ASSOCIAÇÃO
DOS PROFISSIONAIS
DE PROTEÇÃO E
SEGURANÇA DE DADOS

CÓDIGO PROFISSIONAL
DA APDPO

OS DADOS SÃO UM RECURSO CENTRAL DE ACORDO COM OS VALORES ECONÓMICOS MODERNOS. ELES MERECEM O NOSSO PROFISSIONALISMO.

No contexto da digitalização, o tratamento de dados, particularmente de dados pessoais, está cada vez mais no centro da cadeia de valor. Por isso, os requisitos relativos à conformidade legal dos dados e à segurança do seu tratamento estão a crescer acentuadamente. Não apenas a perícia e a experiência nos processos, mas também a quantidade e, em particular, a qualidade dos dados, são decisivas para o sucesso dos negócios e, portanto, devem ser tratadas como um fator fundamental de sucesso e valor corporativo. Num ambiente digital altamente complexo e em rápida mudança, a gestão empresarial, bem como os clientes e os colaboradores, devem poder contar com o apoio de especialistas qualificados, oferecendo experiência e assistência no que diz respeito à segurança e conformidade das informações. Os profissionais de proteção de dados realizam essas tarefas e, em alguns países, já o fazem há algumas décadas. Eles apoiam as empresas no caminho da economia digital e, portanto, concentram-se, por um lado, nos direitos das pessoas envolvidas, principalmente nos direitos pessoais de clientes e funcionários, e, por outro lado, nas necessidades e no sucesso da empresa. Os profissionais de proteção de dados facilitam soluções inovadoras e protegem os valores corporativos, como a imagem corporativa e o valor da marca, construindo e mantendo a confiança do cliente. O manuseio seguro e admissível de dados é cada vez mais objeto de decisões do cliente e, portanto, é uma importante vantagem competitiva. Nesta função, os profissionais de proteção de dados não apenas ajudam a aplicar as leis existentes, mas também contribuem com os seus conhecimentos para garantir que o melhor processo, combinado com uma solução segura, se torne um sucesso para todos os envolvidos.

Tem sido preocupação da APDPO que os profissionais de proteção de dados estejam bem qualificados para que possam enfrentar todos esses desafios. A especialização é particularmente necessária nas seguintes áreas: processos e organização; sistemas e aplicativos de TI; legislação de proteção de dados.

Desde o início que a APDPO definiu os requisitos para esta nova profissão e os conhecimentos necessários aos profissionais de proteção de dados. A elaboração deste Código Profissional é mais um passo para garantir a qualificação destes profissionais. Só os membros da APDPO podem subscrever este Código Profissional.

Lisboa, 25 de outubro de 2023,

A Direção

ASSOCIAÇÃO DOS PROFISSIONAIS DE PROTEÇÃO E SEGURANÇA DE DADOS

ÍNDICE

GLOSSÁRIO

Definições dos termos e abreviaturas utilizadas neste documento:
- RGPD: Regulamento Geral sobre a Proteção de Dados;
- Responsável pelo tratamento: o termo é definido no artigo 4º (7) do RGPD como "*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;*";
- Subcontratante: o termo é definido no artigo 4º (8) do RGPD como *"uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;"*;
- Administração (do responsável pelo tratamento): gerência, conselho de administração, administração da autoridade pública e respetivos dirigentes;
- DPO / EPD: Data Protection Officer / Encarregado de Proteção de Dados;
- Profissional de Proteção de Dados: DPO/EPD, Consultor ou Formador na área da proteção de dados.

SUMÁRIO

Situação inicial

O RGPD, particularmente no capítulo IV, estabelece várias obrigações do responsável pelo tratamento. Para atender a esses requisitos de conformidade, principalmente o dever de demonstrar a conformidade, é essencial operar um sistema de gestão para o campo da proteção de dados.

Exemplos comprovados de sistemas de gestão que já são práticas comuns no seguinte contexto: Gestão da qualidade (DIN EN ISO 9001); Gestão ambiental (DIN EN ISO 14001); Saúde e segurança no trabalho (OHSAS 18001 no futuro DIN EN ISO 45001); Segurança da informação (DIN ISO / IEC 27001).

A diferença, contudo, reside no facto de os requisitos serem determinados pelo legislador da União Europeia, apesar da recente norma DIN EN ISO / IEC 27701 sobre proteção de dados.

Implementação com apoio de profissionais de proteção de dados qualificados

A implementação e monitorização do RGPD na Organização é da responsabilidade da gestão do responsável pelo tratamento, ou seja, do conselho de administração, gerência, direção ou das pessoas em nome individual que efetuem, profissionalmente, o tratamento de dados pessoais. O apoio e suporte por meio de técnicos e por profissionais de proteção de dados qualificados é essencial para cumprir as obrigações do RGPD. Este documento identifica os requisitos pessoais e profissionais para o desempenho profissional qualificado em proteção de dados, bem como as tarefas e atividades a cumprir, decorrentes das exigências da prática profissional para permitir que os desafios da proteção de dados sejam atendidos num mundo cada vez mais digitalizado e em conformidade com o RGPD. Por meio do processo de "compromisso com o código profissional", o responsável pelo tratamento ou o subcontratante pode demonstrar que foram designados profissionais qualificados para a proteção de dados.

1. Exigências pessoais e profissionais

1.1 Exigências profissionais de que depende a adesão ao Código

A adesão ao presente Código Profissional depende da verificação do seguinte:
a) Formação profissional apropriada em, pelo menos, uma das seguintes áreas: jurídica; organização e processos; tecnologias da informação e comunicação (TIC); ou outros equivalentes;
b) Experiência profissional de, pelo menos, seis meses nas áreas referenciadas;
c) Mínimo de 20h de formação numa das áreas indicadas em a);
d) Inscrição como associado na APDPO; e
e) Adesão ao Código Deontológico dos Profissionais de Proteção de Dados da APDPO.

1.2 Competências e conhecimentos

Independentemente do setor e da dimensão da empresa ou da autoridade pública, os profissionais de proteção de dados devem ter um mínimo de conhecimentos especializados e de competências, no âmbito da proteção da dados pessoais e respetiva aplicação prática. Além disso, dependendo das atribuições específicas da empresa ou da autoridade pública, pode ser exigido um conhecimento especializado complementar.

1.2.1 Competência básica em legislação de proteção de dados

Os profissionais de proteção de dados devem demonstrar competências básicas no domínio da legislação de proteção de dados. As competências básicas incluem os seguintes conhecimentos:
- Carta dos Direitos Fundamentais da União Europeia e Tratado sobre o Funcionamento da União Europeia;
- RGPD e outra legislação europeia relevante na proteção de dados;
- Legislação nacional de execução do RGPD e outra legislação relevante para o setor de Atividade;
- Requisitos de legalidade para o tratamento de dados pessoais;
- Requisitos de segurança, na ótica do utilizador, relacionados com a utilização das TIC.

1.2.2 Competência básica em TIC

Os profissionais de proteção de dados devem ter conhecimento técnico e compreender questões relacionadas com as tecnologias de informação e comunicação:
- Organização das TIC;
- Estruturas de sistemas de TI, aplicativos e processos de TI;
- Conhecimentos de segurança da informação, com base nos objetivos de proteção de confidencialidade, integridade, disponibilidade e resiliência;
- Gestão da informação;
- Identificação de riscos no tratamento de dados pessoais resultantes de sistemas de TI, aplicativos e processos de TI.

Além disso, os profissionais de proteção de dados devem reconhecer e avaliar riscos básicos aos direitos e liberdade dos titulares de dados através do tratamento de dados pessoais. Estes profissionais estão em posição de propor melhorias básicas com o recurso às tecnologias, designadamente a aplicação de medidas técnicas e organizativas adequadas aos padrões de segurança do tratamento.

1.2.3 Competência em gestão de empresas e organização

Os profissionais de proteção de dados devem ter os seguintes conhecimentos básicos de administração e organização de negócios para permitir avaliar problemas numa empresa e/ou contexto da administração pública:

- Processos de negócios e/ou processos da administração pública;
- Sistemas de gestão;
- Métodos de avaliação de risco;
- Procedimentos de auditoria e monitorização.

1.2.4 Conhecimento especializado adicional

Além da competência básica, certos setores ou atividades especiais podem exigir uma especialização complementar do profissional de proteção de dados nas áreas de direito, tecnologia e organização, dependendo do ramo ou setor em questão. Isso também pode incluir conhecimentos especiais em códigos de conduta para o respetivo setor.

1.2.5 Atualização dos conhecimentos especializados

O profissional de proteção de dados atualiza, regularmente, os seus conhecimentos, em especial no âmbito jurídico e das tecnologias da informação, necessários ao desempenho das suas funções.

1.3 Outros requisitos pessoais

1.3.1 Integridade

A integridade pessoal deverá ser inerente ao desempenho das funções do profissional de proteção de dados. Para efeitos de análise de carácter, considera-se não existirem condições de integridade para o desempenho do profissional de proteção de dados os seguintes condicionalismos: Condenação por crime de violação de segredo/sigilo; Condenação por crimes de responsabilidade de titulares de cargos políticos; Condenação por crimes informáticos; Demissão anterior por infração grosseira ao disposto na legislação ou por más práticas em matéria de proteção de dados. Nestes casos deverá ter-se em consideração um período de inação por dois anos.

1.3.2 Competência em aconselhamento

Os profissionais de proteção de dados, independentemente da dimensão da empresa ou autoridade pública, devem possuir as aptidões e capacidades necessárias para organizar de forma independente o seu trabalho. Os profissionais de proteção de dados

deverão desenvolver propostas construtivas para soluções compatíveis com a proteção de dados pessoais, conjugando os interesses das partes envolvidas e apresentarem recomendações, informações e esclarecimentos. Isso requer competências como técnicas de comunicação e moderação, bem como métodos de solução de problemas.

1.3.3 Assertividade na sua própria posição profissional

Os profissionais de proteção de dados podem executar tarefas delegadas de forma independente, afirmar a sua posição e evitar limitações. A posição inclui, em particular, independência e autoridade para agir autonomamente.

2. Objetivos e exercício das funções

2.1. Gestão

Os objetivos de gestão em matéria de proteção de dados pessoais traduzem-se em assegurar o respeito pelos princípios relativos ao tratamento de dados pessoais e a consequente conformidade com o RGPD, nomeadamente através da monitorização constante dos procedimentos internos, metodologias, avaliações de impacto, justificação das opções tomadas no tratamento dos dados e outros que evidenciem a *accountability*. Esses princípios terão de ser sempre articulados com as bases de licitude que permitem o tratamento dos dados.

2.2. Informação e Aconselhamento

Para a prossecução dos objetivos enunciados, o profissional, em linha com o RGPD e a Lei nº 58/2019, de 8 de agosto, terá de assegurar a permanente informação e aconselhamento ao Responsável pelo Tratamento, ao Subcontratante e aos Trabalhadores que tratem dados pessoais. Esta informação e aconselhamento traduz-se, na maior parte das vezes, na emissão de pareceres onde são transmitidos os valores que suportam a proteção de dados pessoais e a melhor forma de os observar.

O DPO/EPD deverá ter papéis de aconselhamento e esclarecimento preponderantes, enquanto figura de referência e de suporte nas organizações, relativamente à proteção de dados. Estes papéis deverão ser desempenhados com a máxima consciência ética e responsabilidade, valores indissociáveis das boas práticas que deverão ser sugeridas e adotadas, mostrando sempre disponibilidade e interesse em contribuir para o maior grau de conformidade possível, em função da realidade de cada organização. A norma do artigo 39º nº1 alínea c) do RGPD elege, ainda, uma função de aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controlo da sua realização.

2.3. Interlocutor para a conformidade

O objetivo primordial deverá ser o de capacitar e alertar toda a organização para assegurar a conformidade e implementação dos normativos do RGPD, visando uma atuação corporativa e responsável por parte de todos, quer da perspetiva de identificar as vulnerabilidades, quer da mitigação dos riscos, quer da prevenção, procurando

sempre o alinhamento para com as Políticas da Organização e outras diretrizes e procedimentos e envolvendo cada elemento da organização, sensibilizando-o para uma cultura organizacional como suporte de resultados cada vez mais efetivos de conformidade na proteção de dados.

2.4. Formação

A sensibilização e formação dos trabalhadores constitui outra função do DPO/EPD, bem como a permanente atualização dos seus próprios conhecimentos técnicos possibilitando-lhe o domínio das melhores práticas em matéria de tratamento de dados pessoais.

2.5. Auditorias

O DPO/EPD deverá assegurar que a implementação do RGPD seja auditada de forma regular e sistémica, por forma a identificar eventuais desvios do plano e projeto de implementação previstos e operacionalizados, atuando de forma o mais eficaz e eficiente possíveis, no sentido de mitigar os riscos de não conformidade, recorrendo igualmente às auditorias como registo de histórico da organização contribuindo para a melhoria contínua do nível de conformidade. O DPO/EPD deverá assegurar o controlo e a sensibilização para a conformidade das auditorias, quer periódicas, quer não programadas, aos processos internos de tratamento de dados pessoais.

2.6. Cooperação com a Autoridade de Controlo

O DPO/EPD deverá cooperar com a autoridade de controlo, nos termos do art.º 39º nº1 alínea d) do RGPD e ser ponto de contato para a mesma entidade, relativamente a questões de tratamento de dados e consulta, nomeadamente quando se realiza uma consulta prévia (tal como consta no art.º 36º do RGPD).

3. Requisitos para a prática profissional

3.1. Atitude em relação à prática profissional

O DPO/EDP é representante dos interesses dos titulares de dados na defesa e exercício dos seus direitos, conciliando-os com os interesses do Responsável pelo Tratamento ou do Subcontratante, na monitorização interna da conformidade para com o RGPD. O DPO/EDP fundamenta as suas interpretações legais e fornece os necessários esclarecimentos de forma clara e compreensível, procurando assumir uma avaliação objetiva dos factos. O mesmo se aplica, com as devidas adaptações, aos procedimentos propostos para uma utilização adequada das tecnologias de informação, assegurando um nível de segurança adequado ao risco.

Caso o DPO/EDP identifique conflitos de interesses nos termos do Ponto 3.5.4 deste Código, deverá apresentar os factos ao Responsável pelo Tratamento ou ao Subcontratante, conforme o caso, e, se tal se justificar, requerer escusa na intervenção do procedimento conflituante.

O DPO/EDP deve garantir um alto padrão de qualidade no seu trabalho, pelo que, em matérias específicas, poderão recorrer ao apoio de especialistas, solicitando-lhes parecer.

3.2. Transparência

O DPO/EPD deve reger a sua atividade profissional de forma transparente, pragmática, objetiva e isenta. As suas opiniões e pareceres deverão estar fundamentadas com base em requisitos legais e nas melhores práticas da atividade profissional de privacidade e proteção de dados pessoais. O seu trabalho deverá primar pelo brio profissional, pela organização e rastreabilidade documental, com evidências auditáveis, e contribuir para um entendimento claro dos propósitos dos princípios do RGPD, contribuindo para a sua implementação prática nas operações do dia a dia da sua organização.

3.3. Discrição e confidencialidade

O DPO/EDP tem o dever de manter confidencialidade relativamente a todas as informações que conhece decorrentes do exercício do seu cargo. Tal não se aplica a fatos do conhecimento público. O DPO/ EDP trata, com absoluto sigilo, os detalhes de reclamações, violações de proteção de dados ou identidade dos reclamantes (salvo se estes pretenderem, expressamente, a divulgação de sua identidade). O dever de sigilo/confidencialidade acompanha o término das funções como DPO/EPD, salvo em caso de colaboração com os órgãos jurisdicionais.

3.4. Garantia de qualidade

Devem ser adotadas medidas de controlo de qualidade adequadas para garantir o bom desempenho do seu cargo.

3.4.1 Auto-monitorização

O controlo de garantia de qualidade no bom desempenho das funções deve ser assegurado por meios de auto-monitorização e reflexão. Medidas adicionais devem incluir técnicas de *benchmarking* e oportunidades de participação em fóruns e redes da especialidade. Isso também inclui formação adicional e avançada.

3.4.2 Monitorização através de associações

A APDPO - Associação dos Profissionais de Proteção e de Segurança de Dados desenvolve, no âmbito das suas finalidades, apoios, designadamente formativos e de fóruns de reflexão, aos seus associados. Os associados da APDPO devem pautar a sua conduta profissional com as regras do Código Profissional e honrar o desempenho das suas funções com zelo e dedicação. A constatação, pela APDPO, de atos ou omissões contrárias aos vertidos no Código Profissional, implicará a expulsão de associado desta associação profissional. Esse processo é transparente e está descrito nos documentos de compromisso voluntário. O certificado é personalizado e verificável pela associação profissional.

3.5. Designação como DPO/EPD

3.5.1 Condições de designação

As condições para a designação/contratação como encarregado de proteção de dados resultam de:

- Qualificações pessoais e profissionais;
- Exercer as suas funções de forma totalmente independente e sem conflito de interesses.

3.5.2 Forma e procedimento de designação

Os encarregados de proteção de dados devem ser designados, por escrito, pelo responsável pelo tratamento. Os encarregados de proteção de dados podem executar as suas funções para mais que uma empresa ou autoridade, desde que isso não comprometa sua independência. A autoridade de controlo deve ser notificada da designação e dos dados de contato do encarregado de proteção de dados.

3.5.3 Duração e termo da designação

É recomendado que a designação dos encarregados de proteção de dados seja por determinado prazo. O período de designação inicial deve ser de cinco anos. A renovação da designação pode ser por período mais curto, não inferior a três anos.

3.5.4 Independência da prática profissional

Os encarregados de proteção de dados devem ser capazes de executar as suas tarefas de forma totalmente independente e com autoridade para agir autonomamente. Essa independência advém da liberdade no exercício das funções, da existência dos recursos necessários, bem como na ausência de conflitos de interesses profissionais.

Conflitos de interesse poderão existir se as funções dos encarregados de proteção de dados forem acumuladas com cargos dirigentes ou com atribuições para tomada de decisões no que ao tratamento de dados respeita.

Os responsáveis pelo tratamento são obrigados a fornecer aos DPO/EPD os recursos adequados. Os encarregados de proteção de dados criam as condições básicas necessárias para a confidencialidade e a segurança dos materiais de trabalho, em termos de aspectos espaciais, técnicos e organizacionais.

3.6. Responsabilidade e seguro profissional

O DPO/EPD deverá desenvolver a sua atividade com um grau suficiente de autonomia na sua organização, sem receber orientações relativamente ao exercício das suas tarefas, de forma a realizar as mesmas de forma independente. O Responsável pelo Tratamento ou o Subcontratante são responsáveis pelas tomadas de decisão no âmbito da privacidade e proteção de dados pessoais, sendo que o DPO/EPD deverá poder emitir opiniões contrárias à gestão de topo, na sua missão informativa e de aconselhamento. O DPO/EPD é responsável por definir a estratégia da organização para atingir a conformidade para com o RGPD, disponibilizar informação e aconselhar a gestão de topo sobre o cumprimento dos requisitos do RGPD e atuar como ponto de contacto com as autoridades de controlo. O DPO/EPD deverá priorizar as suas atividades e focar os seus esforços nas temáticas que apresentam um nível elevado de risco.

O papel do DPO/EPD na informação e aconselhamento das temáticas de privacidade e proteção de dados pessoais, assim como na monitorização da conformidade do RGPD, não significa que este seja pessoalmente responsável das situações não conformes da organização. A conformidade para com o RGPD é uma responsabilidade corporativa do Responsável pelo Tratamento ou Subcontratante e não do DPO/EPD.

Se os encarregados de proteção de dados internos forem responsáveis por prejuízos, danos à propriedade e perdas pecuniárias que tenham causado com dolo/intenção, estarão sujeitos à responsabilidade decorrente da lei laboral.

Os encarregados de proteção de dados externos são responsáveis nos termos da lei e do contrato. O DPO/EPD externo deverá ter um seguro de responsabilidade profissional, com cobertura dos riscos de responsabilidade por danos económicos decorrentes do exercício das suas funções e manter a cobertura do seguro pelo prazo da sua designação.

3.6.1. Seguro Profissional

Embora o RGPD assegure alguma proteção para os DPO/EPD, este não os protege de todas as fontes de responsabilização. As garantias de independência asseguradas pelo RGPD são omissas no que pode acontecer ao DPO/EPD caso este falhe no desenvolvimento das suas funções. Assim sendo, os DPO/EPD ficam expostos a um elevado nível de responsabilidade por erros, aconselhamentos imprecisos ou negligência. Se os erros do DPO/EPD resultarem numa ação sancionatória, a exposição potencial de responsabilização do EPD será substancial. O DPO/EPD interno estará coberto pelo seguro de responsabilidade civil da sua organização. O DPO/EPD externo poderá ser responsabilizado profissionalmente, no decurso das suas funções, pelo que deverá, também, acautelar a realização de um seguro de responsabilidade civil, protegendo-se contra eventuais responsabilizações assinaladas pelos seus clientes, como por exemplo:

- Se prestar um aconselhamento grosseiro que leva à violação de princípios de tratamento de dados;

- Se perder informação importante relativa a atividades de tratamento de dados pessoais de clientes;

- Se o cliente sofrer uma sanção pecuniária devido a aconselhamento grosseiro do DPO/EPD em relação à conformidade com o RGPD;

- Caso o DPO/EPD seja responsável pelo desenvolvimento de um software para o tratamento de dados pessoais e o cliente perder todos os dados durante uma atualização desse software.

Será de capital importância que o EPD mantenha um registo de toda a sua atividade profissional, na relação com o Responsável pelo Tratamento ou Subcontratante, de forma a salvaguardar a sua posição profissional em eventual ação jurisdicional.