

GDPR: DA TEORIA À PRÁTICA



02

© MAZIK ANDERSON

WWW.ANDERTOONS.COM



"Before I write my name on the board, I'll need to know how you're planning to use that data."

3 A transformação óbvia

Directiva

- Força Obrigatória;
- Foi transposta para os 28 Estados-Membros;
- É diferente consoante o Estado-Membro;
- Resultou na criação o Grupo de Trabalho do Artigo 29.

GDPR

- É aplicada diretamente;
- Sem necessidade de transposição;
- Confere um certo grau de autonomia específica aos Estados Membros, mas o basilar mantém-se igual em todos, porque o diploma é o mesmo para todos os Estados-Membro;
- Resultou na criação “*European Data Protection Board*”.



4 Dados Pessoais

CONCEITO:

- O conceito de dados pessoais é **fundamental** e propositadamente **amplo**.
- O problema é que, com o evoluir da tecnologia, também o conceito de dados pessoais teve de seguir essa tendência e actualizar-se.
- No Parecer 4/2007, o WP29 estabeleceu quatro "blocos de construção" que compreendem o significado de dados pessoais. A saber:
 - 1.'Qualquer informação';
 - 2.'Relacionada com';
 - 3.'Um titular identificado ou identificável';
 - 4.Que seja uma 'pessoa natural'.

05 Dados Sensíveis

• Certas categorias de dados, por especialmente sensíveis, merecem uma proteção ainda mais elevada dado que o processamento desse tipo de dados poderá criar riscos significativos de ingerência e violação de direitos e liberdades fundamentais e são eles:

- Raciais ou étnicos;
- Opiniões políticas, religiosas ou filosóficas;
- Genéticos;
- Biométricos;
- Saúde;
- Sexualidade; • Orientação sexual.

Controlador dos Dados

A Pessoa física ou jurídica, autoridade pública, agência ou qualquer outro organismo, que:

- Sozinho ou em conjunto com outras entidades;
- Determina os fins e os meios de processamento de dados pessoais.

Na prática é o decisor em relação ao que é modificado no âmbito do tratamento de dados pessoais, dando-se primazia à Empresa, ao invés da pessoa nomeada na empresa que, ao nível de responsabilização decide que dados pessoais serão captados, armazenados, usados, alterados ou divulgados.

7 Processador dos Dados

A pessoa ou entidade que, em nome do controlador e segundo as instruções do controlador, processa os seus dados.

O processador pode até ajudar o Controlador a definir os meios técnicos e organizacionais do processamento mas, em última ratio, é o Controlador que decide o propósito do processamento.

Ex.: Se uma empresa tem uma base de dados de emails de indivíduos que aceitaram receber newsletters e quer fazer um envio massivo de emails, para isso contratando uma empresa de marketing digital, essa empresa vai ser o processador.

8 Etapas do processo, como começar?

1. Consciencialização: Reuniões de Kick-Off com CEO's, COO's, CFO's, CTO's e RH;
2. Conhecer o Fluxo de Dados: o que capta, como capta, onde capta, como armazena, para onde transfere (3^{os}) e com que fim o faz.
3. Conhecer a legislação aplicável ao modelo de negócio: GDPR, E-commerce, E-privacy, etc;
4. Conhecer o processamento dos dados que capta justifica o risco e é vantajoso: se é, ou não, necessário e se pode ser substituído por outros métodos;
5. Organizar mecanismos de resposta aos titulares dos dados: ARCO Rights;
6. Conhecer ou Subscrever o Software de Segurança e Monitorização do Fluxo de Dados;

E ainda ...

7. Termos de Responsabilidade Internos e Online: Segurança, Níveis de Acesso, T&C's, Políticas de Privacidade e Cookies;
8. Rever o procedimento no âmbito de RH: Anúncios de Emprego; BD's dos Candidatos; Captação e tratamento para fins laborais, etc;
9. Proteção Contratual: Controllers e Processors – ter minutas e documentação auxiliar que permita garantir o direito de regresso, ou cláusulas penais;
10. Data Breaches: Ter um procedimento já mecanizado para investigação e comunicação à entidade supervisora;
11. PIA's e Privacidade por defeito: Auditorias periódicas, Avaliação do Risco e Definição do Impacto Reputacional;
12. DPO e Entidade Supervisora: Interno? Ou subcontratação? Definir o DPO e a entidade Supervisora que se aplica ao modelo da empresa.

A sua empresa precisa, ou não de um DPO?

SIM

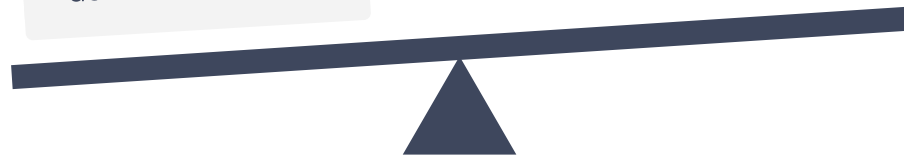
Extensão geográfica do processamento

Número de Titulares de Dados captados

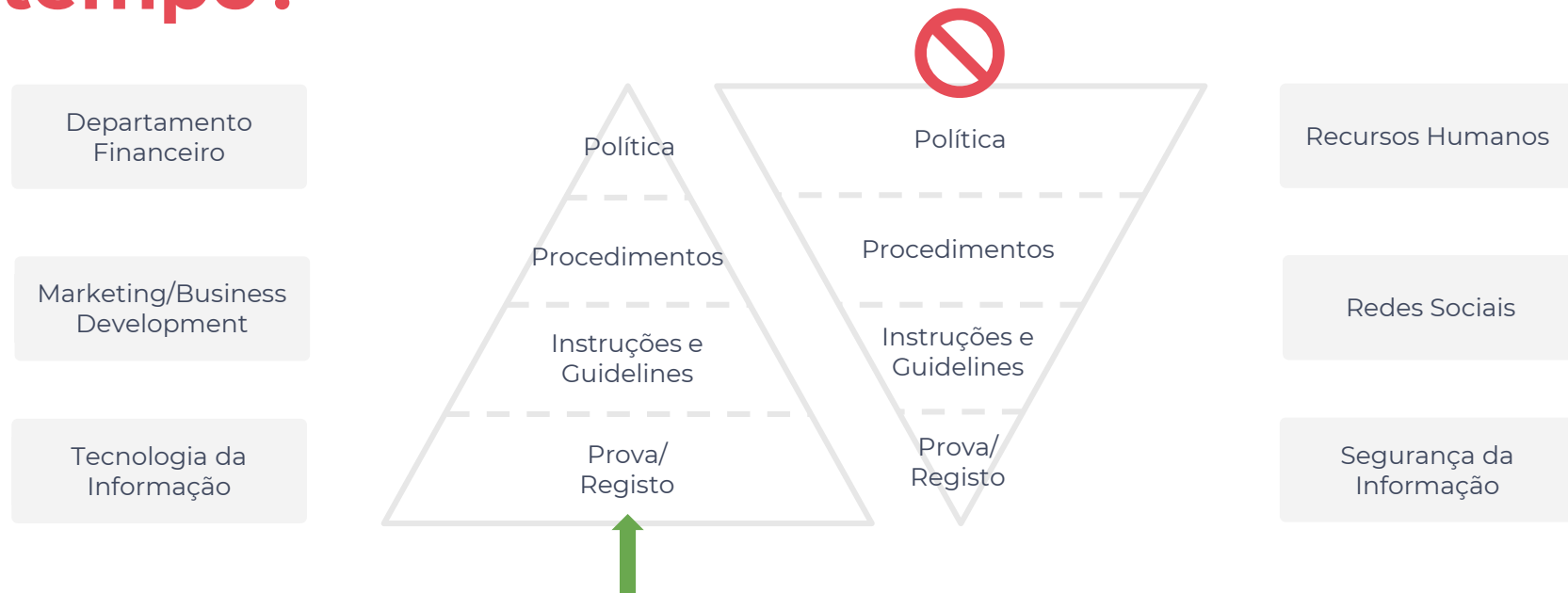
NÃO

Envia uma newsletter esporádica) Titulares

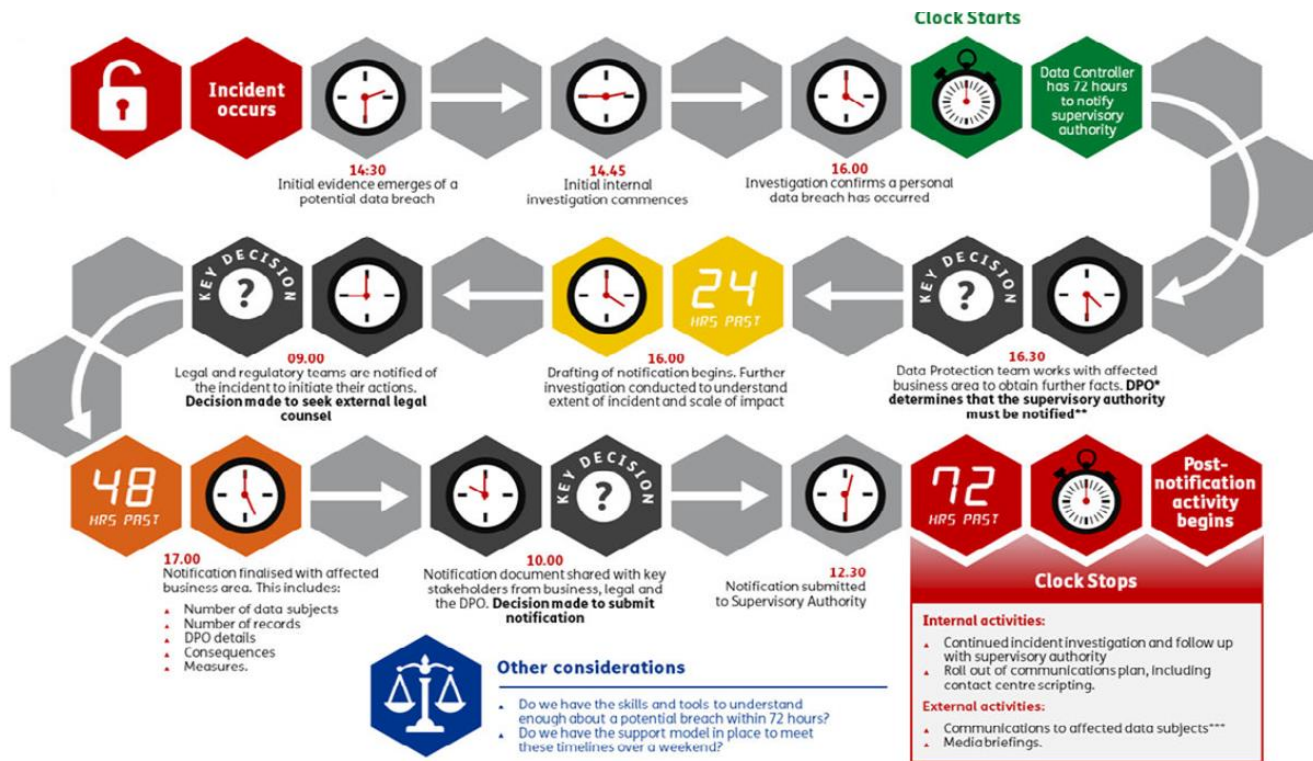
Capta dados para uma inscrição e não armazena



Como deve, o DPO, distribuir o seu tempo?



Houve uma DATA BREACH, e agora?



13

dataja

PRIVACY SOLUTIONS