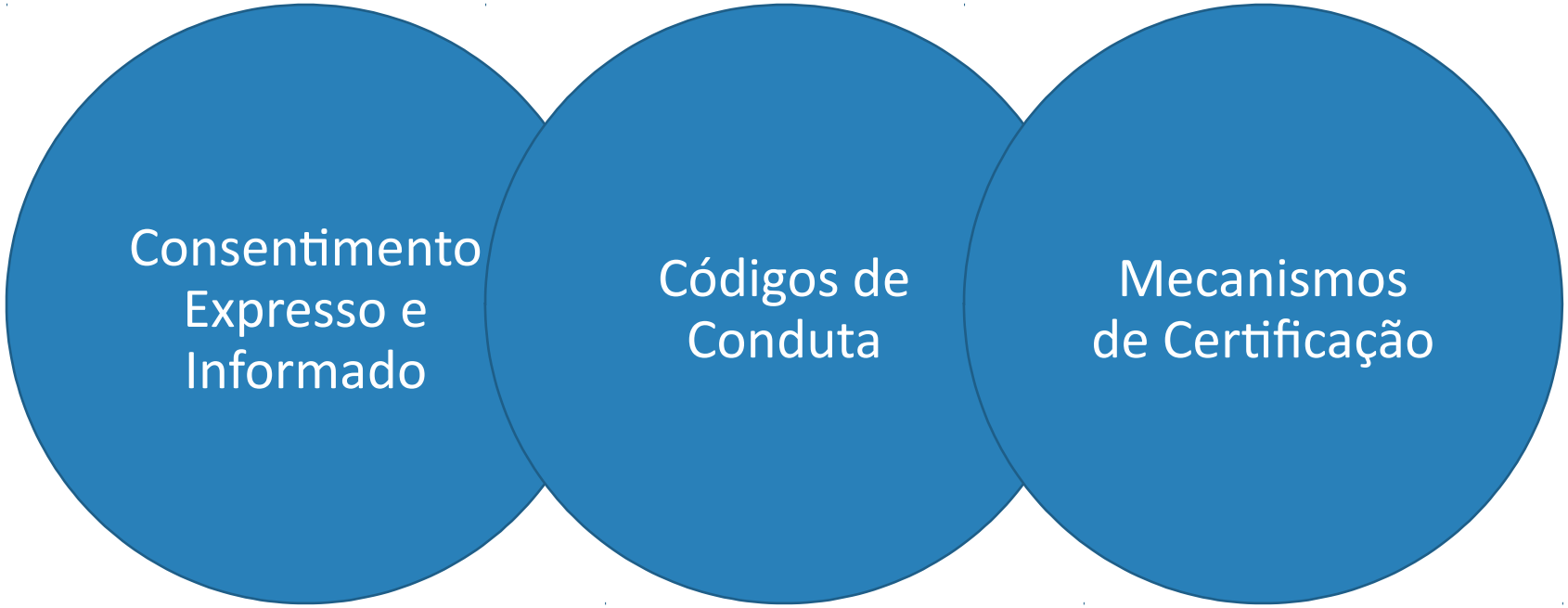
2014
100% = 211.3 Tbps

45x larger



Transferência Internacional

Article 46 e 49 GDPR



Estrutura da GDPR

estrutura básica da GDPR

- **Capítulo I / Artigos 1 – 4 : Disposição gerais** (âmbito e objetivos, definições)
- **Capítulo II / Artigos 5 – 11 : Princípios**
  - Princípios que regem o processamento de dados
  - Bases legais
  - Crianças, categorias especiais de dados pessoais
  - Processamento que não requer identificação
- **Capítulo III / Artigos 12 – 23 : Direitos do titular dos dados**
  - Direito à transparência e à informação
  - Direito ao acesso
  - Direito à retificação
  - Direito ao apagamento (”Direito de ser esquecido”)
  - Direito à retificação
  - Direito à restrição de processamento
  - Direito a portabilidade de dados
  - Direito à objeção
  - Direito a não estar sujeito a decisões automatizadas com efeitos legais ou similares sobre os titulares

estrutura básica da GDPR

- **Capítulo IV / Artigos 24 – 43** :
  - Responsabilidade do “Controller”
  - Privacy by Design and by Default
  - Joint Controllers
  - Representantes de controllers sem estabelecimento na UE
  - Função e obrigações do “Processador”
  - Obrigação de garantir a segurança do processamento de dados
  - Notificação de Violação (Artigos 33, 34)
  - Data Protection Impact Assessment
  - Data Protection Officer / obrigação, escopo e atribuições
  - Códigos de conduta e certificações
- **Capítulo V / Artigos 44 – 50 : Transferência de Dados a outros países**
  - Adequação, model clauses, normas corporativas globais obrigatórias (binding corporate rules - BCIs)

estrutura básica da GDPR

- **Capítulo VI / Artigos 51 – 59 : Autoridades fiscalizadoras independentes (autoridades de proteção de dados/DPAs)**
  - Requisitos, escopo, competência, atribuições e poderes
  - Os poderes incluem o poder de impor uma multa administrativa de até 4% do faturamento global no caso de violação da Regulamentação.
- **Capítulo VII / Artigos 60 – 76 : Cooperação e consistência na aplicação da lei**
  - Cooperação entre DPAs e o princípio do "one-stop-shop" (28 países num lugar só)
  - "Mecanismo de adequaçao"
  - Criação do Conselho Europeu de Proteção de Dados (European Data Protection Board - EDPB)
- **Capítulo VIII / Artigos 77 – 91 : Recursos, responsabilidades e penalidades**
  - Direitos do titular dos dados
  - Providenciar ações representativas em nome dos titulares dos dados, se tais órgãos existirem
  - Condições para a imposição de multas administrativas e outras penalidades

Obrigado!


renato.monteiro@mackenzie.br


Renato Leite Monteiro


@RenatoLeiteM