CÓDIGO DEONTOLÓGICO DOS PROFISSIONAIS DE PROTEÇÃO DE DADOS

3.ª EDIÇÃO, OUTUBRO 2023

INTRODUÇÃO

Os Profissionais de Proteção de Dados têm que cumprir certas regras éticas e deontológicas, como as que decorrem dos deveres gerais de conduta. A honestidade, moralidade, competência e retidão são alguns desses deveres. Mas, para além disso, o profissional de proteção de dados deve cumprir as regras que decorrem especificamente da sua atividade, que são os deveres fundamentais da profissão.

Sendo a ética um dos princípios morais por que um indivíduo rege a sua conduta profissional, este Código Deontológico pretende realçar as regras de conduta de maior relevo a que devem obedecer os profissionais de proteção de dados, apesar da opção, perante uma determinada situação, por um comportamento e não por outro, exigir o compromisso de todas as dimensões do ser humano.

Assim, o Código Deontológico da APDPO pretende reunir um conjunto de normas de comportamento para orientação nos diferentes aspetos profissionais e, particularmente, das relações humanas que se estabelecem no decurso do exercício profissional. As condutas que o Código estabelece são condicionadas pela informação científica e tecnológica disponível. Um Código Deontológico expressa uma determinada realidade temporal, porquanto os valores da Ética Profissional que lhe dão suporte estão em permanente evolução, atualização e adaptação.

Esperamos com este trabalho colaborar na dignificação e garantia de qualidade do Profissional de Proteção de Dados.

Lisboa, 25 de outubro de 2023,

A Direção

ÍNDICE

PREÂMBULO

Todas as entidades e agentes cujas atividades envolvam o tratamento de dados pessoais estão sujeitas ao cumprimento de múltiplas obrigações, decorrentes, não só do Regulamento Geral sobre a Proteção de Dados e respetiva jurisprudência europeia, mas igualmente de legislação nacional sobre segurança e proteção de dados, assim como de decisões e orientações da Comissão Nacional de Proteção de Dados.

Os profissionais de proteção de dados têm um papel muito importante no aconselhamento, consultoria e formação destas entidades, sempre com vista a garantir o respeito pelas liberdades e direitos fundamentais dos titulares dos dados pessoais. Contribuem, igualmente, para a criação de valor nas organizações, públicas e privadas, auxiliando no alcance dos seus objetivos estratégicos, protegendo os seus ativos imateriais e certificando-se da conformidade das ações e processos com a regulamentação em vigor sobre a proteção de dados pessoais.

Portanto, é necessário e pertinente que a profissão se dote de um Código Deontológico, para manter a confiança das entidades respetivas face a estes profissionais e garantir a confidencialidade, a qualidade e o caráter integro das suas funções.

É com este espírito que a APDPO Portugal – Associação dos Profissionais de Proteção e Segurança de Dados concebeu o presente Código Deontológico (a partir de agora designado por Código), com vista a promover uma cultura de qualidade e ética entre os profissionais de proteção de dados, sejam encarregados de proteção de dados, consultores ou formadores no âmbito do Regulamento Geral sobre a Proteção de Dados.

O presente documento formula as regras de conduta que devem reger a ação dos profissionais de proteção de dados, procurando contribuir para a boa aplicação do Regulamento Geral sobre a Proteção de Dados e demais legislação sobre a matéria.

O Código é assim igualmente benéfico para as entidades, pois garante a escolha, para o seio das organizações, de profissionais de proteção de dados que no exercício da sua atividade se orientam por elevados padrões de ética e rigor. Por essa razão, é promovida a divulgação e conhecimento do presente Código pelos responsáveis pelo tratamento e subcontratantes.

1. Disposições gerais

1.1 Definições

Para o tornar mais legível, o documento utiliza termos e abreviaturas baseados nas seguintes definições:

- **RGPD**: Regulamento Geral sobre a Proteção de Dados, aprovado pelo Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que revoga a Diretiva 95/46/CE, de 24 de outubro de 1995.
- **Responsável pelo tratamento**: a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro (Artigo 4.º (7) do RGPD).
- **Subcontratante**: a pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes (Artigo 4.º (8) do RGPD).
- **Gestão (do responsável pelo tratamento ou do subcontratante):** gerência, conselho de administração, direção dos organismos públicos ou respetivos indivíduos.
- **Profissional de proteção de dados**: qualquer pessoa individual que exerça funções de encarregado de proteção de dados, formador, auditor ou consultor na área da segurança e proteção de dados.
- **DPO/EPD**: Data Protection Officer/Encarregado de Proteção de Dados.

1.2 Aprovação do Código

O presente Código é aprovado pela Direção da APDPO PORTUGAL, após consulta dos respetivos associados e submetido para conhecimento da Comissão Nacional de Proteção de Dados (CNPD). O Código deverá ser tornado público por diversos meios, nomeadamente, através da sua publicação no website da APDPO PORTUGAL.

1.3 Adesão ao Código – Campo de Aplicação

A adesão ao Código é voluntária, plena, integral e gratuita, dependendo da qualidade de membro da APDPO. Pode aderir ao Código qualquer profissional de proteção de dados associado da APDPO que comprove o exercício de funções de DPO/EPD, formador, auditor ou consultor na área da segurança e proteção de dados.

A adesão ao Código e subsequentes revalidações são feitas através da área restrita do site da APDPO. A adesão ao Código e as revalidações são válidas pelo período de três anos.

A revogação da adesão ao presente Código é livre e não está sujeita a qualquer formalidade especial, devendo ser comunicada junto da APDPO.

1.4 Direitos inerentes à adesão

A adesão ao presente Código permite ao profissional de proteção de dados a utilização de um logótipo específico. O referido logótipo é propriedade intelectual da APDPO e não deve ser utilizado de forma ostensiva. Em caso algum este logotipo pode ser interpretado como uma garantia de qualidade ou uma avaliação pela APDPO sobre o profissional que o utilize. Sempre que o logótipo seja utilizado num sítio da Web, deve ser estabelecida uma ligação para a página da APDPO, onde se encontra o texto do Código Deontológico para que todos possam tomar conhecimento dos compromissos assumidos (APDPO PORTUGAL – Associação dos Profissionais de Proteção e Segurança de Dados www.dpo-portugal.pt). O profissional de proteção de dados aderente poderá fazer referência à adesão ao presente Código em qualquer meio de apresentação profissional, nomeadamente curriculum vitae, websites, redes sociais, apresentações, propostas, candidaturas, cartões de visita.

A violação de quaisquer regras do presente Código pode conduzir à perda de todos os direitos inerentes à adesão. Compete à Comissão de Ética da APDPO analisar as situações de incumprimento que sejam reportadas ou identificadas pela APDPO, bem como propor à Direção da APDPO que determine a perda dos direitos inerentes à adesão do profissional de proteção de dados incumpridor, quando assim o entender.

1.5 Difusão – Publicação

O Código pode, nomeadamente, ser:

- Comunicado às pessoas interessadas;
- Colocado à disposição em qualquer organização (junto dos trabalhadores, etc.);
- Anexado ao contrato de trabalho ou de prestação de serviços de um profissional de proteção de dados;
- Mencionado como documento de referência no quadro de formações iniciais ou contínuas no âmbito da proteção de dados pessoais;
- Referenciado nos contratos com clientes;
- Mencionado pelos recrutadores nas ofertas de emprego de profissionais de proteção de dados;
- Apresentado por um subcontratante a um responsável pelo tratamento para justificar, com outras medidas técnicas e organizativas adequadas, que ele apresenta as garantias suficientes de acordo com o artigo 28.º do RGPD.

1.6 Atualização do Código

Este Código será revisto e atualizado pela Direção da APDPO sempre que se justifique. Esses melhoramentos serão periodicamente realizados para o adaptar à legislação em vigor e às melhores práticas profissionais. As atualizações do Código são tornadas públicas por todos os meios considerados adequados pela APDPO. Os profissionais de proteção de dados aderentes serão informados de quaisquer atualizações ou modificações.

2. Qualidades pessoais e profissionais

2.1 Deveres do Profissional de Proteção de Dados

O Profissional de Proteção de Dados deve:

- Desempenhar a sua função com honestidade, precisão, equidade e independência;
- Prestar apenas os serviços profissionais para os quais tem plena capacidade de execução;
- Prestar informação adequada ao responsável pelo tratamento (incluindo quaisquer preocupações ou riscos potenciais que verificar);
- Processar como confidenciais todas as informações das operações de tratamento de dados do responsável pelo tratamento, bem como outras a que tenha acesso, durante o exercício das suas funções;
- Assumir como prioridade, em todas as suas ações e considerações, sigilo e confidencialidade sobre os dados pessoais tratados.

2.2 Qualidades Pessoais

Pressupõe-se, seja qual for a formação base, que o Profissional de Proteção de Dados procure obter formação contínua que lhe permita manter-se informado e atualizado, de forma a consolidar conhecimentos e evoluir como profissional.

2.2.1. Probidade

O Profissional de Proteção de Dados deve desempenhar a sua atividade com diligência, lealdade, de forma responsável e honesta, de acordo com o seu conhecimento e perícia, ao serviço do responsável pelo tratamento de dados ou do subcontratante para quem ele trabalhe. Como resultado, o Profissional de Proteção de Dados não pode usar meios ilícitos ou antiéticos durante a execução da sua função.

O Profissional de Proteção de Dados externo deve ser particularmente cuidadoso com a utilização de nomes, marcas, materiais ou recursos de organizações para as quais trabalhe ou referências do negócio, e certificar-se que obtém uma autorização prévia para o efeito.

2.2.2 Imparcialidade

O Profissional de Proteção de Dados deve desempenhar a sua atividade com objetividade, independência, neutralidade, equidade, sem julgamentos prévios, ausência de conflitos de interesses, ausência de preconceitos e resistência à influência abusiva.

2.2.3 Objetividade

O Profissional de Proteção de Dados deve:

- Demonstrar um alto nível de objetividade na sua análise, avaliação

e comunicações com o responsável pelo tratamento de dados ou subcontratante sobre a conformidade da organização;

- Desempenhar as suas funções com imparcialidade, ou seja, de forma justa e sem prejuízo de ou contra uma parte;
- Fazer uma avaliação justa da informação e documentação que receber e fazer o seu julgamento não influenciado por interesses próprios ou de terceiros.

2.2.4 Independência

O responsável pelo tratamento de dados ou o subcontratante deve definir e divulgar meios para garantir a independência do Profissional de Proteção de Dados. Deve abster-se de interferir e deve colocar o Profissional de Proteção de Dados numa situação em que certifique a sua independência, incluindo no que diz respeito aos meios que ele ou ela tem acesso. Consequentemente, o Profissional de Proteção de Dados deve interagir diretamente e com toda a independência com a administração/direção da organização do responsável pelo tratamento de dados ou do subcontratante ou seu representante, de acordo com o artigo 38º do RGPD. O Profissional de Proteção de Dados deve ter o controle total das decisões assumidas e da forma como se organiza para o desempenho da sua atividade. O Profissional de Proteção de Dados deve agir de forma independente, não receber instruções hierárquicas sobre a sua atividade e tomar decisões por conta própria. Esta liberdade não significa que deva agir sozinho ou sem consulta. É livre para consultar a autoridade de supervisão ou pessoas com o conhecimento para ajudá-lo dentro dos limites da sua atividade.

No caso de Profissional de Proteção de Dados a tempo parcial, o mesmo deverá acautelar que o responsável pelo tratamento de dados ou o subcontratante deve:

- limitar ou reduzir outras tarefas para as quais o Profissional de Proteção de Dados tenha responsabilidade no desempenho de outras funções na organização;
- assegurar que o Profissional de Proteção de Dados não seja prejudicado pela realização das suas outras missões durante a avaliação anual do seu trabalho (avaliações de desempenho - RH);
- garantir que o Profissional de Proteção de Dados possa exercer uma carreira normal na organização apesar do cumprimento da sua função de Profissional de Proteção de Dados;
- a organização não poderá imputar quaisquer responsabilidades ao Profissional de Proteção de Dados pelo não cumprimento das medidas de conformidade previstas pelo RGPD, se não proporcionar os meios necessários para o bom desempenho da função de Profissional de Proteção de Dados;
- será da responsabilidade da organização, a contratação de um seguro de responsabilidade civil que cubra os riscos inerentes à atividade de Profissional de Proteção de Dados;

- caso não se verifique o disposto no ponto anterior, o Profissional de Proteção de Dados tem legitimidade para recusar a sua nomeação para a função, devendo a organização criar as condições necessária para que possa retomar a sua atividade profissional, sem prejuízo de quaisquer direitos ou regalias adquiridas anteriormente.

Do mesmo modo, caso se trate de um Profissional de Proteção de Dados externo, o mesmo deverá assegurar-se de que o responsável pelo tratamento de dados ou o subcontratante abstém-se de interferir, especialmente se a renovação do contrato do Profissional de Proteção de Dados está próxima.

2.2.5 Ausência e prevenção de Conflito de Interesses/Incompatibilidades

Além de evitar conflitos de interesses, o Profissional de Proteção de Dados deve evitar conflitos de responsabilidade nas suas funções. Se o Profissional de Proteção de Dados não realizar a sua atividade a tempo inteiro, as suas outras tarefas e responsabilidades não devem levá-lo a tomar decisões sobre as operações de tratamento de dados da sua organização. A sua conduta ética e atuação, ainda que em outros contextos profissionais, pessoais e sociais deverá preconizar um exemplo de respeito pelos Direitos Fundamentais do Homem, princípios básicos da Proteção de Dados Pessoais.

Em concreto, o Profissional de Proteção de Dados:

- Não pode trabalhar para mais de um cliente ou representante caso exista um conflito (ou risco grave de conflito) de interesses entre os clientes ou os representantes;
- Não pode exercer a sua função se surgir um conflito de interesses, se o sigilo profissional estiver em risco ou se a sua independência não puder ser plenamente garantida;
- Não pode aceitar uma função proposta por um novo cliente quando as informações fornecidas por um anterior cliente ou representante são colocados em risco ou o conhecimento desta informação favorece o novo cliente;
- Deve informar o responsável pelo tratamento de dados ou o subcontratante de todos os interesses que possam influenciar o seu julgamento ou comprometer o que tenha de demonstrar.

O Profissional de Proteção de Dados externo, com a devida transparência, avalia com o responsável pelo tratamento de dados ou o subcontratante a possibilidade de ser contratado por outra organização que possa ser vista como concorrente.

2.2.6 Abuso de autoridade e preconceitos

O Profissional de Proteção de Dados deve ter consciência de outras partes que possam tentar influenciar as suas análises e opiniões. O princípio da objetividade implica que o Profissional de Proteção de Dados não deve comprometer o seu julgamento por preconceitos, conflitos de interesse ou outras Influências.

2.2.7 Competência Social

O Profissional de Proteção de Dados assegurará a obtenção, desenvolvimento e manutenção de habilidades relacionadas à comunicação, negociação e gestão de conflitos.

2.3 Qualidades Profissionais

2.3.1 Segredo Profissional

O Profissional de Proteção de Dados está vinculado ao sigilo profissional. Com exceção dos casos previstos na lei, o Profissional de Proteção de Dados trata informações, processos e reclamações durante a sua atividade como informação estritamente confidencial. Não deve utilizar documentos internos ou informações adquiridas durante a sua função para um responsável pelo tratamento de dados ou o subcontratante anterior sem o seu consentimento expresso. Da mesma forma, não pode usar a informação para outras finalidades do que aquelas definidas pelo responsável pelo tratamento de dados ou o subcontratante. Essa confidencialidade também se aplica no ambiente social e continua após o término da sua missão.

2.3.2 Dedicação

O Profissional de Proteção de Dados:

- Deve atuar com ponderação e assumir decisões informadas em todas as situações, demonstrando as suas competências e profissionalismo no exercício das suas funções;
- Fazer as suas avaliações com base nos seus conhecimentos especializados e experiência.

2.3.3 Competências

O Profissional de Proteção de Dados deve dispor de conhecimentos, aptidões e experiências adequados para desempenhar a sua função e atividade profissional. Ao candidatar-se a uma oportunidade de emprego ou uma função como Profissional de Proteção de Dados, não deve assumir competências que não domine. O RGPD define o Profissional de Proteção de Dados como uma pessoa com as qualificações necessárias para a realização da função. As competências devem ter em conta a área de TI e as novas tecnologias, bem como a legislação sobre a proteção de dados pessoais.

Quando o Profissional de Proteção de Dados não cumpre todos os requisitos no momento da nomeação, deve procurar adquiri-los antes de assumir a sua função na organização. O Profissional de Proteção de Dados deve manter as suas competências e conhecimentos na área relevantes para as suas funções, melhorar e expandir o seu conhecimento jurídico, tecnológico e social, inclusive com formação contínua, se necessário. Conforme exigido pelo artigo 38º n.º 2 do RGPD, o responsável pelo tratamento de dados ou o subcontratante deve apoiá-lo neste esforço.

3. Requisitos na prática profissional

3.1 Relação com os titulares dos dados

O Profissional de proteção de dados é o defensor dos interesses legítimos dos titulares dos dados, devendo por isso:

- Fornecer a informação necessária para que o titular dos dados possa exercer os seus direitos;

- Ser diligente e tratar com respeito e cordialidade as reclamações e solicitações dos titulares de dados;

- Responder aos titulares de dados de forma neutra e objetiva, de forma lógica, clara e simples, não comprometendo os seus julgamentos com base em preconceitos ou outras influências indevidas, evitando argumentações com pontos de vista pessoais;

- Ser transparente, objetivo e pragmático nos esclarecimentos prestados;

- Ser imparcial, neutro e resistente a influências;

- Manter sigilosas as comunicações com os titulares.

3.2 Relação com os colaboradores da organização

Na sua relação com os funcionários, gerentes e demais colaboradores da organização, o Profissional de proteção de dados deve:

- Tratar os funcionários ou gerentes de maneira justa e respeitosa;

- Assumir a responsabilidade pelas suas ações, promovendo o desenvolvimento profissional por meio de motivação, formação e comunicação;

- Relacionar-se com os colaboradores com respeito mútuo e qualidade na gestão;

- Rejeitar qualquer manifestação de abuso físico, psicológico, moral ou de autoridade, bem como qualquer outra conduta contrária a gerar um ambiente de trabalho agradável, saudável e seguro;

- Zelar para que não sejam realizadas atividades ilícitas ou comportamentos contrários à ética;

- Fornecer sempre todas as informações necessárias para o acompanhamento adequado da atividade, sem ocultar erros ou violações e tentando corrigir as deficiências e problemas detetados;

- Evitar situações de conflitos de interesse, apresentado à gestão os factos que considere potenciar qualquer conflito de interesses.

3.3 Relação com colaboradores externos e fornecedores

As relações do Profissional de Proteção de Dados com colaboradores externos e fornecedores devem pautar-se por:

- Confiança, respeito, transparência e benefício mútuo;

- Imparcialidade, neutralidade e objetividade nos processos de seleção, aplicando critérios de competência, qualidade e custo, evitando sempre conflitos de interesses e benefícios indevidos.

A contratação de serviços ou compra de bens deve ser feita com total independência de decisão e independentemente de qualquer relação pessoal, familiar ou económica.

3.4 Relação com clientes

Nas relações com clientes, o Profissional de Proteção de Dados deve:

- Tornar conhecido o conteúdo deste código;

- Atuar de forma íntegra e profissional, com o objetivo de alcançar um alto nível de qualidade na prestação dos seus serviços, buscando o desenvolvimento a longo prazo de relacionamentos baseados na confiança e no respeito mútuo;

- Salvaguardar a sua independência, impedindo que a sua atividade profissional seja influenciada por interesses económicos, familiares ou de amizade com os clientes ou ainda de outras relações profissionais fora do contexto da Proteção de Dados, não aceitando destes ou dos seus representantes, presentes, prémios ou favores de qualquer tipo;

- Recusar qualquer pagamento, direta ou indiretamente, num valor superior ao livremente acordado;

- Informar o cliente de qualquer conflito de interesses que possa pôr em causa o bom desempenho profissional;

- Agir de forma diligente, leal, responsável e honesta, de acordo com os seus conhecimentos e as suas especialidades, fornecendo apenas os serviços profissionais para os quais tenha capacidade total de implementação;

- Tratar de forma confidencial qualquer informação que conheça durante o seu trabalho;

- Não promover qualquer atividade (publicidade, material informativo ou outro) que possa induzir os clientes a uma interpretação incorreta do significado das certificações/formações e que possam criar expectativas que não correspondam à realidade;

- Não usar meios ilícitos ou antiéticos durante o exercício das suas funções, devendo ser particularmente cuidadoso com o uso de nomes, marcas ou recursos da organização para a qual trabalha, certificando-se que obtém, antes que qualquer uso, uma autorização clara e explicita do cliente de que os poderá usar;

- Fornecer aos clientes um formulário para preencher em caso de qualquer reclamação relacionada aos serviços prestados.

3.5 Relação com a autoridade de controlo

Neste âmbito, o Profissional de Proteção de Dados deve:

- Colaborar plenamente com qualquer investigação formal ou para resolver reclamações específicas;

- Tratar as comunicações, solicitações e pedidos de informação com diligência e respeitando os prazos previstos na lei;

- Manter um registo de todas as reclamações recebidas relativamente à sua própria atividade e disponibilizar esse registo caso assim seja exigido;

- Desenvolver uma atitude de máxima colaboração e escrupuloso cumprimento das decisões e resoluções da autoridade de controlo;

- Consultar a autoridade de controlo sobre situações que considere poderem vir a constituir conflito de interesses.