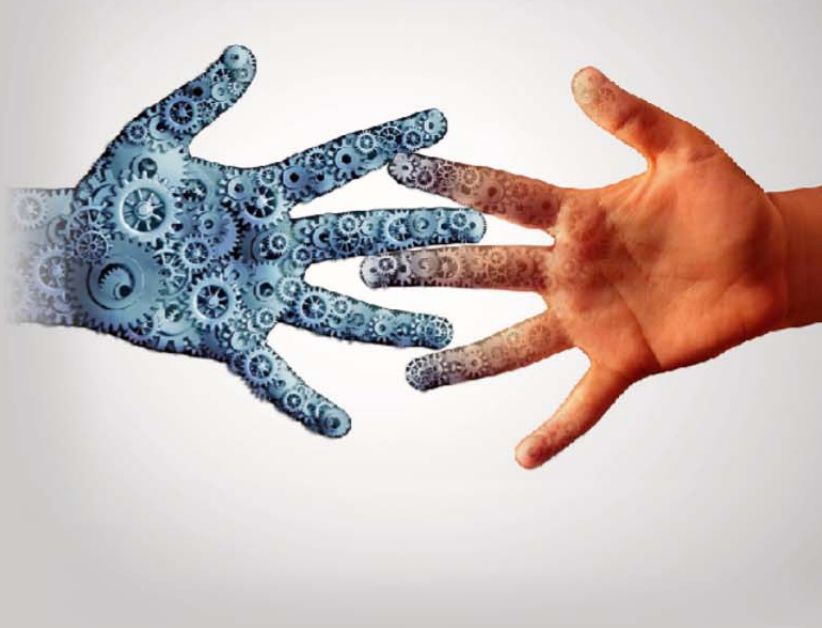
apcc
associação portuguesa de contact centers

Bots or Humans? Or both?

CONFERÊNCIA INTERNACIONAL APCC
16 de maio de 2017, Centro de Congressos do Estoril



O Regulamento Europeu de Proteção de Dados:

os novos desafios do tratamento de dados para as empresas

-

Isabel Ornelas

VIEIRA DE ALMEIDA

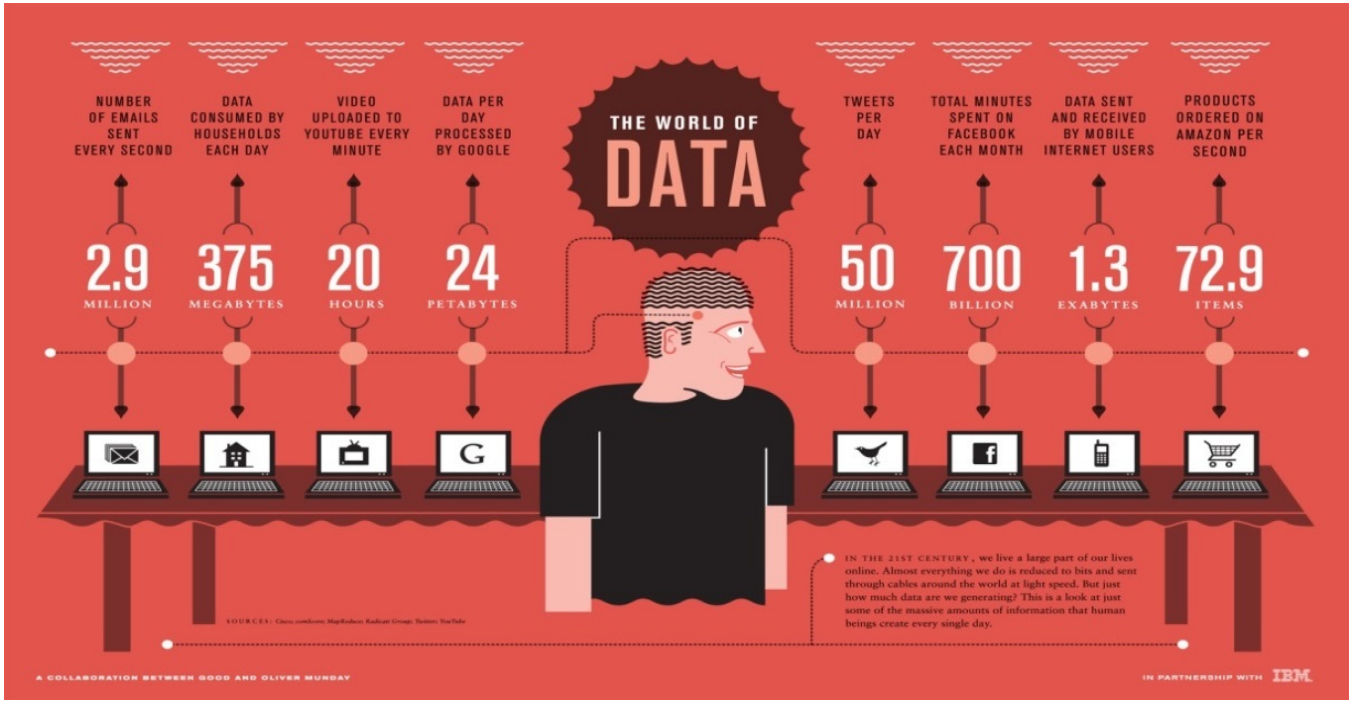
O Regulamento Europeu de Proteção de Dados:
os novos desafios do tratamento de dados para as empresas

Índice

1 | Introdução: a importância dos dados

UM MUNDO CADA VEZ MAIS DIGITAL

CADA VEZ MAIS **INFORMAÇÃO** PRODUZIDA



AUMENTO DO VALOR DA INFORMAÇÃO

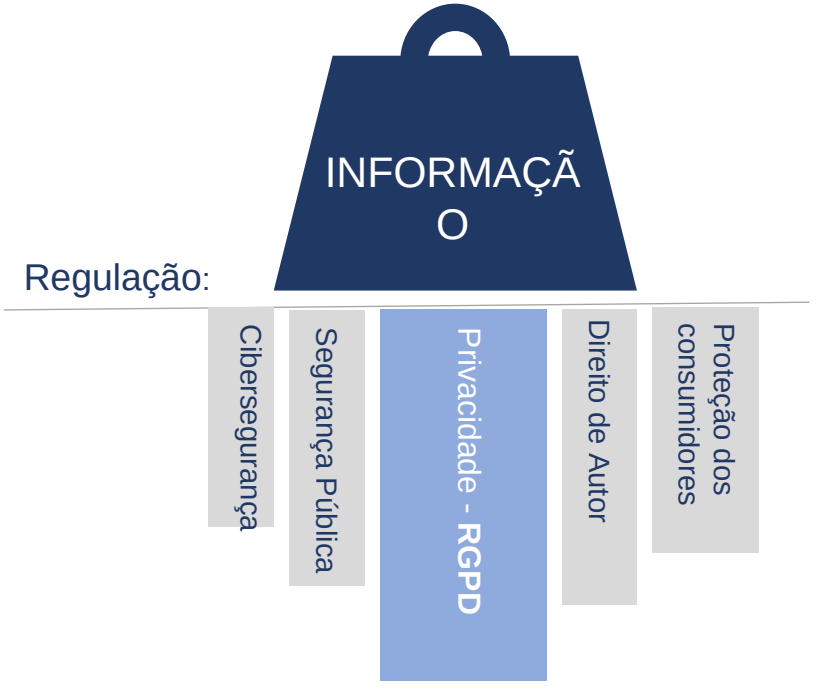
1 | Introdução: a importância dos dados

+ informação produzida em todo o mundo

+ valor económico da informação

+ necessidade de *ownership* da informação

+ proteção da informação



1 | Introdução: a importância dos dados

- Aprovação de um novo regime de dados pessoais
- Entrada em vigor a 24 de maio de 2016, sendo aplicável a partir de **25 de maio de 2018**

Regime de *compliance* relativo à proteção de dados pessoais moderno e baseado na responsabilização das organizações

2 | O novo quadro legal

Atualmente:

A partir de **maio de 2018:**

+ Diretiva de Segurança das Redes e da Informação (SRI)
A Diretiva (UE) 2016/1148, de 6 de julho de 2016 –

+ Proposta de Regulamento sobre a privacidade nas comunicações eletrónicas (ePrivacy) janeiro de 2017

3 | O novo Regulamento Geral sobre a Proteção de Dados Pessoais

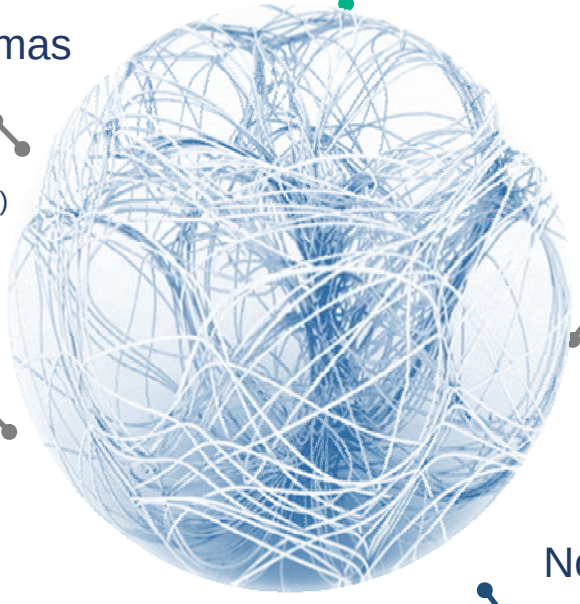
Principais alterações do RGPD

Autorresponsabilização

Privacy by design e by default, privacy impact assessment, registos

Aumento significativo do valor das coimas

Punidas com coimas até €20.000 000
ou 4% do volume anual mundial de negócios (empresas)



Consentimento

Validade do consentimento do titular dos dados

Poder Sancionatório

Sanções e fiscalização das autoridades nacionais de proteção de dados

Novos Direitos dos titulares

Direito de informação e de acesso, de apagamento, limitação do tratamento e portabilidade

Segurança

Notificações de *data breaches* e reforço das medidas de segurança dos dados

3 | O novo Regulamento Geral sobre a Proteção de Dados Pessoais

1 Novos conceitos e novo paradigma para as entidades subcontratadas

- *Privacy Impact Assessment* (PIA)
- *Privacy by Design*
- *Privacy by Default*
- *Direito à portabilidade*
- *Consentimento*
- *Informação*

2 Alargamento do âmbito territorial e o *Mecanismo do One-stop-shop ou balcão único*

3 Exigências reforçadas para o tratamento de dados de perfil

4 *Data Protection Officer*

5 Regime das transferências de dados para fora da UE

6 Notificação de *Data Breaches*

3 | O novo Regulamento Geral sobre a Proteção de Dados Pessoais

Registos das atividades de tratamento:

Responsável pelo Tratamento
conserva registo das atividades de tratamento sob a sua responsabilidade, do qual consta:

- Nome e contactos do responsável;
- Finalidades de tratamento dos dados;
- Descrição das categorias de titulares de dados e das categorias de dados pessoais;
- Categorias de destinatários a quem os dados sejam divulgados;
- Transferências de dados;
- Descrição das medidas técnicas e organizativas de segurança

Subcontratante
conserva um registo de todas as categorias de atividades de tratamento realizadas em nome de um responsável pelo tratamento:

- Nome e contactos do subcontratante e do responsável em nome de quem atua;
- As categorias de tratamento de dados pessoais efetuados em nome de cada responsável;
- Transferências de dados;
- Descrição das medidas técnicas e organizativas de segurança.

Estes registos são efetuados por escrito, em formato eletrónico e devem ser disponibilizados à autoridade de controlo

3 | O novo Regulamento Geral sobre a Proteção de Dados Pessoais

***Privacy Impact Assessment* (PIA)** ou Avaliação de Impacto sobre a Proteção de Dados:

análise destinada a identificar e minimizar os potenciais riscos para o não-cumprimento de disposições legais

- Aplica-se a certos tipos de tratamentos
- Obrigatória em certos casos
- Autoridade de controlo publica lista de operações sujeitas ao requisito de PIA
- São indicados os elementos devem constar da avaliação

Pode dar origem ao mecanismo da **consulta prévia**

- Responsável deve consultar Autoridade se da avaliação resultar elevado risco
- Elementos da comunicação à Autoridade
- Autoridade dá orientações por escrito

3 | O novo Regulamento Geral sobre a Proteção de Dados Pessoais

Data Protection Officer (DPO) – Encarregado de Proteção de Dados

Designação **obrigatória:**

- Organismos Públicos;
- Empresas cujas atividades exijam:
  - controlo regular e sistemático dos titulares em grande escala;
  - Tratamento em grande escala de dados sensíveis ou criminais;

Funções:

- Informar todos os que tratem os dados das suas obrigações;
- Assegurar o cumprimento do Regulamento e demais políticas do responsável/subcontratante;
- Aconselhar e controlar a avaliação de impacto sobre a proteção de dados;
- Cooperar com autoridade de controlo, servindo como ponto de contacto;

Posição:

O Encarregado da Proteção de Dados deve ser envolvido em todas as questões relacionadas com a proteção de dados

3 | O novo Regulamento Geral sobre a Proteção de Dados Pessoais

Regime de notificação de violações de segurança

- Em caso de violação de dados pessoais a autoridade de controlo deve ser notificada, sem demora injustificada e, sempre que possível até **72 horas** após ter tido conhecimento da mesma

- O subcontratante também deve notificar o responsável pelo tratamento após ter conhecimento de uma violação de dados pessoais

- A violação deve ser comunicada ao titular dos dados quando for susceptível de implicar elevado risco para os seus direitos

3 | O novo Regulamento Geral sobre a Proteção de Dados Pessoais

Novo quadro sancionatório:

COIMAS

Há 2 tipos de sanções:

Violação pelo responsável/subcontratante de obrigações relativas a:

- Consentimento relativo a dados de menores
- Obrigações do Subcontratante
- Obrigação de Notificação
- Cooperação com Autoridade
- Comunicação de violações da proteção de dados
- Avaliação de Impacto sobre a Proteção de Dados

- Punidas com coimas até **€10.000 000** ou **2% do volume anual mundial** de negócios (empresas)

- Punidas com coimas até **€20.000 000** ou **4% do volume anual mundial** de negócios (empresas)

Violação pelo responsável/ subcontratante dos:

- Princípios gerais de proteção de dados, incluindo regras de consentimento
- Deveres dos responsáveis perante os titulares (transparência, informação, acesso, esquecimento, portabilidade)
- Regras de transferências internacionais de dados

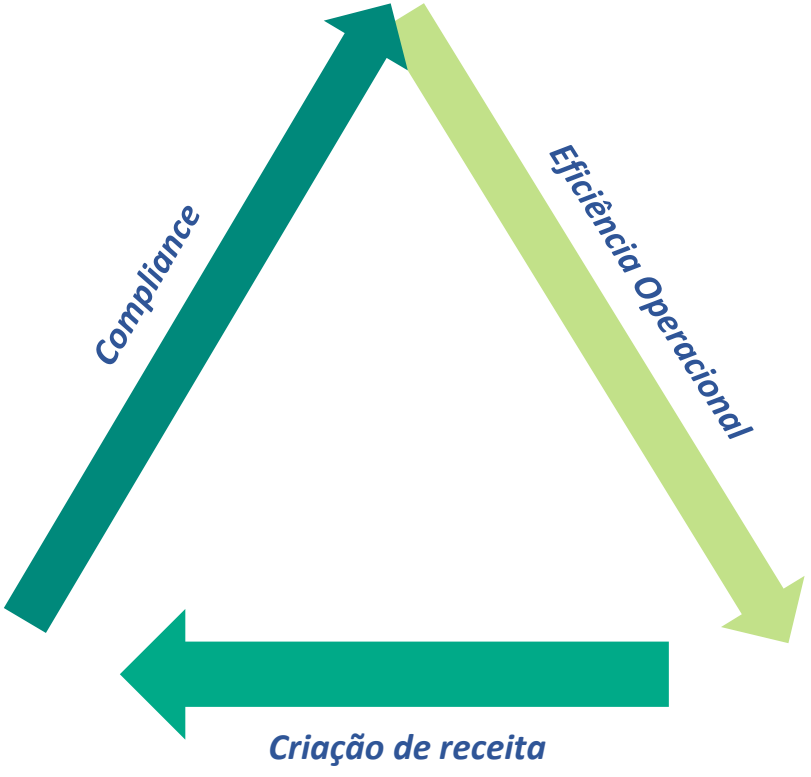
3 | O novo Regulamento Geral sobre a Proteção de Dados Pessoais

Impacto a vários níveis

E AGORA?

4 | O que fazer para estar preparado – as vantagens da preparação adquada

Inovação & monetização da informação...



.... Regulação & *Enforcement*

4 | O que fazer para estar preparado

Documentação do cumprimento do RGPD

Redefinir responsabilidades

Criar e desenvolver políticas de acesso a dados pessoais

Avaliar as categorias de dados tratadas

Criar procedimentos de contratação de terceiros – inclusão de temas de proteção de dados

Definir uma estrutura de *Governance*

Ter um plano de resposta em caso de "incidente"

Rever as condições de segurança dos sistemas

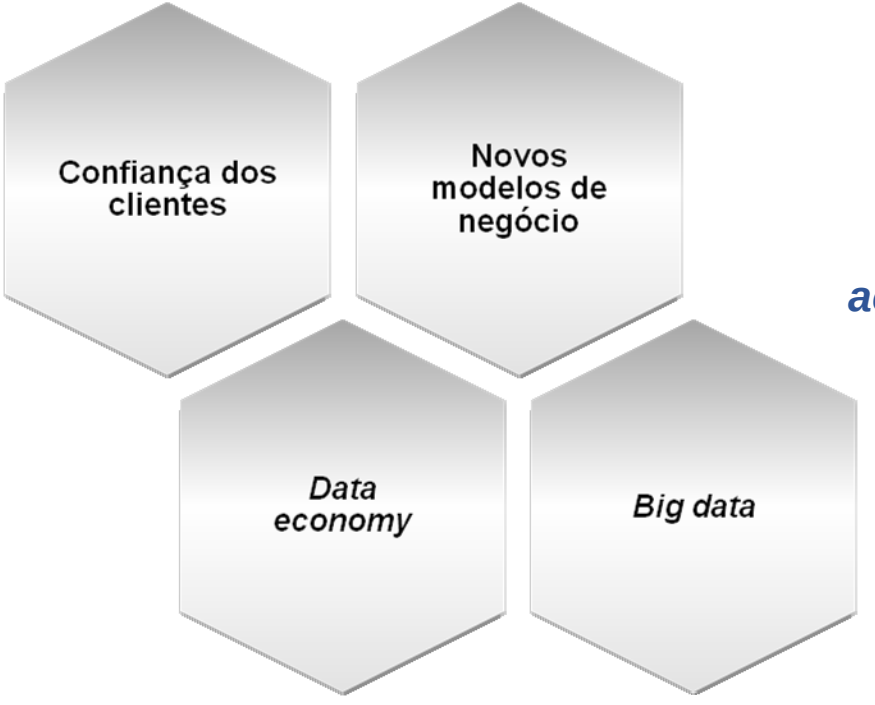
Adoção de códigos de conduta e políticas internas

Mapear alterações a introduzir nos SI

Criação de processos de auditoria interna

4 | O que fazer para estar preparado

O cumprimento do RGPD não evita só a aplicação de coimas, também cria novas **oportunidades de negócio**



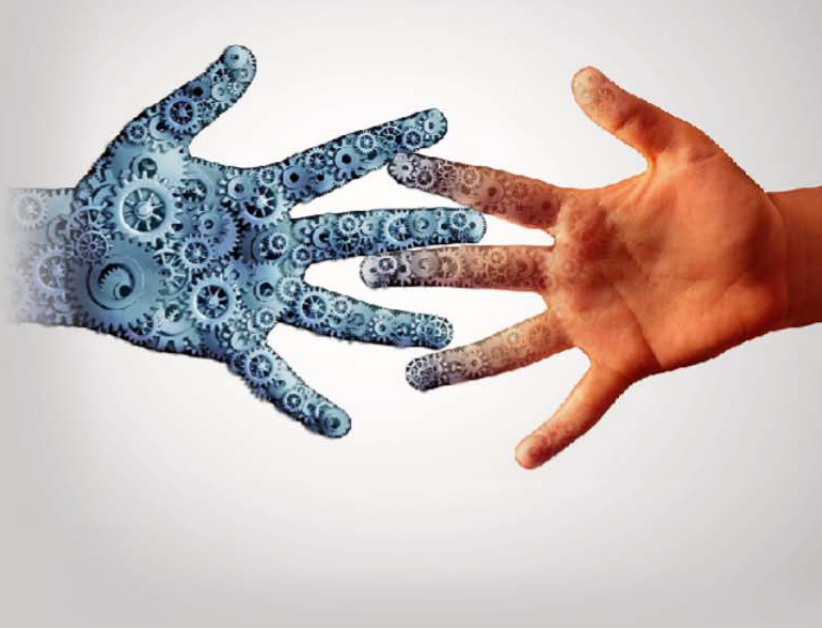
"We should not see privacy and data protection as holding back economic activities. They are, in fact, an essential competitive advantage."

EU's Vice President of the Digital Single Market, Andrus Ansip

apcc
associação portuguesa de contact centers

Bots or Humans? Or both?

CONFERÊNCIA INTERNACIONAL APCC
16 de maio de 2017, Centro de Congressos do Estoril



O Regulamento Europeu de Proteção de Dados:
os novos desafios do tratamento de dados para as empresas

-

Isabel Ornelas

VIEIRA DE ALMEIDA