DIREÇÃO-GERAL
DA QUALIFICAÇÃO
DOS TRABALHADORES
EM FUNÇÕES PÚBLICAS

RGPD PARA CIDADÃOS ATENTOS

Manual de curso online

DIREÇÃO-GERAL DA QUALIFICAÇÃO
DOS TRABALHADORES EM FUNÇÕES PÚBLICAS

FICHA TÉCNICA

Título: RGPD para cidadãos atentos: manual de curso *online*

Autor: Filomena Vieira

Editor: Direção-Geral da Qualificação dos Trabalhadores em Funções Públicas (INA)
Rua Filipe Folque, 44
1069-123 Lisboa – Portugal
Tel.: (+351) 214465300
E-mail: ina@ina.pt
URL: http://www.ina.pt

Local de edição: Lisboa

Data de edição: Novembro de 2018

Cofinanciado por:
COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

ÍNDICE

I. O que é, afinal, o novo Regulamento Geral sobre Proteção de Dados de que todos falam? 1
1. Vamos conhecer o RGPD 1
1.1. O que é o RGPD e quem o aprovou 1
1.2. Quando passou a ser aplicado o RGPD 1
1.3. Principal objetivo a atingir com o RGPD 1
1.4. Entidades obrigadas a cumprir o RGPD e titulares a quem este se aplica 2
1.5. O RGPD como apoio ao desenvolvimento económico assente no Mercado Único Digital 3
1.6. Conclusão: porque é que o RGPD é importante para todas as pessoas 3
2. O que são dados pessoais 3
2.1. O conceito de dados pessoais 3
2.2. Categorias especiais de dados 4
3. Por que motivo foi aprovado o RGPD 4
3.1. A última regulação europeia datava de 1995 4
3.2. A importância das alterações tecnológicas e no modo de vida dos últimos 20 anos 5
3.3. Conclusão: o RGPD como oportunidade de os titulares dos dados retomarem o controlo sobre os seus dados pessoais 5
4. Segurança vs. Proteção de dados pessoais 6
4.1. Conceitos distintos, mas interligados 6
4.2. Necessidade de uma posição ativa do titular dos dados como garantia de segurança 7
II. O RGPD e eu: onde estão os meus dados pessoais e como são tratados? 8
1. Ainda o conceito de dados pessoais 8
2. O conceito de tratamento de dados pessoais 8
3. Os princípios que regem a proteção de dados pessoais 10
3.1. Princípio do tratamento lícito, leal e transparente 10
3.2. Princípio da limitação de finalidades 11
3.3. Princípio da minimização dos dados 11
3.4. Princípio da exatidão 12
3.5. Princípio da limitação de conservação 12
3.6. Princípio da integridade e confidencialidade dos dados 12

4. Em particular, o tratamento de categorias especiais de dados 13
4.1. Consentimento explícito e consentimento inequívico 13
4.2. Outras fontes de licitude de tratamento de dados sensíveis 14
5. O consentimento relativo ao tratamento de dados de menores 15
III. Que direitos tenho sobre os meus dados pessoais? 17
1. Direito de informação 17
2. Direito de acesso 17
3. Direito de retificação e de eliminação 18
4. Direito de apagamento 19
5. Direito de oposição 19
6. Direito à portabilidade dos dados 19
7. Direito à proteção contra decisões automáticas 20
IV. O que posso fazer para exercer os meus direitos e que medidas de segurança devo tomar para proteger os meus dados? 22
1. Como pode o titular dos dados exercer os seus direitos e quais as entidades e meios que pode usar 22
1.1. Junto da organização que detêm os dados 22
1.2. Junto do Encarregado de Proteção de Dados da organização 22
1.3. Junto da Autoridade Nacional de Controlo 23
1.4. Através dos Tribunais: ação judicial 24
2. As Sanções previstas no RGPD em caso de violação dos direitos dos titulares dos dados 24
3. Uma posição ativa do titular dos dados para proteção DOS dados pessoais 24

I. O QUE É, AFINAL, O NOVO REGULAMENTO GERAL SOBRE PROTEÇÃO DE DADOS DE QUE TODOS FALAM?

1. VAMOS CONHECER O RGPD

1.1. O QUE É O RGPD E QUEM O APROVOU

O Regulamento Geral de Proteção de Dados (RGPD) é um Regulamento aprovado, em 2016, por dois órgãos da União Europeia, designados Parlamento Europeu e Conselho, que estabelece novas regras relativas à proteção dos dados pessoais das pessoas singulares, vivas, no que diz respeito ao tratamento e à livre circulação desses dados.

Assim, o RGPD é um ato legislativo da União Europeia, que se aplica diretamente em todos os Estados-Membros sem necessidade de que estes publiquem legislação interna e visa essencialmente garantir uma aplicação uniforme de determinadas regras em toda a União Europeia.

O RGPD foi publicado no Jornal Oficial da União Europeia L 119/1, de 04.05.2016, sob a referência "Regulamento (EU) 2016/679".

1.2. QUANDO PASSOU A SER APLICADO O RGPD

O RGPD é aplicável em toda a União Europeia a partir do dia 25 de maio de 2018, data a partir da qual todas as entidades, a ele sujeitas, são obrigadas a cumprir as normas previstas neste Regulamento.

O Regulamento prevê, no seu artigo 99º, que apenas passaria a ser aplicável em todos os Estados-Membros a partir do dia 25.05.2018, ou seja, dois anos após a sua entrada em vigor, para permitir aos Estados-Membros a adoção de medidas de conformidade às regras impostas pelo Regulamento.

1.3. PRINCIPAL OBJETIVO A ATINGIR COM O RGPD

É importante referir que o RGPD introduz uma alteração significativa relativamente às normas vigentes até ao momento presente em Portugal, na medida em que desloca a centralidade da proteção dos dados pessoais para o titular dos dados.

Quer isto dizer que, de acordo com a nova regulamentação europeia, toda a apreciação, interpretação e aplicação do RGPD tem de ser feita na perspetiva da proteção dos direitos do titular dos dados, ou seja, o que passa a ser importante não é o local onde os dados pessoais são tratados, mas sim o local onde se encontra o titular dos dados pessoais.

Em suma, é possível concluir que o principal objetivo a atingir com a aprovação do RGPD foi a uniformização das regras sobre proteção de dados em todos os Estados-Membros, com a preocupação de colocar o acento tónico no titular dos dados e, com isso, permitir um desenvolvimento adequado do Mercado Único Digital.

1.4. ENTIDADES OBRIGADAS A CUMPRIR O RGPD E TITULARES A QUEM ESTE SE APLICA

O RGPD regula a proteção dos dados pessoais de todas as pessoas singulares, vivas, que se encontrem na UE, não sendo necessário que sejam nela residentes ou nacionais de Estados-Membros.

A proteção abrange o tratamento de dados que é feito por uma entidade - seja pessoa singular, seja pessoa coletiva - situada na UE.

No entanto, tendo por base o facto de o mundo ser hoje global, por força dos meios tecnológicos, o RGPD também é aplicável a entidades que não se situem no território da UE, mas que desenvolvam atividades de oferta de bens e serviços aos titulares dos dados situados na UE, ou que controlem o comportamento dos titulares dos dados, desde que esse comportamento ocorra na UE.

Se uma pessoa que se encontre em Portugal aceder a um *site* de compras online que seja propriedade de uma empresa chinesa, e esse site estiver redigido em línguas falantes na UE, essa empresa, ainda que estando sediada na China, é obrigada a cumprir as normas do RGPD pelo facto de propor a compra de bens ou serviços em línguas faladas na UE, mesmo que o titular dos dados que entrou no site não proceda a nenhum pagamento.

Se essa mesma empresa chinesa, através das pesquisas de produtos que faço no seu *site* registar a informação sobre a minha pesquisa com vista a propor-me, posteriormente, a compra de determinados bens ou serviços relacionados com as pesquisas que efetuei, também está, por esse motivo, obrigada a cumprir as regras do RGPD, ainda que nem a empresa se situe em território na UE, nem o tratamento seja feito em território europeu.

Concluindo, mesmo as empresas que não estejam estabelecidas na UE são obrigadas a cumprir o RGPD sempre que tratem dados de pessoas que se encontrem no território da UE, quando o tratamento dos dados esteja relacionado com a intenção de oferecer bens e serviços, ainda que não ocorra nenhum pagamento, ou sempre que o tratamento estiver relacionado com o controlo de comportamentos do titular, desde que os comportamentos ocorram no espaço da UE.

Como vimos, o RGPD coloca todo o acento tónico no titular dos dados e não em quem procede ao tratamento dos dados pessoais, por isso, não releva nem a natureza das entidades, nem o local onde procedem ao tratamento - o que importa é o facto de tratarem dados pessoais de indivíduos que se situem na União Europeia, não sendo necessário que sejam residentes ou nacionais de um país da UE.

No entanto, e como seria de esperar, o RGPD distingue as situações em que o tratamento dos dados é feito para o que se chama uso doméstico - são as situações da lista de contactos pessoal (telefones, moradas, correios eletrónicos, datas de nascimento, nome, etc.), por exemplo, às quais o RGPD não se aplica.

Na verdade, e com exclusão das situações de uso doméstico, todos aqueles que tratem dados pessoais estão obrigados a cumprir o RGPD, quer sejam pessoas singulares no âmbito da sua atividade, quer sejam organizações, independentemente da sua dimensão e da sua natureza pública ou privada.

Por sua vez, os princípios que regem o RGPD determinam que o responsável pelo tratamento atue de forma mais transparente, mais leal para com o titular dos dados e, assim, este veja reforçados os seus direitos - matéria que trataremos nos capítulos seguintes.

1.5. O RGPD COMO APOIO AO DESENVOLVIMENTO ECONÓMICO ASSENTE NO MERCADO ÚNICO DIGITAL

Isto não significa que o RGPD seja um obstáculo ao desenvolvimento económico.

Pelo contrário, entre os fins a atingir pelo RGPD encontra-se o de implementar o Mercado Único Digital até 2020, cujos principais objetivos assentam na existência de um melhor acesso dos consumidores e das empresas aos bens e serviços, num ambiente propício ao desenvolvimento das redes e serviços digitais, constituindo a economia digital um motor de crescimento económico.

E como é que o RGPD contribui para implementar o Mercado Único Digital? De muitas formas, em todas elas visando o aumento da confiança dos consumidores nos serviços digitais, nomeadamente através da:

- Uniformização das regras legais de proteção de dados pessoais nos países da UE,
- Estabelecimento dessas regras através de um ato legislativo da União que é de aplicação idêntica em todos os Estados-Membros, e, essencialmente,
- Colocando os direitos dos titulares dos dados no centro do tratamento dos dados pessoais.

1.6. CONCLUSÃO: PORQUE É QUE O RGPD É IMPORTANTE PARA TODAS AS PESSOAS

Daqui resulta que o RGPD, apesar de ser um documento muito extenso e complexo, irá ter um enorme impacto na vida dos indivíduos porque obriga as entidades, que com eles se relacionam, a cumprir regras de informação, transparência e lealdade, de forma a que os titulares possam compreender quem utiliza os seus dados, para que efeito e durante quanto tempo - conforme veremos no capítulo II.

A aprovação do RGPD trouxe para o centro da discussão pública o tema da proteção dos dados pessoais e permite a criação de momentos de consciencialização das pessoas relativamente a um tema que constitui um direito fundamental.

Assim, o tema da Proteção de Dados Pessoais passou a estar presente no quotidiano, com impacto direto na vida de todos, como se percebeu, designadamente através dos inúmeros emails e mensagens recebidas no final do mês de Maio de 2018, a solicitar o consentimento para continuação do tratamento dos respetivos dados, para marketing ou newsletters, por exemplo – ainda que, muitas das vezes, os pedidos fossem desnecessários ou erradamente solicitados.

2. O QUE SÃO DADOS PESSOAIS

2.1. O CONCEITO DE DADOS PESSOAIS

Os dados pessoais são todos e quaisquer elementos relativos a uma pessoa singular, ou seja, um indivíduo, que o identificam ou que são suscetíveis de o identificar.

Assim, qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular, que a permita identificar de forma direta ou indireta, imediata ou agregando diversos elementos, é um dado pessoal.

Essa "informação" é todo e qualquer elemento (nome, sexo, ocupação, localização, preferências, etc.), sob qualquer formato, guardada em papel, em suporte digital ou de qualquer outro modo.

Importa compreender que a informação está "relacionada" com o indivíduo sempre que permita identificá-lo ou caracterizá-lo de algum modo, mesmo que agregando várias informações.

Um individuo está "identificado" quando a informação permite, de forma direta e individual, conhecer a respetiva identidade (nome, número de identificação fiscal, de identificação civil, de utente, uma fotografia, análises genéticas, entre outras).

No entanto, muitas vezes, basta que se juntem vários elementos informativos sobre um indivíduo para que ele, não sendo identificado por nenhum deles separadamente, seja identificável através da associação das diversas informações.

Um individuo é "identificável" quando a informação pode, de forma indireta ou agregada com outras informações, conhecer a sua identidade (localização, idade, características físicas, sociais, culturais, entre outras).

Neste último âmbito, o RGPD incorpora as alterações tecnológicas, uma vez que é hoje possível identificar uma pessoa através do designado *Internet Protocol* (IP), dos cookies, em virtude de a navegação online utilizar esta espécie de identificadores que, juntamente com outros registados pelos servidores, permitem saber, em concreto, a identidade, por exemplo, do indivíduo que procedeu a um determinado *download* ou a uma pesquisa.

E sendo verdade que estes mecanismos são muito importantes, por exemplo, no combate à criminalidade que é feita através da internet (matéria que está excluída da aplicação do RGPD), também permitem às entidades que tratam os dados pessoais dirigir a sua ação em função da informação que recolhem sobre os indivíduos.

2.2. CATEGORIAS ESPECIAIS DE DADOS

De entre os dados pessoais, existe uma categoria especial de dados, habitualmente designada dados sensíveis, cujo tratamento é, em regra, proibido ou sujeito a condições especiais.

Os dados sensíveis são elementos que identificam ou permitem identificar inequivocamente uma pessoa através de determinadas características, a saber, a raça ou etnia, as convicções filosóficas ou religiosas, as opiniões políticas, a filiação sindical, bem como dados genéticos, dados biométricos, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

O tratamento destes dados coloca em risco direitos fundamentais das pessoas e, por isso, existem regras mais restritivas para que esse tratamento possa ser feito e que serão vistas no capítulo II.

3. POR QUE MOTIVO FOI APROVADO O RGPD

3.1. A ÚLTIMA REGULAÇÃO EUROPEIA DATAVA DE 1995

Interessa referir, a título de enquadramento, que a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, datada de 23.11.1995 se aplicou nos diversos Estados-Membros através das leis internas que estes aprovaram e vigoraram até 25.05.2018.

Ora, a proteção dos dados pessoais ao abrigo da Diretiva colocava o acento tónico no local onde o tratamento dos dados era feito e também num sistema de autorizações por parte de uma autoridade de controlo que, em Portugal, era a Comissão Nacional de Proteção de Dados (CNPD).

Como é evidente, desde a última regulamentação europeia sobre proteção de dados pessoais, muitas foram as alterações na vida das pessoas que fizeram com que grande parte delas tivesse

perdido o controlo sobre o tratamento feito pelas várias entidades aos seus dados pessoais – o que foi incrementado com a utilização em massa da internet, das redes sociais, das compras *online*.

Ora o RGPD tem por objetivo primeiro garantir o direito à proteção dos dados pessoais das pessoas singulares enquanto direito fundamental, tendo em consideração as características das atividades hoje desenvolvidas pelas pessoas em geral e, mesmo, pela alteração do modo de vida.

3.2. A IMPORTÂNCIA DAS ALTERAÇÕES TECNOLÓGICAS E NO MODO DE VIDA DOS ÚLTIMOS 20 ANOS

O aparecimento e a divulgação em massa da internet, das redes sociais, dos serviços e comércio *online*, do marketing digital, da geolocalização, da *cloud*, sem que as pessoas que a eles acedem ou os utilizam tenham (pleno) conhecimento daquilo que é feito com os seus dados pessoais e, na maior parte das vezes, nem sequer cheguem a saber quais os dados pessoais que são recolhidos, transferidos, conservados ou até transacionados (vendidos), exigia uma tomada de posição para defesa dos indivíduos nestas relações que estabelecem, e onde constituem sempre uma parte menos informada e, por isso, mais desprotegida.

As pessoas habituaram-se a utilizar as novas tecnologias e incorporaram-nas no seu dia-a-dia, sendo possível afirmar que, provavelmente, ninguém conseguiria hoje voltar a viver sem acesso à internet ou sem correio eletrónico.

Todavia, é essencial compreender que também essas tecnologias evoluíram - e a uma velocidade não comparável ao que alguma vez tinha sucedido noutras situações, sendo esse avanço cada vez mais rápido, tornando facilmente desatualizados os processos que utilizamos e fazendo-nos sentir falta dos que já existem e ainda não usamos.

Acresce a tudo isto que o aumento das capacidades de processamento, armazenamento e análise digital, a *big data*, permitiram criar perfis dos titulares dos dados, sem o seu conhecimento, utilizando as opiniões que as pessoas expressam livremente *online*, ou as pesquisas que fazem, ou as compras que efetuam, para lhes direcionar propostas de produtos ou serviços, informação sobre temas sobre os quais se tenham pronunciado ou até a realização de eventos em locais que habitualmente frequentem.

A isto chama-se definição de perfis (referido muitas vezes na expressão em língua inglesa, "*profiling")* e pode ser, sobretudo sempre que o titular dos dados não sabe que está a ser feito, muito intrusivo relativamente à privacidade das pessoas.

Em rigor, o que sucede é que, alguém que eu desconheço e a quem não autorizei, está a seguir e a registar as minhas ações na internet, para depois as utilizar e me propor serviços ou bens, ou vender essas informações a terceiros.

3.3. CONCLUSÃO: O RGPD COMO OPORTUNIDADE DE OS TITULARES DOS DADOS RETOMAREM O CONTROLO SOBRE OS SEUS DADOS PESSOAIS

Sucede que os titulares dos dados, ao fim de anos a interagir com equipamentos que lhes proporcionam vantagens ou maior qualidade nas atividades do seu dia-a-dia, não tinham qualquer possibilidade de saber quem trata os seus dados, para que efeitos, durante quanto tempo.

E, sobretudo, foi possível concluir ao longo dos anos que a grande maioria das pessoas desconhece totalmente a utilização que é dada aos dados pessoais que fornece.

De facto, importa que a generalidade das pessoas que utiliza as tecnologias de informação tome conhecimento de que todos os dados pessoais são relevantes e têm um valor no mercado, sem que esse valor dependa de nenhumas características sociais, académicas ou profissionais do titular dos dados.

No século XXI o poder depende diretamente da informação que se detém, sobre os mais variados assuntos e aspetos, e o desenvolvimento tecnológico veio facilitar o acesso e análise, em massa, de grandes volumes de informação.

Desta forma, essa informação tem hoje um valor económico, existindo mesmo um mercado para ela.

O RGPD constitui, por isso, um marco na vida dos titulares dos dados pessoais em que, simultaneamente, se pode chamar a atenção para a relevância do assunto para todas as pessoas e, com isso, permitir que aumentem a sua consciência digital e compreendam o valor que todos os dados pessoais têm, para si e para quem os trata.

Por outro lado, com o RGPD os titulares dos dados terão mais possibilidades de conhecer quais os dados que são tratados, quais os fins desses tratamentos, durante quanto tempo serão conservados os dados e para que finalidades, já que o RGPD impõe, em cumprimento do princípio do tratamento leal e transparente, que o titular dos dados seja informado, de forma concisa e em linguagem acessível, sobre todos esses aspetos - como se verá, aliás, em detalhe, no capítulo II.

4. SEGURANÇA VS. PROTEÇÃO DE DADOS PESSOAIS

4.1. CONCEITOS DISTINTOS, MAS INTERLIGADOS

É frequente confundir a segurança com a proteção de dados pessoais.

No entanto, se é verdade que a segurança é um aspeto a ter em consideração para a proteção dos dados pessoais, não se confunde com ela.

A proteção de dados pessoais tem essencialmente a ver, no âmbito do RGPD, com a garantia que tem de ser dada ao titular dos dados de que estes serão tratados de acordo com um conjunto de princípios a cumprir pelos organismos que procedem ao tratamento, mas também assegurando ao titular dos dados mecanismos para exercer os seus direitos sobre os dados, de forma que consiga ter controlo sobre o tratamento a que os seus dados pessoais são sujeitos.

A proteção de dados pessoais resulta das normas estabelecidas pelo RGPD no âmbito do direito fundamental à vida privada, enquanto a segurança, por sua vez, se prende com a implementação dos mecanismos técnicos que impedem o acesso não autorizado ou ilícito aos dados pessoais dos titulares.

Ora, uma das formas de assegurar o cumprimento dos princípios que regem o tratamento dos dados pessoais e de garantir o exercício dos direitos aos indivíduos é a de reforçar mecanismos de segurança dirigidos especificamente à proteção dos dados pessoais.

Por exemplo, os dados pessoais devem estar encriptados nos servidores, de forma que só possam a eles aceder as pessoas que necessitem da informação para cumprir alguma finalidade e tenham permissão para o fazer. Ou a colocação de dados pessoais sensíveis em papel dentro de um cofre ou de uma sala segura, ao qual apenas possam ter acesso as pessoas credenciadas para o efeito.

Por isso, a segurança é um dos meios a implementar para proteção de dados pessoais, mas esta não se esgota na adoção de medidas de segurança, exigindo muito mais do que isso, como veremos nos capítulos seguintes.

4.2. NECESSIDADE DE UMA POSIÇÃO ATIVA DO TITULAR DOS DADOS COMO GARANTIA DE SEGURANÇA

Importa, no entanto, compreender que o titular dos dados não pode ter uma atitude meramente passiva relativamente a este fator da segurança, como se se tratasse exclusivamente de um dever que recai sobre a entidade que trata dados pessoais.

Também o titular dos dados tem de incorporar, nas atividades da sua vida diária, mecanismos básicos de segurança dos dados pessoais de que é titular.

Pode referir-se, a título de exemplo, a utilização de *passwords* nos computadores sem que as mesmas se encontrem escritas em *post-its* ou debaixo do teclado, a não utilização de computadores em redes de espaços públicos para aceder a dados relevantes ou para realizar transações comerciais, o não envio, por email, de dados pessoais relevantes como códigos de contas bancárias ou *passwords*.

É essencial que as pessoas compreendam que o seu modo de atuação neste domínio faz parte integrante de qualquer mecanismo de segurança dos seus dados pessoais.

De nada vale que a entidade que procede ao tratamento dos dados tenha inúmeros mecanismos técnicos de segurança nas suas redes, se o titular dos dados, pela forma como age, é o primeiro a não garantir a segurança mínima dos dados. Mas a este assunto se regressará, a título conclusivo, no capítulo 4.

Saber mais

Leia, no Regulamento (UE) 2016/679:

Artigo 1º (e Considerandos 5, 6 e 7)

Artigos 2º e 3º (e Considerandos 22, 23 e 24)

Artigo 4º (e Considerandos 30, 34 e 35)

Artigo 89º (e Considerandos 156, 158, 160, 161, 162)

Artigo 91º (e Considerando 165)

Artigo 99º

II. O RGPD E EU: ONDE ESTÃO OS MEUS DADOS PESSOAIS E COMO SÃO TRATADOS?

1. AINDA O CONCEITO DE DADOS PESSOAIS

Vimos genericamente no capítulo I que o RGPD define os dados pessoais como qualquer informação relativa a uma pessoa singular, viva, identificada ou identificável.

Ainda que o conceito, assim descrito, se mantenha igual face à anterior legislação comunitária, a verdade é que, por força da evolução tecnológica ocorrida nos últimos 20 anos, são inúmeras as informações sobre um indivíduo que o permitem identificar - o que não sucedia há duas décadas e que, como tal, são agora qualificadas como dados pessoais.

Por exemplo, são hoje dados pessoais, isto é, elementos que permitem que uma pessoa possa ser identificada, os dados de localização, identificadores por via eletrónica (IP, cookies, etc.).

2. O CONCEITO DE TRATAMENTO DE DADOS PESSOAIS

De acordo com o RGPD, tratar dados pessoais significa:

a) Realizar uma operação ou um conjunto de operações sobre dados pessoais ou sobre conjuntos de dados pessoais, e fazê-lo

b) Por meios automatizados ou não automatizados

Constituem operações de tratamento de dados 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.

Ou seja, é praticamente impossível encontrar uma operação sobre um dado pessoal que não constitua tratamento.

Veja-se que se um médico tiver as fichas dos seus pacientes em papel, classificadas por ordem alfabética de apelido, isso consubstancia tratamento; do mesmo modo, se um trabalhador consulta os dados de assiduidade de outro trabalhador da mesma organização para efeito de realizar o processamento do salário, também se está perante tratamento de dados pessoais.

Na verdade, a vida atual está, na maioria dos casos, imbuída de atividades, qualificadas como usuais pelas pessoas na sua generalidade, mas que consubstanciam um tratamento dos seus dados pessoais por terceiros, não tendo os titulares dos dados muitas vezes sequer consciência disso.

Por exemplo, quando acedo a uma página de internet para obter uma informação, não imagino, na maior parte dos casos, que a entidade que gere essa página regista informações sobre mim e o acesso que fiz, sabendo, por exemplo, o que pesquisei e em que local me encontro ou em que computador/rede estou a usar.

E com a evolução tecnológica permanente, associada ao facto de as pessoas se terem habituado a utilizar um conjunto de meios que consideram úteis para a sua vida diária, as entidades que procedem ao tratamento dos dados têm uma capacidade cada vez maior de tratar em larga escala informação sobre cada indivíduo, categorizando-o, classificando-o, de acordo com as suas preferências, opiniões expressas, pesquisas e/ou compras efetuadas, locais frequentados.

Como vimos no capítulo I, o tratamento automatizado destes dados permite definir o perfil do titular e direcionar-lhe ofertas ou informações específicas.

Por vezes, ao entrar num centro comercial somos informados de que temos determinados amigos num local perto.

Isto acontece cada vez mais porque, sempre que utilizamos uma aplicação móvel ou pretendemos aceder a uma informação *online*, nos surge o pedido para o titular dos dados autorizar o acesso também à lista de contactos, ao calendário e à localização.

Ou seja, as informações que a entidade que trata os meus dados recolhe e utiliza através de um simples acesso são imensos, e não só não informa sobre o facto de os recolher, como também sobre o destino que lhes dá, a quem os transmite, ou durante quanto tempo os guarda.

E tudo isso consubstancia tratamento de dados pessoais.

E é aqui que reside uma das maiores alterações introduzidas pelo RGPD, que visa precisamente impor às entidades que tratam os dados pessoais um dever de informação, de forma que a opção que cada um tome, em cada momento, seja esclarecida.

Temos vindo sucessivamente a falar sobre tratamento de dados pessoais e já houve oportunidade de identificar os principais atos que estão abrangidos por esse conceito.

De facto, é normal que, perante o conceito de "tratamento" de dados pessoais se pense que se está necessariamente perante uma atividade, um "fazer".

Será que apenas quando alguém transmite dados pessoais nossos a outra pessoa é que está a tratar dados?

Vimos já que não é assim, bastando pensar que um mero sistema de armazenamento de dados num servidor, um *back-up* feito para uma *pen*, ou o *download* de um ficheiro de Excel com dados sobre formandos de uma ação, que realizo do servidor para o ambiente de trabalho do computador, são atos de tratamento de dados pessoais.

Apesar de habitualmente se associar a proteção de dados pessoais apenas ao tratamento automatizado, isto é, às operações que se realizam com o apoio de meios tecnológicos, é essencial referir que o RGPD se aplica igualmente ao tratamento de dados pessoais que é feito em papel.

Daqui decorre a necessidade, por parte das entidades que procedem ao tratamento de dados pessoais, de adaptar, por exemplo, os formulários em papel que entregam.

Uma empresa de formação que permita a realização de inscrições em papel terá obrigatoriamente de adequar a recolha de dados pessoais a que procede aos princípios e normas do RGPD, com vista à proteção dos dados pessoais do formando. E o formando, por sua vez, deverá estar ciente dos dados que podem ou não podem pedir-lhe em cada caso concreto e que se resumem aos que são necessários para a finalidade para a qual são tratados. Se o titular dos dados não necessita de proceder a qualquer pagamento, não existe necessidade de lhe solicitar o número de identificação fiscal. E se for necessário, ainda assim, pedir-lho, o responsável pelo tratamento tem de informar o titular sobre a finalidade para a qual lhe está a solicitar esse dado pessoal.

Os titulares dos dados têm, por isso, de estar despertos para todas as situações do seu dia a dia em que são recolhidos dados pessoais, independentemente de isso ocorrer por vias eletrónicas ou em formato de papel. Em ambos os casos se está perante tratamento de dados pessoais e em ambas as situações é aplicável o RGPD.

3. OS PRINCÍPIOS QUE REGEM A PROTEÇÃO DE DADOS PESSOAIS

É importante perceber que o RGPD, tal como é costume suceder na legislação europeia, aborda a proteção dos dados pessoais dos titulares através do estabelecimento de grandes princípios.

Estes princípios são as regras que norteiam e servem de enquadramento e de apoio à interpretação das restantes normas e da apreciação das situações que vão surgindo na vida concreta.

Existem seis grandes princípios que regem o tratamento de dados pessoais, a saber:

o princípio do tratamento lícito, leal e transparente, o princípio da limitação de finalidades, o princípio da minimização dos dados, o princípio da exatidão, o princípio da limitação de conservação e, finalmente, o princípio da integridade e confidencialidade dos dados.

3.1. PRINCÍPIO DO TRATAMENTO LÍCITO, LEAL E TRANSPARENTE

Este princípio inclui e associa três ideias que se interrelacionam e devem ser aplicadas de forma integrada: o tratamento lícito, leal e transparente.

Tratamento lícito significa que os dados pessoais só podem ser objeto de tratamento tendo por base um fundamento de licitude ou, dito por outras palavras, que o tratamento tem obrigatoriamente de assentar numa das várias fontes constantes do RGPD para que seja permitido.

Importa, portanto, perceber que o RGPD identifica os fundamentos de licitude, e que são várias as formas pelas quais é permitido proceder ao tratamento de dados pessoais.

Vejamos as mais comuns na vida do titular dos dados:

A base legal

Por exemplo, sempre que uma conservatória do registo civil recolhe dados pessoais para proceder ao registo de um recém-nascido, ou recolhe dados biométricos, para emissão do cartão do cidadão, fá-lo com fundamento na legislação relativa à identificação civil.

Assim, nestes casos, o fundamento da recolha e tratamento dos dados é a base legal, isto é, a lei que o regula, não sendo necessário o consentimento do titular.

O consentimento

O consentimento dado pelo titular dos dados constitui um fundamento de licitude, significando isto que o tratamento dos dados pessoais ocorre porque o titular dos dados a ele deu a sua autorização.

A celebração de um contrato

Para efeitos da celebração do contrato, e ainda antes de o assinar, o titular dos dados comunica um conjunto de dados pessoais que são necessários para a assinatura do contrato (o nome, o NIF, o número do Cartão do Cidadão) e sem os quais o contrato não poderia ser celebrado.

Assim, a celebração do contrato e as negociações anteriores constituem um outro fundamento de licitude para o tratamento dos dados pessoais

Por exemplo, quando, uma pessoa está a preparar a celebração de um contrato com uma empresa de telecomunicações, fornece os seus dados necessários para o efeito... No entanto, se a empresa de telecomunicações quiser utilizar os dados pessoais que recolheu, para enviar ações de marketing, isto é, para outra finalidade, nesse caso precisa do consentimento do titular dos dados para esse efeito específico.

A defesa dos interesses vitais do titular ou de terceiro

Também o tratamento de dados pessoais, necessário para defesa dos interesses vitais do titular ou de terceiro, é lícito e não carece de consentimento.

Por exemplo, se estiver em causa a vida de um doente, o seu médico assistente poderá transmitir a outro médico as alergias graves de que o seu paciente sofre, por se tratar de uma situação em que o titular não está em condições de dar o seu consentimento e a sua vida fica em risco se não for urgentemente tratado.Neste caso, a defesa dos interesses vitais do titular dos dados constitui um fundamento de licitude que permite ao médico transmitir os dados a outro médico.

Este princípio associa a transparência à licitude, o que significa, enquanto princípio, que o tratamento tem de ter em consideração o contexto em que ocorre.

A lealdade relaciona-se diretamente com a transparência do tratamento, que significa que o responsável pelo tratamento tem de dar a conhecer ao titular dos dados os riscos, as regras e os direitos do titular, no âmbito do tratamento, e tem de o fazer de uma forma clara, concisa e numa linguagem facilmente compreensível.

Todas as pessoas já se depararam com infindáveis declarações sobre o tratamento de dados pessoais, muitas vezes designadas políticas de privacidade, que ninguém lê porque estão escritas de forma excessivamente técnica e levariam várias horas a ler.

Todavia, as pessoas "aceitam" esses termos de privacidade.

Essa atuação por parte da entidade que procede ao tratamento dos dados tem agora de ser alterada para cumprimento do princípio do tratamento leal e transparente.

3.2. PRINCÍPIO DA LIMITAÇÃO DE FINALIDADES

O princípio da limitação das finalidades significa que os dados pessoais só podem ser tratados para fins específicos, explícitos e legítimos.

Existe uma correlação direta entre o princípio da licitude, lealdade e transparência no tratamento, com o da limitação das finalidades porquanto é obrigatório informar o titular dos dados sobre quais as finalidades para que os dados pessoais são tratados, sendo ilícito o seu tratamento para finalidades distintas e não compatíveis com as que se indicaram ao titular.

Importa ter em consideração que o tratamento subsequente para fins de interesse público, de investigação científica, histórica ou para efeitos estatísticos não é considerado como violando o princípio da limitação das finalidades.

3.3. PRINCÍPIO DA MINIMIZAÇÃO DOS DADOS

O princípio da minimização dos dados significa que apenas podem ser tratados os dados pessoais que sejam relevantes e estritamente necessários para cumprimento da finalidade para a qual são tratados.

Não podem, por isso, recolher-se junto dos titulares mais dados pessoais do que aqueles que são necessários e suficientes para o efeito em causa - o que é muito significativamente espelhado na expressão "*need to know*".

Na inscrição que o titular dos dados faz para uma ação de formação, só deve ser-lhe pedido o NIF se for ele - e não, por exemplo, a sua entidade empregadora -a proceder ao pagamento, ou então se essa exigência resultar de obrigações decorrentes de contratos celebrados pela entidade que

procede ao tratamento, como sucede no caso de uma formação realizada com financiamento comunitário.

3.4. PRINCÍPIO DA EXATIDÃO

O princípio da exatidão exige que os dados pessoais que são objeto de tratamento para uma determinada finalidade estejam sempre atualizados e sejam corretos, devendo ser eliminados ou retificados os que não sejam exatos.

3.5. PRINCÍPIO DA LIMITAÇÃO DE CONSERVAÇÃO

O princípio da limitação de conservação significa que os dados pessoais do titular só podem ser conservados durante o tempo necessário para a prossecução da finalidade para a qual foram recolhidos e são tratados.

A conservação de dados pessoais por uma entidade que procede ao seu tratamento comporta riscos e, desse modo, quanto maior o tempo de conservação, maior a exposição dos dados a riscos de acesso indevido, transferência ou até de perda.

O RGPD impõe, por isso, que a entidade que procede ao tratamento defina qual o período de conservação para cada um dos dados pessoais que trata, podendo ser distintos os prazos de conservação consoante a finalidade.

Pode suceder, por exemplo, que seja necessário manter os dados relativos a faturação e pagamentos por um período de tempo mais alargado, por imposição da lei fiscal, relativamente ao tempo de conservação do correio eletrónico do titular dos dados, que apenas serviu para contacto durante o lapso de tempo em que foi prestado um serviço ou adquirido um bem.

3.6. PRINCÍPIO DA INTEGRIDADE E CONFIDENCIALIDADE DOS DADOS

O princípio da integridade e da confidencialidade do tratamento significa que este tem de ser realizado de forma segura, protegida contra acessos e tratamentos ilícitos e contra perdas acidentais, danos ou destruição.

Constitui obrigação das entidades que procedem ao tratamento tomar as medidas organizativas e técnicas que garantam a segurança dos dados e os protejam contra tratamentos e acessos ilícitos.

A anonimização e a pseudonimização constituem exemplos de mecanismos de reforço do princípio da integridade e confidencialidade dos dados.

Ocorre anonimização dos dados pessoais sempre que a entidade que os trata divide a informação recolhida, de forma que não seja possível identificar o titular, sendo essa operação irreversível.

Diversamente, a pseudonimização é um processo através do qual se separam os dados, de forma que não seja possível a identificação do titular, mas existem formas de os agregar novamente identificando o titular.

É o exemplo típico do que ocorre num exame escolar, em que após o exame a prova fica com um número identificativo, sendo retirado o nome do examinando de forma que a correção do exame seja feita de forma "anónima".

No entanto, posteriormente, os dados voltam a juntar-se, identificando-se o examinando e a prova.

A anonimização é um meio habitualmente utilizado no tratamento para fins estatísticos, enquanto a pseudonimização constitui um típico processo de garantia de confidencialidade e integridade durante um determinado período de tempo, em situações onde se assume que é ou pode ser necessário proceder à identificação do titular dos dados.

4. EM PARTICULAR, O TRATAMENTO DE CATEGORIAS ESPECIAIS DE DADOS

São dados sensíveis, todas as informações pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como os dados genéticos, os dados biométricos, os dados relativos à saúde ou ainda os dados relativos à vida sexual ou à orientação sexual de uma pessoa.

A sujeição desta categoria especial de dados a uma maior limitação de tratamento, ocorre em virtude de este poder mais facilmente afetar direitos, liberdades e garantias dos titulares dos dados, designadamente discriminando-os ilicitamente com base nos referidos aspetos.

O tratamento de dados que assente em características como opiniões políticas, convicções religiosas ou orientação sexual pode gerar, por exemplo, a criação de bases de dados discriminatórias em violação flagrante, não só do direito da igualdade, como dos direitos fundamentais dos indivíduos.

Nem sempre, porém, a qualificação como dado sensível é realizada com facilidade. Se, por exemplo, resultar de uma fotografia a convicção religiosa de uma pessoa, em virtude dos símbolos ou da roupa ou acessórios que utiliza, poderá tratar-se de um dado sensível.

Por isso, o RGPD estabeleceu, como regra, a proibição de tratamento de dados sensíveis, permitindo-o apenas quando ele ocorra em determinadas situações especiais, como as que veremos adiante

4.1. CONSENTIMENTO EXPLÍCITO E CONSENTIMENTO INEQUÍVICO

O consentimento explícito é um meio pelo qual o titular dos dados dá o seu acordo a que seja utilizado um ou mais dados pessoais sensíveis, em determinado contexto especificado.

Este consentimento é mais exigente do que o consentimento que muitas vezes é pedido para autorizar o tratamento dos dados pessoais para receber uma *newsletter* ou marketing ou para integrar uma *mailing list* de uma entidade.

Nestes casos, o RGPD exige que o consentimento seja inequívoco, mas não obriga a que seja explícito.

Qual a diferença entre estes dois tipos de consentimento?

Diz-se que o consentimento é inequívoco quando não existem dúvidas sobre a vontade do titular dos dados.

Utilizando os exemplos que tínhamos dado, não há objeção a que o consentimento para integrar a *mailing list* de uma organização, ou para autorizar o recebimento de uma *newsletter*, seja dado através de a colocação de uma cruz num formulário online, desde que o mesmo não venha pré-preenchido.

O mesmo não pode suceder nas situações em que é exigido o consentimento explícito.

O consentimento explícito, em virtude da especial natureza dos dados e dos riscos envolvidos para o titular dos dados em caso de haver uma violação da proteção dos dados, por se tratar de dados sensíveis, obriga a que o titular dos dados seja informado sobre qual ou quais os dados pessoais específicos a utilizar (o resultado de uma análise ao sangue, uma ressonância magnética,

determinado histórico familiar, etc.), em que formato (em papel, numa base de dados), para que efeito específico (para uma conferência, para uma publicação científica, para análise num grupo, para todos os anteriores), sobre a utilização desses dados de forma anónima ou não, sobre a transferência desses dados (de um, vários ou todos) para outras entidades (identificando quais sejam) e, perante isso, o titular dos dados tem de consentir de forma expressa nesse tratamento, nas condições exatas que lhe foram apresentadas e exclusivamente para essas.

Se é verdade que o RGPD impõe que, sempre que o tratamento de dados pessoais seja feito com base no consentimento do titular, esse consentimento, seja para efeito de tratamento de dados pessoais sensíveis ou não, corresponda a uma concordância dada de forma expressa, livre, específica para dados e finalidades concretos, já quando o tratamento vise dados sensíveis, o mesmo tem de ser explícito.

Para utilizar uma situação relativamente comum, não é possível presumir que, se o titular dos dados autorizou o tratamento dos seus dados médicos para efeitos de uma estatística hospitalar, esse consentimento também possa abranger a publicação numa revista científica sobre esse mesmo estudo.

O titular dos dados sensíveis terá de, explicitamente, consentir no tratamento dos dados para a finalidade da publicação numa revista científica.

Mas se, doutro modo, o titular dos dados deu o seu consentimento para o tratamento automatizado para definição do seu perfil de consumo, pode considerar-se que é inequívoco o seu consentimento para recebimento de marketing de produtos.

Quer isto dizer que temos de distinguir as situações consoante a categoria de dados pessoais que está em causa, tendo plena consciência de que sempre que esteja em causa o tratamento de dados pessoais sensíveis, o consentimento tem de ser explícito.

4.2. OUTRAS FONTES DE LICITUDE DE TRATAMENTO DE DADOS SENSÍVEIS

No entanto, o consentimento explícito não é a única forma de ser permitido o tratamento de dados sensíveis.

O tratamento de dados sensíveis também é lícito - ou seja, é considerado permitido por lei - quando, por exemplo, for efetuado, no âmbito das atividades legítimas e mediante as garantias adequadas, por uma fundação, associação ou outro organismo sem fins lucrativos e desde que o tratamento se refira apenas a membros ou antigos membros desse organismo, sem que haja divulgação a terceiros.

Se, por exemplo, uma associação de apoio a crianças com determinado défice cognitivo tem uma lista, organizada por ordem alfabética ou por ano de frequência, com os nomes e os contactos de todas as crianças que frequentaram as suas atividades, este tratamento - ou seja, esta lista - é feito de forma legal à luz do RGPD.

Já é, no entanto, necessário compreender que se a associação enviar essa lista para o Ministério da Saúde, se torna indispensável o consentimento explícito dos titulares dos dados.

É também lícito, ou seja, admitido por lei como sendo um tratamento possível, aquele que é levado a cabo por exemplo, no âmbito da medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados de saúde, desde que os dados sejam tratados por um profissional sujeito a sigilo profissional.

É muito importante, e está na origem da medicina no trabalho, saber que o trabalhador está em condições médicas para executar uma determinada tarefa que compõe a sua atividade laboral, de forma a apurar, quer a sua capacidade para a desempenhar, quer o impacto negativo na saúde do trabalhador.

Se um trabalhador que passa a dia a fazer transporte de objetos pesados revelar problemas na coluna, é relevante que deixe de exercer aquela atividade e, deste modo, é lícito registar essas informações sobre o estado de saúde, resultados de exames de diagnóstico, queixas do paciente trabalhador.

No entanto, estes dados só podem ser objeto de tratamento, designadamente de acesso, por um médico e não por qualquer trabalhador da empresa que não se encontre sujeito a obrigações de sigilo profissional.

5. O CONSENTIMENTO RELATIVO AO TRATAMENTO DE DADOS DE MENORES

Importa autonomizar, pela sua particular importância, o consentimento necessário para o tratamento de dados de menores de idade.

O RGPD, enquanto regulação conhecedora da realidade atual, estabelece que, no âmbito da prestação de serviços da sociedade de informação, o tratamento de dados pessoais de menores com idade inferior aos 16 anos de idade, tem de ser dado pelos pais ou tutores.

O RGPD permitiu, no entanto, que cada Estado-Membro fixasse uma idade máxima em que é exigido o consentimento dos responsáveis pelo menor, a qual pode situar-se entre os 13 e os 16 anos - mas em caso algum um Estado-Membro pode fixar a possibilidade de um menor com idade inferior a 13 anos prestar autonomamente o seu consentimento no domínio da prestação de serviços da sociedade de informação.

Em Portugal, a legislação encontra-se em discussão na Assembleia da República, definindo a proposta de lei que está a ser apreciada a idade mínima de 13 anos.

Portanto, se um menor com 10 anos de idade der o seu consentimento quando se encontrar a jogar *online* numa aplicação ou numa resposta a um inquérito sobre consumo, esse consentimento não é válido porque tinha de ter sido dado por quem exerce as responsabilidades parentais sobre o menor.

É certo que se coloca a questão de saber como é que o responsável pelo tratamento consegue apurar se quem está a dar o consentimento é ou não menor.

O RGPD determina que o responsável tem o dever de se assegurar, da forma mais adequada e fiável que possa ser tecnologicamente possível, que o consentimento foi dado pelos pais ou tutores do menor e terá o dever de provar.

Saber mais

Leia, no Regulamento (UE) 2016/679:

Artigo 5º (e Considerando 39)

Artigo 6º (e Considerandos 40, 41, 44, 45, 46, 49)

Artigo 7º (e Considerandos 32, 33 e 43)

Artigo 8º (e Considerando 38)

Artigo 9º (e Considerandos 53, 54, 55 e 56)

Artigo 85º (e Considerando 153)

Artigo 86º (e Considerando 154)

Artigos 87º, 88º (e Considerando 155)

Regulamento (EU) nº 536/2014 do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativo aos ensaios clínicos de medicamentos para uso humano

III. QUE DIREITOS TENHO SOBRE OS MEUS DADOS PESSOAIS?

O Regulamento Geral de Proteção de Dados Pessoais ajuda o titular de Dados Pessoais, ou seja, todas pessoas naturais, não sendo empresas/organizações ou instituições, a interagir melhor com os responsáveis pelo tratamento, para que o processo seja transparente e eficaz.

Os titulares de dados pessoais podem decidir, no limite, quem, com que finalidade e durante quanto tempo são os seus dados pessoais tratados.

Assim, e para que o titular de dados pessoais possa melhor proteger os seus dados, deverá conhecer os direitos que lhe são diretamente conferidos pelo RGPD, que se podem enunciar do seguinte modo:

1. DIREITO DE INFORMAÇÃO

No momento em que os dados são recolhidos, ou depois da sua recolha se o solicitar, o titular de dados pessoais tem o direito de ser informado sobre:

- A finalidade do tratamento
- O prazo de conservação dos dados
- Quem é o responsável pelo tratamento dos dados
- A quem é que o responsável pelo tratamento transmite os seus dados

Exemplo: quando faço um seguro de saúde tenho o direito de saber qual vai ser o destino das minhas informações pessoais, durante quanto tempo vão ser as minhas informações tratadas e quem as irá tratar.

O direito de informação é o correlativo do princípio da lealdade e da transparência no tratamento de dados pessoais.

Na verdade, compreende-se que não baste afirmar que o responsável pelo tratamento tem de recolher, conservar, e praticar todas as operações de tratamento de forma transparente. Se ao titular dos dados não forem conferidos os correspondentes direitos que permitam exigir o comportamento transparente por parte do responsável dos dados, então tratar-se-ia de um princípio vazio e totalmente inoperativo.

2. DIREITO DE ACESSO

O titular dos dados tem o direito de aceder, de conhecer, aos dados que o responsável pelo tratamento tem sobre si. Esse direito, para que seja garantido de forma o mais ampla possível, tem de ser exercido do seguinte modo:

- Sem restrições
- Sem demoras ou custos excessivos
- Obtendo as informações disponíveis sobre a origem desses dados.

O exercício do direito de acesso deve ser feito diretamente junto do responsável pelo tratamento dos dados, por exemplo, através de um email de contacto ou de um formulário online.

Importa sublinhar que o direito de acesso a dados de saúde, incluindo os dados genéticos, é exercido por intermédio de médico escolhido pelo titular dos dados, uma vez que os dados médicos apenas podem ser acedidos por esses profissionais.

Os titulares de dados pessoais podem pedir o acesso dos seus dados por escrito ou oralmente.

Exemplo: Eu sou dono dos meus dados de saúde, posso junto do meu médico pedir para ver todos resultados de análises e exames que tenha feito.

Na prática, como titular de dados pessoais, o direito de acesso aos meus dados pessoais, significa que me é possível:

- Confirmar que a entidade está mesmo a tratar os meus dados pessoais
- Obter uma cópia dos meus dados pessoais
- Aceder a toda a informação suplementar que exista sobre mim em resultado do tratamento dos meus dados.

Exemplo: Posso pedir ao meu médico para ver o historial médico que ele reuniu sobre mim através das consultas, exames, análises e outros.

Este direito ao acesso aos meus dados pessoais corresponde a um direito a tomar conhecimento sobre as informações que existam sobre mim.

Por isso, não é possível aceder à informação de outras pessoas (a não ser que esteja em representação de outra pessoa ou que essa informação me diga diretamente respeito)

Exemplo: Tenho um filho de dois anos, posso aceder aos seus dados pessoais porque sou sua representante legal.

Exemplo: Tenho uma conta conjunta com o meu marido, por isso ambos temos acesso aos nossos dados bancários.

3. DIREITO DE RETIFICAÇÃO E DE ELIMINAÇÃO

Este direito significa que o titular dos dados pode exigir que os dados existentes a seu respeito sejam exatos e atuais e, consequentemente, tem o direito de solicitar a sua retificação, isto é, a sua correção.

Em relação direta com o este direito encontra-se o direito de exigir que os seus dados sejam eliminados dos ficheiros de endereços utilizados para marketing, por exemplo.

O direito de retificação e de eliminação é igualmente exercido diretamente pelo titular dos dados junto do responsável pelo tratamento, devendo o responsável pelo tratamento indicar de forma clara o meio pelo qual esse direito pode ser exercido, que terá de ser de simples utilização.

O que fazer quando a informação é recolhida com erros?

Determinar que os dados pessoais são incorretos pode ser mais complexo se a informação em questão for um erro que, entretanto, já foi resolvido.

Na dúvida, tem-se entendido que, apesar do erro ter sido corrigido, as duas informações devem constar no registo do individuo.

Exemplo: Um paciente foi diagnosticado com uma doença, mas passado uma semana o paciente é informado que devido a um erro do laboratório de análises clínicas o resultado das análises foi trocado com os de um paciente verdadeiramente doente.

É provável que seja conservado tanto o registo médico incorreto como o registo médico já corrigido.

Ainda que o historial médico tenha nos seus registos um diagnóstico incorreto, desde que este tenha sido corrigido e atualizado, respeita os direitos do titular, pois embora tenha ocorrido um erro, este faz parte do registo médico e servirá como despiste, caso o paciente tenha de transferir os seus dados para outro profissional.

4. DIREITO DE APAGAMENTO

O direito ao apagamento de dados pessoais ("direito a ser esquecido") é definido pelo direito de as pessoas impedirem a continuação do tratamento dos respetivos dados e de os mesmos serem apagados quando deixarem de ser necessários para as finalidades para as quais foram recolhidos.

Assim, sempre que uma pessoa deixe de permitir o tratamento dos seus dados e não haja razões legítimas para a sua conservação (por exemplo, para fins estatísticos), os dados deverão obrigatoriamente ser apagados.

Exemplo: Estou inscrita num ginásio em Lisboa, mas, por motivos profissionais, vou viver para o Porto, pelo que tenho direito a pedir ao ginásio de Lisboa que apague todas as informações que tem sobre mim.

O mesmo ocorre no caso em que a minha família está inscrita num plano de televisão, telefone, internet com uma operadora de telecomunicações, mas em virtude da venda da casa e mudança para o estrangeiro, não se pretende que a operadora conserve a minha morada, número de telefone e qualquer outro dado que tenha recolhido ao abrigo do contrato celebrado.

5. DIREITO DE OPOSIÇÃO

O RGPD confere ao titular dos dados o direito a opor-se:

- A seu pedido e gratuitamente, ao tratamento dos seus dados pessoais para efeitos de marketing direto ou de qualquer outra forma de prospeção.
- A que os seus dados de cliente sejam utilizados para efeitos de marketing da empresa.
- A que os seus dados pessoais sejam comunicados a terceiros, salvo disposição legal em contrário.

Exemplo: O titular dos dados tem o direito a opor-se a que um hipermercado utilize o seu email para a divulgação de promoções.

6. DIREITO À PORTABILIDADE DOS DADOS

Quando o tratamento de dados pessoais se realize por meios automatizados e se baseie no consentimento do titular dos dados ou na necessidade de cumprimento de uma obrigação contratual, o titular tem o direito a:

- Receber os seus dados pessoais que foram objeto de tratamento num formato estruturado, de uso corrente e leitura automática
- Solicitar à organização que transmita esses dados a outro responsável por tratamento de dados, sem que o primeiro se possa opor
- A disponibilização dos dados tem de ocorrer no prazo máximo de 1 mês e caso o responsável pelo tratamento pretenda resistir ao pedido tem de explicar porquê por escrito.

Exemplo: Tenho direito a pedir a portabilidade dos meus dados pessoais de uma seguradora para outra, caso queira mudar a minha apólice. E esse direito tanto pode ser exercido solicitando que os meus dados me sejam remetidos, num formato que eu consiga ler, como posso solicitar que os dados sejam transmitidos de uma organização à outra (no exemplo acima, que a minha seguradora inicial transmita os meus dados diretamente à segunda seguradora).

7. DIREITO À PROTEÇÃO CONTRA DECISÕES AUTOMÁTICAS

O RGPD prevê que não podem ser tomadas decisões baseadas só em sistemas automáticos sem existir qualquer tipo de envolvimento humano.

Proíbe ainda a definição de perfis (expressão anglo-saxónica que significa o processamento automático de dados pessoais para avaliar certos aspetos de um individuo, conforme visto no capítulo II), sempre que se trate de um mecanismo para tomar decisões automatizadas.

Ou seja, o titular de dados pessoais tem direito a não ser objeto de uma decisão baseada unicamente no tratamento automatizado, incluindo a elaboração de perfis, que produza efeitos jurídicos ou lhe cause qualquer tipo de dano.

Imagine-se que era criado um *software* que automaticamente procedia à abertura de procedimento disciplinar a um trabalhador sempre que detetasse a existência de mais de cinco faltas seguidas injustificadas. Ou que, por força de um perfil de crédito, seja recusada automaticamente a compra de um carro.

Neste âmbito, porém, é necessário ter em atenção que, por vezes, a lei permite a utilização de algoritmos para definir um perfil para determinados efeitos, mas existe sempre obrigatoriamente a possibilidade de o indivíduo de opor ao resultado a que esse tratamento chegou - sendo certo que, em regra, esse resultado só deve ser final após intervenção humana que avalie a aplicação ao caso concreto.

Existem exceções em que é permitida a tomada de decisão automatizada, a saber, sempre que:

- O titular de dados tenha dado o seu consentimento
- Seja necessária para a execução de um contrato
- Esteja permitido pelo Direito da UE com medidas adequadas para proteger os direitos liberdades e garantias dos cidadãos.

Como é evidente, de pouco importa a consagração de direitos se os indivíduos não tiverem forma de os fazer valer nos casos em que considerem que os mesmos não estão a ser considerados corretamente. É o que verá no capítulo IV.

Saber mais

Leia, no Regulamento (UE) 2016/679:

Artigos 7ºe 8º

Artigo 12º (e Considerandos 58, 59 e 60)

Artigos 15º, 16º, 17º (e Considerandos 65 e 66)

Artigos 18º, 19º, 20º (e Considerando 68)

Artigo 21º (e Considerandos 69 e 70)

Artigo 22º (e Considerando 71)

Artigos 25º e 88º

IV. O QUE POSSO FAZER PARA EXERCER OS MEUS DIREITOS E QUE MEDIDAS DE SEGURANÇA DEVO TOMAR PARA PROTEGER OS MEUS DADOS?

1. COMO PODE O TITULAR DOS DADOS EXERCER OS SEUS DIREITOS E QUAIS AS ENTIDADES E MEIOS QUE PODE USAR

Não existem direitos se não existirem mecanismos que permitam exercê-los corretamente. Por isso, importa, neste último capítulo, abordar as possíveis reações que os titulares dos dados têm ao seu dispor para fazer valer os direitos que o RGPD lhes atribui para proteção dos seus dados pessoais.

O que pode, em geral, fazer o titular dos dados sempre que pretenda exercer algum dos direitos que o RGPD lhe garante?

1.1. JUNTO DA ORGANIZAÇÃO QUE DETÊM OS DADOS

Pode, desde logo, contactar a organização que detém os seus dados através dos meios colocados à disposição

Os princípios da lealdade e transparência que enquadram a proteção dos dados pessoais no âmbito do RGPD impõem determinadas obrigações às entidades que procedem ao tratamento.

Entre esses deveres encontra-se o de indicar a forma de contacto para que o titular dos dados exerça os seus direitos no âmbito do tratamento que é levado a efeito pela organização.

Se a entidade tiver um sítio na internet, deverá colocar, de forma visível e fácil de encontrar, um endereço eletrónico, um formulário *online* ou uma linha de contacto telefónico, por exemplo, com a expressa indicação de que se trata de meios de contacto para obter informações e formular pedidos relativos aos dados pessoais, indicando expressamente qual a organização que está a proceder ao tratamento dos dados.

Por isso, em caso de dúvida sobre quais os dados que a organização trata, se os transfere para terceiros ou qual o período de tempo durante o qual os conserva, o titular dos dados deverá utilizar os meios colocados à disposição pela entidade que trata os dados pessoais.

O mesmo deve suceder se pretender solicitar a retificação de dados pessoais, pedir a sua eliminação ou a portabilidade.

Em conclusão, o RGPD impõe que a organização que procede ao tratamento dos dados disponibilize meios de fácil acesso para que o titular dos dados possa exercer os seus direitos.

1.2. JUNTO DO ENCARREGADO DE PROTEÇÃO DE DADOS DA ORGANIZAÇÃO

O RGPD prevê a existência de uma figura designada Encarregado de Proteção de Dados (EPD) à qual o titular dos dados também se pode dirigir para solicitar esclarecimentos sobre os seus dados pessoais.

O EPD (também designado DPO, por ser o acrónimo da designação em língua inglesa *Data Protection Officer*), é de designação obrigatória em todas as entidades e serviços públicos (nomeadamente, municípios, direções-gerais, institutos públicos, órgãos de soberania e, no caso das entidades

privadas, a sua designação é também obrigatória quando estas tratem dados sensíveis em larga escala ou sempre que esteja em causa como atividade principal da organização o controlo regular e sistemático de dados pessoais.

Os hospitais privados são exemplos típicos do primeiro caso, enquanto o controlo de acessos a um prédio de escritórios, quer através de sistema de CCTV, quer através da identificação das pessoas através do nome e um documento de identificação, constituem exemplo do segundo caso referido.

O RGPD atribui ao EPD/DPO uma função global de acompanhar e aconselhar a atividade de tratamento de dados, levada a cabo pela organização, garantindo a sua conformidade com as normas do RGPD. Mas atribui-lhe igualmente uma função de informação e de aconselhamento dos trabalhadores da organização relativamente à matéria da proteção dos seus dados pessoais.

Portanto, se a organização onde o titular dos dados trabalha designou um EPD/DPO poderá sempre contactá-lo para pedir informações ou esclarecer dúvidas sobre os seus dados pessoais e, nessa medida, é o elemento que serve de ponto de contacto entre a organização e o titular dos dados pessoais.

Contudo, o EPD não é o responsável pelo tratamento dos dados pessoais - é uma pessoa, especialmente conhecedora sobre a matéria de dados pessoais e o RGPD, que pode ser trabalhadora da organização ou contratada externamente por esta como prestadora de serviços, e que acompanha o tratamento de dados da organização, de forma a que seja cumprido o RGPD

1.3. JUNTO DA AUTORIDADE NACIONAL DE CONTROLO

O titular dos dados pessoais tem sempre ao seu alcance a possibilidade de contactar a autoridade nacional de controlo, designadamente para lhe solicitar informação relativamente aos direitos do titular dos dados.

O RGPD prevê a existência de uma autoridade nacional de controlo que, em Portugal, deverá ser a Comissão Nacional de Proteção de Dados (CNPD).

A CNPD é uma entidade administrativa independente com poderes de autoridade, que funciona junto da Assembleia da República.

No âmbito do RGPD, a CNPD, como autoridade nacional de controlo, tem como atribuição genérica fiscalizar o tratamento de dados pessoais, realizado pelas organizações públicas e privadas, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União.

A CNPD deve disponibilizar, para o efeito, formulários de reclamação para que os titulares dos dados pessoais não tenham dificuldade em apresentar reclamação sobre eventuais violações dos seus dados pessoais, sendo esse processo gratuito.

A autoridade nacional de controlo tem poderes de inspeção, de fiscalização de todas as organizações, independentemente da sua natureza, para apuramento dos factos e tomada de decisão no âmbito das reclamações apresentadas pelos titulares dos dados (apenas com exceção dos tribunais na parte em que esteja em causa o exercício da função jurisdicional).

Se um trabalhador considera que a empresa onde trabalha utiliza os seus dados pessoais de forma abusiva, pode apresentar uma queixa junto da CNPD.

1.4. ATRAVÉS DOS TRIBUNAIS: AÇÃO JUDICIAL

Sem prejuízo de tudo quanto se referiu acima, o titular dos dados pessoais pode propor uma ação judicial junto do tribunal. E é possível propor uma ação judicial contra:

- A organização que, no entender do titular dos dados, violou os seus direitos em matéria de proteção de dados pessoais. Importa referir que a ação pode ser proposta mesmo que esteja a correr uma queixa junto da autoridade nacional de controlo/CNPD,
- Contra a autoridade nacional de controlo/CNPD.

Se o titular dos dados pessoais considerar que:

- A autoridade nacional de controlo não tratou a reclamação/queixa de forma correta,
- A resposta dada pela autoridade nacional de controlo não está correta ou não é adequada,
- Se a autoridade nacional de controlo não tiver informado o titular dos dados sobre o andamento ou o resultado da reclamação/queixa no prazo de três meses a contar do dia de apresentação da mesma.

2. AS SANÇÕES PREVISTAS NO RGPD EM CASO DE VIOLAÇÃO DOS DIREITOS DOS TITULARES DOS DADOS

A autoridade nacional de controlo/CNPD pode impor diversas sanções às organizações, incluindo a suspensão ou cessação do tratamento de dados e a aplicação de uma coima.

A autoridade nacional de controlo/CNPD poderá aplicar sanções sempre que se verifiquem situações de incumprimento por parte de uma organização, designadamente:

- Violação de normas relativas aos princípios básicos do tratamento,
- Violação de normas relativas aos direitos de titulares de dados,
- Violação de normas relativas a transferências de dados pessoais para um destinatário num país terceiro ou uma organização internacional.

O RGPD prevê coimas com limite máximo muito alto, com o objetivo de fomentar o cumprimento das normas por parte das organizações. O limite máximo previsto é de 20 000 000€ (20 milhões de euros) ou, caso de trate de uma empresa, 4% do volume de negócios anual a nível mundial correspondente ao exercício anterior.

A lei de cada Estado-membro, e também a lei portuguesa, irá fixar os limites mínimos das coimas a aplicar em caso de incumprimento do RGPD.

3. UMA POSIÇÃO ATIVA DO TITULAR DOS DADOS PARA PROTEÇÃO DOS DADOS PESSOAIS

Ainda que o RGPD não tenha por objeto apenas o tratamento informatizado dos dados pessoais, é inegável a relevância que a sociedade de informação tem neste âmbito. Importa, por isso, dar particular atenção ao facto de, quase como correlativo dos direitos que o RGPD garante aos titulares dos dados, existir um conjunto de comportamentos para os quais os titulares devem estar despertos.

Considera-se particularmente relevante indicar algumas atitudes que os titulares dos dados pessoais devem ter presente, com vista a uma proteção ativa dos seus dados pessoais, quando utilizam meios informáticos, navegam na internet e fazem partilhas nas redes sociais.

Não se trata de regressar ao passado e deixar de utilizar as novas tecnologias - o que seria uma proposta inaceitável e injustificada.

Trata-se, no entanto, de cada um ter presente uma forma de atuação mais responsável para integrar o modelo complexo de proteção que o RGPD visa implementar.

Assim:

a) Ações de segurança que devo tomar (não partilhar informação relevante, designadamente nºs de cartões de identificação, de contas bancárias, de passaportes, fotografias de que no futuro posso não gostar; não clicar em links cuja origem não tenha a certeza absoluta); apenas fazer pagamentos em *sites* com segurança certificada para o efeito e, preferencialmente, por sistemas que não permitam aceder em situações futuras; fazer as atualizações dos sistemas; apagar de imediato e sem abrir emails desconhecidos, a não ser quando se conheça sem qualquer dúvida o respetivo remetente.

b) Exercer os direitos que são conferidos pelo RGPD, de forma consciente e responsável, solicitando informação sobre os dados pessoais, pedindo a respetiva retificação ou eliminação, quer junto das redes sociais que utilizo, quer das entidades que me prestam serviços ou junto dos serviços públicos;

c) Ler e responder, de forma consciente, às perguntas sobre privacidade dos dados que são feitas sempre que adiro a um serviço, a uma rede social ou utilizo uma aplicação móvel. Deve ter-se em atenção que, por causa do RGPD, as perguntas e informações prestadas são feitas de forma mais clara e compreensível do que sucedia anteriormente.

d) Compreender que a cada um cabe também respeitar e proteger os dados pessoais de terceiros, não os expondo indevidamente. Em particular, deve reduzir-se a partilha de informações nas redes sociais sobre crianças e jovens ainda menores, pois para além de colocar a sua segurança em risco e potenciar fenómenos criminosos deve ter-se presente que também as crianças são salvaguardadas pelo RGPD e têm direito à proteção dos seus dados pessoais.

Saber mais

Leia, no Regulamento (UE) 2016/679:

Artigo 55º

Artigos 37º, 38º, 39º (Considerando 97), Artigo 51º (Considerandos 117, 119 e 123), Artigo 52º (Considerandos 118 e 120)

Artigo 58º (Considerando 129)

Artigo 77º (Considerando 141)

Artigo 78º (Considerando 143)

Artigo 79º (Considerando 145)

Artigo 80º (Considerando 142)

Artigo 82º (Considerando 146), 83º (Considerando 150).

Artigo 84º