Regulamento Geral sobre Proteção de Dados

GUIA INFORMATIVO PARA MICRO E PME'S

18 de maio de 2018

AHRESP®
ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
Instituição de Utilidade Pública

Regulamento Geral sobre Proteção de Dados (RGPD)

GUIA INFORMATIVO PARA MICRO E PME'S

I. O RGPD

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, designado por RGPD - Regulamento Geral sobre a Proteção de Dados, veio estabelecer novas e exigentes regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, substituindo a Diretiva 95/46/CE e o atual quadro jurídico nacional instituído pela Lei n.º 67/98, de 26 de outubro, retificada pela Declaração de Retificação n.º 22/98, de 28 de novembro e alterada pela Lei n.º 103/2015, de 24 de agosto – Lei da Proteção de dados pessoais.

Este é um Regulamento Comunitário, com aplicação direta no ordenamento jurídico nacional, sem necessidade de qualquer transposição ou outro ato, podendo ser exigido o seu cumprimento, quer por parte do órgão fiscalizador competente nesta matéria, quer pelos próprios titulares dos dados pessoais, a partir de 25 de maio de 2018.

As alterações introduzidas por este Regulamento, quando comparadas com as que já existem na nossa Lei atual, são muitas e complexas, e o seu impacto em cada organização irá depender da atividade desenvolvida, e da natureza, dimensão e tratamento dos dados que são recolhidos.

Com a aplicação do RGPD, deixa também de existir o controlo prévio por parte da Comissão Nacional de Proteção de Dados (CNPD), para o tratamento de determinados dados pessoais, passando a responsabilidade para as próprias empresas, sendo o controlo de legalidade efetuado à *posteriori*.

Este documento consiste num Guia meramente informativo, tendo como fonte a Comissão Europeia, e não dispensa o apoio técnico especializado nesta matéria.

Como princípio basilar nesta matéria, tenha sempre presente que apenas deve recolher os dados pessoais absolutamente necessários e a eles só deve ter acesso quem deles necessite absolutamente – princípio da «minimização dos dados».

II. Aplicação do RGPD

O RGPD é aplicável a todas as entidades que recolham e tratem dados pessoais, sejam pessoas singulares ou coletivas, sejam entidades públicas ou privadas.

Importa assim, atender à definição de **«dados pessoais»**: informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»). É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou

mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Por **«tratamento»** de dados pessoais, entende-se uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

As regras de proteção de dados não se aplicam assim aos dados relativos a empresas, mas sim apenas a dados pessoais relativos a pessoas singulares. Não dizem respeito a dados relativos a empresas nem a outras entidades jurídicas. No entanto, as informações respeitantes a empresas unipessoais podem constituir dados pessoais caso permitam a identificação de uma pessoa singular. As regras também se aplicam a todos os dados pessoais relacionados com pessoas singulares no âmbito de uma atividade profissional, como os trabalhadores de uma empresa/organização, incluindo endereços de correio eletrónico profissionais como «nome.apelido@empresa.eu» ou os números de telefone profissionais dos trabalhadores.

Caso se trate de uma micro, pequena ou média empresa, que faça tratamento de dados pessoais como acima descrito, então já terá de cumprir as regras do RGPD. No entanto, se o tratamento de dados pessoais não for uma parte principal do seu negócio e a sua atividade não criar riscos para as pessoas, então algumas obrigações do RGPD não se aplicam (por exemplo, a nomeação de um Encarregado da Proteção de Dados (EPD). Importa salientar que as «atividades principais» incluem atividades em que o tratamento de dados é uma parte indestrinçável da atividade do responsável pelo tratamento ou do subcontratante.

A sua empresa/organização só tem de nomear um EPD, quer seja um responsável pelo tratamento, quer um subcontratante, se as suas atividades principais envolverem o tratamento de dados sensíveis em grande escala ou se as suas atividades principais envolverem o controlo sistemático, regular e em grande escala de pessoas. Neste contexto, o controlo do comportamento das pessoas inclui todas as formas de rastreamento e definição de perfis na internet, nomeadamente para efeitos de publicidade comportamental.

Os seguintes dados pessoais são considerados «sensíveis» e estão sujeitos a condições de tratamento específicas:

- Dados pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas;
- Filiação sindical;
- Dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano;
- Dados relacionados com a saúde;
- Dados relativos à vida sexual ou orientação sexual da pessoa.

Caso necessite de um EPD, este pode ser um funcionário da sua organização ou pode ser contratado externamente com base num contrato de prestação de serviços. O EPD pode ser uma pessoa ou uma organização.

Como função, o EPD auxilia o responsável pelo tratamento ou o subcontratante em todas as questões relacionadas com a proteção de dados pessoais. O EPD deve, concretamente:

- Informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os seus trabalhadores, sobre as respetivas obrigações nos termos da lei da proteção de dados;

- Controlar o cumprimento, por parte da organização, de toda a legislação relacionada com a proteção de dados, nomeadamente em auditorias, atividades de sensibilização e formação do pessoal implicado nas operações de tratamento;
- Prestar aconselhamento sempre que tenha sido realizada uma avaliação de impacto da proteção de dados (AIPD) e controlar a sua realização. Esta avaliação é necessária sempre que o tratamento seja suscetível de resultar num elevado risco para os direitos e as liberdades das pessoas (exemplo: avaliação sistemática e completa dos aspetos pessoais, incluindo a definição de perfis, tratamento de dados sensíveis em grande escala, controlo sistemático de zonas públicas em grande escala);
- Atuar como ponto de contacto para pedidos de pessoas relativamente ao tratamento dos seus dados pessoais e ao exercício dos seus direitos;
- Cooperar com a Autoridade de Proteção de Dados (APD) e atuar como ponto de contacto das mesmas sobre questões relacionadas com o tratamento.

A organização tem de envolver o EPD nas suas atividades em tempo útil. O EPD não deve receber instruções do responsável pelo tratamento nem do subcontratante relativamente ao exercício das suas funções. O EPD responde diretamente perante o nível mais elevado de administração da organização.

III. PRINCÍPIOS DO RGPD

O tipo e a quantidade de dados pessoais que uma empresa/organização pode tratar dependem do motivo pelo qual estão a efetuar o tratamento (motivo jurídico) e da finalidade do mesmo. A empresa/organização deve respeitar várias regras fundamentais, nomeadamente:

- Os dados pessoais devem ser tratados de **forma lícita e transparente**, garantindo a lealdade do tratamento para com as pessoas cujos dados pessoais estão a ser tratados («licitude, lealdade e transparência»);
- Devem existir **finalidades específicas** para o tratamento dos dados e a empresa/organização deve comunicá-las às pessoas aquando da recolha dos seus dados pessoais. Uma empresa-organização não pode simplesmente recolher dados pessoais para fins indefinidos («limitação das finalidades»);
- A empresa/organização deve recolher e tratar **apenas os dados pessoais necessários para cumprir essa finalidade** («minimização dos dados»);
- A empresa/organização deve garantir que os dados pessoais são exatos e estão atualizados, tendo em conta as finalidades para as quais são tratados, e corrigi-los caso tal não se verifique («exatidão»);
- A empresa/organização não pode utilizar os dados pessoais para outras finalidades que não sejam **compatíveis** com a finalidade original da recolha;
- A empresa/organização deve garantir que os dados pessoais são **conservados apenas durante o tempo necessário** às finalidades para as quais foram recolhidos («limitação da conservação»);
- A empresa/organização deve instalar **garantias técnicas e organizativas** adequadas para garantir a segurança dos dados pessoais, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as tecnologias adequadas («integridade e confidencialidade»).

Assim, quando recolhe os dados pessoais dos seus clientes, deve explicar em linguagem clara e simples o motivo pelo qual precisa dos dados, de que modo os irá utilizar e durante quanto tempo tenciona conservá-los. O tratamento deve ser efetuado de forma a respeitar os princípios fundamentais da proteção de dados.

A finalidade do tratamento de dados deve ser conhecida e as pessoas cujos dados estão a ser tratados têm de ser informadas. Não é possível indicar simplesmente que os dados pessoais serão recolhidos e tratados. Este princípio é conhecido como o princípio da «limitação das finalidades».

No entanto, se a sua empresa/organização tiver recolhido dados com base em interesses legítimos, num contrato ou em interesses vitais, pode utilizá-los para outra finalidade, mas apenas depois de verificar que a nova finalidade é compatível com a finalidade original.

Devem ser ponderados os seguintes aspetos:

- A ligação entre a finalidade original e a finalidade nova/subsequente;
- O contexto em que os dados foram recolhidos (qual é a relação entre a sua empresa e a pessoa?);
- Qual o tipo e a natureza dos dados (são sensíveis?);
- As possíveis consequências do tratamento subsequente previsto (de que modo irá afetar a pessoa?);
- A existência de proteções adequadas (como cifragem ou pseudonimização).

Caso a sua empresa/organização tenha recolhido os dados com base em **consentimento ou num requisito legal**, não poderá efetuar o tratamento subsequente para além do que se encontra abrangido pelo consentimento original ou pela disposição legal. Qualquer tratamento subsequente exigirá a obtenção de um **novo consentimento** ou de uma nova base jurídica.

Sempre que sejam necessários dados pessoais, estes devem ser **adequados, pertinentes e limitados ao que é necessário relativamente à finalidade em questão («minimização dos dados»)**. É da responsabilidade da sua empresa/organização, enquanto responsável pelo tratamento, avaliar qual a quantidade de dados necessária e garantir que não são recolhidos dados não pertinentes.

Os dados devem ser conservados durante **o mínimo de tempo possível**. Este período deve ter em conta os motivos pelos quais a sua empresa/organização precisa de efetuar o tratamento dos dados, bem como eventuais obrigações legais de conservação dos dados durante um determinado período de tempo (por exemplo, legislação nacional em matéria laboral, fiscal ou antifraude que o obrigue a conservar os dados pessoais relativos aos seus trabalhadores durante um período definido, período de garantia de produtos, etc.).

A sua empresa/organização deve estabelecer **prazos** para o **apagamento ou revisão** dos dados conservados.

A sua empresa/organização também deve garantir que os dados que possui são exatos e atualizados.

No momento da recolha dos dados, as pessoas devem ser informadas, pelo menos, do seguinte:

- **Quem é** a sua empresa/organização (os seus contactos e os do EPD, se existir);
- **Porque é** que a sua empresa/organização irá utilizar os seus dados pessoais (finalidades);
- As categorias de dados pessoais em causa;
- A **justificação jurídica** para o tratamento dos seus dados;
- **Durante quanto tempo** serão conservados os dados;
- **Quem mais** poderá receber os dados;
- Se os dados pessoais serão **transferidos** para um destinatário fora da UE;
- Que a pessoa tem o direito a obter uma **cópia dos dados** (direito de acesso aos dados pessoais), bem como outros **direitos básicos** no domínio da proteção de dados (ver a lista completa dos direitos, no Anexo I);
- Que a pessoa tem o **direito de apresentar uma reclamação** à APD;

- Que a pessoa tem o **direito de retirar o seu consentimento** em qualquer altura;
- Se aplicável, a existência de **decisões automatizadas** e a lógica envolvida, incluindo as suas consequências.

Estas informações podem ser fornecidas **por escrito ou oralmente** a pedido da pessoa desde que a sua identidade seja comprovada por outros meios ou por meios eletrónicos se tal for apropriado. A sua empresa/organização deve fazê-lo de forma **concisa, transparente, inteligível e de fácil acesso,** utilizando uma **linguagem clara e simples** e **gratuitamente.**

Se os dados forem obtidos de outra empresa/organização, a sua empresa/organização deve fornecer as informações indicadas acima à pessoa à qual dizem respeito o mais tardar um mês após a sua empresa/organização ter obtido os dados pessoais; ou, caso a sua empresa/organização comunique com a pessoa, quando os dados forem utilizados para comunicar; ou, se estiver prevista a divulgação a outra empresa, aquando da primeira divulgação dos dados pessoais.

Salvo algumas exceções, a sua empresa/organização também tem de informar sobre as categorias dos dados e sobre a fonte a partir da qual os obteve, incluindo se foram obtidos de fontes acessíveis ao público.

IV. FUNDAMENTO JURÍDICO DO TRATAMENTO DE DADOS

A sua empresa/organização só pode efetuar o tratamento de dados nas circunstâncias seguintes:

- Com o **consentimento** das pessoas em causa;
- Quando existir uma **obrigação contratual** (um contrato entre a sua empresa/organização e um cliente);
- Para cumprir uma **obrigação legal** (prevista na legislação da UE ou na legislação nacional);
- Quando o tratamento for necessário para o desempenho de uma tarefa de **interesse público** (prevista na legislação da UE ou na legislação nacional);
- Para proteger os **interesses vitais** de uma pessoa;
- Tendo em vista os **interesses legítimos** da sua organização, mas apenas após ter confirmado que os direitos e as liberdades fundamentais da pessoa cujos dados está a tratar não serão gravemente afetados. Se os direitos da pessoa prevalecerem sobre os seus interesses, não pode ser efetuado o tratamento com base em interesses legítimos. A avaliação com vista a determinar se os interesses legítimos da sua empresa/organização no tratamento prevalecem sobre os das pessoas em causa depende das circunstâncias específicas do caso.

Quanto ao **consentimento,** quando este seja necessário ao tratamento de dados pessoais, para que o mesmo seja válido têm de estar preenchidas as seguintes condições:

- Deve ser **dado de livre vontade;**
- Deve ser **informado;**
- Deve ser dado para uma **finalidade específica;**
- Todos os motivos para o tratamento devem ser indicados de forma clara;
- É **explícito** e dado através de um ato positivo (por exemplo, uma caixa de verificação em linha que a pessoa tem de marcar explicitamente ou uma assinatura num formulário);
- **Utiliza linguagem clara e simples** e é claramente visível;
- É possível **retirar o consentimento** e tal facto é explicado (por exemplo, uma ligação para cancelamento da subscrição no final de uma mensagem de correio eletrónico).

Para que o consentimento seja **dado de livre vontade**, a pessoa tem de poder escolher livremente e de poder recusar ou retirar o consentimento sem sofrer qualquer desvantagem. O consentimento não é dado de livre vontade se, por exemplo, existir um desequilíbrio claro entre a pessoa e a empresa/organização (por exemplo, relação empregador/trabalhador) ou se for pedido à pessoa que consinta no tratamento de dados desnecessários como condição prévia à execução de um contrato ou serviço.

Para que o consentimento seja **informado**, a pessoa tem de receber, pelo menos, as seguintes informações:

- A identidade da organização que efetua o tratamento dos dados;
- Os fins para os quais os dados estão a ser tratados;
- O tipo de dados que serão tratados;
- A possibilidade de retirar o consentimento dado (por exemplo, uma ligação para cancelamento da subscrição no final de uma mensagem de correio eletrónico);
- Se aplicável, o facto de os dados irem ser utilizados para decisões exclusivamente automatizadas, incluindo a definição de perfis;
- Se o consentimento estiver relacionado com uma transferência internacional, os possíveis riscos das transferências de dados para países terceiros que não estejam sujeitos a uma decisão de adequação por parte da Comissão e quando não existam proteções adequadas.

Lembre-se: quando alguém consente no tratamento dos seus dados pessoais, a empresa só pode efetuar o tratamento dos dados para as finalidades para as quais o consentimento foi dado.

Se o consentimento dado por uma pessoa antes de o Regulamento Geral sobre a Proteção de Dados (RGPD) ser aplicável (25 de maio de 2018), estiver em conformidade com as condições do RGPD, não é necessário solicitar de novo o consentimento. A sua empresa/organização tem de garantir que o consentimento dado antes do RGPD cumpre as condições previstas no RGPD.

O consentimento deve ser tão fácil de retirar como de dar. Se o consentimento for retirado, a sua empresa/organização deixa de poder efetuar o tratamento dos dados. Uma vez retirado o consentimento, a sua empresa/organização tem de garantir que os dados são apagados, a menos que exista outro fundamento jurídico para o respetivo tratamento (por exemplo, obrigatoriedade de conservação ou necessidade dos dados para a execução do contrato).

Se os dados estavam a ser tratados para várias finalidades, a sua empresa/organização não pode utilizar os dados pessoais para a parte do tratamento relativamente à qual o consentimento foi retirado ou para nenhuma finalidade, consoante a natureza da retirada do consentimento.

Caso se trate de crianças, a sua empresa/organização só pode efetuar o tratamento dos seus dados pessoais com base no consentimento se tiver o consentimento explícito do progenitor ou tutor da criança até uma determinada idade. O limite etário para a obtenção de consentimento parental varia entre os 13 e os 16 anos, dependendo da idade que venha a ser definida em cada Estado-Membro da UE.

Tendo em conta a tecnologia disponível, tem de se feito um esforço adequado para verificar se o consentimento dado está efetivamente em conformidade com a lei. Isto significa que a sua empresa/organização tem de aplicar medidas de verificação da idade (por exemplo, perguntas de controlo, ações no sítio *web*).

V. OBRIGAÇÕES

O **responsável pelo tratamento** determina as **finalidades** e os **meios** pelos quais os dados pessoais são tratados. Portanto, a sua empresa/organização é a responsável pelo tratamento se decide «porquê» e «como» os dados pessoais devem ser tratados. Os trabalhadores que efetuam o tratamento de dados pessoais na sua organização fazem-no para cumprir as suas tarefas enquanto responsável pelo tratamento.

A sua empresa/organização é **responsável conjunto pelo tratamento** quando determina, em conjunto com uma ou mais organizações, «porquê» e «como» os dados pessoais devem ser tratados. Os responsáveis conjuntos pelo tratamento devem celebrar um acordo que defina as respetivas responsabilidades pelo cumprimento das regras do RGPD. Os principais aspetos desse acordo devem ser comunicados às pessoas cujos dados são objeto de tratamento.

O **subcontratante** só efetua o tratamento de dados pessoais **em nome do responsável pelo tratamento**. O subcontratante é geralmente um terceiro externo à empresa; contudo, no caso dos grupos de empresas, uma empresa pode atuar como subcontratante para outra empresa.

Os deveres do subcontratante perante o responsável pelo tratamento devem ser especificados num contrato ou noutro ato jurídico. Por exemplo, o contrato deve indicar o que acontece aos dados pessoais uma vez terminado o contrato. O subcontratante só pode subcontratar uma parte das suas tarefas a outro subcontratante ou nomear um subcontratante conjunto se tiver recebido autorização prévia por escrito do responsável pelo tratamento dos dados.

Existem situações em que uma entidade pode ser um responsável pelo tratamento, um subcontratante ou ambos.

Uma outra entidade (uma pessoa singular ou coletiva ou qualquer outro organismo), **pode efetuar o tratamento de dados pessoais** em seu nome desde que **exista um contrato ou outro ato jurídico**. É importante que o subcontratante nomeado por si apresente garantias suficientes para a aplicação de medidas técnicas e organizativas destinadas a assegurar que o tratamento cumprirá as normas do Regulamento Geral sobre a Proteção de Dados (RGPD) e a garantir a proteção dos direitos das pessoas.

O subcontratante nomeado não pode, posteriormente, nomear outro subcontratante sem a sua autorização prévia, específica ou geral, por escrito. O contrato ou ato jurídico celebrado entre a sua empresa/organização e o subcontratante deve incluir os seguintes elementos:

- O tratamento só pode ser efetuado com base em instruções documentadas do responsável pelo tratamento;
- O subcontratante garante que as pessoas autorizadas a efetuar o tratamento de dados pessoais assumiram um compromisso de confidencialidade ou se encontram sujeitas a uma obrigação legal de confidencialidade adequada;
- O subcontratante deve oferecer um nível mínimo de segurança definido pelo responsável pelo tratamento;
- O subcontratante deve ajudá-lo a garantir a conformidade com o RGPD.

VI. VIOLAÇÃO DE DADOS

Uma violação de dados ocorre quando a sua empresa/organização sofre um incidente de segurança relativo aos dados pelos quais é responsável que resulta numa violação da confidencialidade, da disponibilidade ou da integridade dos dados. Se tal ocorrer, e se a violação for suscetível de representar um risco para os direitos e as liberdades de uma pessoa, a sua empresa/organização tem de **notificar a autoridade de controlo sem demora injustificada e, o mais tardar, no prazo de 72 horas após tomar conhecimento da violação**. Se a sua empresa/organização for um subcontratante, tem de notificar todas as violações de dados ao responsável pelo tratamento.

Se a violação de dados representar **um elevado risco para as pessoas afetadas**, estas devem também ser informadas (a menos que existam medidas de proteção técnicas e organizativas eficazes ou outras medidas destinadas a garantir que não é provável que o risco se volte a concretizar).

Enquanto organização, é fundamental aplicar medidas técnicas e organizativas adequadas para evitar possíveis violações de dados.

VII. LIDAR COM OS TITULARES DOS DADOS

As pessoas podem contactar a sua empresa/organização para exercerem os direitos que lhes são conferidos pelo RGPD (direitos de acesso, retificação, apagamento, portabilidade, etc.). Se os dados pessoais forem tratados por meios eletrónicos, a sua empresa/organização deve dispor de meios que permitam que os pedidos sejam efetuados por via eletrónica. A sua empresa/organização deve responder aos pedidos sem demora injustificada e, em princípio, no prazo de **um mês a contar da receção do pedido**.

Pode pedir informações suplementares para confirmar a identidade da pessoa que efetua o pedido.

Se a sua empresa/organização rejeitar o pedido, tem de informar a pessoa sobre os motivos para tal e sobre o direito de apresentar uma reclamação à APD, bem como de intentar ação judicial.

O tratamento dos pedidos das pessoas **deve ser efetuado gratuitamente**. Se os pedidos forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, é possível cobrar uma taxa razoável ou recusar-se a dar seguimento ao pedido.

VII.i Acesso aos dados

Quando uma pessoa solicita acesso aos seus dados pessoais, a empresa/organização deve:

- Confirmar se está ou não a efetuar o tratamento de dados pessoais que lhe digam respeito;
- Apresentar uma cópia dos dados pessoais que possui a respeito dessa pessoa;
- Prestar informações sobre o tratamento (nomeadamente as finalidades, as categorias de dados pessoais, os destinatários dos dados, etc.).

A sua empresa/organização deve fornecer à pessoa uma cópia dos seus dados pessoais gratuitamente. No entanto, as eventuais cópias suplementares poderão estar sujeitas a uma taxa de valor razoável.

O exercício do direito de acesso está estreitamente ligado ao exercício do direito à portabilidade dos dados, que permite à pessoa transmitir os seus dados para outra organização.

É importante que no aviso de privacidade da sua empresa/organização se distingam claramente estes dois direitos. Assim, ambos os direitos terão de ser brevemente mencionados em separado.

VII.ii Apagamento dos dados

O Regulamento Geral sobre a Proteção de Dados (RGPD) dá às pessoas **o direito de pedirem que os seus dados sejam apagados** e as organizações têm **a obrigação de o fazer, exceto** nos casos seguintes:

- Os dados pessoas que a sua empresa/organização possui são necessários para exercer o direito à liberdade de expressão;
- Quando uma obrigação jurídica o obriga a conservar os dados;
- Por motivos de interesse público (por exemplo, saúde pública, investigação científica ou histórica).

Se a sua empresa/organização tiver efetuado o tratamento de dados ilicitamente, terá de os apagar. Se se tratar de uma pessoa cujos dados pessoais tenham sido recolhidos quando a pessoa era menor, os mesmos terão de ser apagados.

No que se refere ao direito a ser esquecido em linha, as organizações devem tomar medidas razoáveis (por exemplo, medidas técnicas) para informar outros sítios *web* de que uma determinada pessoa solicitou o apagamento dos seus dados pessoais.

Os dados também podem ser conservados caso tenham sido submetidos a um processo de anonimização adequado.

VII.iii Oposição ao tratamento dos dados

As pessoas têm o **direito de se opor ao tratamento de dados pessoais** se apresentarem motivos específicos que os afetem. Se uma tal situação específica existe ou não, é uma questão que tem de ser examinada caso a caso e que pode ser afetada por alterações das circunstâncias, mudanças na qualidade da intervenção ou por uma nova situação de perigo.

As pessoas têm direito a opor-se nos casos em que uma administração pública esteja a efetuar o tratamento dos dados no contexto das suas atribuições públicas ou em que uma empresa esteja a efetuar o tratamento dos dados com base nos seus interesses legítimos. Nestes casos, a sua empresa/organização já não pode efetuar o tratamento dos dados, a menos que consiga demonstrar que tem de efetuar o tratamento por motivos que devam prevalecer sobre os direitos e as liberdades das pessoas ou caso precise dos dados para a declaração, o exercício ou a defesa de um direito num processo judicial.

As pessoas têm também o direito de se opor, em qualquer altura, ao tratamento dos seus dados pessoais para **efeitos de comercialização direta**. A comercialização direta é entendida, no Regulamento Geral sobre a Proteção de Dados, como qualquer ação, por parte de uma empresa, destinada a comunicar material publicitário ou de comercialização, dirigida a pessoas específicas. A sua empresa/organização deve informar as pessoas, no seu aviso de privacidade ou pelo menos no momento da primeira comunicação com as mesmas, de que irá utilizar os seus dados pessoais para efeitos de comercialização direta e de que estes têm o direito a opor-se gratuitamente. Sempre que uma pessoa se opõe ao tratamento dos dados pessoais para efeitos de comercialização direta, a sua empresa/organização deixa de poder efetuar o tratamento dos seus dados pessoais para esse efeito.

VII.iv Portabilidade dos dados

As pessoas têm o direito de portabilidade dos dados, ou seja, de receber, da sua empresa/organização, os dados pessoais que lhe forneceram num formato estruturado de leitura automática, e de pedir a sua transferência para outra empresa/organização (direito à portabilidade dos dados). Este direito só pode ser exercido se os dados pessoais tiverem sido recolhidos no contexto de um contrato ou com base no consentimento, e se forem tratados por meios automatizados.

VIII. EXECUÇÃO E SANÇÕES

O Regulamento Geral sobre a Proteção de Dados (RGPD) disponibiliza diferentes opções às autoridades de proteção de dados em caso de incumprimento das regras de proteção de dados:

- Infração provável – pode ser emitida uma advertência;
- Infração – podem ser aplicadas as sanções de repreensão, proibição temporária ou definitiva do tratamento e uma coima máxima de 20 milhões de euros ou 4 % do volume de negócios total anual da empresa.

Importa notar que, no caso de uma infração, a APD pode impor uma coima monetária ao invés, ou além, da repreensão e/ou da proibição do tratamento.

A autoridade deve garantir que as coimas impostas em cada caso são **eficazes, proporcionadas** e **dissuasivas**. Terá em conta vários fatores, como a natureza, a gravidade e a duração da infração, o seu caráter intencional ou negligente, eventuais ações tomadas para atenuar os danos sofridos pelas pessoas, o grau de cooperação da organização, etc.

As pessoas podem pedir uma indemnização se uma empresa ou organização tiver infringido o Regulamento Geral sobre a Proteção de Dados (RGPD) e se uma pessoa tiver sofrido danos patrimoniais como, por exemplo, um prejuízo financeiro ou danos não patrimoniais como, por exemplo, danos à sua reputação ou sofrimento psicológico. O RGPD garante que estes danos sejam indemnizados, independentemente do número de organizações envolvidas no tratamento dos seus dados. A indemnização pode ser pedida diretamente à organização ou junto dos tribunais nacionais competentes. As ações são intentadas junto dos tribunais do Estado-Membro da UE onde o responsável pelo tratamento tem o seu estabelecimento ou onde reside o cidadão que solicita a indemnização (residência habitual).

Fonte: Comissão Europeia (www.ec.europa.eu)

Lisboa, 18 de maio 2018

***

Anexo I

"Artigo 13.º

Informações a facultar quando os dados pessoais são recolhidos junto do titular

1. Quando os dados pessoais forem recolhidos junto do titular, o responsável pelo tratamento faculta-lhe, aquando da recolha desses dados pessoais, as seguintes informações:

a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;

b) Os contactos do encarregado da proteção de dados, se for caso disso;

c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;

d) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro;

e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;

f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.º ou 47.º, ou no artigo 49.º, n.º 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.

2. Para além das informações referidas no n.º 1, aquando da recolha dos dados pessoais, o responsável pelo tratamento fornece ao titular as seguintes informações adicionais, necessárias para garantir um tratamento equitativo e transparente:

a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;

b) A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;

c) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea a), ou no artigo 9.º, n.º 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;

d) O direito de apresentar reclamação a uma autoridade de controlo;

e) Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;

f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

3. Quando o responsável pelo tratamento pessoais tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos, antes desse tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes, nos termos do n.º 2.

4. Os n.ºs 1, 2 e 3 não se aplicam quando e na medida em que o titular dos dados já tiver conhecimento das informações."

RGPD - GUIA INFORMATIVO PARA MICRO E PME'S

AHRESP®

ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL

Instituição de Utilidade Pública

www.ahresp.com