MARÇO
2018

FORMAÇÃO

Regulamento Geral de Proteção de Dados

EVE0218-1

Filipa Magalhães

www.occ.pt

FICHA TÉCNICA

Título: Regulamento Geral de Proteção de Dados

Autor: Filipa Magalhães

Capa e paginação: DCI – Departamento de Comunicação e Imagem da Ordem dos Contabilistas Certificados

Impresso por Jorge Fernandes, Lda em março de 2018

Depósito-Legal:

ÍNDICE

Introdução

A aproximação da entrada plena em vigor do Novo Regulamento Geral de Proteção de Dados (Regulamento Europeu n.º 2016/679) coloca novos desafios aos responsáveis pelo tratamento de dados estreitamente relacionados com os direitos dos titulares dos dados pessoais.

E não obstante não se trate de um texto recente, porquanto foi precedido de uma discussão que durou 4 anos e já se encontra publicado desde 27 de Abril de 2016, a verdade é que a proximidade da sua entrada plena em vigor – 25 de maio de 2018 – associada ao alarmismo social gerado à volta do tema, têm suscitado questões para as quais os esclarecimentos nem sempre estão ao alcance de quem os procura.

Os Contabilistas Certificados têm, neste domínio, um papel importantíssimo, enquanto conselheiros dos seus clientes, que buscam os melhores conselhos e apoio, mas também enquanto responsáveis pelo tratamento de dados dos seus próprios clientes e como subcontratados, a quem são confiados os dados recolhidos pelos seus clientes, e que assim se tornam responsáveis pelo seu tratamento.

É nosso objetivo, com o presente Manual, criar um documento prático e facilmente compreensível no qual o Contabilista Certificado possa encontrar respostas para as suas questões ao mesmo tempo que encontra orientações quanto à forma de implementar o presente regulamento e de cumprir com as obrigações por este impostas às entidades Responsáveis pelo Tratamento de dados.

Prosseguindo este desiderato este será um manual no qual abandonaremos um estilo estritamente descritivo para adotar um estilo mais gráfico e enunciativo, com listas, esquemas e outros estilos de discurso que nos permitam simplificar a informação.

A publicação no dia 27 de Abril de 2016o novo Regulamento Geral de Proteção de Dados – RGPD – constitui um marco fundamental na regulação do tratamento dos dados pessoais, tendo como escopo responder aos novos desafios na área de proteção de dados pessoais gerados pela evolução das novas tecnologias e pela globalização dos mercados. Este regulamento faz parte do pacote da União Europeia relativo à reforma da proteção de dados e passará a ser aplicado direta e obrigatoriamente a partir de 25 de maio de 2018, trazendo impactos significativos na vida das organizações.

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

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

O RGPD introduz um conjunto de novas regras, entre as quais se destaca a obrigação de designar um encarregado para a proteção de dados, regras sobre pseudonimização de dados, a alteração das regras sobre obtenção de consentimento, novas regras sobre consentimento de menores, a eliminação do sistema de notificações e autorizações, a implementação do direito ao esquecimento, a

criação de obrigações acrescidas para os subcontratados, a introdução de coimas de valor muito elevado e obrigações de informação relativas a quebras de segurança, são algumas das inovações introduzidas por este diploma.

NOTA: No momento em que terminávamos este Manual foi aprovada em Conselho de Ministros a Proposta de Lei com vista a assegurar a execução do Regulamento Comunitário no ordenamento jurídico nacional. Não obstante esta Proposta, no momento em que for publicada sob a forma de Lei, passar a integrar, conjuntamente com o RGPD, o regime jurídico da proteção de dados em Portugal, neste momento ainda não é seguro associá-la ao conteúdo deste Manual, não sendo igualmente correto não lhe fazer qualquer referência. Por esse motivo, no final do Manual poderá encontrar um capítulo com o regime da Proposta, o qual pode, no entanto, sofrer alterações de pormenor até à data da sua efetiva publicação.

O Regulamento de Proteção de Dados (RGPD) e o novo paradigma no tratamento de dados

1. O regime jurídico do tratamento de dados

O Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (doravante RGPD) opera uma mudança de paradigma no modelo de tratamento de dados pessoais e de livre circulação dos mesmos, com vista à garantia do mercado único sem restrições em virtude do diferente enquadramento legal e salvaguarda do direito à proteção dos dados pessoais.

Não é, no entanto, correto dizer que este é o diploma que trata e regula pela primeira vez a matéria da proteção de dados, porquanto esta preocupação já existe e se encontra plasmada em alguns diplomas atualmente em vigor.

Exemplo disso é a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, de 4.11.1950 que já consagrava no seu art. 8.º o direito pelo respeito à vida privada e familiar.

Pode ler-se no art. 8.º deste texto o seguinte:

1. *Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicilio e da sua correspondência.*
2. *Não pode haver ingerência da autoridade públoca no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providencia que, numa sociedade democrática, seja necessário para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a promoção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.*

Consciente dos perigos e desafios da massificação e globalização da informação bem como da necessidade de dar novas respostas às questões colocadas pela generalização das redes sociais e da internet e dos perigos que lhe estão associados, o Parlamento Europeu, o Conselho e a Comissão aprovaram mais recentemente a Carta dos Direitos Fundamentais da União Europeia (2016C 202/2) que reconhece e consagra os seguintes direitos aos nacionais da União Europeia:

Artigo 7.º
Respeito pela vida privada e familiar

Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.

Artigo 8.º
Proteção de dados pessoais

1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

Este quadro comunitário não ficaria completo se não referíssemos a nossa Constituição da República Portuguesa, que para além de reconhecer timidamente o Direito à Privacidade no art. 26.º, n.º 1, remete para a lei o estabelecimento de garantias efetivas contra a utilização abusiva de informações relativas às pessoas e famílias (cfr. n.º 2 do art. 26.º).

E percebendo o legislador constituinte que um dos maiores perigos para os nossos dados se encontra na generalização dos acessos e da utilização da Internet serviu-se do art. 35.º da CRP para proteger este direito fundamental.

É, pois, curioso ver como este artigo, que já se encontrava na versão inicial da Constituição em 1976, embora com uma extensão bastante menor e referindo apenas os registos mecanográficos dos dados, foi alterado em 1982, altura em que ganhou mais dimensão e passou a fazer referência aos registos informáticos, mais tarde, em 1989, passando a ter a partir de 1997 a versão que vos apresentamos de seguida em que confere aos dados tratados em ficheiros manuais proteção idêntica à atribuída aos dados tratados em suporte informatizado.

Artigo 35.º
Utilização da informática

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

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

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

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

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

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

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

Em complemento a este artigo e numa perspetiva da relação entre a Administração Pública e os administrados, o art. 18.º do Código do Procedimento Administrativo (doravante CPA) estabelece que: *os particulares têm direito à proteção dos seus dados pessoais e à segurança e integridade dos suportes, sistemas e aplicações utilizados para o efeito, nos termos da lei.*

A finalizar o enquadramento jurídico nacional da Proteção de Dados importa aqui referir a Lei n.º 67/98, de 26 de outubro que transpõe para a ordem jurídica interna a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

2. O RGPD e o novo paradigma do regime de tratamento de dados

O RGPD, por ser um Regulamento Comunitário e não uma Diretiva (como sucedia com a Diretiva n.º 95/46/CE) tem aplicação direta na ordem jurídica de cada Estado Membro, sendo essa, justamente uma das maiores razões pelas quais o RGPD se sucede à Diretiva – para garantir o tratamento uniforme destas matérias em todos os estados europeus.

De facto, a diferença entre o Regulamento e a Diretiva reside na imposição aos Estados-Membros e no facto de o primeiro, ao contrário da segunda, não carecer de transposição para o ordenamento jurídico dos Estados-Membros, assegurando um tratamento uniforme dos dados dentro do espaço da União Europeia e, mesmo fora do espaço europeu, sempre que esteja em causa o tratamento de dados de cidadãos europeus. Todavia, este Regulamento tem uma singularidade quando comparado com os restantes Regulamentos Comunitários e que consiste no facto de pedir aos Estados-Membros uma substancial intervenção interna por forma a conseguir abarcar as suas diferentes tradições. Verifica-se esta necessidade de intervenção ao nível da definição da idade dos menores para a utilização dos seus dados na sociedade de informação, no regime contraordenacional, na articulação entre a proteção dos dados pessoais e a liberdade de expressão, entre outros.

Podemos assim concluir que o novo RGPD se aplica não só às pessoas coletivas e singulares que tratam dados pessoais na União Europeia como também a todas aquelas que, mesmo estando fora do espaço europeu, recolhem e tratam dados de cidadãos europeus. Fica assim claro que o âmbito de aplicação do RGPD extravasa claramente o espaço da União Europeia.

O art. 3.º do Regulamento estabelece que este *se aplica ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União, aplicando-se ainda ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com: a oferta de bens ou serviços a esses titulares de dados na União e o controlo do seu comportamento, desde que este ocorra na União.* Por ultimo, o RGPD *aplica-se ainda ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido num lugar em que se aplique o direito de um Estado-Membro por força do Direito Internacional Público.*

Este Regulamento, não sendo, como vimos no ponto anterior, uma completa novidade no domínio do tratamento de dados, altera o paradigma do regime da proteção de dados estabelecendo um conjunto de novas regras aplicáveis à proteção dos dados pessoais, novos direitos dos titulares dos dados e a previsão de elevadas coimas em caso de incumprimento, entre outros.

Falamos, no entanto, de um texto com alguma complexidade, não tanto ao nível da semântica, pois nesse aspeto a preocupação de tornar a mensagem clara e acessível se destaca, mas pelo facto de ter mais de 170 considerandos e 99.º artigos e apesar de o articulado prevalecer sobre os considerandos estes são claramente um enorme auxilio à interpretação não se conseguindo compreender o diploma sem conhecer os considerandos.

Uma última nota para o facto de o discurso público e o alarmismo social olharem para este diploma como se se tratasse de um documento completamente inovador no domínio da proteção de dados, quando a verdade é que é um documento de continuidade no regime jurídico que já hoje protege os dados pessoais e no que respeita aos princípios fundamentais e uma parte substancial dos direitos e conceitos não serem distintos do que se encontra hoje plasmado na Lei.

3. A quem se aplica o RGPD?
Qual o papel do contabilista certificado no tratamento de dados?

Definido o âmbito de aplicação territorial, importa agora definir a quem se aplica o RGPD, ou seja, quem está obrigado a respeitar as regras de tratamento de dados e, nomeadamente, se se aplica à atividade do Contabilista Certificado.

Para esta questão é muito importante o que resulta do art. 4.º - com epígrafe definições, designadamente nos números 7), 8), 9) e 10), que definem como entidades com responsabilidades ao nível da proteção de dados os responsáveis pelo tratamento, subcontratantes, destinatários e terceiros.

Resulta assim deste artigo que assumem responsabilidade no tratamento de dados e, como tal, são abrangidos pelo presente regulamento:

- Responsável pelo tratamento – pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoas;
- Subcontratante – pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;
- Destinatário – pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro;
- Terceiro – pessoa singular ou coletiva, autoridade pública, serviço ou organismo que não seja titular dos dados, responsável pelo tratamento, subcontratante e as pessoas que, sob a autoridade direta do responsável

4. Tratamento de dados

Considera-se tratamento de dados, para efeitos da aplicação do RGDP, *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 [cfr. art. 4.º, número 2)].

Relativamente à definição de tratamento de dados não existem alterações muito significativas relativamente à definição constante da atual Lei da Proteção de Dados [cfr. art. 3.º, alínea b) da Lei 67/98, de 26 de outubro]: *qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição.*

5. O contabilista certificado e o RGPD

Depois de analisar o elenco das várias operações de tratamento de dados e de elencar todos aqueles que têm responsabilidades no tratamento de dados, facilmente se percebe o papel que o Contabilista Certificado assume nessas operações, quer enquanto Responsável pelo Tratamento de dados, quer enquanto Subcontratado de tantas outras entidades e que, nesse papel, tem acesso aos dados recolhidos pelos responsáveis pelo tratamento.

Em face do exposto é inquestionável a importância do RGPD para o trabalho dos Contabilistas Certificados, que procedem ao tratamento de dados pessoais *(informação relativa a uma pessoa singular identificada ou identificável, como, um nome, um número de identificação, dados de localização, identificadores por via eletrónica, elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social)* por si recolhidos – sempre que o Contabilista assuma o papel de responsável pelo tratamento de dados; ou que lhe são entregues pelo responsável pelo tratamento para posterior tratamento – situação em que assume o papel de subcontratante.

Por esse motivo enunciaremos aqui as obrigações que resultam para os responsáveis pelo tratamento e subcontratantes no que respeita ao tratamento de dados, bem como os princípios de tal tratamento.

Uma das maiores diferenças introduzidas pelo RGPD no regime de tratamento de dados reside no facto de se ter alterado o regime de supervisão, deixando a Autoridade de Controlo Nacional[1] de desenvolver uma atividade intensa de controlo prévio como regra para assumir uma função fiscalizadora e de produção de *guidelines*. Assistimos assim a uma mudança de paradigma que consiste na substituição do controlo prévio pela fiscalização a *posteriori* e consequente deslocação da responsabilidade para o interior das organizações que, de forma direta (Responsáveis pelo Tratamento) ou mediata (Subcontratantes), procedam ao tratamento de dados. O princípio da auto-responsabilização substitui-se assim ao princípio da necessidade de autorização e notificação para tratamento de dados da Comissão Nacional de Proteção de Dados, passando-se de um modelo de hetero-regulação para um modelo de autorregulação. Paralelamente a esta alteração do modelo de responsabilidade, o RGPD faz recair sobre os Responsáveis pelo Tratamento e Subcontratados o dever de comprovar que o tratamento foi feito em conformidade com o RGPD – *compliance*.

[1] Tudo indica – ideia reforçada pela Proposta de Lei de Proteção de Dados – que a autoridade de controlo nacional será a Comissão Nacional de Proteção de Dados, razão pela qual doravante nos referiremos à Autoridade de Controlo como CNPD.

Veja-se em particular o artigo 28.º do RGPD, uma inovação face à lei atual, que vem exigir aos Subcontratantes que efetuem tratamento de dados por conta do Responsável do Tratamento (v.g. processamento salarial), a apresentação de garantias suficientes de execução de medidas técnicas e organizativas adequadas, de uma forma que o tratamento satisfaça os requisitos do Regulamento, e assegure a defesa dos direitos dos titulares dos dados.

Em virtude desta transferência de responsabilidade é possível que os Responsáveis pelo Tratamento dos dados que recorram aos serviços de Subcontratantes venham requerer a apresentação destas garantias, para as quais os Contabilistas Certificados se devem preparar, demonstrando o cumprimento das obrigações previstas no RGPD.

Não estando em causa, neste Regulamento, a garantia da inexistência de qualquer ato de violação de dados, estamos sim perante uma norma Europeia que impõe um conjunto de obrigações a quem trata dados pessoais, que têm como escopo minimizar a possibilidade de concretização de violações de dados.

Ciente da impossibilidade prática de alcançar um estado de "zero violações de dados" o Regulamento prevê que sempre que se verifique uma violação de dados, esta seja imediatamente – o mais tardar 72h após o seu conhecimento ou sem demora injustificada - comunicada à Autoridade de Controlo - acompanhada da descrição da situação, titulares abrangidos e medidas reparadoras adotadas. Esta notificação não implicará, no entanto, qualquer coima ou outra sanção, se o Responsável pelo Tratamento ou Subcontratante conseguirem demonstrar que não lhes é imputável qualquer responsabilidade, porquanto cumpriram as normas de tratamento de dados previstas no Regulamento.

Desde modo, o que verdadeiramente está em causa neste Regulamento é uma mudança que se pretende realizar no *modus operandi* de tratamento dos dados, em respeito pelos direitos dos seus titulares, e sobretudo pelos princípios definidos neste diploma legal. Mais do que garantir que não existirá nenhuma violação de dados – missão impossível!! – deve o Responsável pelo Tratamento ou Subcontratante centrar os seus esforços no cumprimento das obrigações e regras de tratamento do Regulamento e nas evidências de tal *compliance* por forma a ser exonerado de qualquer responsabilidade que lhe possa ser imputável – proteção de dados desde a conceção e por defeito.

É, a este propósito, muito importante o **considerando 146** que refere que o Responsável pelo Tratamento ou o Subcontratado **pode ser exonerado da responsabilidade se provar que o facto que causou o dano não lhe é de modo algum imputável.**

Em face do exposto, parece-nos que o Regulamento cuja entrada em vigor se aproxima, coloca desafios e responsabilidades ao Contabilista no tratamento dos dados pessoais, os quais não devem ser encarados com apreensão – e o receio das elevadas e draconianas coimas que parece dominar o discurso vigente – mas antes, como uma oportunidade de proceder ao tratamento de dados, respeitando os direitos dos titulares dos dados em cumprimento das obrigações do Regulamento. Fazendo-o, estaremos certamente a adotar o comportamento que, devidamente documentado, nos poderá desonerar de responsabilidades.

6. Direitos dos titulares dos dados

O presente Regulamento tem como objetivo central garantir o funcionamento do mercado único para o qual os distintos regimes de proteção de dados pessoais se assumiam como um obstáculo.

A necessidade de um Regulamento, em substituição de uma Diretiva transposta de diferentes formas para a legislação nacional, que se impusesse de forma transversal e uniforme a todos os Estados, revelou-se essencial para que a transferência de dados dentro da União Europeia não encontrasse obstáculos na legislação interna dos vários Estados.

Por essa razão, o RGPD dedica a sua parte inicial à consagração dos direitos fundamentais dos titulares dos dados, cujo elenco passa a contar com novos direitos.

Assim, ao Direito de Informação (cfr. art. 10.º), Direito de acesso (cfr. art. 11.º), Direito de oposição do titular dos dados (cfr. art. 12.º) e Decisões individuais automatizadas (cfr. art, 13.º) consagrados na Lei 67/98, de 26 de outubro (Lei da Proteção de Dados em vias de ser revogada pela próxima Lei e pelo RGPD) são agora acrescentados os direitos de retificação, ao apagamento, à limitação do tratamento e à portabilidade.

O Capítulo III – Direitos do titular dos dados – consagra nos artigos 12.º e seguintes os seguintes direitos que analisaremos em seguida.

6.1. Direito à transparência das informações, comunicações e regras para exercício dos direitos

O primeiro direito consagrado neste Capítulo é um direito cuja sistemática é perfeitamente compreensível pela própria natureza do Regulamento. De facto, tendo como principais destinatários os titulares de dados pessoais, este direito mais não é do que a consagração da necessidade de utilização de uma linguagem e procedimentos transparentes.

Resulta assim do art. 12.º que o responsável pelo tratamento deverá adotar as medidas adequadas para fornecer ao titular todas as informações a que se referem os artigos 13.º e 14.º, bem como as comunicações previstas nos artigos 15.º a 22.º e ainda a comunicação da existência de uma violação de dados a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, particularmente quando as informações se dirijam especificamente a crianças.

Todas estas informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos. Estas informações podem ainda ser prestadas oralmente, se o titular dos dados o solicitar, desde que a identidade do titular possa ser comprovada por outros meios.

O responsável pelo tratamento deverá facilitar o exercício dos direitos do titular

dos dados tal como previstos nos artigos 15.º a 22.º.

Mesmo quando o responsável pelo tratamento conseguir demonstrar que o tratamento de dados não permite identificar o respetivo titular, o responsável pelo tratamento não pode recusar-se a dar seguimento ao pedido do titular no sentido de exercer os seus direitos, a menos que demonstre que não está em condições de identificar o titular dos dados.

O responsável pelo tratamento fornece ao titular as informações sobre as medidas tomadas, mediante pedido apresentado, sem demora injustificada e no prazo de um mês a contar da data de receção do referido pedido, sem prejuízo da possibilidade de prorrogar este prazo até dois meses, se tal se revelar necessário em virtude da complexidade do pedido e o número de pedidos.

Para tal, o responsável pelo tratamento deverá informar o titular dos dados desta prorrogação bem como dos motivos da demora no prazo de um mês a contar da data de receção do pedido.

Se o titular dos dados apresentar o pedido por meios eletrónicos, a informação deverá, sempre que possível, ser fornecida por meios eletrónicos, salvo pedido em contrário do titular.

Diferentemente, se o responsável pelo tratamento não der seguimento ao pedido apresentado pelo titular dos dados, deverá informá-lo sem demora e, o mais tardar, no prazo de um mês a contar da data de receção do pedido, das razões que o levaram a não tomar medidas e da possibilidade de apresentar reclamação a uma autoridade de controlo e intentar ação judicial.

Tanto as informações fornecidas ao titular dos dados aquando da recolha dos mesmos como as comunicações e medidas tomadas em virtude do exercício dos seus direitos são fornecidas a título gratuito.

O Regulamento prevê uma exceção a este principio da gratuitidade sempre que os pedidos apresentados por um titular de dados sejam manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, cabendo ao responsável pelo tratamento demonstrar o caráter manifestamente infundado ou excessivo do pedido.

Neste caso, o responsável pelo tratamento poderá exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações ou da comunicação, ou de tomada das medidas solicitadas ou, em alternativa, recusar-se a dar seguimento ao pedido.

Quando o responsável pelo tratamento tiver dúvidas razoáveis quanto à identidade da pessoa singular que apresenta o pedido poderá solicitar que lhe sejam fornecidas as informações adicionais que forem necessárias para confirmar a identidade do titular dos dados.

As informações a fornecer pelos titulares dos dados poderão ser dadas em combinação com ícones normalizados a fim de dar, de uma forma facilmente visível, inteligível e claramente legível, uma perspetiva geral significativa do tratamento previsto.

Se forem apresentados por via eletrónica, os ícones deverão ser de leitura automática.

6.2. Direito à informação

Um dos direitos mais importantes dos titulares dos dados é o direito à informação, direito que permite que o titular dos dados seja informado quanto a todos os dados relevantes sobre o tratamento de dados – quem é o responsável de tratamento, o *DPO* e seus contactos, a finalidades do tratamento e prazo de conservação e os seus direitos e a forma como pode exercê-los – devendo tais informações ser prestadas no momento da recolha dos dados junto do seu titular (cfr. art. 13.º) ou quando os dados não tenham sido recolhidos na presença do titular (cfr. art. 14.º).

E não obstante as informações a prestar aos titulares dos dados não sejam muito distintas numa e noutra situação, ainda assim justifica-se proceder aqui a essa análise.

O art. 13.º do RGPD estabelece que, quando os dados pessoais sejam recolhidos junto do titular, o responsável pelo tratamento faculta-lhe, aquando da recolha daqueles, as seguintes informações:

- A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
- Os contactos do encarregado da proteção de dados (doravante *DPO*), se existir;
- As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
- Os interesses legítimos do responsável pelo tratamento ou de um terceiro, sempre que o tratamento de dados se baseie nessa causa de legitimidade [cfr. art. 6.º, n.º 1, f) do RGPD];
- Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
- Eventualmente, 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 a referencia às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas;
- Prazo de conservação dos dados pessoais, ou se não for possível, os critérios usados para definir esse prazo;
- 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;
- A existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento propriamente dito sempre que o tratamento dos dados se baseie no consentimento do titular ou seja necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados, s interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros;
- O direito de apresentar reclamação a uma autoridade de controlo;
- 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;
- A existência de decisões automatizadas, incluindo a definição de perfis e as informações úteis relativas à lógica subjacente bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

Quando o responsável pelo tratamento tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim distinto daquele para o qual foram recolhidos, antes de proceder a esse tratamento deve fornecer ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes.

Esta obrigação de prestar informações não existe se o titular dos dados já tiver conhecimento delas.

Importará aqui fazer referencia à expressão do art. 13.º, n.º 1 *"o responsável pelo tratamento faculta-lhe, aquando da recolha dos dados pessoais, as seguintes informações..."*.Apesar de não se fazer ex-

pressamente referência ao modo como tais informações deverão ser facultadas, a verdade é que o ónus da prova do respeito pelo Regulamento é do responsável pelo tratamento, pelo que nos parece que deverá garantir-se a existência de uma prova de que tais informações foram prestadas ao titular dos dados.

Ciente de que nem sempre os dados são recolhidos na presença do seu titular, o art. 14.º faz o paralelo do exercício do direito à informação para os casos em que os dados pessoais não são recolhidos junto do seu titular. Nestes casos, o responsável pelo tratamento deve fornecer-lhes – e não facultar como sucedia no art. 13.º – as seguintes informações:

- A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
- Os contactos do encarregado da proteção de dados (doravante DPO), se existir;
- As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
- As categorias dos dados pessoais em questão – informação não prestada quando os dados são recolhidos na presença do titular;
- Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
- Eventualmente, 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 a referencia às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas;
- Prazo de conservação dos dados pessoais, ou se não for possível, os critérios usados para definir esse prazo;
- Os interesses legítimos do responsável pelo tratamento ou de um terceiro, sempre que o tratamento de dados se baseie nessa causa de legitimidade [cfr. art. 6.º, n.º 1, f) do RGDP];
- 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;
- A existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento propriamente dito sempre que o tratamento dos dados se baseie no consentimento do titular ou seja necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados, s interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros;
- O direito de apresentar reclamação a uma autoridade de controlo;
- A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público – informação não prestada quando os dados são recolhidos na presença do titular;
- A existência de decisões automatizadas, incluindo a definição de perfis e as informações úteis relativas à lógica subjacente bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

No caso da recolha dos dados não ser na presença dos respetivos titulares estas informações deverão ser prestadas num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados; se os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação ao titular dos dados; ou se estiver prevista a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação desses dados.

Caso o responsável pelo tratamento tenha intenção de proceder ao tratamento posterior dos dados pessoais para um fim distinto do fim para o qual os dados pessoais foram obtidos, deve fornecer ao titular dos dados informações sobre esse fim e outras informações antes de dar inicio a esse tratamento.

A prestação destas informações não é necessário quando e na medida em que:

- o titular dos dados já tenha conhecimento das informações;

- se comprove a impossibilidade de disponibilizar a informação ou então quando o esforço envolvido seja desproporcionado, nomeadamente para tratamento para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos (caso em que deve, ser adotadas as medidas adequadas para defender os direitos, liberdades e interesses legítimos do titular dos dados;

- a obtenção ou divulgação dos dados esteja expressamente prevista no direito da União ou do Estado-Membro; ou

- os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional regulamentada pelo direito da União ou de um Estado-Membro, inclusive uma obrigação legal de confidencialidade.

A diferença entre o modo de prestar a informação reside no facto de, quando os dados são recolhidos na presença do titular (cfr. art. 13.º) a informação ser facultada no próprio momento e, quando os dados não forem recolhidos na sua presença (cfr. art. 14.º) a informação ser facultada no próprio momento ou, o mais tardar, 30 dias após a recolha dos dados ou aquando da próxima comunicação ao titular dos dados.

6.3. Direito de acesso

O art. 15.º consagra o direito do titular dos dados de obter do responsável pelo tratamento a confirmação de que os seus dados pessoais são ou não objeto de tratamento e, se estiverem a ser tratados, o direito de acederem aos seus dados pessoais e às seguintes informações:

- as finalidades do tratamento dos dados;

- as categorias dos dados pessoais em questão;

- os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;

- caso seja possível, o prazo previsto de conservação do dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;

- a existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais ou ainda o direito de e opor a esse tratamento;

- o direito de apresentar reclamação a uma autoridade de controlo;

- se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;

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

Quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional, o titular dos dados te o direito de ser informado das garantias adequadas relativamente à transferência de dados.

O exercício deste direito por parte do titular de dados confere-lhe o direito a receber uma cópia dos dados pessoais em fase de tratamento, fornecida pelo responsável pelo tratamento, podendo ser exigido o pagamento de uma taxa razoável tendo em conta os custos administrativos.

Se o titular dos dados apresentar o seu pedido por meios eletrónicos deve a informação ser fornecida num formato eletrónico de uso corrente, exceto se o titular dos dados solicitar o contrário.

6.4. Direito de retificação

Consagrado no art. 16.º do RGPD este direito dá ao titular dos dados a garantia de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito.

Atendendo às finalidades do tratamento, o titular dos dados tem ainda direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.

6.5. Direito ao apagamento dos dados ("Direito a ser esquecido")

Possivelmente o direito mais carismático e distinto do RGPD é também o direito que mais obstáculos encontra à sua efetivação.

O direito ao apagamento dos dados, ou direito a ser esquecido ou também o direito à desconexão encontra-se previsto no art. 17.º do Regulamento como o direito do titular a obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, devendo o responsável pelo tratamento apagar os seus dados pessoais, também sem demora injustificada, quando se verifique um dos seguintes motivos:

- Os dados se revelem desnecessários para as finalidades para a finalidade que motivou a sua recolha ou tratamento;

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

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

- Quando os dados pessoais tenham sido tratados ilicitamente;

- Quando os dados pessoais tenham de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; ou, não menos importante,

- quando os dados pessoais tenham sido recolhidos no contexto da oferta de serviços da sociedade da informação.

A dificuldade de efetivar este direito não se resume ao facto de, por outros motivos ou interesses prevalecentes, os dados não poderem ser apagados, residindo também no facto de, sempre que o responsável pelo tratamento tenha tornado públicos os dados pessoais e seja obrigado a apaga-los, se encontre obrigado a tomar as medidas que forem razoáveis, incluindo de carácter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o seu titular solicitou o apagamento das ligações para esses dados bem como das cópias e reproduções dos mesmos. Estamos assim perante um direito ao apagamento "em cadeia" que se impõe a todos os sucessivos responsáveis pelo tratamento efetivo sempre que tal se revele razoável, tecnicamente possível e economicamente viável.

Como já havíamos referido, este direito terá muitos obstáculos e circunstâncias que determinam a sua não aplicação, é o que sucede sempre que o tratamento dos dados se revele necessário:

- ao exercício da liberdade de expressão e de informação;

- ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento;

- por motivos de interesse público no domínio da saúde pública;

- para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos e o direito ao esquecimento torne impossível ou prejudique gravemente a obtenção dos objetivos desse tratamento; ou

- para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

6.6. Direito à limitação do tratamento

Em paralelo ao direito do apagamento e precisamente para dar resposta aos casos de impossibilidade de proceder ao apagamento dos dados, o legislador previu no art. 18.º o Direito à limitação do tratamento que confere ao titular dos dados o direito de obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma das seguintes situações:

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

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

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

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

A limitação do tratamento dos dados implica que, com exceção da conservação dos dados, os dados pessoais apenas possam ser objeto de tratamento com o consentimento do titular, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos poderosos de interesse público da União ou de um Estado-Membro.

O titular dos dados a quem tenha sido deferida a limitação do tratamento tem direito a ser informado pelo responsável do tratamento antes de ser anulada a limitação ao referido tratamento.

6.7. Obrigação de notificação do cumprimento dos deveres do responsável pelo tratamento

O responsável pelo tratamento terá que comunicar a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento, a menos que essa comunicação se revele impossível ou implique um esforço desproporcionado. Se o titular dos dados o solicitar, o responsável pelo tratamento informa-o ainda dos referidos destinatários.

6.8. Direito de portabilidade dos dados

Em auxílio ao direito consagrado no art. 20.º do RGPD – Direito de Portabilidade dos Dados – foi publicada no passado dia 5 de janeiro a Resolução do Conselho de Ministros n.º 2/2018 que procedeu à revisão do Regulamento Nacional de Interoperabilidade Digital.

Este direito é a consagração da necessidade de dar ao titular dos dados o completo domínio sobre os seus dados pessoais, permitindo que estes possam ser-lhe entregues quando o solicite ou entregues a outra entidade por si nomeada.

Resulta assim deste artigo que o titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato que possa ser facilmente lido por outro responsável pelo tratamento, e o direito de transmitir esses dados a outro responsável pelo tratamento, quando:

- o tratamento se baseie no consentimento, seja necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados ou ainda no âmbito de um contrato ou procedimentos pré-contratuais;

- o tratamento for realizado por meios automatizados.

O titular dos dados, ao exercer o seu direito de portabilidade, tem direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.

Este direito não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento.

6.9. Direito de oposição

O art. 21.º consagra o direito do titular dos dados se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no exercício de funções de interesse público ou da autoridade pública de que está investido o responsável pelo tratamento ou quando seja necessário para efeitos dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros ou ainda quando o tratamento seja para fins distintos daqueles para que os dados foram recolhidos, incluindo a definição de perfis com base nessas decisões. Neste caso, o responsável pelo tratamento deverá cessar o tratamento de dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.

O direito do titular dos dados se opor ao tratamento dos seus dados pessoais devera ser explicitamente comunicado ao seu titular e apresentado de modo claro e distinto de quaisquer outras informações o mais tardar no momento d primeira comunicação ao titular dos dados.

No contexto da utilização dos serviços da sociedade da informação o titular dos dados pode exercer o seu direito de oposição por meios automatizados, utilizando especificações técnicas.

Quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos o titular dos dados tem o direito de se opor, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, a menos que o tratamento seja necessário para a prossecução de atribuições de interesse público.

6.10. Decisões individuais automatizadas, incluindo a definição de perfis

Por último, não menos importante do que os anteriores direitos, é consagrado no art. 22.º o Direito do titular dos dados de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

O titular dos dados não poderá exercer este direito quando a decisão seja necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento, seja autorizado pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados ou for baseada no consentimento explícito do titular dos dados.

Nos casos em que o titular dos dados não se possa opor a decisão com base nos perfis, o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter a intervenção humana por parte do responsável para manifestar o seu ponto de vista e contestar a decisão.

7. Limitações ao exercício dos direitos

À semelhança do que sucede com qualquer diploma que consagre e reconheça direitos aos particulares estes nunca são ilimitados tendo sempre como limite o direito de outros particulares ou, numa dimensão maior, direitos dos cidadãos em geral.

Nesse sentido, não será de estranhar o disposto no art. 23.º - Limitações – que consagra algumas exceções ao exercício dos direitos. Resulta, pois, deste artigo que o direito da União ou dos Estados-Membros a que estejam sujeitos o responsável pelo tratamento ou o seu subcontratante pode limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º, bem como no artigo 34.º - direito a conhecer a existência de uma violação de dados – e ainda no art. 5.º - princípios relativos ao tratamento de dados pessoais, na medida em que essas disposições correspondam aos direitos e obrigações previstos nos artigos 12.º a 22.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar, designadamente:

- a segurança do Estado;
- a defesa;
- a segurança pública;
- a prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública;
- outros objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo nos domínios monetário, orçamental ou fiscal, da saúde pública e da segurança social;

- a defesa da independência judiciaria e dos processos judiciais;

- a prevenção, investigação, deteção e repressão de violações de deontologia de profissões regulamentadas;

- uma missão de controlo, de inspeção ou de regulamentação associada, ainda que ocasionalmente, ao exercício da autoridade pública;

- a defesa do titular dos dados ou dos direitos e liberdades de outrem;

- a execução de ações cíveis.

Estas medidas legislativas devem, contudo, incluir quando for relevante, disposições explícitas relativas, pelo menos:

- às finalidades do tratamento ou às diferentes categorias de tratamento;

- às categorias de dados pessoais;

- ao alcance das limitações impostas;

- às garantias para evitar o abuso ou o acesso ou transferência ilícitos;

- à especificação do responsável pelo tratamento ou às categorias de responsáveis pelo tratamento;

- aos prazos de conservação e às garantias aplicáveis, tendo em conta a natureza, o âmbito e os objetivos do tratamento ou das categorias de tratamento;

- aos riscos específicos para os direitos e liberdades dos titulares dos dados; e

- ao direito dos titulares dos dados a serem informados da limitação, a menos que tal possa prejudicar o objetivo da limitação.

8. Dos intervenientes no tratamento dos dados

O tratamento de dados, nas suas distintas operações, poderá ser feito pelo Responsável pelo Tratamento ou pelo Subcontratante e não obstante cada um deles possa assumir diferentes papéis e responsabilidades, importa aqui esclarecer qual o papel e responsabilidades de cada um, tanto mais que já tivemos oportunidade de ver que o Contabilista Certificado pode assumir qualquer um destes papéis. Por outro lado, uma das grandes mudanças operadas pelo RGPD relativamente ao regime atual reside no facto de, com o novo regime, o subcontratante poder ser diretamente responsabilizado pelo incumprimento do Regulamento.

8.1. O Responsável pelo Tratamento de Dados

Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deverá aplicar as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento.

Tais medidas não são, contudo, estáticas, devendo ser revistas e atualizadas consoante as necessidades.

Entre estas medidas deve prever-se a aplicação de políticas adequadas em matéria de proteção de dados pelo responsável pelo tratamento.

Nomeadamente, considera-se que a existência de um Código de Conduta ou de procedimentos de certificação – quando estes estiverem implementados, poderá ser utilizado como elemento que atesta o cumprimento das obrigações do responsável pelo tratamento.

Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, como é o caso do princípio da minimização, e a incluir as garantias necessárias no tratamento, de forma a cumprir os requisitos deste regulamento e a proteger os direitos dos titulares dos dados.

Deve ainda, o responsável pelo tratamento, aplicar as medidas técnicas e organizativas para assegurar que, por defeito, apenas sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, prazo de conservação e acessibilidade.

Decorre do principio da minimização – na recolha, na quantidade, na extensão do tratamento, no prazo de conservação e na acessibilidade – que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

Um procedimento de certificação pode conseguir demonstrar o cumprimento destas obrigações.

Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios do tratamento, serão ambos os responsáveis pelo tratamento devendo, nessa qualidade, acordar entre si e determinar, de modo transparente as respetivas responsabilidades pelo cumprimento do regulamento, nomeadamente no que respeita ao exercício dos direitos dos titulares dos dados e aos respetivos deveres de informação. Esta obrigação não existe apenas e na medida em que as respetivas responsabilidades sejam determinadas pelo direito da União ou do Estado-Membro a que estejam sujeitos.

O acordo pode designar um ponto de contacto para os titulares dos dados e deve refletir devidamente as funções e relações respetivas dos responsáveis conjuntos pelo tratamento em relação aos titulares dos dados.

A essência do acordo é disponibilizada ao titular dos dados para que possa beneficiar de total transparência no exercício dos seus direitos.

8.2. O Representante

Quando o responsável pelo tratamento não se encontre estabelecido na União deverá nomear por escrito um representante seu na União, a menos que estejam em causa:

- operações de tratamento ocasionais, que não abranjam o tratamento em grande escala de categorias de dados sensíveis, ou o tratamento de dados pessoais relativos a condenações penais

e infrações que não representem riscos para os direitos e liberdades das pessoas singulares, tendo em conta a natureza, o contexto, o âmbito e as finalidades do tratamento; ou

- tratamento feito por autoridades ou organismos públicos.

O representante deve estar estabelecido num dos Estados-Membros onde se encontram os titulares dos dados cujos dados pessoais são objeto de tratamento no contexto da oferta que lhes é feita de bens ou serviços ou cujo comportamento é controlado.

O responsável pelo tratamento ou subcontratante deve nomear um representante para ser contactado em complemento ou em substituição do responsável pelo tratamento ou do subcontratante, em especial por autoridade de controlo e por titulares, relativamente a todas as questões relacionadas com o tratamento.

Não obstante a designação do representante as ações judiciais que possam vir a ser intentadas serão intentadas contra o responsável pelo tratamento ou subcontratante.

8.3. O Subcontratante

Quando o tratamento dos dados for efetuado por sua conta, o responsável pelo tratamento recorre apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados.

O domínio sobre os dados recolhidos continua a pertencer ao responsável pelo tratamento, razão pela qual o subcontratante não poderá contratar outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral. Com base nesta autorização geral por escrito, o subcontratante fica obrigado a comunicar ao responsável pelo tratamento todas as alterações que pretenda realizar no que respeita às entidades que possam vir a tratar dados.

O tratamento de dados em subcontratação é regulado por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento. Sendo este o título que habilita o subcontratante a tratar os dados e que, simultaneamente, o responsabiliza diretamente por esse tratamento, deve constar desse contrato que o subcontratante:

a) Trata os dados pessoais apenas mediante instruções documentadas

b) do responsável pelo tratamento, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, exceto se for obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso o responsável pelo tratamento desse requisito jurídico antes do tratamento;

c) Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;

d) Adota todas as medidas de segurança no tratamento de dados (cfr. art. 32.º);

e) Apenas contratará outro subcontratante com autorização do responsável pelo tratamento;

f) Toma em conta a natureza do tratamento, e na medida do possível, presta assistência ao responsável pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos;

g) Presta assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações de segurança no tratamento de dados, de notificação de eventuais violações de dados e outras, tendo em conta a natureza do tratamento e a informação de que disponha;

h) A pedido do responsável pelo tratamento procederá ao apagamento ou à devolução de todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros – na eventualidade de alguma instrução violar o presente regulamento ou outras disposições do direito da União ou dos Estados-Membros em matéria de proteção de dados, o subcontratante deve informar imediatamente o responsável pelo tratamento.;

i) Disponibiliza ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no presente artigo e facilita e contribui para as auditorias, inclusive as inspeções, conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado.

Se o subcontratante contratar outro subcontratante para a realização de operações específicas de tratamento de dados por conta do responsável pelo tratamento, o outro subcontratante terá as mesmas obrigações em matéria de proteção de dados que aquelas que se encontram no contrato ou ato normativo existente entre o subcontratante e o responsável pelo tratamento, nomeadamente a obrigação de apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento seja conforme com os requisitos deste regulamento.

Em caso de incumprimento das suas obrigações em matéria de proteção de dados, o subcontratante inicial continua a ser plenamente responsável perante o responsável pelo tratamento, pelo cumprimento das obrigações desse outro subcontratante.

O cumprimento de um código de conduta pelo subcontratante ou de um procedimento de certificação aprovado pode ser utilizado como elemento para demonstrar as garantias suficientes de cumprimento das obrigações do regulamento em matéria de proteção de dados.

Embora possa existir um contrato individual entre o responsável pelo tratamento e o subcontratante, o contrato ou ato normativo entre os dois pode basear-se, totalmente ou em parte, nas cláusulas contratuais-tipo constantes dos n.ºs 7 e 8 do art. 28.º, inclusivamente quando fazem parte de uma certificação concedida ao responsável pelo tratamento ou ao subcontratante, sem prejuízo de outras cláusulas contratuais-tipo que a Comissão ou a Autoridade de controlo possam vir a estabelecer.

Em todo o caso, estes contratos ou outro ato normativo devem ser feitos por escrito, incluindo em formato eletrónico.

Considera-se responsável pelo tratamento o subcontratante que, em violação do presente regulamento, determine as finalidades e os meios de tratamento.

O subcontratante ou qualquer outra pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais não procede ao tratamento de dados, exceto por instrução do responsável pelo tratamento, salvo se a tal for obrigado por força do direito da União ou dos Estados-Membros.

Da análise do papel do subcontratante conclui-se que o Contabilista Certificado, quando assuma este papel deverá prestar todas estas garantias de tratamento dos dados em conformidade com o RGPD, devendo tal constar de um contrato ou outro ato normativo.

Não podemos ainda deixar de aqui referir que o subcontratante é diretamente responsável pelo incumprimento do Regulamento, razão pela qual deve acautelar o cumprimento das obrigações do Regulamento e reunir os documentos probatórios de tal tratamento.

8.4. O Encarregado de Proteção de Dados

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

O encarregado de proteção de dados tem o seu regime previsto nos arts. 37.º, 38.º e 39.º do Regulamento e ainda na *Guideline* do Grupo de trabalho do Artigo 29.º adotada em 13 de dezembro de 2016, com a última redação revista e adotada em 5 de abril de 2017.

O DPO é o responsável formal do cumprimento do Regulamento que deve ser designado pelo responsável pelo tratamento ou subcontratante sempre que:

- o tratamento for efetuado por uma autoridade ou organismo público, excetuando os tribunais no exercício da sua função jurisdicional;

- as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou

- as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados e de dados pessoais relacionados com condenações penais e infrações.

Um grupo empresarial poderá também designar um único encarregado de proteção de dados desde que haja um encarregado de proteção de dados que seja facilmente acessível a partir de cada estabelecimento.

Idêntica solução podem adotar as autoridades ou organismos públicos porquanto, tendo em conta a respetiva estrutura organizacional e dimensão podem designar um único DPO.

Nos casos não previstos anteriormente, em que, como tal, não seja obrigatória a nomeação de um DPO, o responsável pelo tratamento ou o subcontratante ou as associações e outros organismos que representem categorias de responsáveis pelo tratamento ou de subcontratantes podem, ou, se tal lhes for exigido pelo direito da União ou dos Estados-Membros, designar um DPO que agirá em nome das associações e de outros organismos que representem os responsáveis pelo tratamento ou os subcontratantes.

Desmistificando uma ideia que se instalou na opinião de algumas pessoas – de que o DPO teria que ser obrigatoriamente certificado – o n.º 5 do art. 36.º refere que o DPO é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções que lhe estão atribuídas.

O DPO tanto pode ser um trabalhador da entidade responsável pelo tratamento ou subcontratante, como pode exercer as suas funções com base num contrato de prestação de serviços.

Os contactos do DPO devem ser publicados e comunicados à autoridade de controlo.

O DPO deve ser envolvido, de forma adequada e em tempo útil, a todas as questões relacionadas com a proteção de dados pessoais que sejam tratadas pelo responsável pelo tratamento e subcontratante devendo, estes últimos, apoiar o DPO no exercício das suas funções, fornecendo-lhe os recursos necessários ao seu desempenho e à manutenção dos seus conhecimentos, bem como devem dar-lhe acesso aos dados pessoais e às operações de tratamento.

O DPO é isento e imparcial no exercício das suas funções, não devendo receber instruções do responsável do tratamento ou subcontratante quanto ao modo como devera exercer as suas funções, bem como não pode ser destituído ou penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções. O DPO deverá informar diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante.

Os titulares dos dados podem contactar o DPO sobre todas as questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos seus direitos.

O DPO está sujeito ao dever de sigilo ou de confidencialidade no exercício das suas funções, bem como ao dever de incompatibilidade, não podendo exercer quaisquer funções e atribuições de que resulte um conflito de interesses com o exercício das funções de DPO.

No que respeita às suas funções, o DPO tem, pelo menos, as seguintes atribuições:

- informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como todos os trabalhadores que tratem os dados, a respeito das suas obrigações no que respeita ao tratamento de dados pessoais;

- controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as politicas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal, bem como a necessidade de proceder a auditorias;

- coopera com a autoridade de controlo;

- ponto de contacto para a autoridade de controlo sobre aquestões relacionadas com o tratamento, incluindo a consulta previa, e consulta a autoridade de controlo sobre qualquer outro assunto.

No desempenho das suas funções, o DPO tem em conta os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto, as finalidades de tratamento.

9. Dos princípios de tratamento de dados

Por forma a nortear o tratamento de dados e estabelecer orientações quanto aos cuidados e regras a seguir no seu tratamento, o art. 5.º do RGPD estabelece um conjunto de princípios a seguir. São eles:

- o **princípio da licitude, lealdade e transparência**: apenas podem ser objeto de tratamento os dados relativamente aos quais se verifique um dos fundamentos de tratamento constantes do artigo 6.º; o tratamento deve encontrar-.se devidamente enquadrado no que foi transmitido ao titular no momento da recolha e o titular dos dados poderá verificar como é feito o tratamento dos seus dados;

- o **princípio da limitação das finalidades e da conservação:** os dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados para finalidades distintas a menos que exista um claro interesse superior que o preveja (v.g. fins de arquivo de interesse público); por outro lado, os dados deverão ser conservados durante o tempo estritamente necessário;

- o **princípio da minimização dos dados:** os dados pessoais recolhidos devem ser adequados, pertinentes e limitados ao que é necessário;

- o **princípio da exatidão:** os dados devem ser exatos e atualizados sempre que necessário;

- o **princípio da integridade e confidencialidade:** os dados deverão ser tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental.

Estes princípios deverão ser cumpridos pelo responsável pelo tratamento de dados que deverá ser capaz de demonstrar – por evidencias – tal respeito.

10. Questões que exigem a nossa maior atenção

De tudo o que anteriormente foi referido, e sem ter aqui a pretensão de elencar todos os pontos para a implementação do RGPD nas organizações, algumas questões assumem especial importância e não poderão ser ignoradas.

Falamos, sem qualquer pretensão de avançar com um elenco detalhado e minucioso, das seguintes preocupações:

a) Obtenção do consentimento

De acordo com o princípio da licitude do tratamento dos dados uma das situações de legitimidade para o tratamento de dados reside na necessidade de consentimento do titular de dados, para uma ou mais finalidades especificas. Este consentimento, não sendo a única situação de legitimidade de tratamento – porquanto o art. 6.º ainda prevê o tratamento necessário para a execução de um contrato ou procedimentos pré-contratuais, para cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito ou quando seja necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular, quando seja necessário ao exercício de funções de interesse púbico ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento ou ainda quando o tratamento seja necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros – será com certeza o caso que se verifica

na recolha e tratamento de dados no âmbito de cartões de clientes, compras e disponibilização de fotografias e comentários nas redes sociais e em páginas na internet. Importa, por isso, verificar se o tratamento de dados se encontra numa das situações previstas no art. 6.º, n.º 1, alíneas b), c), d), e) e f) ou se, pelo contrário, teremos que ter o consentimento do seu titular para fazer esse tratamento.

Caso seja essencial o consentimento do titular, este terá que ser dado nos termos do art. 7.º, ou seja, que ser livre, específico, informado, explícito e prestado através de ato inequívoco.

Sendo expectável que vários consentimentos já existentes não cumpram com todos os requisitos do RGPD, deve procurar-se obter o consentimento correto antes da entrada em vigor do Regulamento, sob pena de não existir legitimidade para proceder a este tratamento.

b) Provar (por evidência) que cumprem o RGPD

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

- Que os dados pessoais que possuem são legítimos e estão limitados ao que é necessário;
- Que os dados estão atualizados, seguros e confidenciais;
- Que têm políticas, procedimentos, códigos de conduta e instruções internas, formalizadas e capazes de serem disponibilizadas às entidades de supervisão;
- Que possuem sistemas para monitorizar se as políticas e procedimentos estão a ser seguidas.

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

c) Notificação da Violação de Dados

Uma das grandes diferenças relativamente ao regime atual da proteção de dados consiste na obrigatoriedade de comunicação à Autoridade de Controle e ao titular dos dados de qualquer violação de dados que represente perigo para os seus direitos, liberdades e garantias.

Deste modo, os artigos 33.º e 34.º são a assunção de que o Regulamento não visa impedir a existência de qualquer violação de dados, ele prevê a sua existência e obriga à sua comunicação, na certeza de que, se o responsável pelo tratamento ou o subcontratante conseguirem provar o cumprimento do Regulamento poderão ser exonerados da responsabilidade pela violação de dados (considerando 146).

Deste modo, resulta do art. 33.º que as organizações estão obrigadas a notificar a CNPD no prazo de 72 horas de todas as violações de dados com risco para o titular, acompanhada das medidas adotadas ou propostas para a sua reparação inclusive, se for o caso, medidas para atenuar os seus efeitos negativos. Para tal, é fundamental que o responsável pelo tratamento seja capaz de detetar qualquer violação de dados assim que a mesma ocorra.

Caso a referida violação represente perigo para os direitos, liberdades e garantias dos titulares de dados, deverá ainda ser comunicada a estes no mais curto prazo de tempo, nos termos do art. 34.º.

d) Reforço da segurança de Dados

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

Este sistema de segurança deve ter não só como alvo o tratamento de dados em suporte informatizado como também o seu tratamento em suporte físico.

11. *Check list* de apoio à implementação do RGPD

Cientes do apoio que os Contabilistas, à semelhança do que sucede em tantas outras áreas, podem ser chamados a prestar na implementação do Regulamento, recomendamos que verifiquem sobretudo se os dados pessoais recolhidos são:

- Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados;
- Recolhidos para finalidades determinadas, explícitas e legítimas;
- Exatos e atualizados sempre que necessário;
- Adequados, pertinentes e limitados ao que é necessário;
- Conservados de forma a que permitam a identificação dos titulares dos dados apenas durante o período necessário;
- Tratados de forma a que garantam a segurança, incluindo a proteção contra o tratamento não autorizado ou ilícito e contra a perda, destruição ou danificação acidental;
- Tratados apenas se o titular tiver dado o seu consentimento para uma ou mais finalidades específicas.

As organizações deverão aplicar **medidas técnicas e organizativas que assegurem e comprovem que o tratamento é realizado em conformidade com o RGPD e permitem:**

- A pseudonimização (quando os campos de identificação contidos num registo de dados são substituídos por um ou mais identificadores artificiais) e a cifragem (quando os dados são codificados de forma a que apenas possam ser lidos por pessoas autorizadas);
- Assegurar a confidencialidade, integridade, disponibilidade e resiliência permanente dos sistemas e dos serviços de tratamento;
- Restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
- Testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas;

Ao avaliar o nível de segurança, a organização deverá ter em conta os riscos apresentados pelo tratamento, destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

O cumprimento de códigos de conduta ou de procedimentos de certificação poderá ser utilizado como elemento para demonstrar o cumprimento do RGPD.

Uma última questão importante é proceder a auditorias e verificações periódicas ao sistema implementado por forma a dar resposta a novas questões, rever procedimentos e criar mecanismos que impeçam a ocorrência de violações de dados.

12. Consequências da violação do Regulamento

É incorreto e impreciso o que tanto se tem ouvido na opinião pública de que a violação do Regulamento implicará uma coima de 20.000.000,00€ (vinte milhões de euros), por um lado porque a definição do valor em concreto das coimas é da competência dos Estados-Membros, tendo como limite máximo o montante dos vinte milhões de euros – e o que consta da Proposta de Lei aprovada em sede de Conselho de Ministros são valores inferiores a este – por outro lado porque existem outras sanções que podem ser aplicadas em alternativa ou conjuntamente com as coimas.

O Regulamento dedica o seu Capítulo VIII às vias de recurso, responsabilidade e sanções e começa, desde logo, por referir que, sem prejuízo de qualquer outra via de recurso administrativo ou judicial, todos os titulares de dados têm direito a apresentar reclamação a uma autoridade de controlo, no Estado-Membro em que residem habitualmente ou do seu local de trabalho ou ainda do local onde foi alegadamente praticada a infração.

A pessoa coletiva ou singular que não concorde com a decisão da autoridade de controlo poderá intentar uma ação judicial contra as decisões juridicamente vinculativas das autoridades de controlo que lhes digam respeito.

Se os titulares de dados considerarem que houve uma violação dos direitos que o Regulamento lhe confere, na sequencia do tratamento dos seus dados pessoais efetuado em violação deste Regulamento, podem intentar uma ação judicial.

Independentemente das ações que corram junto das autoridades de controlo, pode qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos. Muito mais preocupante do que as coimas, é esta possibilidade constante do art. 82.º de qualquer pessoa poder exigir uma indemnização pelos danos materiais ou imateriais pelos danos sofridos.

As sanções a aplicar pela Autoridade de Controlo poderão ser:

- coimas –

- correção de comportamento – advertência para que sejam respeitadas as indicações da Autoridade de Controlo;

- repreensão.

As coimas devem ser efetivas, proporcionadas e dissuasivas, sendo que na sua definição devem ser tidos em conta os seguintes aspetos: natureza, gravidade e duração da infração, o seu caráter doloso, as medidas tomadas para atenuar os danos sofridos, o grau de responsabilidade ou eventuais infrações anteriores, a via pela qual a infração chegou ao conhecimento da autoridade de controlo, o cumprimento das medidas ordenadas contra o responsável pelo tratamento ou subcontratante, o cumprimento de um código de conduta ou quaisquer outros fatores agravantes ou atenuantes.

Conclusão

Concluída esta nossa análise do Regulamento Geral de Proteção de Dados (RGPD) procurando não aderir à onda de alarmismo social com que esta matéria tem sido tratada, cremos que ficou bem patente o papel do Contabilista Certificado neste regime de proteção de dados.

E embora não se trate de um regime completamente novo de proteção de dados, sendo antes uma continuidade do regime atualmente em vigor, alguns dos novos direitos dos titulares, das novas obrigações de tratamento, as sanções elevadas e a previsão da figura do Encarregado de Proteção de Dados fazem com que este Regulamento mereça a nossa especial atenção.

É incontornável o papel do Contabilista Certificado no tratamento de dados, quer o faça enquanto Responsável pelo Tratamento quer o faça enquanto Subcontratante e uma vez que qualquer um destes é diretamente responsável pelo incumprimento do regulamento é importantíssimo conhecer as regras e princípios a que deve obedecer o tratamento de dados.

Por outro lado, é essencial conhecer os direitos dos titulares dos dados pessoais – conhecimento benéfico inclusivamente do ponto de vista de titular de dados – e criar mecanismos que facilitem o exercício destes direitos.

Por último, uma palavra para esclarecer que o que este Regulamento verdadeiramente estabelece é um conjunto de regras que se impõem aos responsáveis pelo tratamento e subcontratante para o tratamento de dados pessoais. Respeitando estas obrigações e princípios reduziremos a possibilidade de existência de uma violação de dados, embora não seja possível afirmar que tal se encontra absolutamente vedado pelo Regulamento, sendo disso prova o facto de o próprio Regulamento estabelecer o procedimento de atuação em caso de violação de dados pessoais – comunicação à Autoridade de Controle e aos titulares de dados.

Mais do que uma visão de pânico que parece acompanhar qualquer leitura e referencia a este diploma, consideramos que esta mudança de paradigma deverá ser encarada por todas as organizações como uma oportunidade de rever procedimentos internos, normas de segurança e comportamentos que possam comprometer os dados pessoais que tratamos diariamente.

Bibliografia

FAZENDEIRO, Ana, Regulamento Geral Sobre a Proteção de Dados – Algumas notas sobre o RGPD, Reimpressão da 2.ª Edição, Almedina, 2018;

MAGALHÃES, Filipa Matias, Regulamento Geral de Proteção de Dados – Manual Prático, 2.ª Edição Revista e Ampliada, Vida Económica, fevereiro de 2018;

Siglas

CNPD – Comissão Nacional de Proteção de Dados

RGPD – Regulamento Geral de Proteção de Dados

DPO – Data Protection Officer