PROTEÇÃO DE DADOS PESSOAIS

11 de dezembro 2023 | Évora

CCDR ALENTEJO
Comissão de Coordenação
e Desenvolvimento Regional do Alentejo, I.P.

Enquadramento legal

- No quadro do Conselho da Europa, Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Em 2018, os signatários da Convenção chegaram a acordo sobre um protocolo de alteração para a atualizar: a Convenção 108+);

- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 – Regulamento Geral sobre a Proteção de Dados Pessoais (em vigor deste 25 de maio de 2018);

- Instrumentos europeus que foram acolhidos no direito interno pelas Leis n.ºs 58/2019 e 59/2019, de 8 de agosto.

Terminologia sobre proteção de dados

❑ Dados Pessoais

O Regulamento Geral da Proteção de Dados Pessoais (RGPD), no ponto 1 do seu artigo 4.º, define «dados pessoais» como *informação relativa a uma pessoa singular identificada ou identificável («Titular dos dados»).*

Ou seja,

- Tratam-se de informações sobre uma pessoa singular;
- Para aferição daquela identidade ou identificabilidade, relevam todos os meios razoáveis suscetíveis de ser utilizados para reconhecer a pessoa direta ou indiretamente;
- Se forem tratados dados sobre essa pessoa, esta é designada como «titular dos dados».

Terminologia sobre proteção de dados

❑ Dados Pessoais

Deste modo,

as informações contêm dados sobre uma pessoa se:

- Essa pessoa estiver identificada ou for identificável por essas informações;

ou se

- Essa pessoa, embora não identificada, puder ser individualizada por estas informações de uma forma que permita descobrir quem é o titular dos dados mediante a realização de pesquisas adicionais.

TJUE, acórdão de 29 de janeiro de 2008 no processo C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [GS], n.º 45;

TJUE, acórdão de 13 de maio de 2014 (Grande Secção), Google Spain e Google (C-131/12, EU:C:2014:317).

Terminologia sobre proteção de dados

❑ Dados Pessoais

Em suma,

Para estarmos perante uma situação enquadrável no âmbito do regime jurídico da proteção de dados, não é necessária a identificação efetiva da pessoa em causa, bastando que esta seja identificável.

Será identificável se estiverem disponíveis suficientes elementos de identificação que permitam identificar direta ou indiretamente essa pessoa.

De acordo com o considerando 26 do RGPD, importa saber se é provável que meios razoáveis de identificação estarão disponíveis e serão administrados por utilizadores previsíveis da informação, o que inclui as informações detidas por terceiros/destinatários.

Terminologia sobre proteção de dados

❑ Dados Pessoais

Exemplo:

Uma Junta de Freguesia decide recolher dados sobre os veículos que ultrapassam o limite de velocidade nas ruas da freguesia. Para tal, fotografa os veículos, registando automaticamente a hora e o local, a fim de transmitir os dados à autoridade competente para que esta possa aplicar multas àqueles que violaram os limites de velocidade.

Uma das pessoas em causa apresenta uma queixa, alegando que nenhuma disposição da legislação sobre proteção de dados habilita aquela autarquia local a recolher esses dados.

A Junta de Freguesia entende que não está a recolher dados pessoais, afirmando que as matrículas são dados anónimos, dado não ter competência para consultar o registo automóvel geral para saber a identidade do proprietário ou condutor do veículo.

Terminologia sobre proteção de dados

❑ Dados Pessoais

Este argumento é incompatível com o disposto no considerando 26 do RGPD.

Uma vez que a finalidade da recolha dos dados é claramente identificar e multar aqueles que ultrapassam os limites de velocidade, é previsível que se tente proceder àquela identificação. Embora a Junta de Freguesia não tenha diretamente ao seu dispor os meios de identificação, os dados serão transmitidos à autoridade competente — a polícia — que possui tais meios;

O considerando 26 também prevê expressamente um cenário em que é previsível que outros destinatários dos dados, além do utilizador imediato, possam tentar identificar a pessoa;

À luz do considerando 26, os atos da autoridade local equivalem à recolha de dados sobre pessoas identificáveis e, como tal, necessitam de uma base legal ao abrigo da legislação sobre proteção de dados.

Terminologia sobre proteção de dados

❑ Anonimização

De acordo com o RGPD (princípio de limitação da conservação), os dados devem ser conservados *de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados* [*cfr*. alínea *e)* do ponto 1 do artigo 5.º];

Consequentemente, os dados têm de ser apagados ou anonimizados se um responsável pelo tratamento os desejar conservar depois de estes deixarem de ser necessários e de cumprirem a sua finalidade inicial;

O processo de anonimização dos dados significa que todos os elementos de identificação são eliminados de um conjunto de dados pessoais, de forma que o seu titular já não possa ser identificado.

Sobre as técnicas de anonimização:

Parecer 05/2014, do Grupo de Trabalho do Artigo 29.º [Com a entrada em vigor do RGPD, este Grupo deixou de existir e foi substituído pelo Comité Europeu para a Proteção de Dados (CEPD)].

Terminologia sobre proteção de dados

❑ Anonimização

Principais conclusões:

- Reconhecendo o valor potencial de tais técnicas, sublinha que algumas delas não resultam necessariamente em todos os casos;

- Para encontrar a melhor solução numa determinada situação, o processo adequado de anonimização deve ser decidido caso a caso;

- Independentemente da técnica utilizada, a identificação deve ser evitada de forma irreversível. Ou seja, para a anonimização dos dados, não deve ser deixado nenhum elemento nas informações que possa servir, mediante o exercício de um esforço razoável, para reidentificar a(s) pessoa(s) em causa;

- O risco de reidentificação pode ser apreciado tendo em conta *os prazos, esforços ou recursos necessários à luz da natureza dos dados, do contexto da sua utilização, das técnicas de reidentificação disponíveis e dos respetivos custos*.

Terminologia sobre proteção de dados

❑ Anonimização

Sendo anonimizados com êxito deixam de ser dados pessoais e a legislação sobre a proteção de dados deixa de ser aplicável.

O RGPD prevê que a pessoa ou a organização responsável pelo tratamento dos dados pessoais não podem ser obrigadas a manter, obter ou tratar informações suplementares para identificar o titular dos dados com o único objetivo de dar cumprimento ao regulamento;

Contudo, esta regra tem uma exceção importante:

Sempre que o titular dos dados, com a finalidade de exercer os direitos de acesso, retificação, apagamento, limitação do tratamento e portabilidade dos dados, fornecer informações adicionais ao responsável pelo tratamento que permitam a sua identificação, esses dados que tinham sido previamente anonimizados voltam a ser dados pessoais (*cfr*. artigo 11.º do RGPD).

Terminologia sobre proteção de dados

❑ Anonimização

ENTIDADE PÚBLICA XPTO, E.P.E.

DADOS CIDADÃOS

NOME	CARTÃO CIDADÃO	CORREIO ELETRÓNICO	N.º DE PROCESSO
Bartolo de SassoFerrato	125789	Bsassoferrato@hotmail.com	A125789
André Horta	548355	Andre.Horta@gmail.com	A125790
Ricardo Costa	879654	Costa.ricardo@yahoo.com	A12591
Mickey Mouse	759125	Mmouse@disney.com	A12592

ENTIDADE PÚBLICA XPTO, E.P.E.

DADOS CIDADÃOS

NOME	CARTÃO CIDADÃO	CORREIO ELETRÓNICO	N.º DE PROCESSO
Bxxxxxxxxxxto	1xxxxx	Bxxxxxxxx@hotmail.com	A125789
Axxxxxxxa	5xxxxx	Axxxxx@gmail.com	A125790
Rxxxxxxxa	8xxxxx	Cxxxxx@yahoo.com	A12591
Mxxxxxxxxe	7xxxxx	Mxxxx@disney.com	A12592

Terminologia sobre proteção de dados

❑ Pseudonimização

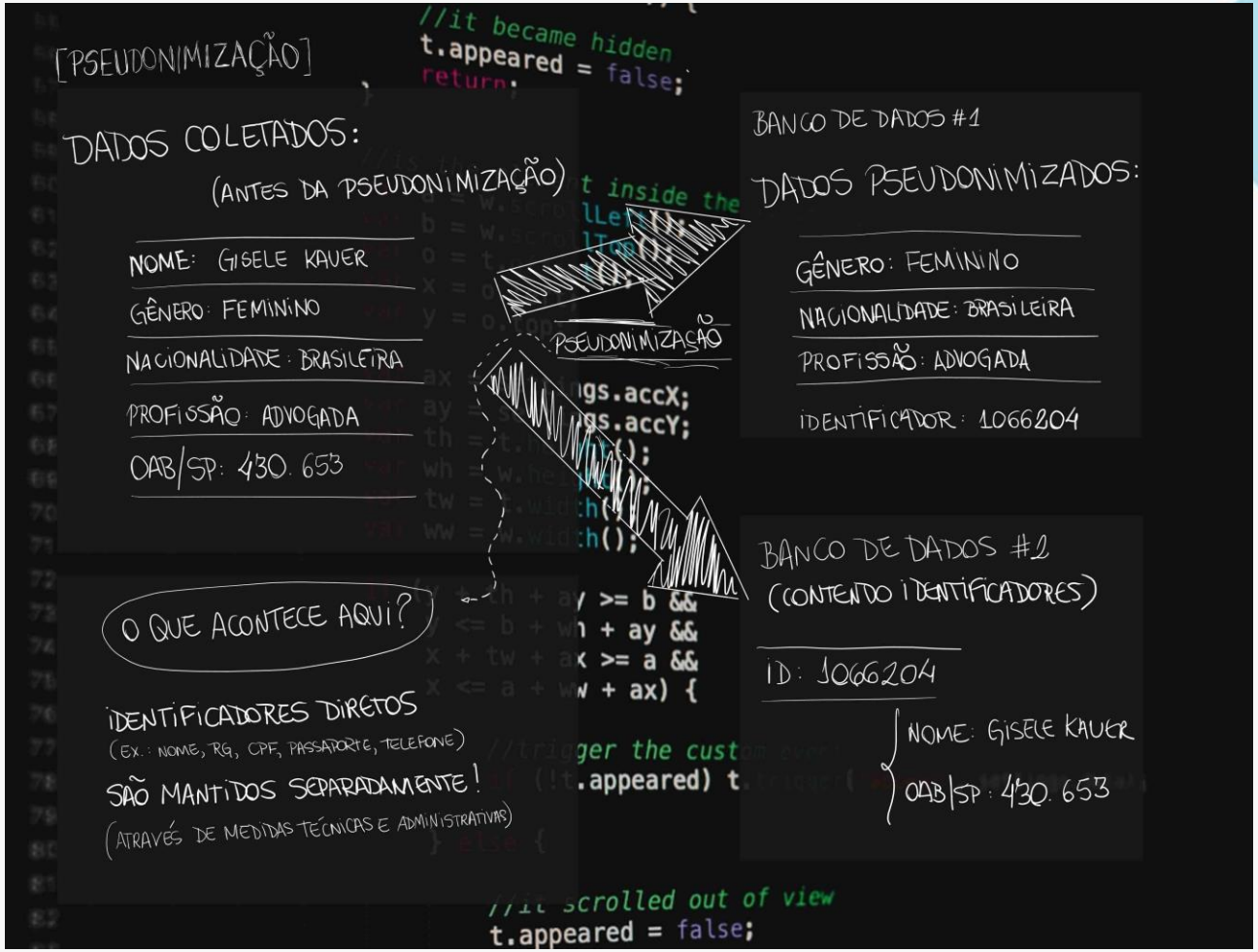
As informações pessoais contêm atributos, como o nome, data de nascimento, sexo, morada, ou outros elementos que podem levar à identificação;

O RGPD define «pseudonimização» como *o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sejam sujeitas a medidas técnicas e organizativas destinadas a assegurar que os dados pessoais não sejam atribuídos a uma pessoa singular identificada ou identificável* (*cfr.* ponto 5 do artigo 4.º);

O processo de pseudonimizar dados pessoais significa que estes atributos são substituídos por um pseudónimo;

Terminologia sobre proteção de dados

❑ Pseudonimização



- Medida através da qual os dados pessoais deixam de poder ser atribuídos ao titular de dados sem recorrer a informações suplementares, as quais são mantidas separadamente;
- A *chave* que permite a reidentificação dos titulares dos dados deve ser mantida separada e segura;
- Os dados que tenham sido objeto de um processo de pseudonimização continuam a ser dados pessoais;
- Uma forma de pseudonimizar dados é através da cifragem dos dados.

Terminologia sobre proteção de dados

❑ Categorias específicas de dados pessoais

Existem categorias específicas de dados pessoais que podem, pela sua própria natureza, representar um risco para as pessoas em causa quando são tratados e que, por essa razão, exigem uma proteção reforçada;

Em regra, estes dados estão sujeitos a um princípio de proibição e existe um número limitado de situações em que o seu tratamento é legal;

No quadro do disposto no artigo 9.º do RGPD, são considerados dados sensíveis os enquadráveis nas seguintes categorias:

- Dados pessoais que revelem a origem racial ou étnica;
- Dados pessoais que revelem as opiniões políticas, as convicções religiosas ou outras, incluindo convicções filosóficas;
- Dados pessoais que revelem filiação sindical;
- Dados genéticos e dados biométricos tratados para efeitos de identificação de uma pessoa;
- Dados relativos à saúde, à vida sexual ou à orientação sexual.

Terminologia sobre proteção de dados

❑ Tratamento de dados

- «Tratamento [de dados pessoais]» corresponde a [...] *uma operação* [...] *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, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição de dados pessoais* (*cfr*. ponto 2 do artigo 4.º);

- Exemplo 1: Os empregadores recolhem e tratam dados sobre os seus trabalhadores, incluindo informações relativas aos seus salários. Qual o fundamento?

O contrato de trabalho constitui a base legal para que o possam fazer legitimamente.

- Exemplo 2: Os empregadores são obrigados a reencaminhar os dados sobre os salários do seu pessoal para as autoridades fiscais. Este reencaminhamento constitui «tratamento» RGPD. Qual o fundamento?

A operação de tratamento que resulta na transferência de dados sobre salários do empregador para as autoridades fiscais, resulta das disposições da legislação fiscal.

Na ausência destas disposições — e de qualquer outro motivo legítimo de tratamento — a transmissão dos dados constituí um tratamento ilegal!!

Terminologia sobre proteção de dados

❑ Tratamento de dados

O tratamento de dados pode ser:

- Automatizado

Que se refere às operações efetuadas sobre dados pessoais por meios total ou parcialmente automatizados.

Exemplo: gestão de recursos humanos, pagamento de vencimentos, acesso/consulta de bases de dados de contactos da qual constem dados pessoais, armazenamento de endereços IP, publicação/colocação de fotografias de pessoas num sítio *web*, gravação de vídeo)

- Não automatizado

Tratamento de dados pessoais num sistema de ficheiros manual (ficheiro em papel estruturado de acordo com critérios específicos).

Exemplo: se o empregador mantém um ficheiro em papel intitulado "férias e licenças dos trabalhadores", que contenha todas as informações sobre férias e licenças gozadas pelo pessoal no ano anterior e que está ordenado por ordem alfabética, o ficheiro constitui um sistema de ficheiros manual e, portanto, sujeito às regras sobre proteção de dados.

Terminologia sobre proteção de dados

❑ Utilizadores dos dados

- **Responsável pelo tratamento**

A pessoa que determina os meios e as finalidades do tratamento de dados pessoais de terceiros é o «responsável pelo tratamento» (*cfr*. ponto 7 do artigo 4.º do RGPD);

Se a decisão for tomada em conjunto por várias pessoas, estas poderão ser consideradas como «responsáveis conjuntos pelo tratamento»;

- **Subcontratante**

Uma pessoa singular ou coletiva que trata os dados pessoais por conta do responsável pelo tratamento (*cfr*. ponto 8 do artigo 4.º do RGPD);

Este passa a ser considerado «responsável pelo tratamento» quando ele próprio determine os meios e as finalidades do tratamento de dados;

Estão obrigados

- A conservar um registo de todas as categorias de atividades de tratamento para demonstrar a observância das suas obrigações previstas no regulamento (*cfr*. artigo 30.º, n.º 2 do RGPD);

Terminologia sobre proteção de dados

❑ Utilizadores dos dados

- A aplicar as medidas técnicas e organizativas adequadas para assegurar a segurança do tratamento (*cfr*. artigo 32.º do RGPD);
- A designar um encarregado da proteção de dados em determinadas situações (*cfr*. artigo 37.º do RGPD); e
- A notificar o responsável pelo tratamento das violações de dados pessoais (*cfr*. artigo 32.º, n.º 2 do RGPD).

Por razões de transparência, os elementos concretos da relação entre o responsável pelo tratamento e o subcontratante devem constar de um contrato reduzido a escrito (*cfr*. artigo 28.º, n.ºs 3 e 9 do RGPD), do qual conste, designadamente, o objeto, a natureza, a finalidade e a duração do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados. Também deve estipular as obrigações e direitos do responsável pelo tratamento e do subcontratante, tais como os requisitos relativos à confidencialidade e à segurança.

- Destinatários e terceiros

Um «terceiro» é alguém juridicamente distinto do responsável pelo tratamento e do subcontratante.

O «destinatário» poderá ser a pessoa ou entidade não pertencente ao responsável pelo tratamento ou ao subcontratante — caso em que seria então um terceiro — ou pertencente ao responsável pelo tratamento ou ao subcontratante, tal como um trabalhador ou outra divisão da mesma empresa ou autoridade.

Terminologia sobre proteção de dados

❑ Consentimento

O consentimento constitui um dos seis fundamentos de legitimidade para o tratamento de dados pessoais (*cfr*. artigo 6.º, n.º 1 do RGPD).

Entende-se por consentimento *uma manifestação de vontade*[...] *livre, específica, informada e explícita* [do titular dos dados] (*cfr*. artigo 4.º, n.º 11 do RGPD).

O consentimento será válido quando:

- Seja dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito (Esse ato pode ser uma ação ou uma declaração);
- Se garanta o direito do titular de dados a retirar o seu consentimento a qualquer momento;
- No contexto de uma declaração escrita que diga também respeito a outros assuntos, como «condições de serviço», os pedidos de consentimento devem ser apresentados numa linguagem clara e simples, de modo inteligível e de fácil acesso e de uma forma que os distinga claramente desses outros assuntos.

O consentimento só será válido na aceção da legislação sobre proteção de dados se todos estes requisitos estiverem preenchidos.

Princípios fundamentais

O artigo 5.º do RGPD estabelece os princípios que regem o tratamento de dados pessoais.

Estes princípios incluem:

- A licitude, a lealdade e a transparência;
- A limitação das finalidades;
- A minimização dos dados;
- A exatidão dos dados;
- A limitação da conservação;
- A integridade e a confidencialidade.

Princípios fundamentais

❑ Os princípios da licitude, da lealdade e da transparência do tratamento

Aplicam-se a todo o tratamento de dados pessoais.

Nos termos do RGPD, a licitude exige uma das seguintes condições:

- O consentimento do titular dos dados;
- A necessidade de celebrar um contrato;
- Uma obrigação legal;
- A necessidade para a defesa dos interesses vitais do titular dos dados ou de outra pessoa;
- A necessidade para o exercício de funções de interesse público;
- A necessidade para os interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos do titular dos dados.

Princípios fundamentais

❑ Os princípios da licitude, da lealdade e da transparência do tratamento

O tratamento dos dados pessoais deve ser feito de forma leal.

- O titular de dados deve ser informado do risco para garantir que o tratamento não tem efeitos negativos imprevisíveis.

O tratamento dos dados pessoais deve ser feito de forma transparente.

- Os responsáveis pelo tratamento devem informar os titulares dos dados antes do tratamento dos seus dados, entre outros elementos, sobre a finalidade do tratamento e sobre a identidade e a morada do responsável pelo tratamento;
- A informação sobre as operações de tratamento deve ser fornecida em linguagem clara e simples para permitir aos titulares dos dados compreender facilmente as regras, riscos, salvaguardas e direitos envolvidos;
- Os titulares dos direitos têm o direito de aceder aos respetivos dados independentemente do local onde sejam tratados.

Princípios fundamentais

❑ O princípio da limitação das finalidades

- A finalidade do tratamento de dados tem de estar definida antes de as operações de tratamento terem início.

- Não é permitido o tratamento posterior dos dados que seja incompatível com a finalidade inicial, embora o RGPD preveja exceções a esta regra para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos.

Exemplo: Uma companhia aérea recolhe dados dos seus passageiros para efetuar reservas, com vista a assegurar a correta operação do voo (números dos lugares dos passageiros; restrições físicas especiais, tais como necessidades de uma cadeira de rodas; e requisitos alimentares especiais, tais como alimentos *kosher* ou *halal)*.

Se for pedido às companhias aéreas que transfiram esses dados contidos no Registo de Identificação de Passageiros para as autoridades de imigração no aeroporto de destino, esses dados estarão a ser utilizados para fins de controlo da imigração, que são diferentes da finalidade para que foram inicialmente recolhidos.

Como tal, a transmissão desses dados para uma autoridade de imigração exige uma base legal autónoma.

Princípios fundamentais

❑ O princípio da minimização dos dados

- O tratamento de dados deve ser limitado ao que é necessário para cumprir uma finalidade legítima;
- O tratamento de dados pessoais só deve acontecer quando a finalidade do tratamento não possa ser razoavelmente cumprida por outros meios;
- O tratamento de dados não pode interferir de forma desproporcional com os interesses, direitos e liberdades em causa;

Exemplo: Os utilizadores regulares do sistema municipal de transportes públicos utilizam um cartão com chip (passe), o qual contém o nome do utilizador (escrito no cartão e em forma eletrónica no chip). Quando utiliza o autocarro, o passageiro tem de passar o cartão por um dispositivo de leitura. Os dados lidos pelo dispositivo são eletronicamente comparados com uma base de dados com os nomes das pessoas que compraram o passe.

Este sistema não cumpre da melhor forma o princípio da minimização: para verificar se uma pessoa está ou não autorizada a utilizar determinados meios de transporte, não é necessário comparar os dados pessoais constantes do chip do cartão com uma base de dados. Bastaria, por exemplo, incluir uma imagem eletrónica especial, como um código de barras, no chip do cartão que o passageiro passaria em frente do dispositivo de leitura para confirmar se o cartão era ou não válido, não registando o nome dos utilizadores, o transporte utilizado ou a hora da utilização.

Princípios fundamentais

❑ O princípio da exatidão dos dados

- O responsável pelo tratamento deve aplicar o princípio da exatidão dos dados em todas as operações de tratamento;

- Os dados inexatos devem ser apagados ou retificados sem demora;

- Pode ser necessário controlar regularmente e manter atualizados os dados para assegurar a exatidão.

ATENÇÃO:

A obrigação de assegurar a exatidão dos dados tem de ser interpretada no respetivo contexto, porque haverá situações em que a respetiva finalidade é documentar acontecimentos como «instantâneos» históricos (por exemplo, o registo de uma cirurgia) e outras em que é absolutamente necessário atualizar e controlar regularmente a exatidão dos dados, devido aos potenciais danos que o titular dos dados poderá sofrer se os dados se mantiverem inexatos (por exemplo, um registo da situação financeira de um determinado cidadão)

Princípios fundamentais

O princípio da limitação da conservação

Tanto o artigo 5.º, n.º 1, alínea *e)* do RGPD como o artigo 21.º da Lei n.º 58/2019, de 8 de agosto exigem que os dados pessoais sejam conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados.

Assim,

- Cabe ao responsável pelo tratamento fixar os prazos para o apagamento ou a sua revisão periódica;
- Quando as finalidades que justificaram o tratamento tenham sido atingidas, devem os dados ser apagados ou anonimizados;
- A limitação temporal do armazenamento de dados pessoais só é aplicável aos dados conservados sob uma forma que permita a identificação dos titulares dos dados (sendo possível armazenar licitamente dados, desde que mediante a respetiva anonimização).

Princípios fundamentais

❑ O princípio da segurança dos dados

- A segurança e a confidencialidade dos dados pessoais são fundamentais para impedir os efeitos negativos para o titular dos dados;

- As medidas de segurança podem ser de natureza técnica e/ou organizativa;

- A pseudonimização é um processo que pode proteger dados pessoais;

- A adequação das medidas de segurança deve ser decidida caso a caso e revista com regularidade.

Princípios fundamentais

O princípio da responsabilidade

- A responsabilidade exige a implementação ativa e contínua de medidas pelos responsáveis pelo tratamento e pelos subcontratantes para promoverem e salvaguardarem a proteção de dados nas suas atividades de tratamento;

- Compete aos responsáveis pelo tratamento e aos subcontratantes assegurar a conformidade das suas operações de tratamento com a legislação sobre proteção de dados e respetivas obrigações;

- Os responsáveis pelo tratamento devem estar em condições de demonstrar, em qualquer momento, a conformidade com as disposições sobre proteção de dados aos titulares dos dados, ao público em geral e às autoridades de controlo;

- Os subcontratantes também devem cumprir algumas obrigações estritamente relacionadas com a responsabilidade (como conservar um registo de operações de tratamento e designar um encarregado da proteção de dados).


WHAT
NOW?

Road Map RGPD

❑ Da implementação aos resultados

A implementação do RGPD depende de uma identificação e mitigação de riscos.

O processo inicia-se com a identificação das ameaças e da probabilidade de estas acontecerem.

Este levantamento deve considerar quatro dimensões fundamentais:

- Hardware e software;
- Processos e procedimentos relacionados com operações de processamento de informação;
- Partes interessadas e envolvidas nas operações de processamento da informação;
- Setor de atividade e escala do processamento.

Road Map RGPD

❑ *Da implementação aos resultados*

A metodologia utilizada orienta-se nos seguintes objetivos :

- Dar resposta direta às necessidades da entidade (em sede de aplicação do RGPD);
- Passar o conhecimento obtido aos trabalhadores e subcontratantes da entidade.

Objetivos que se mesclam ao longo do projeto, dado que em todas as fases terão de ser efetuados os *reports* considerados necessários.

- No primeiro objetivo, é estruturante a caracterização das ações de recolha, tratamento, conservação e segurança dos dados pessoais no âmbito dos processos administrativos desenvolvidos;
- Com base nas respetivas atribuições e competências, importa mapear os principais processos em que se identificou o tratamento de dados pessoais, e identificar os respetivos responsáveis internos, para a caraterização dos tratamentos e identificação dos fatores de risco associados.

Road Map RGPD

❑ Da implementação aos resultados

Matriz		Princípios	Resultados Previstos
Identificação dos Processos de Negócio	Atividades		Política de Privacidade Registos de Atividades de Tratamento
	Ações		
Recolha	Que informação recolho?	Minimização dos dados	Novos Formulários Declaração de Consentimento Formas de Comunicação
	De que forma recolho a informação?	Minimização dos dados	
	Qual a finalidade da informação recolhida?	Limitação das finalidades	
	Tenho autorização para utilizar a informação?	Licitude	
Tratamento	O que fazemos aos dados recolhidos?	Exatidão Responsabilidade	Documentação de procedimentos
	Qualidade dos dados		
	Legitimidade legislativa/normativa		
Conservação	Onde encontramos os dados (papel/digital/misto)?	Limitação da conservação	Documentação de procedimentos (eliminação dos dados após o prazo legal/administrativo)
	Durante quanto tempo conservamos?		
Segurança	Avaliação global de impacto	Integridade Confidencialidade	Plano de gestão de incidentes Plano de gestão de acessos

Matriz de caracterização de resultados que permitirá:

- Documentar procedimentos
- Definir prazos de conservação adequados
- Definir e publicitar regras internas de tratamento e gestão de dados pessoais
- Melhorar o procedimento relativo à obtenção de consentimento por parte do titular dos dados
- Estabelecer formas de comunicação interna e externa

Road Map RGPD

❑ Da implementação aos resultados

- Política de privacidade

Visa a publicitação das regras de tratamento e gestão dos dados pessoais, integrando os requisitos do regulamento de proteção de dados;

Este documento traduz o compromisso da entidade com a proteção de dados pessoais e marca o conjunto de alterações que são promovidas para o cumprimento dos princípios;

A política de privacidade não será estanque devendo ser revista e atualizada periodicamente, de acordo com as práticas que sejam adotadas, garantindo maior transparência na informação prestada aos titulares dos dados.

- Registos de atividades de tratamento

Obrigação imposta pelo artigo 30.º do RGPD para os responsáveis pelo tratamento e para os subcontratantes;

O conteúdo dos registos é distinto consoante se trate de um responsável pelo tratamento ou de um subcontratante;

Quando uma entidade realize tratamentos de dados enquanto responsável pelo tratamento e enquanto subcontratante, deve manter dois registos diferenciados.

Road Map RGPD

❑ Da implementação aos resultados

- Comunicação

Atento o princípio da licitude, importa analisar a forma como está a ser efetuada a gestão dos dados pessoais nos diversos canais de comunicação (evitar outros processamentos ou reutilizações não previstas, quer a nível legal como contratual).

- Documentação de procedimentos

Tendo por objetivo verificar o cumprimento dos princípios da exatidão e da responsabilidade, importa responder às seguintes questões:

O que fazemos aos dados que são recolhidos? Qual a sua finalidade? Qual a sua fonte de legitimação?

E, se necessário, rever fluxos e procedimentos de modo a adotar as medidas adequadas para manter os dados exatos e atualizados, e a documentar os procedimentos de modo a comprovar a atuação do responsável pelo tratamento.

Road Map RGPD

❑ *Da implementação aos resultados*

- Violação de dados ou *Data Breach*

Sempre que 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 (*cfr*. artigo 4.º, ponto 12 do RGPD);

O dever de notificação à autoridade nacional de controlo (CNPD) constitui uma obrigação do responsável pelo tratamento, até 72 horas após conhecimento da mesma (*cfr*. n.º 1 do artigo 33.º do RGPD);

Importa definir e implementar uma política interna de gestão de incidentes (por exemplo, em sede de código de conduta).

ATENÇÃO:

Mesmo que se considere que não é exigível a notificação à CNPD, o responsável pelo tratamento está obrigado a documentar quaisquer violações de dados (*cfr*. n.º 5 do artigo 33.º do RGPD).

Road Map RGPD

❑ Conclusões

- Este projeto, comummente pensando como forma de adequar as entidades ao contexto jurídico, é dinâmico o que obriga a um acompanhamento contínuo, atentas as constantes mudanças decorrentes da própria Administração Pública;

- É necessário garantir que todos os que têm relações com as entidades, seja a nível interno como externo, têm plena consciência das exigências a nível de tratamento de dados pessoais, o percurso dos mesmos e como estão salvaguardados;

- Ações de divulgação, formações e mapeamento de processos são fundamentais para garantir a adequabilidade pretendida;

- Abordagem multidisciplinar no acompanhamento, operacionalização e implementação das políticas de privacidade.

CCDR ALENTEJO
Comissão de Coordenação e Desenvolvimento Regional do Alentejo

MUITO OBRIGADO!!

Nuno Sousa
Contactos:
E-mail: nuno.sousa@ccdr-a.gov.pt
Telefone: 266740300