O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

Nuno Mateus-Coelho
nuno.coelho@islagaia.pt.pt
https://www.linkedin.com/in/nunormc/
www.nrmc.pt

Com o apoio da AdC Advogados

Licenciado no ISLA em Engª. Sistemas Multimédia;

Mestre no ISEP em Engª. Informática;

Doutor na UTAD e na UMIST em *Ciências da Computação;*

Membro da Ordem dos Engenheiros como Sénior Nível2;

Data Protecion Officer - Universidade de Roma "La Sapienza";

Membro da Associação Portuguesa de DPO's

Experiencia e Prática de Implementação do RGPD

REN
Redes Energéticas Nacionais

SHIFT.UP
CONSULTING

cuf

PSICOGAB PORTO

Sheraton
PORTO HOTEL & SPA

CROWNE PLAZA
HOTELS & RESORTS

altran

CENTROS DE FORMAÇÃO
TALENTO

VISÃO

vodafone

TEDx Oporto
x = independently organized TED event

IPCA
INSTITUTO POLITÉCNICO
DO CÁVADO E DO AVE

Nuno Mateus Coelho GRPD - DPO

"Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide."

Interpol, no website www.interpol.int

“O cibercrime é uma grande indústria. Os retornos são grandes e os riscos são pequenos. Estimamos que o custo global do cibercrime para a economia global rondará os 445 mil milhões de dólares [...].”

McAfee. 2014. Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II: Intel Security & McAfee. Summary

Vídeo

Proteção de dados RGPD - Enquadramento

Nuno Mateus Coelho GRPD - DPO

Diretiva 95/46/CE de 24 de Outubro de 1995

- Saída da Conselho Europeu antes de aparecer o Windows 95;
- Não existia sequer o Google;
- Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;
- Estabelecer uma união cada vez mais estreita entre os povos europeus, em fomentar relações mais próximas entre os Estados que pertencem à Comunidade;

Lei 67/98 de 26 de Outubro de 1998

- Em Portugal adapta a diretiva e o resultado é a Lei de Proteção de dados;
- Artigo 2.º - O tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais.
- Um total de 52 artigos;
- Revogou a Lei n.º 28/94, de 29 de Agosto de 1994

Lei n.º 28/94, de 29 de Agosto de 1994

- Aprovava medidas de reforço da proteção de dados pessoais em vigor à altura 10/91;

Lei 10/91 Lei da Proteção de Dados Pessoais face à Informática;

Dados pessoais - quaisquer informações relativas a pessoa singular identificada ou identificável, considerando-se identificável a pessoa cuja identificação não envolva custos ou prazos desproporcionados;

Lei n.º 28/94, de 29 de Agosto de 1994

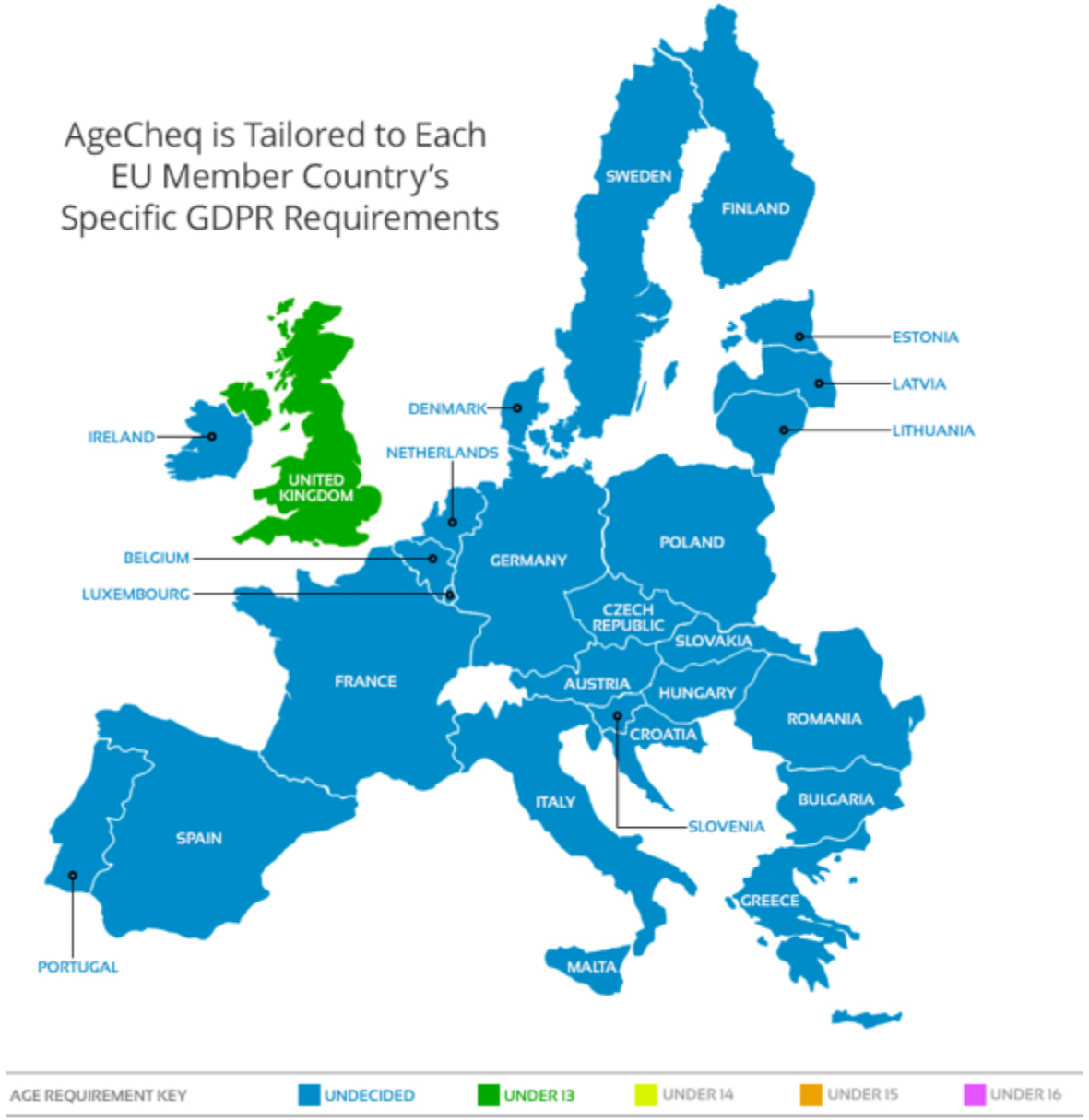
Definição de Dados pessoais no novo Regulamento:

«Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

Lei n.º 2/94, de 19 de Fevereiro de 1994

- Estabelece os mecanismos de controlo e fiscalização do Sistema de Informação Schengen

- Tudo leis entre os 7 e os 50 artigos.



Proteção de dados EU

- Vários países;
- Várias ideias;
- Vários pontos de vista;
- Vários interesses;
- Uma norma geral.

O que é o RGPD?

Regulamento (EU) 2016/679, de 27 de abril de 2016

- Está em vigor, no chamado período de transição (não necessita de transposição para os ordenamentos jurídicos dos estados-membros).
- Revoga a Diretiva 95/46/CE.
- Aplica-se a partir de 25 de maio de 2018.
- Um dos pilares do *EU Digital Single Market*.

- Um único regulamento que difere de uma diretiva;
- Entrou em vigor, de forma simultânea, no dia 25 de Maio de 2016, em todos os Estados membros da União Europeia;
- Sem necessidade de transposição impõe uma disciplina totalmente uniforme entre os vários Estados membros a partir de Maio de 2018;
- Em maio deste ano termina o período transitório previsto de dois anos.

Regulamento Geral de Proteção de Dados
O que é?

- Harmoniza a legislação sobre proteção e tratamento de dados pessoais de residentes UE, tornando clara e transversal a política a seguir por todos os que recolhem e tratem dados pessoais;

- Protege e fortalece a privacidade de dados pessoais dos residentes UE, devolvendo-lhes o controlo sobre os mesmos;

- Remodela a forma como as organizações passarão a abordar a privacidade dos dados pessoais.

Adaptar as regras de privacidade à nova era digital e criar confiança nos meios digitais.

É obrigatório a sua adoção a 100% em Portugal?

Por regra, a transposição de regulamentos segue quase "à risca" o texto proveniente das instâncias europeias – exceto nos artigos e alíneas em que os próprios regulamentos dão a possibilidade de decisão final aos estados membros.

Portanto, a resposta é SIM!

É aplicado em Portugal sem mais pacotes legislativos?

Há uma proposta de lei para ajustar a penalização por não cumprimento do RGPD?

- Sim!

- Formulada pela Presidência do Conselho de Ministros e pelo Ministério da Justiça que visa isentar o estado das responsabilidades que imputa à sociedade;

- O tratamento de dados indevido ou o acesso não autorizado poderá ser punido com penas de um ou dois anos de prisão, ou 120 e 240 dias de multa.

- Por força da proposta de lei, DPO terão de aliar conhecimentos da área jurídica específica aos conhecimentos avançados em informática.

- A proposta de lei prevê que os DPO não só garantam a realização de auditorias e de sistemas de monitorização de informação, como ainda devem «acautelar a existência de procedimentos de instalação de software antivírus e software antispam em todas as estações de trabalho e servidores utilizados» e «garantir a definição de uma política de salvaguarda da informação e do sistema (backup) que garanta a sua confidencialidade, integridade e disponibilidade»;

- As empresas que dispõem de serviços na Internet apenas possam tratar e armazenar dados de utilizadores com mais de 13 anos de idade (RGPD recomenda 16 anos);

- Profundas alteração nos sistemas de CCTV.

Será que necessitamos mesmo do RGPD?

Vídeo

A quem se aplica o RGPD?

Regulamento Geral de Proteção de Dados
A quem se aplica?

A todas as entidades que recolham[1] ou que processem[2] dados de pessoas (residentes) na UE

1 seja ou não por forma automatizada

2 incluem-se fornecedores de espaço para armazenamento em *cloud*

A que tipo de dados se aplica?

Qualquer informação relativa a uma pessoa singular identificada ou identificável.

É considerada identificável a pessoa que possa ser identificada, direta ou indiretamente, por referência a um identificador, como:

- Nome;
- Números de identificação (incluindo matrícula automóvel, número de cliente, aparelhos de portagem, etc.);
- Dados de localização;
- Quaisquer identificadores por via eletrónica (email, endereço IP, etc.);
- Quaisquer elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social
- (fotografias, voz, impressão digital, videovigilância, publicações em redes sociais, historial clínico e/ou escolar, etc.).

Algumas combinações de identificadores indiretos também permitem essa identificação*, pelo que os identificadores indiretos têm o mesmo nível de proteção que os indicadores diretos.

*um estudo recente realizado nos EUA concluiu que a data de nascimento, código postal e sexo, quando cruzados com alguns dados de localização geográfica, permitiam a identificação de 87% dos nacionais.

O que são dados pessoais?

- Todos os dados que podem ser usados direta ou indiretamente para identificar uma pessoa[1].

- Quaisquer informação relacionada com uma pessoa, quer se relacione com a sua vida privada, profissional ou pública.

[1]definição dada pela Comissão Europeia.

Categorias de dados pessoais abrangidos pelo RGPD:

- Dados pessoais[1] (nome, morada, endereço de email, endereço IP, ID de dispositivo);
- Dados pseudo-anónimos[2] (endereço de email criptografado, ID de usuário);
- Dados anónimos[3] (scripts de trilha, ID de rastreio).

[1]permitem diretamente a identificação do seu titular.

[2]permitem a identificação do seu titular através de informações adicionais.

[3]não deveriam permitir a identificação do seu titular *tout court*.

Regulamento Geral de Proteção de Dados

O que são dados pessoais?

Regulamento Geral de Proteção de Dados

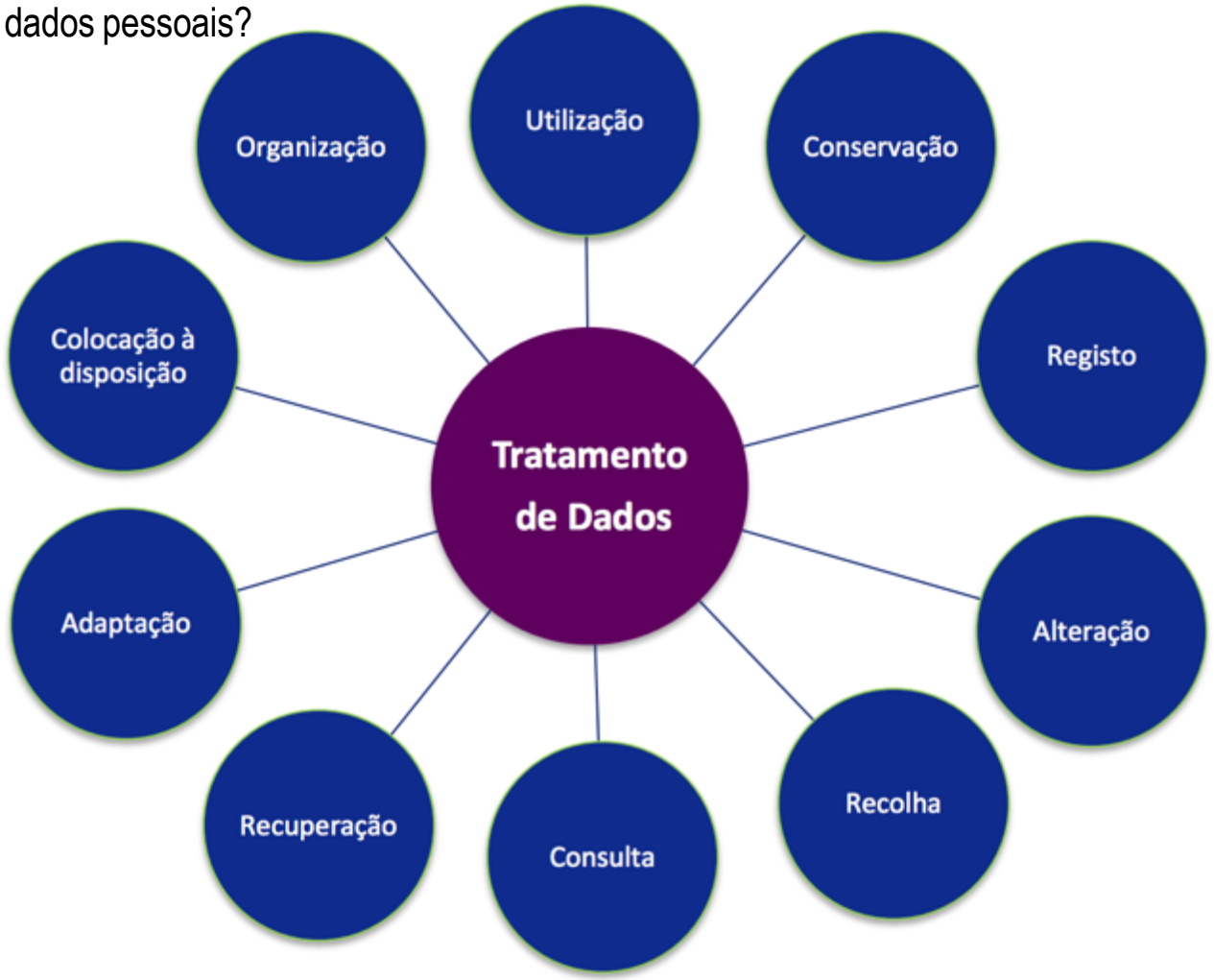
O que são dados pessoais?

Vídeo

O que é tratamento de dados pessoais?

Regulamento Geral de Proteção de Dados

O que é tratamento de dados pessoais?



- **Qualquer operação sobre dados pessoais, realizada com ou sem recurso a meios automatizados.**
  - Recolha, consulta, registo, utilização, organização, comunicação por transmissão ou difusão, conservação,
  - Destruição, eliminação, adaptação ou alteração.

Notas:

- A notificação prévia deixa de ser a regra e princípio geral, passando-se para um modelo de autorregulação ou autorresponsabilidade;
- A fiscalização e o cumprimento passam a ser responsabilidade das entidades;
- Agrava-se muito substancialmente o regime sancionatório.

- Os dados devem ser objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados;

- Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades;

- O tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos;

- Não é considerado incompatível com do artigo 89.o, n.o 1
  - Limitação das finalidades;
  - Estatísticas;
- Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

- Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);

A quem se aplica o RGPD?

Governance

Recursos Humanos

Clientes

Marketing

IT

Fornecedores

Relacionamento com Autoridade de Proteção de Dados (CNPD)

O que exige o RGPD?

- Novos direitos para os titulares dos dados.
- Novos deveres para as entidades que lidam com dados pessoais;

Princípios Gerais

- Licitude, lealdade e transparência.
- Limitação das finalidades (recolha e tratamento para finalidades determinadas, explícitas e legítimas).
- Minimização dos dados (devem ser adequados, pertinentes e limitados ao necessário relativamente à finalidades).
- Exatidão (devem ser exatos e atualizados).
- Limitação da conservação (devem ser conservados apenas durante o período em que são necessários face às finalidades).
- Integridade e confidencialidade (medidas técnicas e organizativas adequadas para garantir a privacidade dos titulares).
- Responsabilidade (ónus de demonstração do cumprimento da lei).

Licitude nas operações.

- Consentimento.
- Execução de um contrato.
- Cumprimento de obrigação legal.
- Defesa dos interesses vitais do titular.
- Exercício de funções de interesse público ou por uma autoridade pública.
- Interesses legítimos do responsável pelo tratamento ou de terceiros, contanto não devam prevalecer os interesses ou direitos do titular.

Consentimento.

- Um dos pilares do RGPD é o consentimento do titular dos dados para uma finalidade que tem que estar claramente definida.
- O consentimento tem que ser livre, específico, informado, explícito e por ato inequívoco (linguagem simples e não será possível opções pré-selecionadas).
- Revogar o consentimento tem que ser tão simples quanto conceder.
- Qualquer tratamento de dados pessoais, mesmo que recolhidos antes do RGPD, terá que cumprir os requisitos (pelo que poderá ser necessário novo).

Prova e Evidência de Cumprimento.

(*Accountability*)

- Que os dados são legítimos e limitados à finalidade definida.
- Que os dados estão atualizados, são seguros e confidenciais.
- Que têm políticas, procedimentos, códigos de conduta e instruções internas, formalizadas e capazes de serem disponibilizadas às A.S.
- Que possuem sistemas para monitorizar se tal está a ser seguido.

As organizações têm o ónus de provar que cumprem o regulamento.

Direitos e deveres dos titulares dos dados

Nuno Mateus Coelho GRPD - DPO

Novos Direitos. Adaptação e Prova.

- Direito ao esquecimento: o titular tem direito a solicitar a eliminação dos dados.
- Direito de portabilidade: o titular tem direito a solicitar a transferência dos seus dados de um prestador de serviço para outro.
- Direito de acesso à informação: o titular tem direito à consulta e edição dos dados.
- Direito de não sujeição a nenhuma decisão tomada apenas com base no tratamento automatizado (encaminhamento com base em tendências).

Importa também acautelar registos de prova de cumprimento do RGPD.

Possuem o direito a:

- Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados;

- Respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças;

- Informações sobre as medidas tomadas, mediante pedido apresentado para ter acesso aos dados, ou à portabilidade dos mesmos, sem demora injustificada e no prazo de um mês a contar da data de receção do pedido;

Possuem o direito a:

- Ser informado sem demora e, o mais tardar, no prazo de um mês a contar da data de receção do pedido, das razões que o levaram a não tomar medidas e da possibilidade de apresentar reclamação a uma autoridade de controlo e intentar ação judicial.

- Quando os dados pessoais são recolhidos, o responsável pelo tratamento deve facultar a identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;

- As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
- Categorias de destinatários dos dados pessoais, se os houver;

Possuem o direito a:

- Se os dados forem fornecidos a terceiros fora da EU, possuem o direito a receber uma cópia dos dados transmitidos;
- Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;
- Solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento, ou o direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;
- O direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;
- O direito de apresentar reclamação a uma autoridade de controlo;

Possuem o direito a informação relativa a:

- A existência de decisões automatizadas, incluindo a definição de perfis, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

Se os dados forem e não forem recolhidos junto do titular:

- A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
- Os contactos do encarregado da proteção de dados, se for caso disso;
- As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
- As categorias dos dados pessoais em questão;
- Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
- Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para fixar esse prazo.

Possuem o direito ao Acesso e à Retificação [A 15 e A16]:

- O direito de aceder aos seus dados pessoais para perceber como estão categorizados, a quem foram divulgados, onde estão a ser tratados;
- À Retificação, sem demora injustificada, pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito;

O direito ao esquecimento (apagamento dos dados) [A 17]:

- Sem demora justificada, quando:
  - Deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
  - O titular retira o consentimento;
  - O titular opõe-se ao tratamento;
  - Os dados pessoais foram tratados ilicitamente.

Possuem o direito a limitação do tratamento [A 18]:

- O titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento;
- 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 (enquanto aguarda feedback do regulador);

Possuem o direito a Portabilidade [A 20]:

- O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir;
- O direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível;

Possuem o direito de Oposição [A 21]:

- O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a licitude;
- Oposição à comercialização direta (venda de bases de dados). O titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados, incluindo os que abrangem a definição de perfis.
- Oposição desde que não colidam com a diretiva 2002/58/CE do Parlamento Europeu.
    - Relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações.

Tudo isto morre se:

a)A segurança do Estado;

b) A defesa;

c) A segurança pública;

Possuem o dever de:

- Se a comunicação de dados pessoais constitui ou não uma obrigação legal, o titular está obrigado a fornecer os dados pessoais e as eventuais e a aceitar as consequências de não fornecer esses dados;
  - Pergunta: quem se enquadra no ponto anterior?

- Ao pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações ou da comunicação, ou de tomada das medidas solicitadas;
- Facultar a sua cabal identidade para ser identificado como titular dos dados;
- Não solicitar abusivamente informações relativas aos dados;
- O dever de manter dos seus dados atuais quando o tratador é uma autoridade;

Direitos e deveres das Entidades

Nuno Mateus Coelho GRPD - DPO

Responsabilidades do Responsável pelo Tratamento [A24]:

- Contrariamente ao Titular dos dados, o Responsável pelo Tratamento tem responsabilidades acrescidas e menores direitos.

- Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento deve aplicar as medidas técnicas e organizativas adequadas para assegurar e poder comprovar que o tratamento é realizado em compliance com o RGPD.

Responsabilidades do Responsável pelo Tratamento [A24]:

- A criação e o cumprimento de códigos de conduta para demonstrar o cumprimento das obrigações do responsável pelo tratamento;

Proteção de dados desde a conceção e por defeito [A25]:

- Aplicar, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas destinadas a cumprir com os princípios da proteção de dados:
    - Pseudonimização;
    - Minimização;
    - Encriptação;
    - Segmentação;
    - Microserviços (etc).

- Aplicar medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento;

- Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade.

- As medidas anteriores asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

Reforço da Segurança de Dados.

- Implementação de um sistema de gestão de segurança da informação, controlando e restringindo o acesso aos dados pessoais.
- Proteção da informação com recurso a sistemas de segurança capazes.
- Introdução do conceito *Privacy by Design e Default:*
  - proteção de dados desde a conceção e por defeito (levará a um novo desenho dos programas e procedimentos).
- Verificações constantes que permitam confirmar a integridade dos dados, bem como ser-se capaz de evidenciar essa integridade a todo o tempo.
- Incentivo à pseudonimização (encriptação, separação, chaves de acesso, etc.).

A privacidade como prioridade.

Responsáveis conjuntos pelo tratamento [A26]:

- Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento;

- Estes determinam, por acordo entre si e de modo transparente as respetivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respetivos deveres de fornecer as informações referidas nos artigos 13.o e 14;

- O acordo pode designar um ponto de contacto para os titulares dos dados

Representantes dos responsáveis pelo tratamento ou os subcontratantes não estabelecidos na União [A27]:

- Não podem efetuar o tratamento de dados pessoais relativos a condenações penais e infrações;
- O representante deve estar estabelecido num dos Estados-Membros onde se encontram os titulares dos dados cujos dados pessoais são objeto do tratamento no contexto da oferta que lhes é feita de bens ou serviços ou cujo comportamento é controlado.
- O representante é mandatado pelo responsável pelo tratamento ou pelo subcontratante para ser contactado em substituição do responsável destes.

Subcontratante [A27]:

- Quando o tratamento dos dados for efetuado por sua conta, o responsável pelo tratamento recorre apenas a subcontratantes que garantam cumprir o RGPD;

- O subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral;

- Só é possível recorrer à subcontratação caso se estabeleça um contrato que identifique o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento.

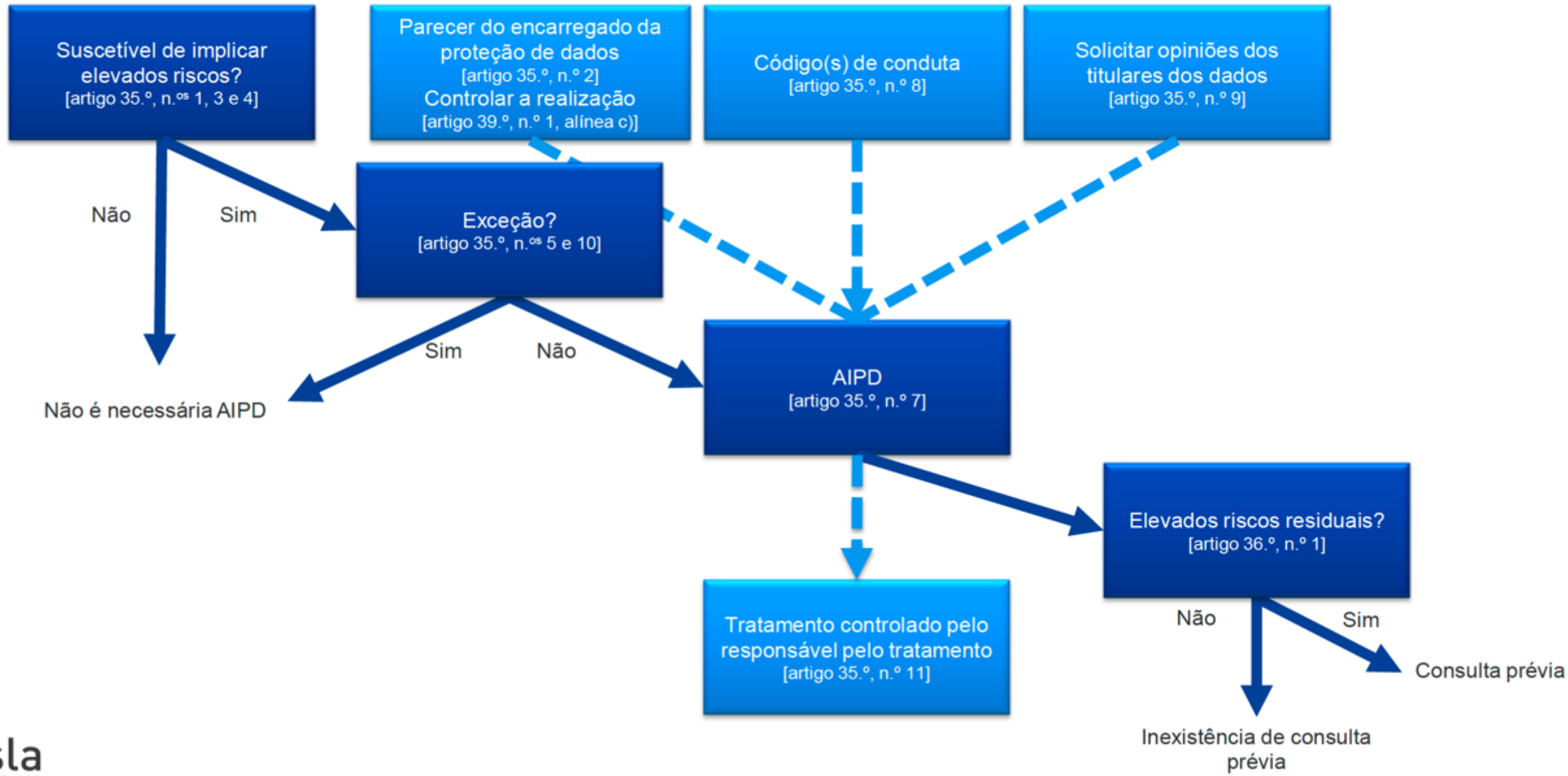
Atividades do Responsável [A30]:

- Cada responsável pelo tratamento conserva um registo de todas as atividades de tratamento sob a sua responsabilidade.
- Desse registo constam todas seguintes informações:
  1. O nome e os contactos do responsável pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados;
  2. As finalidades do tratamento dos dados;
  3. A descrição das categorias de titulares de dados e das categorias de dados pessoais;
  4. As categorias de destinatários a quem os dados pessoais foram divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais;
  5. Se possível, os prazos previstos para o apagamento das diferentes categorias de dados;
  6. Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança.

Consulta Prévia e Avaliação de Impactos [A35 e A36]:

- Quando um certo tipo de tratamento, em particular que utilize novas tecnologias for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento pela mão do DPO procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.

A figura seguinte ilustra os princípios básicos relacionados com a AIPD no RGPD:

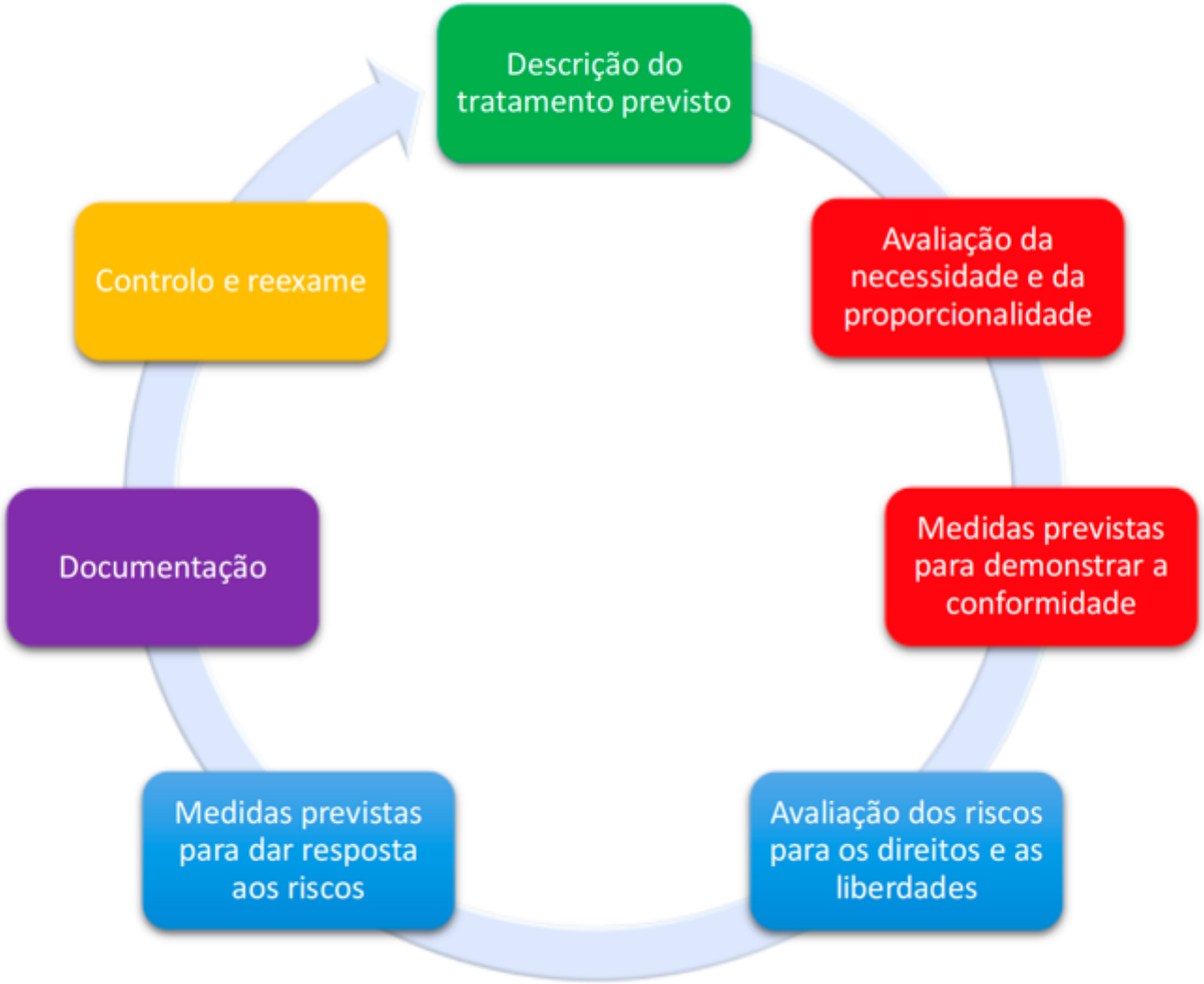


Consulta Prévia e Avaliação de Impactos [A35 e A36]:

- O responsável pelo tratamento consulta a autoridade de controlo antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados nos termos do artigo 35.o indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco.

Exemplos de tratamento	Critérios pertinentes possíveis
Um hospital que faz o tratamento dos dados genéticos e de saúde dos seus doentes (sistema de informação do hospital).	- Dados sensíveis ou dados de natureza altamente pessoal. - Dados relativos a titulares de dados vulneráveis. - Dados tratados em grande escala.
Utilização de um sistema de câmaras para controlar o comportamento dos condutores nas autoestradas. O responsável pelo tratamento pretende utilizar um sistema inteligente de análise através de vídeo para selecionar carros específicos e reconhecer automaticamente as matrículas.	- Controlo sistemático. - Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais.
Uma empresa que controle sistematicamente as atividades dos seus empregados, incluindo o controlo dos computadores, da atividade internet, etc. dos seus empregados.	- Controlo sistemático. - Dados relativos a titulares de dados vulneráveis.

Tratamento de «dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado» (considerando 91).	- Dados sensíveis ou dados de natureza altamente pessoal. - Dados relativos a titulares de dados vulneráveis.
Revista em linha que utilize uma lista de endereços de correio eletrónico para enviar fascículos diários genéricos da revista para os seus subscritores.	- Dados tratados em grande escala.
Um sítio web de comércio em linha que mostre anúncios de peças de automóveis antigos envolvendo a utilização limitada de perfis com base nos itens visualizados ou comprados no seu próprio sítio web.	- Avaliação ou classificação.


Descrição do tratamento previsto
Avaliação da necessidade e da proporcionalidade
Medidas previstas para demonstrar a conformidade
Avaliação dos riscos para os direitos e as liberdades
Medidas previstas para dar resposta aos riscos
Documentação
Controlo e reexame

E se alguma coisa corre mal como o caso Ashley Madisson ou o E-Toupeira?

- Notificação obrigatória à CNPD de todas as violações de dados com risco para o respetivo titular, no prazo máximo de 72h.

Os organizações terão que ser capazes de detetar uma fuga de dados em tempo útil, com um plano e sistemas adequados.

Encarregado de Proteção de Dados [A37, A39, A39].

- Uma das principais novidades do RGPD é a figura do Encarregado de Proteção de Dados, embora não o seja em alguns países da EU, nomeadamente os que estão a norte dela, cuja legislação previa já uma figura deste estilo.
- Em Portugal assume assume um especial relevo pela novidade do papel que desempenhará junto de uma entidade que proceda a tratamento de dados.
- Este elemento deverá estar alinhado com a direção, ou seja, sem hierarquia e sem outras tarefas que possam por em causa a sua parcialidade. Este e o elemento é o garante do cumprimentos do RGPD mas não o fará pela imposição mas pela observância de regras a implementar.
- Juridicamente, a sua responsabilidade termina com a indicação de medidas a implementar.

Encarregado de Proteção de Dados quando é necessário?

- Autoridade ou um organismo público;

- As atividades consistam em operações de tratamento que, exijam um controlo regular e sistemático dos titulares dos dados em grande escala ou dados pessoais relacionados com condenações penais e infrações (pode existir apenas um para várias entidades);

- Um grupo empresarial pode também designar um único encarregado da proteção de dados desde que seja facilmente acessível a partir de cada estabelecimento;

- O DPO é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos no domínio do direito e das práticas de proteção de dados.

- ;

Encarregado de Proteção de Dados quando é necessário?

- O DPO pode ser um elemento do pessoal da entidade responsável pelo tratamento ou do subcontratante, ou exercer as suas funções com base num contrato de prestação de serviços;
- Os seus contactos são comunicados à autoridade de controlo;
- Não receber instruções relativamente ao exercício das suas funções. O encarregado não pode ser destituído nem penalizado pelo facto de exercer as suas funções;
- O encarregado da proteção de dados informa diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante;
- Os titulares dos dados podem contactar o encarregado da proteção de dados sobre todas questões relacionadas com o tratamento dos seus dados pessoais.

Encarregado de Proteção de Dados quando é necessário?

- O encarregado da proteção de dados está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com o direito da União ou dos Estados-Membros.

- O encarregado da proteção de dados pode exercer outras funções e atribuições. O responsável pelo tratamento ou o subcontratante assegura que essas funções e atribuições não resultam num conflito de interesses.

E como se materializam estas normas?

- Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;

- Controla a conformidade do RGPD (*compliance*);

- Coopera com a autoridade de controlo;

E como se materializam estas normas?

- Presta aconselhamento e leva a cabo a organização das tarefas que respeitam à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35º;

- Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto;

- Está em auditoria constante. Tanto de processos novos como os existentes, para garantir que o RGPD é implementado e seguido à letra;

E como se materializam estas normas?

- No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento;

- Desenvolve e implementa o código de conduta.

Data Protection Officer (DPO)

- Nas entidades públicas ou de interesse público (exceto tribunais).
- Nas entidades que em grande escala (5.000 titulares) que tratem regularmente dados pessoais.
- Nas entidades que tratem dados sensíveis (ex.: criminais/c.o. e área da saúde).
- Nas entidades com 250 ou mais trabalhadores (conceito de grande empresa).

Nas entidades que tratem dados que não careçam de DPO deve ser sempre designado um responsável de dados pessoais (existe possibilidade de *outsourcing*).

Obrigatoriedade quase transversal.

EPD em regime de *outsourcing*.

- Os subcontratados para o papel de responsável pelo tratamento e/ou proteção de dados pessoais passam a ter responsabilidades acrescidas;
- Os contratos existentes têm que ser revistos;
- Novos contratos devem ser escritos e prever o balizamento de atuações das partes, em conformidade com o regulamento;
- Cabe a cada uma das partes fazer prova do cumprimento do que lhes cabe, nomeadamente nas matérias de confidencialidade e segurança.

Necessidade de contratos e de revisão dos existentes.

Autoridades de Supervisão

- ➢ Cada estado-membro terá uma A.S.
- ➢ Fiscaliza o cumprimento do regulamento.
- ➢ Recebe e investiga queixas.
- ➢ Aplica coimas e sanções.
- ➢ Recebe e trata notificações prévias (são expandidas para incluir o tempo de armazenamento dos dados e os contactos de quem recolhe os dados e do responsável pelo tratamento).
- ➢ Cooperam entre si dentro da UE.
- ➢ Reportam à EDPB (*European Data Protection Board*).
- ➢ Se uma entidade tiver mais que um estabelecimento na UE, terá apenas uma A.S. para todo o espaço UE.

O que fazer para cumprir o RGPD?

Nuno Mateus Coelho GRPD - DPO

Avaliação do impacto do RGPD.

- Inventariar os dados pessoais existentes (quais são, onde estão, para onde são transmitidos, quem tem acessos, qual o propósito principal para o seu processamento, por quanto tempo são retidos).
- Definir consentimentos válidos aplicáveis e finalidades do tratamento dos dados e verificar os requisitos de licitude desse tratamento.
- Avaliar os riscos de privacidade.
- Avaliar como assegurar os direitos dos titulares dos dados.
- Definir políticas e procedimentos num documento próprio.
- Contratação de responsáveis e serviços.

Adequação ao RGPD.

- Identificar os riscos existentes.
- Localizar os dados pessoais existentes e eliminar os não conformes.
- Consultar especialistas da legislação aplicável.
- Consultar especialistas em sistemas informáticos.
- Identificação do que é necessário para o cumprimento.
- Estudar as opções existentes de sistemas e serviços.
- Estabelecer um cronograma de atuação e de investimento.

Implementação das medidas.

- Aplicar o documento de políticas e procedimentos.
- Implementar os mecanismos de consentimento válido.
- Rever ou celebrar contratos com responsáveis e serviços subcontratados.
- Ter sistemas de monitorização e controlos adequados.
- Ter em funções um EPD ou responsável pelo tratamento dos dados.
- Implementar um sistema de gestão de riscos de privacidade.
- Assegurar os direitos dos titulares dos dados.
- Assegurar um sistema de gestão de segurança da informação.
- Ter evidência (registos) de que o regulamento é cumprido em toda a linha.

Compliance contínuo do RGPD.

- Avaliação de toda a atividade pelo EPD ou responsável pelos dados.
- Formação interna e atenção para o cumprimento da privacidade.
- Auditorias regulares de conformidade (*compliance* e *awareness*).
- Avaliar impacto quando um novo tipo de tratamento de dados é introduzido (*privacy impact assessment*).
- Teste regular e identificação das vulnerabilidades de intrusão e acesso aos dados, que permitam aferir os mecanismos de prevenção (*vulnerability mapping* e *intrusion test*).

O valor dos nossos dados

Vídeo

O RGPD não é um *one-off project* nem é algo temporário. Vejam-no como uma obrigação como o é a de inscrever os trabalhadores na segurança social.

“Privacy’s not dead. It’s hiring.”

Phil Lee, Partner at Fieldfisher

Proteção de dados – O dia-a-dia

Amanhecer 7h-9h

Abertura de emails

Consultar o email a partir do seu telemóvel pode ser em alguns casos perigoso, já que pode não ser capaz de ver toda a informação do Remetente. Se não conhece a fonte, não o abra. Se suspeita que alguma coisa possa ser perigosa, ex, Phishing, quando chegar ao escritório reporte o mais rápido possível à equipa de IT ou reporte através do botão Report Phishing presente no ecrã.

Conversar

Tenha atenção ao que está a dizer e se está a falar muito alto. Podem estar pessoas próximas de si a ouvi-lo e algumas conversas mais sensíveis podem ser classificadas de "dados pessoais".

Usar o seu telemóvel para troca de emails

Verificar se os endereços de email, conteúdos e anexos estão corretos antes de enviá-los, é uma tarefa difícil de fazer no telemóvel. Se for possível, espere até chegar ao escritório. Caso contrário, tenha a certeza de que está a utilizar o sistema de email da sua empresa.

No escritório 9h-17h

Download de documentos

Durante o trabalho, pode encontrar uma app, um browser ou um sistema de IT que acredita que vai melhorar a performance do negócio e, por isso, terá vontade de subscrevê-lo ou fazer download. Todas as requisições de software (instalações ou aplicações web) têm de ser sempre aprovadas pela equipa de IT, de forma a evitar um virus ou outro tipo de problemas.

Envio seguro de emails a partir do escritório

Utilize apenas o sistema oficial de email da empresa para assegurar que os emails são vistos e enviados de forma segura, et assim quaisquer controlos adicionais (ex. Virus, rastreio de malware, monitorização) não deixarão de ser feitos. Siga todas as políticas de segurança da equipa de IT da sua empresa, no que respeita "screen-locks", proteção de "password" e armazenamento.

Visionamento de dados pessoais ou sensíveis

Já viu dados pessoais ou sensíveis? Assegure-se que os dados são seguros. Evite partilhá-los a não ser por uma razão justificada.

Tranferência de dados pessoais

E sobre o envio de dados a parceiros? Espere até saber que a sua empresa tem um contrato ou assinou um acordo de divulgação dos mesmos. Quando aprovada a transferência, utilize uma solução segura para partilhar essa informação.

Remover ou arquivar ficheiros antigos

Tem ficheiros ou relatórios antigos? Arquive ou apague-os se não precisa mais deles. Verifique com a equipa de IT sobre processos locais aprovados, incluindo quaisquer políticas de retenção de documentos, marcação e destruição.

Fim de tarde 17h-19h

Deixar informação "disponível"

Não deixe o seu PC aberto ou com o ecrã desbloqueado. Lembre-se de bloquear sempre o seu ecrã quando deixa o PC e desligue-o totalmente quando vai para casa.

Levar dados para fora do escritório

Pode necessitar de levar dados para fora do escritório quando trabalha em casa ou está numa viagem de negócios., especialmente se estão no seu PC. Não negligencie o seu uso, independentemente de onde está a utilizá-los. Tudo o que está numa USB ou numa pasta deve continuar a ser gerido, de acordo com os habituais processos da empresa.

Eliminação de dados confidenciais

Não deixe documentos confidenciais perdidios (tal como no comboio ou noutro lugar) – tenha a certeza que os guarda, ou se não precisa mais deles, triture-os ou coloque numa zona de lixo segura.

Estar online

No regresso a casa, pense duas vezes antes de se conectar a uma rede WiFi pouca segura (ex. Viagem de comboio, ou metro). Se pretende aceder a dados pessoais, use sempre VPN (Rede Privada Virtual) que encripta os dados mesmo que através de uma rede potencialmente segura.