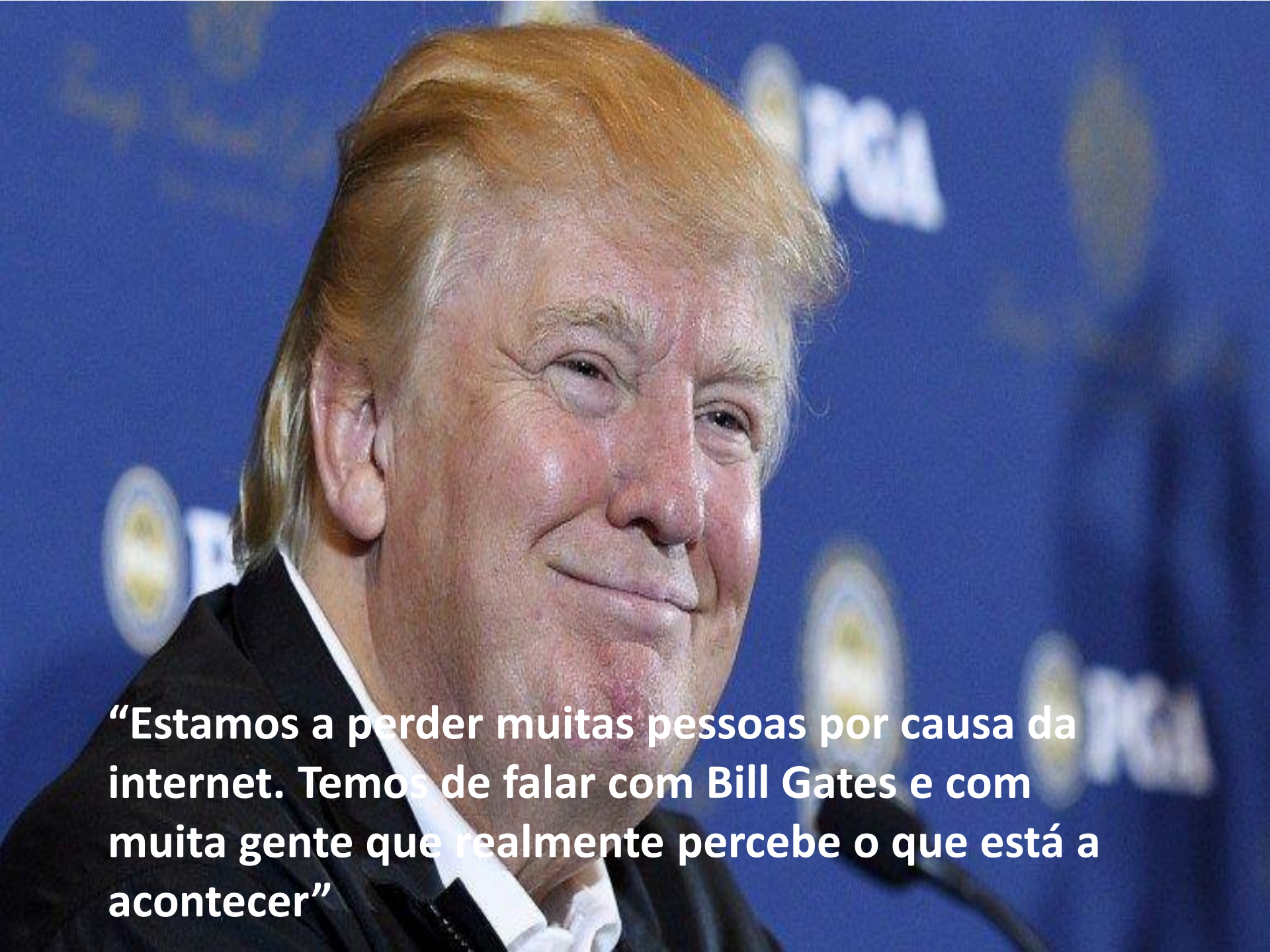
O REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS


“Estamos a perder muitas pessoas por causa da internet. Temos de falar com Bill Gates e com muita gente que realmente percebe o que está a acontecer”

O Regulamento Geral de Protecção de Dados

Está quase……..

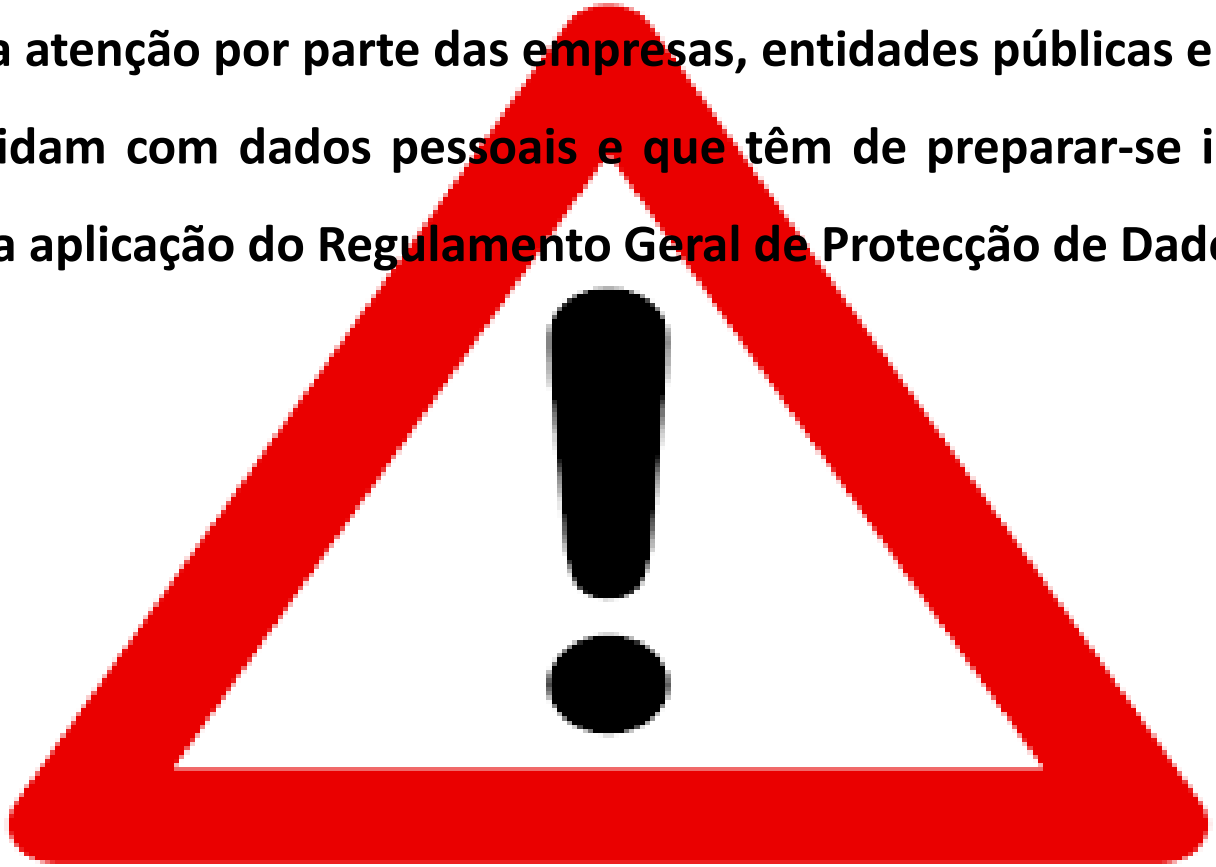
O Regulamento Geral de Protecção de Dados

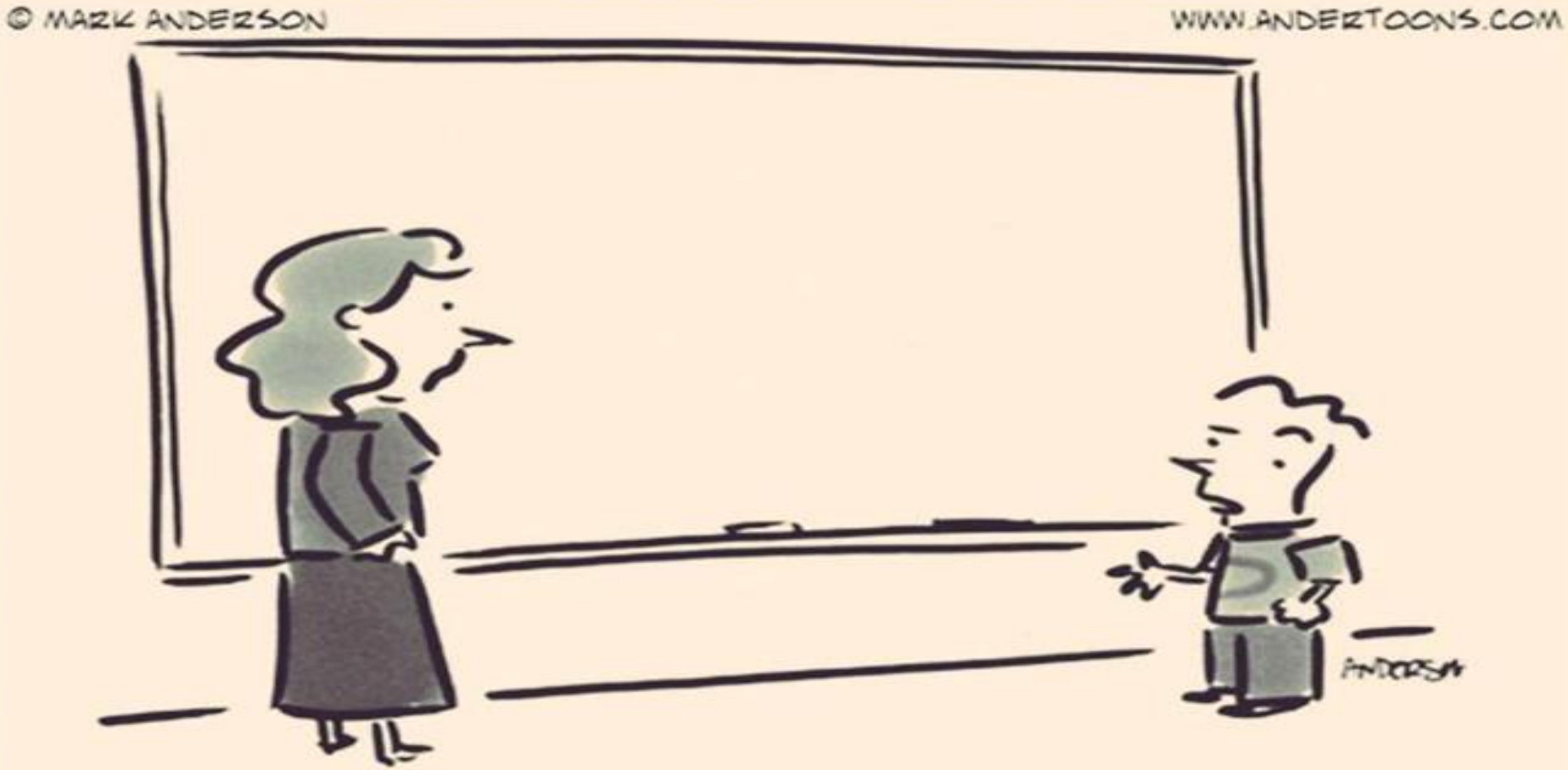
- Aproxima-se a data da entrada em vigor do Novo Regulamento Comunitário de Protecção de Dados, o próximo dia 25 de maio de 2018 será marcado pela aplicação plena do Regulamento Europeu n.º**2016/679**.

- Este Regulamento – cuja aplicação na ordem jurídica dos Estados membros, não carece de transposição – estabelece um conjunto de novas regras aplicáveis à proteção dos dados pessoais e prevê elevadas coimas em caso de incumprimento. Mas é mesmo assim?

O Regulamento Geral de Protecção de Dados

Muita atenção por parte das empresas, entidades públicas e profissionais que lidam com dados pessoais e que têm de preparar-se internamente para a aplicação do Regulamento Geral de Protecção de Dados (RGPD).




© MARK 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."

O Regulamento Geral de Protecção de Dados

Novas normas????

Mudança de paradigma???

Enquadramento legal e constitucional……..

O Regulamento Geral de Protecção de Dados

Convenção 108 de 1981 do Conselho da Europa – garantia, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados»).

Lei da Protecção de Dados pessoais - Lei n.º 67/98, de 26 de outubro, que transpõe a Directiva 95/46/CE do Parlamento Europeu e do Conselho
A Directiva surge aquando da criação da União Europeia – Mercado Único

O novo Regulamento é o seguimento e não o início da legislação sobre protecção de dados pessoais!

O Regulamento Geral de Protecção de Dados

Constituição da República Portuguesa – Direitos liberdades e garantias

Artigo 35.º
Utilização da informática

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.

O Regulamento Geral de Protecção de Dados

3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.

O Regulamento Geral de Protecção de Dados

5. É proibida a atribuição de um número nacional único aos cidadãos.

6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei.

O Regulamento Geral de Protecção de Dados

Código do Procedimento Administrativo

Artigo 18.º

Princípio da proteção dos dados pessoais

Os particulares têm direito à protecção dos seus dados pessoais e à segurança e integridade dos suportes, sistemas e aplicações utilizados para o efeito, nos termos da lei.

O Regulamento Geral de Protecção de Dados

O que é o Regulamento Geral de Proteção de Dados?

- **um marco fundamental na regulação do tratamento dos dados pessoais, tendo como escopo responder aos novos desafios na área de proteção de dados pessoais gerados pela evolução das novas tecnologias e pela globalização dos mercados.**

- parte do pacote da União Europeia relativo à **reforma da proteção de dados** e passará a ser aplicado direta e obrigatoriamente a partir de 25 de maio de 2018, trazendo impactos significativos na vida das organizações.

O Regulamento Geral de Protecção de Dados

- O Parlamento Europeu e o Conselho da União Europeia consideraram necessário implementar "*um quadro de proteção de dados sólido e mais coerente, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno".*

- *O RGPD consagra a responsabilização das entidades e empresas que passam a ter de demonstrar o cumprimento das regras – de modelo de hetero-regulação passamos ao modelo de auto-regulação*

O Regulamento Geral de Protecção de Dados

- fundamental devolver às pessoas singulares o **poder controlar a utilização que é feita dos seus dados pessoais**, devendo ser **reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas.**

O Regulamento Geral de Protecção de Dados

- **Porquê Regulamento e não Directiva?**

É urgente uniformizar!

- **1) Completa reforma do sistema de controlo preventivo do tratamento de dados pessoais** – os pedidos de registo ou de autorização às autoridades nacionais (em Portugal CNPD) nos diversos Estados membros apresentavam resultados diferentes, com alguns a demorar mais tempo do que o desejável na resposta;

–retirou-se às entidades administrativas a função de prevenção que passou para dentro das entidades;

O Regulamento Geral de Protecção de Dados

2) Criação da figura de DPO – *Data Protection Officer* – Encarregado da protecção de dados

- cada instituição pública tem de ter um DPO

- cada instituição privada que trate dados sensíveis ou dados em larga escala tem de ter um DPO

- A Figura de DPO já existe desde há muito por exemplo na Alemanha

- O RGPD não exige qualquer certificação obrigatória para exercício do cargo de DPO!

O Regulamento Geral de Protecção de Dados

3) Uniformização na transferência de dados transfronteiras

- As Comissões e autoridades de controlo tinham *modus operandi* e decisões diferentes umas das outras

- exigência de uma entidade que caucione a aplicação do RGPD que não pode ser posta em causa por entidades nacionais - *"One stop Shop"*

O Regulamento Geral de Protecção de Dados

É um verdadeiro Regulamento?

Não carece de legislação nacional complementar?

- Há várias disposições do Regulamento que remetem para legislação nacional de cada Estado membro, ex: artigo 85.º e seguintes

- falta concretizar a aplicação de sanções - não há norma sancionatória expressa ou qualquer alusão a prescrição

- falta fixar valores mínimos de sanções

- é possível aplicar apenas admoestação? 1 dos 170 Considerandos admite-o

- é necessária legislação nacional em áreas sensíveis – tratamento dados clínicos ou privacidade no local de trabalho

O Regulamento Geral de Protecção de Dados

É um verdadeiro Regulamento?

Não carece de legislação nacional complementar?

- A Administração Pública vai ter coimas? Como os privados?

- 3 tipos de sanções:

a) corretiva – correção comportamento

b) financeira – 2 níveis consoante gravidade

c) reputacional- dano de imagem e perda de confiança

OPINIÕES SOBRE PRIVACIDADE NA INTERNET

O FILÓSOFO:

"PRIVACIDADE" É UMA FORMA POUCO PRÁTICA PARA PENSAR SOBRE OS DADOS EM UM MUNDO DIGITAL TÃO DIFERENTE DAQUELE NO QUAL A NOSSA SOCIE...

MUITO CHATO.

O AFICIONADO POR CRIPTOGRAFIA:

MEUS DADOS ESTÃO SEGUROS ATRÁS DE SEIS CAMADAS DE ALGORITMOS SIMÉTRICOS E DE CHAVES PÚBLICAS.

QUE DADOS SERIAM ESSES?

A MAIOR PARTE SÃO EMAILS PESSOAIS SOBRE CRIPTOGRAFIA

O CONSPIRADOR:

ESSES VAZAMENTOS SÃO APENAS A PONTA DO ICEBERG. EXISTE UM ARMAZÉM EM UTAH, ONDE O NSA TEM TODO O ICEBERG.

EU NÃO SEI COMO ELES CONSEGUIRAM.

O NIILISTA:

QUE PIADA, TODOS ELES RECOLHENDO TODOS ESSES DADOS A MEU RESPEITO COMO SE ALGO QUE EU FIZESSE SIGNIFICASSE ALGUMA COISA...

O EXIBICIONISTA:

HUMMM, ESPERO QUE A NSA NÃO ESTEJA ME ASSISTINDO MORDER ESSES SUCULENTOS MORANGOS!!!

OOOPS, PINGOU NA MINHA CAMISA! MELHOR TIRÁ-LA.

GOOGLE, VOCÊ ESTÁ AÍ?

GOOGLE, ESSA LOÇÃO TEM UM CHEIRO MUIIIITO BOM.

HUM.

O SÁBIO:

EU NÃO SEI OU ME IMPORTO QUAIS DADOS *QUALQUER UM* POSSUI SOBRE MIM.

DADOS SÃO IMAGINÁRIOS. ESSE BURRITO É REAL.

O Regulamento Geral de Protecção de Dados

Novas regras introduzidas pelo RGPD

- obrigação de designar um encarregado para a proteção de dados - 37.º;
- regras sobre pseudonimização de dados – definição e 25.º;
- regras sobre a alteração das regras sobre obtenção de consentimento - 7.º;
- novas regras sobre consentimento de menores - 8.º;
- eliminação do sistema de notificações e autorizações;
- implementação do direito ao esquecimento – 17.º – Acórdão Google espanhola;
- criação de obrigações acrescidas para os subcontratados - 28.º;

O Regulamento Geral de Protecção de Dados

- Introdução de coimas de valor muito elevado – 83.º
- Direito à portabilidade de dados - 20.º
- Obrigações de informação relativas a quebras de segurança – 33.º e 34.º
- Criação autoridade de controlo principal e Comité – 60.º e seguintes

O Regulamento Geral de Protecção de Dados

Alguns conceitos fundamentais

- **Dados pessoais** todos e quaisquer dados relativos a pessoas singulares identificadas ou identificáveis, como o nome, morada, e-mail, idade, estado civil, dados de localização, genéticos, fisiológicos, económica, cultural ou social.

- **Responsáveis pelos dados** as pessoas singulares ou coletivas que, individualmente ou em conjunto com outras, determinam as finalidades e os meios de tratamento de dados pessoais.

O Regulamento Geral de Protecção de Dados

- **Tratamento de dados** a operação ou um conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

O Regulamento Geral de Protecção de Dados

- **Consentimento** do titular dos dados consiste numa manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.

- Verifica-se a **violação de dados pessoais** sempre que a violação provoque, de modo acidental ou ilícito a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

O Regulamento Geral de Protecção de Dados

Conceitos fundamentais

Âmbito territorial e material

- Num primeiro momento deve-se clarificar se a Instituição (âmbito territorial) e os dados a processar (âmbito material) estão abrangidos pelo RGPD.

O Regulamento Geral de Protecção de Dados

Relativamente ao âmbito territorial é necessário avaliar se o estabelecimento do responsável pelo tratamento ou do subcontratado está:

- Situado na União Europeia (EU), independentemente de o tratamento ocorrer dentro ou fora da UE

- Não situado na EU, mas:

  - Que oferece bens/serviços aos residentes da EU;

  - Controlam o comportamento de residentes da EU.

  - Não situado na EU, mas em local que se aplique a legislação de um Estado-Membro por força do direito internacional público.

O Regulamento Geral de Protecção de Dados

Relativamente ao âmbito material torna-se premente verificar se:

- O tratamento de dados pessoais é feito por meios total ou parcialmente automatizados, ou por meios não automatizados contidos em ficheiros;

- A informação a tratar é considerada como dados pessoais. São dados pessoais todos e quaisquer dados relativos a pessoas singulares identificadas ou identificáveis, como o nome, morada, e-mail, idade, estado civil, dados de localização, genéticos, fisiológicos, económica, cultural ou social. Existem, no entanto, várias categorias de dados pessoais:

O Regulamento Geral de Protecção de Dados

- **Dados pessoais comuns;**

- **Categorias especiais de dados pessoais - dados sensíveis**: dados relacionados com a origem racial ou étnica, as opiniões políticas, crenças religiosas ou filosóficas ou afiliação sindical, os dados genéticos, dados biométricos com o objetivo de identificar de maneira exclusiva uma pessoa física e os dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual.

O Regulamento Geral de Protecção de Dados

- Apesar de ser proibido o tratamento de dados sensíveis, **o RGPD prevê algumas exceções entre as quais se destacam a obtenção do consentimento explícito, a imposição legal que decorre da legislação laboral, de segurança social ou proteção social, quando esteja em causa a proteção dos interesses vitais do titular e o mesmo esteja incapacitado para dar o consentimento, quando o tratamento seja necessário ao exercício ou à defesa de um direito num processo judicial, quando o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde.**

O Regulamento Geral de Protecção de Dados

Intervenientes no âmbito do procedimento

- É necessário conhecer os principais intervenientes e identificar o seu papel.

- **Responsável pelo tratamento**: Pessoas singulares ou coletivas que, individualmente ou em conjunto com outras, determinam as finalidades e os meios de tratamento de dados pessoais.- artigo 4.º- artigo 24.º

O Regulamento Geral de Protecção de Dados

- **Subcontratante**: aquele que trata os dados pessoais em nome do Responsável pelo Tratamento – erro de tradução deve ler-se subcontratado! - artigo 4.º – artigo 28.º;

- **Representante**: Pessoa, singular ou colectiva, designada por escrito pelo Responsável pelo Tratamento ou Subcontratado, que representa o Responsável pelo Tratamento ou o Subcontratado no que se refere às suas obrigações nos termos do regulamento – artigo 4.º – artigo 27.º;

O Regulamento Geral de Protecção de Dados

- **Destinatário**: Uma pessoa singular ou colectiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que possam receber dados pessoais no âmbito de inquéritos específicos nos termos do direito da União ou dos Estados-Membros não são consideradas destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das finalidades do tratamento – artigo 4.º;

O Regulamento Geral de Protecção de Dados

- **Terceiro**: Pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais - 4.º;

- **Encarregado da proteção de dados (DPO)**: Pessoa a quem é atribuída a responsabilidade formal de assegurar que o Organismo que o contrata está em conformidade com as regras da proteção de dados – artigo 37.º;

- **Titular dos dados**: Pessoa singular identificada ou identificável a quem os dados dizem respeito – artigo 4.º.

EU SEI ONDE VOCÊ NASCEU, ONDE VIVEU, EM QUE ESCOLA ANDOU, QUEM SÃO OS SEUS AMIGOS, QUE CARRO CONDUZ

SEI QUE RESTAURANTES FREQUENTA, A QUE CINEMAS VAI, QUE LIVROS LÊ, A QUEM TELEFONA, EM RESUMO: SEI **TUDO**

QUE TENCIONA FAZER QUANTO A ISSO?

PENSEI QUE SOUBESSE SABIA QUE VOCÊ IA DIZER ISSO.

O Regulamento Geral de Protecção de Dados

O tratamento dos dados pessoais

- Considera-se tratamento de dados a operação ou um conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

O Regulamento Geral de Protecção de Dados

O tratamento de dados pessoais **é permitido** quando o responsável pelo tratamento possui fundamento para tratar as categorias de dados pessoais solicitados.

O tratamento **só é considerado lícito se tiver subjacente**:

1- Execução de um contrato no qual o titular dos dados é parte;

2- Cumprimento de uma obrigação jurídica;

O Regulamento Geral de Protecção de Dados

3- Defesa de interesses vitais do titular dos dados;

4- Exercício de funções de interesse público ou ao exercício da autoridade pública;

5- Efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento. Neste caso, todavia, deve-se atentar à exceção contemplada no RGPD que determina que prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

O Regulamento Geral de Protecção de Dados

O consentimento dado pelo titular dos dados

O consentimento do titular dos dados consiste numa manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento. Nota-se que no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e da sua abrangência. Artigo 7.º

O Regulamento Geral de Protecção de Dados

O tratamento de dados sensíveis é em regra proibido.

Direitos dos particulares/titulares dos dados

- Direito de apagamento
- Direito de portabilidade dos dados
- Direito à limitação do tratamento
- Direito de acesso
- Direito de retificação
- Direito de oposição e decisões individuais automatizadas

O Regulamento Geral de Protecção de Dados

Direitos dos titulares

Direito de acesso - artigo 15.º

É garantido aos titulares dos dados o direito a saber se estão, ou não, a ser tratados dados pessoais que lhe digam respeito**, garantindo-se ainda o direito ao** titular dos dados de aceder aos mesmos. Esse direito de acesso deve ser tendencialmente gratuito, não obstante possa ser criada uma taxa para permitir tal acesso no caso de pedidos infundados ou excessivos.

Direito de retificação – artigo 16.º

É assegurado aos titulares dos dados o direito a obterem a retificação dos seus dados pessoais que estejam desatualizados, incorretos ou incompletos.

O Regulamento Geral de Protecção de Dados

Direito de apagamento – artigo 17.º

Este direito é uma das novidades introduzidas pelo RGPD que possibilita aos titulares dos dados o direito de solicitar ao responsável pelo tratamento dos dados o apagamento dos seus dados.

Deste modo, garante-se aos titulares dos dados, dentro das limitações estabelecidas por lei, o direito de obter a eliminação dos seus dados pessoais desde que:

Os dados se revelem desnecessários para as finalidades para os quais foram recolhidos ou tratados;

O titular retire o consentimento, quando o tratamento for necessariamente fundamentado neste e não exista outro fundamento legal para o tratamento dos dados;

O titular se oponha ao tratamento de dados pessoais utilizados para fins automatizados e/ou de profiling;

Quando os dados pessoais tenham sido tratados de forma ilícita

O Regulamento Geral de Protecção de Dados

- Na eventualidade destes serem públicos, o responsável pelo tratamento deverá informar os restantes responsáveis pelo tratamento dos dados que o titular solicitou o “apagamento das ligações para esses dados” bem como das “cópias e reproduções” dos mesmos, tomando “as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação.”

O Regulamento Geral de Protecção de Dados

Direito à limitação do tratamento – artigo 18.º

Em paralelo ao direito do apagamento, o legislador introduziu o direito à limitação do tratamento ao prever que o titular dos dados tem o direito de exigir a limitação do tratamento nas seguintes situações:

Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão;

O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização;

O responsável pelo tratamento deixar de precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;

Se se tiver oposto ao tratamento até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

O Regulamento Geral de Protecção de Dados

Direito de portabilidade dos dados – artigo 20.º

Uma das grandes novidades introduzidas pelo RGPD consiste no reconhecimento do direito de portabilidade dos dados, sendo conferido aos titulares o direito a solicitarem ao responsável pelo tratamento dos dados, os seus dados pessoais, num formato de uso comum e mesmo a sua transferência para outro responsável pelo tratamento. Todavia, o titular dos dados apenas poderá exigir que os seus dados sejam entregues a outro responsável pelo tratamento se tal for "tecnicamente possível ". O RGPD não implica para os responsáveis de tratamento a obrigatoriedade de adotar ou manter sistemas de tratamento que sejam tecnicamente compatíveis, mas os responsáveis pelo tratamento são encorajados a desenvolver formatos interoperáveis.

O Regulamento Geral de Protecção de Dados

Direito de oposição a decisões individuais automatizadas – artigo 21.º

O titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito que tenham por base interesses legítimos ou interesse público. Caso se verifique a oposição, o responsável pelo tratamento deve cessar o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

O Regulamento Geral de Protecção de Dados

Principais alterações introduzidas pelo RGPD

Entre as alterações introduzidas pelo RGPD interessa destacar:

- Maior clareza no conceito de dados pessoais;
- Maior rigor relativo ao consentimento dos titulares dos dados para o processamento dos seus dados;
- Maior facilidade e transparência no acesso aos dados pessoais pelo seu titular (ex.: tempo de resposta dada no prazo de um mês);

O Regulamento Geral de Protecção de Dados

- O direito do titular ao esquecimento, que obriga a que o responsável pelo tratamento assegure que os dados pessoais, incluindo os que foram transmitidos a terceiros, sejam efetivamente eliminados logo que tal seja solicitado pelo seu titular – difícil implementar – ver n.º 3 artigo 17.º;

- O direito do titular à portabilidade dos dados, que obriga a que o responsável pelo tratamento (entidade 1), sempre que solicitado pelo titular, disponibilize os dados pessoais que lhe tenham sido facultados num formato que possa ser facilmente transferido para um novo responsável pelo tratamento (entidade 2);

O Regulamento Geral de Protecção de Dados

- O direito do titular à oposição;

- O direito de o titular, de não ser objeto de uma medida com base na definição de perfis (“profiling”);

- Cabe aos responsáveis pelo tratamento suportar o ónus da prova do cumprimento do Regulamento;

- Os Responsáveis pelo tratamento têm que notificar a autoridade competente (até 72 horas após a ocorrência) e o titular dos dados, sobre qualquer violação de dados pessoais;

- Os responsáveis pelo tratamento efetuam uma análise do impacto do tratamento de dados, em função do risco para os direitos e liberdades dos titulares;

O Regulamento Geral de Protecção de Dados

- Sempre que o tratamento for efetuado por um organismo público, deve ser designado uma pessoa como encarregado da proteção de dados que poderá exercer outras funções e atribuições desde que não resultam num conflito de interesses.

- Os responsáveis pelo tratamento podem voluntariamente submeter-se a processo de certificação em matérias se proteção de dados;

- Em caso de incumprimento, está previsto o pagamento de coimas que poderão atingir os 10 milhões de euros ou 2% do volume de negócios anual, segundo o valor mais elevado, para violações de menor gravidade, e os 20 milhões de euros ou 4% do volume de negócios anual, nos casos mais graves.

O Regulamento Geral de Protecção de Dados

Os principais desafios para as instituições

- Obtenção do consentimento

Um dos princípios fundamentais da licitude do tratamento dos dados reside na necessidade de consentimento do titular de dados para uma finalidade claramente definida. O consentimento do titular tem que ser livre, específico, informado, explícito e por ato inequívoco. Ora é expectável que vários consentimentos já existentes não cumpram com todos os requisitos do RGPD, pelo que, estando qualquer tratamento de dados pessoais obrigado a respeitar o regulamento, deverá ser obtido um novo consentimento.

O Regulamento Geral de Protecção de Dados

Provar *by design* (por evidência) que cumprem o RGPD- 25.º

As organizações têm de conseguir provar que cumprem com o regulamento, nomeadamente:

- Que os dados pessoais que possuem são legítimos e estão limitados ao que é necessário;

- Que os dados estão atualizados, seguros e confidenciais;

- Que têm políticas, procedimentos, códigos de conduta e instruções internas, formalizadas e capazes de serem disponibilizadas às entidades de supervisão;

- Que possuem sistemas para monitorizar se as políticas e procedimentos estão a ser seguidas.

.

O Regulamento Geral de Protecção de Dados

Provar *by design* (por evidência) que cumprem o RGPD

- Sempre que possível recorrer à pseudonimização e cifragem dados estão atualizados, seguros e confidenciais;

- Que possuem sistemas para monitorizar se as políticas e procedimentos estão a ser seguidas.

.

O Regulamento Geral de Protecção de Dados

Provar *by default* (por defeito) que cumprem o RGPD

- Divulgação por todos os utilizadores das respectivas responsabilidades individuais quanto à segurança na utilização do sistema de registo dos dados pessoais.

- o acesso às funções do sistema deve ser reflectido em perfis de acesso diferenciados em razões da necessidade de conhecer e da segregação de funções.

- as credenciais de autenticação de cada utilizador devem ser únicas e intransmissíveis.

- não devem ser permitidas contas partilhadas.

O Regulamento Geral de Protecção de Dados

Provar *by default* (por defeito) que cumprem o RGPD

- a password de acesso a cada conta deve mudar a cada 180 dias e o desbloqueio de qualquer conta deve ter a intervenção do DPO.

- Autenticação mediante a impressão digital (20€ a 40€)

O Regulamento Geral de Protecção de Dados

- É assim necessário definir e **aplicar as regras do RGPD** mas também **acautelar registos probatórios do cumprimento do regulamento.**

O Regulamento Geral de Protecção de Dados

Notificação da Violação de Dados – artigo 33.º

- As organizações estão obrigadas a notificar a Comissão Nacional de Proteção de Dados no prazo de 72 horas de todas as violações de dados com risco para o titular. Para tal, é fundamental que o responsável pelo tratamento seja capaz de detetar qualquer violação de dados assim que a mesma ocorra.

O Regulamento Geral de Protecção de Dados

- **A notificação deve conter**:

  - A descrição da natureza da violação de dados pessoais, incluindo, sempre que possível, as categorias e o número aproximado de pessoas em causa, bem como as categorias e o número aproximado de registros de dados pessoais em questão;

  - O nome e os dados de contato do responsável pela proteção de dados;

  - Descrição das consequências prováveis da violação de dados pessoais;

O Regulamento Geral de Protecção de Dados

- Descrição das medidas tomadas/propostas Responsável pelo Tratamento, para reparar a violação de dados pessoais, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos negativos.

- O responsável pelo tratamento dos dados deve ainda comunicar ao titular dos dados, em linguagem acessível, e sem demora injustificada, a violação ocorrida, se esta representar um alto risco para os direitos e liberdades das pessoas em causa – artigo 34.º.

O Regulamento Geral de Protecção de Dados

- **Reforço da segurança de Dados**

- A Segurança passa pela capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento. Assim o responsável pelos dados é obrigado a implementar um sistema de gestão de segurança da informação.

O Regulamento Geral de Protecção de Dados

O *Data Protection Officer* (DPO)

- Uma das principais novidades introduzidas pelo RGPD é a figura do Encarregado de Proteção de Dados, o *Data Protection Officer* (DPO).

- As **autoridades ou organismos públicos**, **entidades que controlem regularmente dados pessoais em grande escala (Considerando 91)** e/ou que **tratem dados sensíveis em grande escala** devem nomear um DPO. O DPO reporta diretamente ao mais alto nível da organização, porquanto as funções que lhe são atribuídas pelo RGPD requer a satisfação de determinadas condições.

O Regulamento Geral de Protecção de Dados

Um DPO tem a responsabilidade de assegurar que a empresa que o contrata está devidamente *compliant* com as regras da proteção de dados.

O DPO deve informar, aconselhar e orientar a direção da organização, bem como os seus trabalhadores, a respeito das obrigações constantes do RGPD, servindo ainda como ponto de contacto com a autoridade de controlo nacional, a Comissão Nacional de Proteção de Dados.

O Regulamento Geral de Protecção de Dados

- O DPO deve notificar a Autoridade de Controlo para os casos de quebra de segurança e/ou violação de dados, melhorando os processos de gestão por forma a evitar:

- i) ataques de códigos maliciosos não autorizados;

- ii) violação de sistemas de segurança;

- iii) acessos não autorizados;

- iv) incidentes com sistemas e equipamentos de apoio

O Regulamento Geral de Protecção de Dados

- A função do DPO deverá ser integrada numa equipa multidisciplinar, com as seguintes competências e critérios:

- i) Nível de especialização: ter em conta a sensibilidade e complexidade dos dados; comunicação com os restantes departamentos

- ii) Qualidades profissionais: conhecimento da lei, regras e sistemas de informação; formação contínua

- iii) Capacidade para desempenhar as funções: integridade e ética; promoção de uma cultura de protecção de dados

O Regulamento Geral de Protecção de Dados

- A função do DPO deverá ser:

- i) independente, não recebendo instruções quanto à forma de tratar uma questão;

- ii) não deve receber instruções no sentido de adotar determinada perspectiva ou resultado de qualquer questão;

- iii) deve elaborar um relatório anual de actividades a apresentar ao Conselho de Administração

- iv) não pode ser penalizado ou destituído pelo exercício regular das suas funções

- v) não tem responsabilidade pessoal – artigo 24.º

O Regulamento Geral de Protecção de Dados

- O DPO deve:

- i) ter em consideração os riscos associados às operações de tratamento – natureza, âmbito, contexto, finalidade;

- ii) centrar esforços em questões de maior risco, identificando áreas que devam ser objecto de auditorias;

- iii) colaborar com a Autoridade de controlo, nomeadamente com consultas prévias;

- iv) ser ponto de contacto com os titulares dos dados – contacto directo é crucial para que nenhuma consequência nefasta advenha da violação registada

O Regulamento Geral de Protecção de Dados

v) conhecer bem a organização e o negócio;

vi) proceder a acções de consciencialização;

vii) estar preparado para incorporar na organização conceitos de privacy by design e privacy by default;

viii) adoptar procedimentos de detecção de incidentes; adoptar procedimentos de reacção ao incidente; adoptar procedimentos para cumprir prazos de resposta ao titular dos dados (30 dias) e de comunicação de qualquer violação (72 horas)

O Regulamento Geral de Protecção de Dados

Avaliação de impacto (PIA – Privacy Impact Assessments)

- Quando o tratamento de dados pessoais for susceptível de resultar em um alto risco para os direitos e liberdades das pessoas em causa, o Responsável pelo Tratamento, antes de iniciar o tratamento, deverá efetuar uma Avaliação de Impacto (PIA) das operações de tratamento sobre a proteção de dados, que contará com o parecer do Encarregado da proteção de dados sempre que do tratamento dos dados poder resultar num elevado risco para os direitos e liberdades dos titulares dos dados .

- Está previsto que a autoridade de controlo elabore e torne publica uma lista com os tipos de operações consideradas de elevado risco.

O Regulamento Geral de Protecção de Dados

Implementação do RGPD nos serviços de Recursos Humanos

- Perante a iminência da implementação do RGPD, as instituições devem procurar verificar a sua conformidade com o estatuído no Regulamento de modo a delinear uma abordagem que lhes permita adequar a sua actuação.

- De forma a optimizar essa validação recomenda-se que as instituições elaborem uma *checklist* que possa, de seguida, ser cruzada com a informação resultante de uma auditoria a ser conduzida nos seus serviços (levantamento de processos e dos dados tratados no âmbito desses processos)

O Regulamento Geral de Protecção de Dados

Implementação do RGPD nos serviços de Recursos Humanos

O desenvolvimento de um Programa de Conformidade prevê 3 componentes:

1- **Jurídica**

i) licitude do tratamento

ii) salvaguarda dos direitos dos titulares

Iii) cumprimento da lei

iv) adequação contratual com clientes e subcontratados

O Regulamento Geral de Protecção de Dados

Implementação do RGPD nos serviços de Recursos Humanos

2- **Processual**

i) recolha, processamento e armazenamento dos dados

ii) procedimento de notificação

Iii) políticas e processos

3- **Tecnológica**

i) segurança da plataforma e criação de passwords

O Regulamento Geral de Protecção de Dados

Violações de sistemas de protecção de dados famosas nos últimos meses:

- ZOMATO – 17 milhões de utilizadores – acesso a todos os dados de utilizadores registados na plataforma

- PIZZA HUT – ataque informático acedeu a todos os números de cartões de crédito de clientes

- Deloitte – ataque informático aos registos financeiros de clientes. 4 clientes avançaram com processos em tribunal por se considerarem prejudicados em negócios que tinham em curso

- Clube VII Ginásio – ataque informático acedeu a todos os dados dos utilizadores incluindo números de contas bancárias associadas a débito directo

Obrigada a todos pela Vossa Atenção!

Ao dispor para qualquer questão

filipamatiasmagalhaes@gmail.com